Principally polarized abelian varieties with CM: Shimura class groups & superspecial abelian varieties

Bogdan Adrian Dina

ELTE Budapest,
&
Einstein Institute of Mathematics Jerusalem

Seminar in Real and Complex Geometry,
Tel Aviv University,
30 January 2025

Overview

1. Motivation
2. Principally polarized abelian varieties with complex multiplication.
3. The group $\mathcal{C}_K$ and its action on principally polarized abelian varieties
4. Superspecial principally polarized abelian surfaces

Motivation: Cryptographic group actions from isogenies

Our goal today. To explore principally polarized abelian varieties with CM, together an action by the Shimura class group, from the perspective of cryptographic group actions.

Motivation: Cryptographic group actions from isogenies

Our goal today. To explore principally polarized abelian varieties with CM, together an action by the Shimura class group, from the perspective of cryptographic group actions.

Let $\star : G \times S \to S$ be a group action. From the cryptographic point of view, we endow $\star$ with some hardness properties. Of our main interest today are one-way group actions: given randomly chosen $s_1, s_2 \in S$, it is hard to find an $g \in G$, such that

$$g \star s_1 = s_2.$$

Motivation

Question. Why to care about cryptographic group actions?

Quantum computers threaten to break most of the cryptography we are currently using to secure critical computer systems.

Motivation

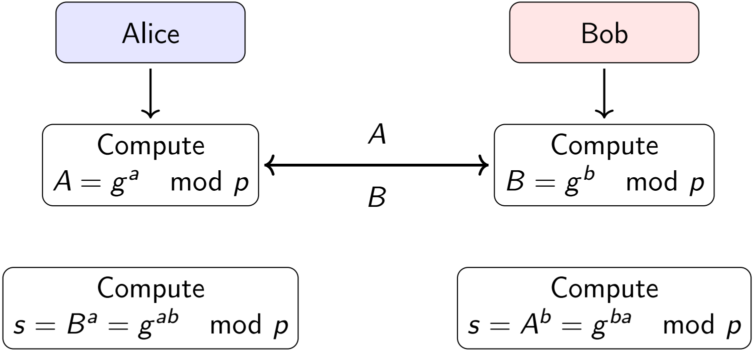
Question. Why to care about cryptographic group actions?

Quantum computers threaten to break most of the cryptography we are currently using to secure critical computer systems.

Isogeny-based cryptography is a specific type of post-quantum cryptography that uses isogenies between abelian varieties over finite fields as its core building block. Its main advantages are relatively small keys and its rich mathematical structure.

The Diffie-Hellman key exchange protocol

Before talking about Isogeny-based cryptography, let's see how the quantum computer will break the Diffie-Hellman key exchange protocol: Let p be prime, and let g be a generator of G, of order n.



Alice

Compute $A = g^a \mod p$

Bob

Compute $B = g^b \mod p$

A

B

Compute $s = B^a = g^{ab} \mod p$

Compute $s = A^b = g^{ba} \mod p$

Shared secret:

$$s = g^{ab} \pmod{p}$$

How the quantum computer breaks Diffie-Hellman

Remark. The obvious way to attack this scheme is to recover one of the secrets a, b from the publicly transmitted values g^a, g^b. This is known as the discrete-logarithm problem, which appears to be computationally hard for classical computers when the group G is well-chosen.

How the quantum computer breaks Diffie-Hellman

Remark. The obvious way to attack this scheme is to recover one of the secrets a, b from the publicly transmitted values g^a, g^b. This is known as the discrete-logarithm problem, which appears to be computationally hard for classical computers when the group G is well-chosen.

Unfortunately, one thing that quantum computers are particularly good at is finding periods of computable functions using an algorithm by Shor, which can be used to solve DLP in polynomial time.

How the quantum computer breaks Diffie-Hellman

The approach.

- The public values g^x are simply group elements, respecting

$$g^x \cdot g^y = g^{x+y}.$$

- This is exactly what we need to find a period and to break the D-H scheme: Given g and $A = g^a$, define a group hom.

$$f : \mathbb{Z}^2 \to G, \ (x, y) \mapsto g^x \cdot A^y = g^{x+ay}.$$

How the quantum computer breaks Diffie-Hellman

The approach.

- The public values g^x are simply group elements, respecting

$$g^x \cdot g^y = g^{x+y}.$$

- This is exactly what we need to find a period and to break the D-H scheme: Given g and $A = g^a$, define a group hom.

$$f : \mathbb{Z}^2 \to G, \ (x, y) \mapsto g^x \cdot A^y = g^{x+ay}.$$

The map f is periodic, i.e. $\forall\ (x, y) \in \mathbb{Z}^2,\ (\widetilde{x}, \widetilde{y}) \in \Lambda$, where

$$\begin{aligned}\Lambda := \ker(f) &= \{(\widetilde{x}, \widetilde{y}) \in \mathbb{Z}^2 : g^{\widetilde{x}+a\widetilde{y}} = 1\}\\ &= \{(\widetilde{x}, \widetilde{y}) \in \mathbb{Z}^2 : \widetilde{x} + a\widetilde{y} \equiv 0 \pmod{n}\},\end{aligned}$$

we have $$f(x + \widetilde{x}, y + \widetilde{y}) = f(x, y).$$

How the quantum computer breaks Diffie-Hellman

The approach.

- Shor's algorithm finds in polynomial time a basis of this lattice from an „efficient description" of the map f.
- Look for a vector of the form $(\tau, -1) \in \Lambda$; it satisfies codition

$$\tau + a(-1) \equiv 0 \pmod{n} \Leftrightarrow \tau \equiv a \pmod{n}.$$

How the quantum computer breaks Diffie-Hellman

The approach.

- Shor's algorithm finds in polynomial time a basis of this lattice from an „efficient description“ of the map f.
- Look for a vector of the form $(\tau, -1) \in \Lambda$; it satisfies codition

$$\tau + a(-1) \equiv 0 \pmod{n} \Leftrightarrow \tau \equiv a \pmod{n}.$$

- Together, $(\tau, -1) \equiv (a, -1) \pmod{n}$, and finding $(\tau, -1) \in \Lambda$ identifies $a \mod n$.

How the quantum computer breaks Diffie-Hellman

The approach.

- Shor's algorithm finds in polynomial time a basis of this lattice from an „efficient description“ of the map f.
- Look for a vector of the form $(\tau, -1) \in \Lambda$; it satisfies codition

$$\tau + a(-1) \equiv 0 \pmod{n} \Leftrightarrow \tau \equiv a \pmod{n}.$$

- Together, $(\tau, -1) \equiv (a, -1) \pmod{n}$, and finding $(\tau, -1) \in \Lambda$ identifies $a \mod n$.

Luckily, after the discovery of Shor's algorithm, the traditional Diffie–Hellman framework has been extended to schemes which have similar traits, but do not rely on exponentiation maps in groups being one-way. One of these variants uses isogeny graphs.

Motivation

Remark. What primitives can we build from cryptographic group actions from isogenies?

- In a nutshell, an isogeny is a morphism of abelian varieties, that preserves the group structure.
- The central objects of study in isogeny-based cryptography are isogeny graphs, whose vertices represent abelian varieties, and whose edges represent isogenies between them.
- We focus today on complex multiplication (CM) grphs, which arise from horizontal isogenies of CM abelian varieties.

The Dawn of Isogeny-Based Cryptography

A brief historical overview.

- Isogeny-based cryptography was first proposed by Couveignes in 1996, but not published at the time. The same idea was independently rediscovered by Rostovtsev-Stolbunov later. Couveignes-Rostovtsev–Stolbunov (CRS) suggested a post-quantum key exchange protocol based on the group action of an ideal class group on ordinary elliptic curves.

The Dawn of Isogeny-Based Cryptography

A brief historical overview.

- Isogeny-based cryptography was first proposed by Couveignes in 1996, but not published at the time. The same idea was independently rediscovered by Rostovtsev-Stolbunov later. Couveignes-Rostovtsev–Stolbunov (CRS) suggested a post-quantum key exchange protocol based on the group action of an ideal class group on ordinary elliptic curves.
- A major breakthrough for isogeny-based group actions was the Commutative Supersingular Isogeny Diffie-Helman (CSIDH) key-exchange protocol; it is similar to the CRS key-exchange protocol but the class group of an imaginary quadratic order acts on the set of supersingular elliptic curves defined over $\mathbb{F}_p$. It was the first efficient post-quantum action and its efficient public-key validation gives rise to non-interactive key exchange.

The Dawn of Isogeny-Based Cryptography

A brief historical overview.

- The next mile step in isogeny-based cryptography was the Commutative Supersingular Isogeny based Fiat-Shamir (CSI-FiSh) signatures scheme, pronounce „sea-fish“: It is a digital signature scheme based on CSIDH-512. Its security relies on the computational hardness of the following problem.

  Given m-curves $E_1, \ldots, E_m$ with all the same endomorphism ring $\mathcal{O}$, find an ideal $\mathfrak{a} \subset \mathcal{O}$ such that

  $$E_i = \mathfrak{a} \star E_j, \text{ for some } i, j \in \{0, \ldots, m\}, i \neq j.$$

The Dawn of Isogeny-Based Cryptography

A brief historical overview.

- SCALLOP: SCALable isogeny action based on oriented supersingular curves with prime conductor.
  - It is a framework for isogeny-based cryptographic group actions.
  - It improves commutative isogeny-based group actions by using oriented supersingular elliptic curves with prime conductors.
  - Further, the authors describe a computationally effective method to compute orientations on supersingular elliptic curves via the kernel representation of isogenies.

The Dawn of Isogeny-Based Cryptography

Our approach. Using conceptual ideas from SCALLOP, we develop a new isogeny-based group actions protocol on oriented principally polarized superspecial abelian surfaces over $\mathbb{F}_q$ with CM by the maxmial order in quartic CM fields with Galois groups C_4, D_4.

Abelian varieties

Let k be a field. An abelian variety (av) A/k is a proper connected group variety over k. Any abelian variety is smooth, projective, and commutative.

Abelian varieties

Let k be a field. An abelian variety (av) A/k is a proper connected group variety over k. Any abelian variety is smooth, projective, and commutative.

Examples:

- A 1-dimensional abelian variety is the same as an elliptic curve.
- Every abelian variety of dimension g over $k = \mathbb{C}$ is of the form $\mathbb{C}^g/\Lambda$, for a lattice Λ of rank $2g$ in $\mathbb{C}^g$.
- A complex torus is an abelian variety if and only if it has a positive definite Riemann form, as we will discuss later.
- If C/k is a curve, then there exists an abelian variety $J(C)/k$ called the Jacobian, s.t. for any extension $k \subset k'$ with $C(k') \neq 0$, we have $J(C)(k') = \mathrm{Pic}^0(C_{k'})$.

Abelian varieties with complex multiplication

- We say A of dimension g has *complex multiplication* (CM) by a CM field K of degree $2g$ if there exists an embedding

$$\iota : K \hookrightarrow \mathrm{End}(A) \otimes \mathbb{Q}.$$

- We say A has CM by an order $\mathcal{O}$ in K if the same holds with $\iota^{-1}(\mathrm{End}(A)) = \mathcal{O}$.

Abelian varieties with complex multiplication

Example. Consider the elliptic curve $E : y^2 = x^3 + x$ over a field k, and assume there is a $j \in k$ satisfies $j^2 = -1$. Let $K = \mathbb{Q}(i)$ and $\mathcal{O} = \mathbb{Z}[i]$. Then E has CM by $\mathcal{O}$ via the embedding ι given by

$$\iota(i)(x, y) = (-x, jy).$$

Polarizations: Line bundles & Riemann forms

An abelian variety $A = \mathbb{C}^g/\Lambda$ over $\mathbb{C}$ is a complex torus which comes equipped with an algebraic embedding

$$\mu : A \hookrightarrow \mathbb{P}^n_{\mathbb{C}},$$

where $\mu = \mu_{\mathscr{L}}$ is associated to an ample line bundle $\mathscr{L}$ on $\mathbb{C}^g/\Lambda$.

- A polarization on an abelian variety $A/\mathbb{C}$ is an isogeny

  $$\eta_{\mathscr{L}} : A \to A^{\vee},$$

  where $\mathscr{L} = \mathscr{L}(H)$ is a class of ample line bundles on A, and where H is a positive definite Hermitian form, whose imaginary part takes integer values on $\Lambda \times \Lambda$.
- We call a polarization $\eta_{\mathscr{L}}$ principal, if $\deg(\eta_{\mathscr{L}}) = 1$.

Product polarizations for $g = 2$

Example. For any effective divisor L on E^2, define an isogeny

$$\varphi_L : E^2 \to (E^2)^\vee,\ \varphi_L(\alpha) = Cl(L_\alpha - L) \in (E^2)^\vee,$$

where L_α is the translation of L by α, and where Cl means the linear equivalence class. The map φ_L always define polarizations over algebraically closed fields.

Define devisor $X = (E \times \{\mathcal{O}_E\}) + (\{\mathcal{O}_E\} \times E)$ on E^2.

Product polarizations for $g = 2$

Example. For any effective divisor L on E^2, define an isogeny

$$\varphi_L : E^2 \to (E^2)^\vee,\ \varphi_L(\alpha) = Cl(L_\alpha - L) \in (E^2)^\vee,$$

where L_α is the translation of L by α, and where Cl means the linear equivalence class. The map φ_L always define polarizations over algebraically closed fields.

Define divisor $X = (E \times \{\mathcal{O}_E\}) + (\{\mathcal{O}_E\} \times E)$ on E^2.

Claim. $\varphi_X : E^2 \to (E^2)^\vee$ is an isomorphism.

We show that $H := \ker(\varphi_X)$ is trivial: Let $(e_1, e_2) \in H$, then

$$X \sim_{\text{lin}} X + (e_1, e_2).$$

Restricting H to the sub-varieties $E \times \{\mathcal{O}_E\}$ (, resp. to $\{\mathcal{O}_E\} \times E$) of E^2, shows that $\mathcal{O}_E \sim_{\text{lin}} e_1$ (, resp. to $\mathcal{O}_E \sim_{\text{lin}} e_2$). This implies, that $e_1 = e_2 = \mathcal{O}_E$, and $H = \{(\mathcal{O}_E, \mathcal{O}_E)\}$.

Example for canonical principal polarization on $J(C)$

Example. Let $J(C) = \mathrm{Pic}^0(C)$ be the Jacobian of a curve C of genus 2. Consider the AJ-embedding

$$u : C \hookrightarrow J(C), \text{ and define } \Theta = u(C),$$

the Theta divisor on $J(C)$. The divisor Θ induces a canonical principal polarization,

$$\varphi_\Theta : J(C) \to \mathrm{Pic}^0(C), \; \varphi_\Theta(\alpha) = Cl(\Theta_\alpha - \Theta).$$

CM fields and CM types

- A Complex Multiplication (CM) field K is a totally imaginary quadratic extension of a totally real number field K_0.

CM fields and CM types

- A Complex Multiplication (CM) field K is a totally imaginary quadratic extension of a totally real number field K_0.
- Let K be a CM field of degree $2g$ over $\mathbb{Q}$. A CM type of K is a set Φ of g embeddings

$$\Phi = \{\varphi : K \hookrightarrow \mathbb{C}\},$$

  such that $\mathrm{Hom}(K, \mathbb{C}) = \Phi \sqcup \Phi\rho$, where $\rho \in \mathrm{Aut}(K)$ the unique element identifying complex conjugation on K.
- We call a CM type primitive if it is not induced by a proper CM subfield.

CM fields and CM types

- A Complex Multiplication (CM) field K is a totally imaginary quadratic extension of a totally real number field K_0.
- Let K be a CM field of degree $2g$ over $\mathbb{Q}$. A CM type of K is a set Φ of g embeddings

  $$\Phi = \{\varphi : K \hookrightarrow \mathbb{C}\},$$

  such that $\mathrm{Hom}(K, \mathbb{C}) = \Phi \sqcup \Phi\rho$, where $\rho \in \mathrm{Aut}(K)$ the unique element identifying complex conjugation on K.
- We call a CM type primitive if it is not induced by a proper CM subfield.
- We call two CM types Φ, Φ' equivalent if there exists an automorphism $\alpha \in \mathrm{Aut}(K)$ such that $\Phi' = \Phi\alpha$.

In the following we call a tuple (K, Φ) a CM type, where K is a CM field and where Φ is a CM type of K.

CM fields and CM types

Example.

- The sextic cyclic CM field $K = \mathbb{Q}(\zeta_7)$ has subfields $K_0 = \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$, $F = \mathbb{Q}(\sqrt{-7})$, and $\mathbb{Q}$.
- We count 8 CM types of K, from which 2 are induced by F, hence 6 CM types are primitive.

Fact. We have 2 CM types of K up to equivalence, 1 primitive and 1 imprimitive. Representatives up to equivalence are given by $\{0, 1, 2\}$ for the primitive case, and $\{0, 2, 4\}$ for the imprimitive case, induced by F.

Existence and Construction of ppav's with CM

Let (K, Φ) be a CM type where K is a CM field of degree $2g$. Use Φ to define a map $K \to \mathbb{C}^g$ given by

$$x \mapsto \Phi(x) = (\varphi_1(x), \ldots, \varphi_g(x)).$$

If $\mathfrak{a}$ is a fractional $\mathcal{O}_K$-ideal, then

Existence and Construction of ppav's with CM

Let (K, Φ) be a CM type where K is a CM field of degree $2g$. Use Φ to define a map $K \to \mathbb{C}^g$ given by

$$x \mapsto \Phi(x) = (\varphi_1(x), \ldots, \varphi_g(x)).$$

If $\mathfrak{a}$ is a fractional $\mathcal{O}_K$-ideal, then

- $\Phi(\mathfrak{a}) \subset \mathbb{C}^g$ is a full lattice for any $g \geq 1$ and $\mathbb{C}^g/\Phi(\mathfrak{a})$ is a complex torus of type (K, Φ).

Existence and Construction of ppav's with CM

Let (K, Φ) be a CM type where K is a CM field of degree $2g$. Use Φ to define a map $K \to \mathbb{C}^g$ given by

$$x \mapsto \Phi(x) = (\varphi_1(x), \ldots, \varphi_g(x)).$$

If $\mathfrak{a}$ is a fractional $\mathcal{O}_K$-ideal, then

- $\Phi(\mathfrak{a}) \subset \mathbb{C}^g$ is a full lattice for any $g \geq 1$ and $\mathbb{C}^g/\Phi(\mathfrak{a})$ is a complex torus of type (K, Φ).
- Two complex tori $\mathbb{C}^g/\Phi(\mathfrak{a})$ and $\mathbb{C}^g/\Phi(\mathfrak{a}')$ of type (K, Φ) are isomorphic if and only if $\mathfrak{a}' = (\alpha)\mathfrak{a}$ for some α in K^*.

Existence and Construction of ppav's with CM

Let (K, Φ) be a CM type where K is a CM field of degree $2g$. Use Φ to define a map $K \to \mathbb{C}^g$ given by

$$x \mapsto \Phi(x) = (\varphi_1(x), \ldots, \varphi_g(x)).$$

If $\mathfrak{a}$ is a fractional $\mathcal{O}_K$-ideal, then

- $\Phi(\mathfrak{a}) \subset \mathbb{C}^g$ is a full lattice for any $g \geq 1$ and $\mathbb{C}^g/\Phi(\mathfrak{a})$ is a complex torus of type (K, Φ).
- Two complex tori $\mathbb{C}^g/\Phi(\mathfrak{a})$ and $\mathbb{C}^g/\Phi(\mathfrak{a}')$ of type (K, Φ) are isomorphic if and only if $\mathfrak{a}' = (\alpha)\mathfrak{a}$ for some α in K^*.
- For any g-dimensional complex torus (A, ι) of type (K, Φ) there exists some fractional $\mathcal{O}_K$-ideal $\mathfrak{a}$ such that A is isomorphic to $\mathbb{C}^g/\Phi(\mathfrak{a})$.

Existence and Construction of ppav's with CM

Polarization. According to our discussion, a polarization is a certain class of ample line bundle $\mathscr{L} = \mathscr{L}(H)$ on $\mathbb{C}^g/\Lambda$, where $\Lambda = \Phi(\mathfrak{a})$.

Take a tuple $(\mathfrak{a}, \xi)$, where

1. $\mathfrak{a}$ is a fractional $\mathcal{O}_K$-ideal.
2. ξ is an element in K such that $-\xi^2$ is totally positive in the totally real subfield K_0 of K, $\varphi(\xi)$ is an positive imaginary element for any $\varphi \in \Phi$, and

$$(\xi) = (\mathfrak{a}\bar{\mathfrak{a}}\mathfrak{D}_{K|\mathbb{Q}})^{-1}$$

where $\mathfrak{D}_{K|\mathbb{Q}}^{-1} = \{\alpha \in K : \mathrm{Tr}_{K|\mathbb{Q}}(\alpha\mathcal{O}_K) \subseteq \mathbb{Z}\}$.

Existence and Construction of ppav's with CM

Then $E = E_{\Phi,\xi} : \Phi(K) \times \Phi(K) \to \mathbb{Q}$, where

$$E(\Phi(v), \Phi(w)) = \mathrm{Tr}_{K/\mathbb{Q}}(\xi \overline{v} w)$$

for any $v, w \in K$ can be uniquely extended to a positive definite hermitian form

$$H = E(iv, w) + iE(v, w) \text{ on } \mathbb{C}^g,$$

whose imaginary part takes integer values on $\Phi(\mathfrak{a}) \times \Phi(\mathfrak{a})$.

Existence Theorem

Let (K, Φ) be a CM type where K is a CM field of degree $2g$ over $\mathbb{Q}$. Then the following holds.

1. Any triple $(\Phi, \mathfrak{a}, \xi)$ as above defines a principally polarized abelian variety $A(\Phi, \mathfrak{a}, \xi) = (\mathbb{C}^g/\Phi(\mathfrak{a}), E)$ of dimension g over $\mathbb{C}$ with CM by $\mathcal{O}_K$ of type (K, Φ).

Existence Theorem

Let (K, Φ) be a CM type where K is a CM field of degree $2g$ over $\mathbb{Q}$. Then the following holds.

1. Any triple $(\Phi, \mathfrak{a}, \xi)$ as above defines a principally polarized abelian variety $A(\Phi, \mathfrak{a}, \xi) = (\mathbb{C}^g/\Phi(\mathfrak{a}), E)$ of dimension g over $\mathbb{C}$ with CM by $\mathcal{O}_K$ of type (K, Φ).
2. Any principally polarized abelian variety of dimension g over $\mathbb{C}$ with CM by $\mathcal{O}_K$ of type (K, Φ) is isomorphic to $A(\Phi, \mathfrak{a}, \xi)$ for some triples $(\Phi, \mathfrak{a}, \xi)$ as in (1).

Existence Theorem

Let (K, Φ) be a CM type where K is a CM field of degree $2g$ over $\mathbb{Q}$. Then the following holds.

1. Any triple $(\Phi, \mathfrak{a}, \xi)$ as above defines a principally polarized abelian variety $A(\Phi, \mathfrak{a}, \xi) = (\mathbb{C}^g/\Phi(\mathfrak{a}), E)$ of dimension g over $\mathbb{C}$ with CM by $\mathcal{O}_K$ of type (K, Φ).
2. Any principally polarized abelian variety of dimension g over $\mathbb{C}$ with CM by $\mathcal{O}_K$ of type (K, Φ) is isomorphic to $A(\Phi, \mathfrak{a}, \xi)$ for some triples $(\Phi, \mathfrak{a}, \xi)$ as in (1).
3. The abelian variety $A(\Phi, \mathfrak{a}, \xi)$ is simple if and only if Φ is primitive. In this case $\iota : K \to \mathrm{End}^0(A)$ is an isomorphism.

Existence Theorem

Let (K, Φ) be a CM type where K is a CM field of degree $2g$ over $\mathbb{Q}$. Then the following holds.

1. Any triple $(\Phi, \mathfrak{a}, \xi)$ as above defines a principally polarized abelian variety $A(\Phi, \mathfrak{a}, \xi) = (\mathbb{C}^g/\Phi(\mathfrak{a}), E)$ of dimension g over $\mathbb{C}$ with CM by $\mathcal{O}_K$ of type (K, Φ).
2. Any principally polarized abelian variety of dimension g over $\mathbb{C}$ with CM by $\mathcal{O}_K$ of type (K, Φ) is isomorphic to $A(\Phi, \mathfrak{a}, \xi)$ for some triples $(\Phi, \mathfrak{a}, \xi)$ as in (1).
3. The abelian variety $A(\Phi, \mathfrak{a}, \xi)$ is simple if and only if Φ is primitive. In this case $\iota : K \to \mathrm{End}^0(A)$ is an isomorphism.
4. For any pair of triples $(\Phi, \mathfrak{a}, \xi)$ and $(\Phi, \mathfrak{a}', \xi')$ as above, $A(\Phi, \mathfrak{a}, \xi)$ and $A(\Phi, \mathfrak{a}', \xi')$ are isomorphic as principally polarized abelian varieties with CM if there is an element $\gamma \in K^*$ such that $(\mathfrak{a}', \xi') = (\gamma\mathfrak{a}, (\gamma\overline{\gamma})^{-1}\xi)$. Is Φ primitive, then the converse holds.

The spaces $\mathcal{M}_{\mathcal{O}_K}, \mathcal{M}_{\mathcal{O}_K}(\Phi)$, and the group $\mathcal{C}_K$

Given a CM field K, let

- $\mathcal{M}_{\mathcal{O}_K}$ be the set of isomorphism classes of ppav's with CM by $\mathcal{O}_K$.
- Fix a CM type Φ, then $\mathcal{M}_{\mathcal{O}_K}(\Phi) \subset \mathcal{M}_{\mathcal{O}_K}$ is the subset of ppav's that admit CM of type Φ.

In order to understand the Galois action of $\mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$ on $\mathcal{M}_{\mathcal{O}_K}$, we need the following definition.

The spaces $\mathcal{M}_{\mathcal{O}_K}, \mathcal{M}_{\mathcal{O}_K}(\Phi)$, and the group $\mathcal{C}_K$

Given a CM field K, let

- $\mathcal{M}_{\mathcal{O}_K}$ be the set of isomorphism classes of ppav's with CM by $\mathcal{O}_K$.
- Fix a CM type Φ, then $\mathcal{M}_{\mathcal{O}_K}(\Phi) \subset \mathcal{M}_{\mathcal{O}_K}$ is the subset of ppav's that admit CM of type Φ.

In order to understand the Galois action of $\mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$ on $\mathcal{M}_{\mathcal{O}_K}$, we need the following definition.

The Shimura class group $\mathcal{C}_K$ of K is the abelian group of equivalence classes

$$\mathcal{C}_K = \left\{(\mathfrak{b}, \beta) : \mathfrak{b} \subset K,\ \beta \in (K_0^*)^+ \text{ with } \mathfrak{b}\overline{\mathfrak{b}} = \beta\mathcal{O}_K\right\} / \sim$$

where $(\mathfrak{b}, \beta) \sim (\mathfrak{b}', \beta')$ if $(\mathfrak{b}', \beta') = (x\mathfrak{b}, x\overline{x}\beta)$ for $x \in K^*$.

The group $\mathcal{C}_K$

The structure of $\mathcal{C}_K$ is given by the sequence

$$1 \to \frac{(\mathcal{O}_{K_0}^*)^+}{N_{K|K_0}(\mathcal{O}_K^*)} \xrightarrow{u \longmapsto (\mathcal{O}_K, u)} \mathcal{C}_K \xrightarrow{(\mathfrak{b}, \beta) \longmapsto \mathfrak{b}} \mathrm{Cl}(K) \xrightarrow{N_{K|K_0}} \mathrm{Cl}^+(K_0),$$

where:

- $(\mathcal{O}_{K_0}^*)^+ \subset \mathcal{O}_{K_0}^*$ is the group of totally positive units, and
- $\mathrm{Cl}^+(K_0)$ is the narrow class group of K_0, where elements correspond to equivalence classes of fractional K_0-ideals modulo totally positive principal fractional K_0-ideals, for any embedding of K_0 into $\mathbb{R}$.

Some results related to the cardinality of $\mathcal{M}_{\mathcal{O}_K}$

Let K be a CM field and let L be its Galois closure. The number of pairs (Φ, A), where Φ is a CM type of K (not necessary primitive), and where A is an isomorphism class of ppav's with CM by $\mathcal{O}_K$ of type (K, Φ), is

$$s_K = \frac{h(K)}{h(K_0)} \#(\mathcal{O}_{K_0}^*/N_{K|K_0}(\mathcal{O}_K^*)).$$

Some results related to the cardinality of $\mathcal{M}_{\mathcal{O}_K}$

Let K be a CM field and let L be its Galois closure. The number of pairs (Φ, A), where Φ is a CM type of K (not necessary primitive), and where A is an isomorphism class of ppav's with CM by $\mathcal{O}_K$ of type (K, Φ), is

$$s_K = \frac{h(K)}{h(K_0)} \#(\mathcal{O}_{K_0}^* / N_{K|K_0}(\mathcal{O}_K^*)).$$

1. Streng: For $g = 2$, $|\mathcal{M}_{\mathcal{O}_K}| = \alpha \cdot s_K$, where α is 1 if and only if K is cyclic, and 2 otherwise.

Some results related to the cardinality of $\mathcal{M}_{\mathcal{O}_K}$

Let K be a CM field and let L be its Galois closure. The number of pairs (Φ, A), where Φ is a CM type of K (not necessary primitive), and where A is an isomorphism class of ppav's with CM by $\mathcal{O}_K$ of type (K, Φ), is

$$s_K = \frac{h(K)}{h(K_0)} \#(\mathcal{O}^*_{K_0}/N_{K|K_0}(\mathcal{O}^*_K)).$$

1. Streng: For $g = 2$, $|\mathcal{M}_{\mathcal{O}_K}| = \alpha \cdot s_K$, where α is 1 if and only if K is cyclic, and 2 otherwise.
2. Sijsling-Ionica-Dina: For $g = 3$,

$$|\mathcal{M}_{\mathcal{O}_K}| = \begin{cases} |\mathcal{C}_K| = \frac{1}{8}s_K & \text{if } K \text{ is Galois,} \\ 3\,|\mathcal{C}_K| = \frac{3}{8}s_K & \text{if } \mathrm{Gal}(L|\mathbb{Q}) \cong D_6, \\ 4\,|\mathcal{C}_K| = \frac{1}{2}s_K & \text{if } \mathrm{Gal}(L|\mathbb{Q}) \cong C_2^3 \rtimes C_3 \text{ or } C_2^3 \rtimes S_3, \end{cases}$$

since $s_K = 8\,|\mathcal{C}_K|$ in all cases, and where the numerator represents the number of equivalence classes of primitive CM types of K.

The action of $\mathcal{C}_K$ on $\mathcal{M}_{\mathcal{O}_K}$, and some consequences

Some properties.

1. Let $(\mathfrak{a}, \xi)$ representing a ppav with CM by $\mathcal{O}_K$. Let $(\mathfrak{b}, \beta)$ be a representative of the Shimura class group $\mathcal{C}_K$ of K. Then

$$(\mathfrak{b}, \beta)(\mathfrak{a}, \xi) = (\mathfrak{b}^{-1}\mathfrak{a}, \beta\xi) \mapsto A(\mathfrak{b}^{-1}\mathfrak{a}, \beta\xi)$$

is a principally polarized abelian variety with CM by $\mathcal{O}_K$.

The action of $\mathcal{C}_K$ on $\mathcal{M}_{\mathcal{O}_K}$, and some consequences

Some properties.

1. Let $(\mathfrak{a}, \xi)$ representing a ppav with CM by $\mathcal{O}_K$. Let $(\mathfrak{b}, \beta)$ be a representative of the Shimura class group $\mathcal{C}_K$ of K. Then

$$(\mathfrak{b}, \beta)(\mathfrak{a}, \xi) = (\mathfrak{b}^{-1}\mathfrak{a}, \beta\xi) \mapsto A(\mathfrak{b}^{-1}\mathfrak{a}, \beta\xi)$$

   is a principally polarized abelian variety with CM by $\mathcal{O}_K$.

2. For a CM type Φ of K, the set $\mathcal{M}_{\mathcal{O}_K}(\Phi)$ is a torsor under $\mathcal{C}_K$; i.e., $\mathcal{M}_{\mathcal{O}_K}(\Phi)$ is non-empty on which $\mathcal{C}_K$ acts freely and transitively.

Galois conjugation

Fix a primitive CM type Φ of K, and with it, a component $\mathcal{M}_{\mathcal{O}_K}(\Phi)$.

Goal. To identify Galois orbits of $\mathcal{M}_{\mathcal{O}_K}(\Phi)$ under $\mathrm{Gal}(\overline{\mathbb{Q}}\,|\,\mathbb{Q})$.

Galois conjugation

Fix a primitive CM type Φ of K, and with it, a component $\mathcal{M}_{\mathcal{O}_K}(\Phi)$.

Goal. To identify Galois orbits of $\mathcal{M}_{\mathcal{O}_K}(\Phi)$ under $\mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$.

Remark. Recall that $\sigma\Phi = \Phi \iff \sigma \in G^r := \mathrm{Gal}(\overline{\mathbb{Q}}|K^r)$, where K^r is the reflex field of (K, Φ). With the consequence, that $\mathcal{M}_{\mathcal{O}_K}(\Phi)$ is stable under the action of G^r.

Galois conjugation

Fix a primitive CM type Φ of K, and with it, a component $\mathcal{M}_{\mathcal{O}_K}(\Phi)$.

Goal. To identify Galois orbits of $\mathcal{M}_{\mathcal{O}_K}(\Phi)$ under $\mathrm{Gal}(\overline{\mathbb{Q}}\,|\,\mathbb{Q})$.

Remark. Recall that $\sigma\Phi = \Phi \iff \sigma \in G^r := \mathrm{Gal}(\overline{\mathbb{Q}}\,|\,K^r)$, where K^r is the reflex field of (K, Φ). With the consequence, that $\mathcal{M}_{\mathcal{O}_K}(\Phi)$ is stable under the action of G^r.

Combine the norm map $N = N_{K^r|\mathbb{Q}} : K^r \to \mathbb{Q}_{>0}$ with the reflex type norm map

$$N_{\Phi^r} : \mathrm{Cl}(K^r) \to \mathrm{Cl}(K),\ [\mathfrak{a}] \mapsto \mathcal{O}_K \cap \prod_{\varphi\in\Phi^r} \varphi(\mathfrak{a})\mathcal{O}_L$$

in order to get a map

$$\mathcal{N}_{\Phi^r} : \mathrm{Cl}(K^r) \to \mathcal{C}_K,\ [\mathfrak{a}] \mapsto (N_{\Phi^r}(\mathfrak{a}), N(\mathfrak{a})).$$

Galois conjugation

Theorem (Main Theorem of Complex Multiplication)

Let $(A, E) \cong A(\mathfrak{a}, \xi)$ *in* $\mathcal{M}_{\mathcal{O}_K}(\Phi)$*, and let* $\sigma \in G^r = \mathrm{Gal}(\overline{\mathbb{Q}} \,|\, K^r)$*. Suppose that under the Artin map, the element* σ *corresponds to the class of the ideal* $\mathfrak{b}$*. Then*

$$A(\mathfrak{a}, \xi)^\sigma \cong A(\mathcal{N}_{\Phi^r}(\mathfrak{b})(\mathfrak{a}, \xi)).$$

Then, Galois orbits of $\mathcal{M}_{\mathcal{O}_K}(\Phi)$ under the group G^r correspond to elements of the quotient

$$\mathcal{C}_K / \operatorname{im}(\mathcal{N}_{\Phi^r}).$$

Let's talk about supersingular abelian surfaces in characteristic $p > 0$.

Supersingular vs. superspecial abelian surfaces

Let k be an algebraically closed finite field of char. $p > 0$. Let A be an abelian variety of dimension 2 (a surface) over k. We call

1. A supersingular (ss) if and only if $A/k \sim E^2/k$,
2. A superspecial (spsp) if and only if $A/k \cong E^2/k$,

where E is a supersingular elliptic curve over k.

Supersingular vs. superspecial abelian surfaces

Let k be an algebraically closed finite field of char. $p > 0$. Let A be an abelian variety of dimension 2 (a surface) over k. We call

1. A supersingular (ss) if and only if $A/k \sim E^2/k$,
2. A superspecial (spsp) if and only if $A/k \cong E^2/k$,

where E is a supersingular elliptic curve over k.

Remark. By Deligne-Ogus-Shioda, it is known that any products of two supersingular elliptic curves are isomorphic. More precisely,

- Shioda showed, that for any E_1, E_2 supersingular elliptic curves,

$$E_1 \times E_2 \sim E \times E.$$

- Deligne-Ogus, showed that supersingular abelian varieties are determined up to isomorphism by their „supersingular type“. For dimension 2, all supersingular abelian surfaces

$$A \sim E^2.$$

The construction of supersingular abelian surfaces

Let α_p be the finite group scheme

$$\alpha_p = \mathrm{Spec}(k[x]/(x^p)).$$

As a finite group scheme, $E[p]$ has a non-split exact sequence,

$$0 \to \alpha_p \to E[p] \to \alpha_p \to 0.$$

Then by Oort, any supersingular (especially, superspecial) abelian surface A/k, is of the form

$$(E \times E)/(i,j)(\alpha_p),$$

given by an exact sequence

$$0 \to \alpha_p \xrightarrow{(i,j)} E \times E \xrightarrow{\pi} A \to 0,$$

and

$$\left(\alpha_p \xrightarrow[\sim]{i} \ker(F : E \to E^{(p)}) \xrightarrow[\sim]{j^{-1}} \alpha_p\right) = \frac{i}{j} \in k \cong \mathrm{End}_k(\alpha_p).$$

Superspecial abelian surfaces

Remarks. Ignoring any (principal) polarization, there exists only one superspecial abelian surface; that is, every superspecial abelian surface A is isomorphic to a product of supersingular elliptic curves.

Depending on the polarization, there are two types of (principally) polarized superspecial abelian surfaces (A, η) over k:

Superspecial abelian surfaces

Remarks. Ignoring any (principal) polarization, there exists only one superspecial abelian surface; that is, every superspecial abelian surface A is isomorphic to a product of supersingular elliptic curves.

Depending on the polarization, there are two types of (principally) polarized superspecial abelian surfaces (A, η) over k:

1. Jacobian-type, $(J_p(C), \eta_\Theta)$, where $J_p(C)$ is Jacobian of a hyperelliptic curve of genus 2, with canonical principal polarization η_Θ, induced by the divisor Θ.

2. Product-type, consisting of products $E \times E$ with principal product polarization η_X, from the divisor

$$X = (E \times \{\mathcal{O}_E\}) + (\{\mathcal{O}_E\} \times E).$$

Superspecial abelian surfaces

Fact. By Oort, as principally polarized abelian surfaces

$$A = (E \times E)/(i,j)(\alpha_p) \cong J_p(C),$$

if and only if $j \neq 0$ and $\frac{i}{j} \notin \mathbb{F}_{p^2}$.

The Deuring-Correspondence

Let E be a supersingular elliptic curve and let $B_{p,\infty} = \mathrm{End}(E) \otimes \mathbb{Q}$ be a quaternion algebra ramified at p, ∞. Deuring described a functorial equivalence between

- the set supersingular elliptic curves over k, up to Galois conjugation, and the set of maximal orders in $B_{p,\infty}$, up to isomorphisms.
- Morphisms $\varphi : E \to E'$ between supersingular elliptic curves are isogenies, and on the quaternion-side, φ corresponds to a free submodule $\mathbb{Z} \subset I_\varphi \subset B_{p,\infty}$ of rank 4 over $\mathbb{Q}$.

The Ibukiyama-Katsura-Oort-Correspondence

Ibukiyama-Katsura-Oort generalized Deuring's construction to supersingular principally polarized abelian surfaces over k, by representing (principal) polarizations on superspecial abelian surfaces via matrices in $B_{p,\infty}$.

More precisely. Fix a maximal order $\mathcal{O}$ in $B_{p,\infty}$ with $\pi \in \mathcal{O}$, such that $\pi^2 + p = 0$. Then, there is an equivalence of categories

The Ibukiyama-Katsura-Oort-Correspondence

Ibukiyama-Katsura-Oort generalized Deuring's construction to supersingular principally polarized abelian surfaces over k, by representing (principal) polarizations on superspecial abelian surfaces via matrices in $B_{p,\infty}$.

More precisely. Fix a maximal order $\mathcal{O}$ in $B_{p,\infty}$ with $\pi \in \mathcal{O}$, such that $\pi^2 + p = 0$. Then, there is an equivalence of categories

- **Objects:** Isomorphism classes of principally polarized superspecial abelian surfaces over k.
  Morphisms: Isogenies with maximal Weil isotropic kernels of prime power degree ℓ^{2n}.

The Ibukiyama-Katsura-Oort-Correspondence

Ibukiyama-Katsura-Oort generalized Deuring's construction to supersingular principally polarized abelian surfaces over k, by representing (principal) polarizations on superspecial abelian surfaces via matrices in $B_{p,\infty}$.

More precisely. Fix a maximal order $\mathcal{O}$ in $B_{p,\infty}$ with $\pi \in \mathcal{O}$, such that $\pi^2 + p = 0$. Then, there is an equivalence of categories

- **Objects:** Isomorphism classes of principally polarized superspecial abelian surfaces over k.
  Morphisms: Isogenies with maximal Weil isotropic kernels of prime power degree ℓ^{2n}.
- **Objects:** Conjugacy classes of positive definite Hermitian matrices in $M_2(\mathcal{O})^*$.
  Morphisms: Conjugation by $M_2(\mathcal{O})$ sending one class to an ℓ^n- multiple of the other; for H_1, H_2 Hermitian matrices, a morphism takes the form $H_2 = gH_1(\bar{g})^t \cdot \ell^n$, where $g \in M_2(\mathcal{O})$.

Let's talk about work in progress: This is a joint project with P. Kutas (ELTE Budapest), G. Lorenzon, and W. Castryck (KU Leuven).

Basic definitions

Let k be an algebraically closed field of characteristic $p > 0$.

- Let $S_{2,1}$ be the supersingular locus, inside the moduli space $\mathcal{A}_{2,1}$ of principally polarized abelian surfaces over k.

Definition

Let K be a quartic CM field with ring of integers $\mathcal{O}_K$. Let (A, η) be a principally polarized superspecial abelian surface over k. We say that A has CM by $\mathcal{O}_K$, if there exists an embedding

$$\iota : \mathcal{O}_K \hookrightarrow M_2(\mathcal{O}) = \mathrm{End}(A),$$

such that the Rosati involution induced by η induces complex multiplication on $\mathcal{O}_K$. We call ι an orientation, and we say that (A, η, ι) is a oriented ppssas over k.

Some categorial perspective

Let K be a quartic CM field with maximal order $\mathcal{O}_K$. Consider the category $\mathcal{S}^{\mathcal{O}_K} = \mathcal{S}_{2,1}^{\mathcal{O}_K}$, were

- **Objects:** Elements in $S_{2,1} \subset \mathcal{A}_{2,1}$, represented by tuples (A, η), where A is a superspecial (spsp) abelian surface with CM by $\mathcal{O}_K$, a principal polarization $\eta : A \to A^\vee$, and $\iota : \mathcal{O}_K \hookrightarrow \mathrm{End}(A)$, a fixed orientation.

Some categorial perspective

Let K be a quartic CM field with maximal order $\mathcal{O}_K$. Consider the category $\mathcal{S}^{\mathcal{O}_K} = \mathcal{S}_{2,1}^{\mathcal{O}_K}$, were

- **Objects:** Elements in $S_{2,1} \subset \mathcal{A}_{2,1}$, represented by tuples (A, η), where A is a superspecial (spsp) abelian surface with CM by $\mathcal{O}_K$, a principal polarization $\eta : A \to A^\vee$, and $\iota : \mathcal{O}_K \hookrightarrow \mathrm{End}(A)$, a fixed orientation.
- **Morphisms:** Morphism are isogenies $\varphi : A \to A'$ respecting polarizations and orientations, i.e.

$$\varphi^*(\eta') = [\ell] \cdot \eta, \ \ell = \deg(\varphi)^2 \in \mathbb{Z}_+, \text{ and}$$
$$\varphi \circ \iota(\alpha) = \iota'(\alpha) \circ \varphi \Longleftrightarrow \iota'(\alpha) = \deg(\varphi)^{-1} \varphi \circ \iota(\alpha) \circ \hat{\varphi}$$

for all $\alpha \in \mathcal{O}_K$.

Some categorial perspective

Question. Is $\mathcal{S}^{\mathcal{O}_K}$ non-empty?

Consider a principally polarized superspecial abelian surface

$$(A_p = E^2, \eta_p) \in S_{2,1}.$$

Some categorial perspective

Question. Is $\mathcal{S}^{\mathcal{O}_K}$ non-empty?

Consider a principally polarized superspecial abelian surface

$$(A_p = E^2, \eta_p) \in S_{2,1}.$$

Let $R = W(k)$ be the rind of Witt-vectors with residue field k. If (A_p, η_p) admits a lift

$$(A/R, \eta)$$

to an abelian scheme with CM, consisting of a principally polarized abelian scheme over R, together with an embedding of rings

$$\iota : \mathcal{O}_K \hookrightarrow \mathrm{End}_S(A),$$

such that the Rosati involution defined by η induces complex conjugation on K, and such that

$$(A, \eta, \iota) \otimes_R k \cong (A_p, \eta_p, \iota),$$

then $(A_p, \eta_p, \iota) \in Obj(\mathcal{S}^{\mathcal{O}_K})$.

Liftings to characteristic zero

Theorem (Goren-Lauter, 2007)

Let (A_p, η_p, ι) be an abelian variety with CM over an algebraically closed field k of characteristic p. Then (A_p, η_p, ι) admits a lifting to characteristic zero.

Liftings to characteristic zero & the action of $\mathcal{C}_K$

Let $(A_p, \eta_p, \iota) \in Obj(\mathcal{S}^{\mathcal{O}_K})$ be a spsp principally polarized abelian surface over k admitting CM by $\mathcal{O}_K$.

- Consider a lift $(A, \eta, \iota) \in \mathcal{M}_{\mathcal{O}_K}(\Phi)$ to a principally polarized abelian surface over $\mathbb{C}$ with CM by $\mathcal{O}_K$ of primitive type (K, Φ). Identify (A, η) by a tuple $(\mathfrak{a}, \xi)$.

Liftings to characteristic zero & the action of $\mathcal{C}_K$

Let $(A_p, \eta_p, \iota) \in Obj(\mathcal{S}^{\mathcal{O}_K})$ be a spsp principally polarized abelian surface over k admitting CM by $\mathcal{O}_K$.

- Consider a lift $(A, \eta, \iota) \in \mathcal{M}_{\mathcal{O}_K}(\Phi)$ to a principally polarized abelian surface over $\mathbb{C}$ with CM by $\mathcal{O}_K$ of primitive type (K, Φ). Identify (A, η) by a tuple $(\mathfrak{a}, \xi)$.
- If $(\mathfrak{b}, \beta)$ is a representative in the Shimura c.g. $\mathcal{C}_K$, then

$$(\mathfrak{b}, \beta)(\mathfrak{a}, \xi) = (\mathfrak{b}^{-1}\mathfrak{a}, \beta\xi) \mapsto A(\mathfrak{b}^{-1}\mathfrak{a}, \beta\xi)$$

is a simple principally polarized abelian variety with CM by $\mathcal{O}_K$, where $\mathfrak{b}$ induces an isogeny

$$\varphi_{\mathfrak{b}} : A(\mathfrak{a}, \xi) \to A(\mathfrak{a}', \xi') := A((\mathfrak{b}, \beta)(\mathfrak{a}, \xi))$$

of degree $N(\mathfrak{b})$, and an embedding

$$\iota' : \mathcal{O}_K \hookrightarrow \mathrm{End}(A(\mathfrak{a}', \xi')), \text{such that}$$
$$\iota'(\alpha) = N(\mathfrak{b})^{-1}\varphi_{\mathfrak{b}} \circ \iota(\alpha) \circ \hat{\varphi}_{\mathfrak{b}}, \text{ for all } \alpha \in \mathcal{O}_K.$$

A commutative diagram

The setup. Consider a principally polarized superspecial abelian surface over k,

$$(A_p/k, \eta_p, \iota : \mathcal{O}_K \hookrightarrow \mathrm{End}(A_p))$$

with CM, together with the following diagram

$$\begin{tikzcd}
A(\mathfrak{a}_0, \xi_0) \arrow[r, dash, "="] \arrow[d, "\text{mod } p"'] & A(\mathfrak{a}_0, \xi_0) \arrow[r, "{(\mathfrak{b}, \beta)}"] & A(\mathfrak{a}, \xi) \arrow[r, dash, "="] & A(\mathfrak{a}, \xi) \arrow[d, "\text{mod } p"'] \\
{[(A_p, \eta_p)]} \arrow[r, dash, "\cong"] & (A_p, \eta_p) \arrow[r, "{(\mathfrak{b}, \beta)}"] \arrow[u, bend left, "\text{lift}"] & (A'_p, \eta'_p) \arrow[r, dash, "\cong"] \arrow[u, bend left, "\text{lift}"] & {[(A'_p, \eta'_p)]}
\end{tikzcd}$$

Some observations

1. Given $B_{p,\infty}$ and (A_p, η_p) as above, is there always a quartic CM field K with ring of integers $\mathcal{O}_K$, and an embedding

$$\iota : \mathcal{O}_K \hookrightarrow \mathrm{End}(A_p),$$

such that the Rosati involution induced by η_p induces complex multiplication on $\mathcal{O}_K$.

Some observations

1. Given $B_{p,\infty}$ and (A_p, η_p) as above, is there always a quartic CM field K with ring of integers $\mathcal{O}_K$, and an embedding

$$\iota : \mathcal{O}_K \hookrightarrow \mathrm{End}(A_p),$$

such that the Rosati involution induced by η_p induces complex multiplication on $\mathcal{O}_K$.

2. Let $(\mathfrak{b}, \beta)$ be an element in $\mathcal{C}_K$. Does the isogeny

$$\varphi_{\mathfrak{b}} : (A_p, \eta_p) \to (A'_p, \eta'_p)$$

induced by $\mathfrak{b}$, always respects embeddings, i.e.

$$\varphi_{\mathfrak{b}} \circ \iota(\alpha) = \iota'(\alpha) \circ \varphi_{\mathfrak{b}} \Longleftrightarrow \iota'(\alpha) = \deg(\varphi_{\mathfrak{b}})^{-1} \varphi_{\mathfrak{b}} \circ \iota(\alpha) \circ \hat{\varphi}_{\mathfrak{b}} \quad (1)$$

for all $\alpha \in \mathcal{O}_K$.

Some observations

Observations.

- We have discovered computationally, that (2) is true, if $N(\mathfrak{b}) \in \mathbb{Q}$. After lifting to characteristic zero, $N(\mathfrak{b}) \in \mathbb{Q}$ is equivalent to say that $(\mathfrak{b}, \beta) \in \mathrm{im}(\mathcal{N}_{\Phi^r})$, where

$$\mathcal{N}_{\Phi^r} : \mathrm{Cl}(K^r) \to \mathcal{C}_K, \; [\mathfrak{a}] \mapsto (N_{\Phi^r}(\mathfrak{a}), N(\mathfrak{a}))$$

is the reflex type norm map.

Some observations

Observations.

- We have discovered computationally, that (2) is true, if $N(\mathfrak{b}) \in \mathbb{Q}$. After lifting to characteristic zero, $N(\mathfrak{b}) \in \mathbb{Q}$ is equivalent to say that $(\mathfrak{b}, \beta) \in \mathrm{im}(\mathcal{N}_{\Phi^r})$, where
$$\mathcal{N}_{\Phi^r} : \mathrm{Cl}(K^r) \to \mathcal{C}_K,\ [\mathfrak{a}] \mapsto (N_{\Phi^r}(\mathfrak{a}), N(\mathfrak{a}))$$
is the reflex type norm map.
- Further, by the Main Theorem of Complex Multiplication, this implies, that $G^r = \mathrm{Gal}(K^r|\mathbb{Q})$ is acting trivial on objects of $\mathcal{S}^{\mathcal{O}_K}$.

Some observations

Observations.

- We have discovered computationally, that (2) is true, if $N(\mathfrak{b}) \in \mathbb{Q}$. After lifting to characteristic zero, $N(\mathfrak{b}) \in \mathbb{Q}$ is equivalent to say that $(\mathfrak{b}, \beta) \in \mathrm{im}(\mathcal{N}_{\Phi^r})$, where

  $$\mathcal{N}_{\Phi^r} : \mathrm{Cl}(K^r) \to \mathcal{C}_K,\ [\mathfrak{a}] \mapsto (N_{\Phi^r}(\mathfrak{a}), N(\mathfrak{a}))$$

  is the reflex type norm map.
- Further, by the Main Theorem of Complex Multiplication, this implies, that $G^r = \mathrm{Gal}(K^r|\mathbb{Q})$ is acting trivial on objects of $\mathcal{S}^{\mathcal{O}_K}$.
- Then, Galois orbits of $\mathcal{M}_{\mathcal{O}_K}(\Phi)$ under the group G^r correspond to elements of the quotient

  $$\mathcal{C}_K / \mathrm{im}(\mathcal{N}_{\Phi^r}).$$

Some observations

3. Compute orbits in $\mathcal{S}^{\mathcal{O}_K}$ under morphism induced by $\mathcal{C}_K$.

Proof Sketch. Since $h(\mathcal{C}_K) \neq 0$ in general, $\mathcal{C}_K$ induces non-trivial morphisms on $\mathcal{S}^{\mathcal{O}_K}$. By the previous observation, we are interested in determining the group $\mathrm{im}(\mathcal{N}_{\Phi^r}) \subset \mathcal{C}_K$ since (computationally) this corresponds to the maximal subgroup in $\mathcal{C}_K$ which respects orientations.

Some observations

3. Compute orbits in $\mathcal{S}^{\mathcal{O}_K}$ under morphism induced by $\mathcal{C}_K$.

Proof Sketch. Since $h(\mathcal{C}_K) \neq 0$ in general, $\mathcal{C}_K$ induces non-trivial morphisms on $\mathcal{S}^{\mathcal{O}_K}$. By the previous observation, we are interested in determining the group $\mathrm{im}(\mathcal{N}_{\Phi^r}) \subset \mathcal{C}_K$ since (computationally) this corresponds to the maximal subgroup in $\mathcal{C}_K$ which respects orientations.

In characteristic zero we know that the index of $\mathrm{im}(\mathcal{N}_{\Phi^r})$ in $\mathcal{C}_K$ is a power of two. Since $\mathcal{C}_K$ acts freely and transitively on the space $\mathcal{M}_{\mathcal{O}_K}(\Phi)$, of simple principally polarized abelian surfaces, we expect $\mathcal{S}^{\mathcal{O}_K}$ to have one single orbit of length $\#\,\mathrm{im}(\mathcal{N}_{\Phi^r})$.

Some observations

4. Give some „explicit“ criteria, such that the CM lift (A, η) of (A_p, η_p), is
$$(A, \eta) \cong_{\mathbb{C}} (J(C), \eta_\Theta).$$

Some observations

4. Give some „explicit" criteria, such that the CM lift (A, η) of (A_p, η_p), is

$$(A, \eta) \cong_{\mathbb{C}} (J(C), \eta_{\Theta}).$$

5. If $(A, \eta) \cong_{\mathbb{C}} (E \times E, \eta_X)$ is in the boundary (i.e. a degenerate point) in the moduli space $\mathcal{A}_{2,1}(\mathbb{C})$, can we impose some conditions on η_X, such that $\eta_X \cong \eta_{\Theta}$, where Θ is the divisor on a Jacobian of a hyperelliptic curve of genus 2 over $\mathbb{C}$.

Some observations

4. Give some „explicit“ criteria, such that the CM lift (A, η) of (A_p, η_p), is

$$(A, \eta) \cong_{\mathbb{C}} (J(C), \eta_{\Theta}).$$

5. If $(A, \eta) \cong_{\mathbb{C}} (E \times E, \eta_X)$ is in the boundary (i.e. a degenerate point) in the moduli space $\mathcal{A}_{2,1}(\mathbb{C})$, can we impose some conditions on η_X, such that $\eta_X \cong \eta_{\Theta}$, where Θ is the divisor on a Jacobian of a hyperelliptic curve of genus 2 over $\mathbb{C}$.

By assumption (A_p, η_p) has CM by $\mathcal{O}_K$, and $K = \mathcal{O}_K \otimes \mathbb{Q}$ is a CM field. Any CM lift (A, η) cannot be in the boundary, since in this case, $\mathrm{End}(E \times E) \cong M_2(\mathcal{O})$ and $\mathrm{End}^0(E \times E) \cong M_2(B_{p,\infty})$.

Then, $M_2(B_{p,\infty})$ splits over $\mathbb{C}$, as

$$M_2(B_{p,\infty}) \otimes_{\mathbb{Q}} \mathbb{C} \cong M_2(M_2(\mathbb{C})) \cong M_4(\mathbb{C}),$$

which is of dimension 16 over $\mathbb{Q}$.