

Superspecial surfaces for algebraists

Péter Kutas

ELTE and University of Birmingham

AM-PQC, Ohrid , 12th August, 2026

Outline

- The simplest description of $SQ\text{sign}$
- Endomorphism rings of superspecial surfaces
- Surfaces with real multiplication
- Surfaces with complex multiplication

Simplest description of SQIsign

Algebra good, Geometry bad

Philosophy of the talk: understanding geometric objects through algebra is usually easier.

Principally polarized superspecial abelian surfaces

- The SIDH attacks opened a portal to higher dimensions
- Even isogenists struggled/struggle to truly understand higher-dimensional phenomena
- Common questions: why are some isogenies good (polarized) and some bad (not polarized)? why is it hard to evaluate some isogenies (not answered in this talk)? why is everything so different from dimension 1, and why do I have to care about principal polarizations (and what even are those?)
- Since algebra is good and geometry is bad, we will think algebraically
- Starting point: endomorphism algebras of principally polarized superspecial abelian surfaces are **central simple $\mathbb{Q}$ -algebras with a positive involution of the first kind** coming from the Rosati involution

The Rosati involution

- Let $\varphi: E_1 \rightarrow E_2$ be an isogeny. Then its dual $\hat{\varphi}$ is defined by $\varphi \circ \hat{\varphi} = [d]$

The Rosati involution

- Let $\varphi: E_1 \rightarrow E_2$ be an isogeny. Then its dual $\hat{\varphi}$ is defined by $\varphi \circ \hat{\varphi} = [d]$
- Have you actually ever seen the proof of why this exists?

The Rosati involution

- Let $\varphi: E_1 \rightarrow E_2$ be an isogeny. Then its dual $\hat{\varphi}$ is defined by $\varphi \circ \hat{\varphi} = [d]$
- Have you actually ever seen the proof of why this exists?
- This actually tells you that the dual isogeny goes between the dual varieties

The Rosati involution

- Let $\varphi: E_1 \rightarrow E_2$ be an isogeny. Then its dual $\hat{\varphi}$ is defined by $\varphi \circ \hat{\varphi} = [d]$
- Have you actually ever seen the proof of why this exists?
- This actually tells you that the dual isogeny goes between the dual varieties
-

$$\hat{\varphi}: E_2 \xrightarrow{\kappa_2} \text{Pic}^0(E_2) \xrightarrow{\varphi^*} \text{Pic}^0(E_1) \xrightarrow{\sigma_1} E_1, \quad \hat{\varphi} = \sigma_1 \circ \varphi^* \circ \kappa_2.$$

The Rosati involution

- Let $\varphi: E_1 \rightarrow E_2$ be an isogeny. Then its dual $\hat{\varphi}$ is defined by $\varphi \circ \hat{\varphi} = [d]$
- Have you actually ever seen the proof of why this exists?
- This actually tells you that the dual isogeny goes between the dual varieties

-

$$\hat{\varphi}: E_2 \xrightarrow{\kappa_2} \text{Pic}^0(E_2) \xrightarrow{\varphi^*} \text{Pic}^0(E_1) \xrightarrow{\sigma_1} E_1, \quad \hat{\varphi} = \sigma_1 \circ \varphi^* \circ \kappa_2.$$

- Trick: use the principal polarizations to define an involution on endomorphisms

The Rosati involution

- Let $\varphi: E_1 \rightarrow E_2$ be an isogeny. Then its dual $\hat{\varphi}$ is defined by $\varphi \circ \hat{\varphi} = [d]$
- Have you actually ever seen the proof of why this exists?
- This actually tells you that the dual isogeny goes between the dual varieties

$$\hat{\varphi}: E_2 \xrightarrow{\kappa_2} \text{Pic}^0(E_2) \xrightarrow{\varphi^*} \text{Pic}^0(E_1) \xrightarrow{\sigma_1} E_1, \quad \hat{\varphi} = \sigma_1 \circ \varphi^* \circ \kappa_2.$$

- Trick: use the principal polarizations to define an involution on endomorphisms

Definition 1

Let (A, λ) be a principally polarized abelian variety and let $\sigma: A \rightarrow A$ be an endomorphism. Then the Rosati involution is defined by

$$\sigma^\dagger = \lambda^{-1} \hat{\sigma} \lambda.$$

Involutions of the first kind

- A central simple K -algebra A is a finite-dimensional K -algebra whose center is K
- An involution is a map $\sigma: A \rightarrow A$ that is K -linear, reverses multiplication ($\sigma(ab) = \sigma(b)\sigma(a)$), and satisfies $\sigma^2 = \text{id}$
- An involution is of the first kind if it fixes the center
- Examples: $M_2(\mathbb{C})$ and transposition (taking the adjoint would be an involution of the second kind)
- Let $K = \mathbb{Q}$; then an involution is positive if $\text{Trd}(a\sigma(a)) > 0$ iff $a \neq 0$

Quaternion algebras

- Let K be a field of characteristic different from 2. A quaternion algebra over K is a central simple algebra of dimension 4 over K
- Can be given by a quaternion basis $1, i, j, ij$ such that $i^2 = a$, $j^2 = b$, $ij = -ji$ where $a, b \in K^*$; this is then often denoted by $(a, b)_K$
- Quaternion conjugation: for $z = a_1 + a_2i + a_3j + a_4ij$, we have $\bar{z} = a_1 - a_2i - a_3j - a_4ij$
- Interesting property: $\bar{z}z \in K$ and is actually the reduced norm, and $z + \bar{z} \in K$ and is the reduced trace
- In general, involutions for which $a\sigma(a)$ is in the center are called standard involutions

Central simple algebras with involutions

- Which algebras admit an involution of the first kind?
- Albert, Merkurjev: tensor products of quaternion algebras
- Over $\mathbb{Q}$ these are really just matrix algebras over quaternion algebras (any two quaternion algebras contain a common splitting field by Hasse–Minkowski)
- Endomorphism algebras that appear later: $M_g(B_{p,\infty})$, so the quaternion algebra is always fixed and is ramified at p and infinity (very happy to explain what this means, if someone is curious!), which in practice is $(-1, -p)_{\mathbb{Q}}$

Maximal orders

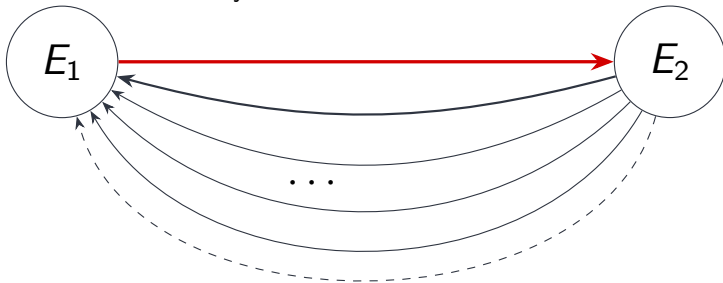
- Let $K = \mathbb{Q}$ (for now)
- In a non-commutative setting, integral elements (elements whose minimal polynomial is monic and has integer coefficients) do not form a ring; they live in a collection of “big rings”
- Order: contains 1, is a subring, and is a $\mathbb{Z}$ -lattice of the same rank as the dimension of the algebra
- Maximal order: an order that is not contained in any other order
- These are really the arithmetic objects

Why do we love quaternions?

- Standard involutions only exist for quaternion algebras
- Quaternion conjugation is really a canonical involution in many aspects
- Maximal orders of quaternion algebras are automatically stable under quaternion conjugation (proof: the trace of an element is in $\mathbb{Z}$!)
- Quadratic subrings are automatically closed under quaternion conjugation
- Endomorphism rings of supersingular elliptic curves are maximal orders in $B_{p,\infty}$
- We often forget the importance of quaternion conjugation as it is so canonical (on the geometry side we say that elliptic curves have a canonical principal polarization coming from the point at infinity)

Deuring correspondence

- The endomorphism rings of supersingular elliptic curves are maximal orders in $B_{p,\infty}$
- Let E_1, E_2 be two supersingular elliptic curves. Then $\text{Hom}(E_1, E_2)$ carries a natural left $\text{End}(E_2)$ - and right $\text{End}(E_1)$ -module structure
- The picture below shows how you can make a Hom set into an ideal:



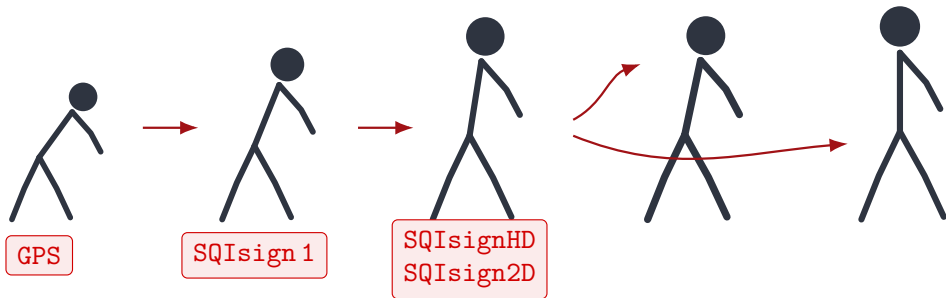
- The Hom sets are also 4-dimensional Euclidean lattices with the degree as the norm
- The algebraic equivalent of the isogeny problem is finding a left ideal of $\text{End}(E_1)$

The birth of SQIsign

- Finding isogenies is hard
- Finding a connecting ideal is easy, but the norm of the ideal (the gcd of the quaternion norms) is big and non-smooth if done naively, so you cannot translate it to an isogeny
- Kohel–Lauter–Petit–Tignol (2014): you can find a connecting ideal of smooth norm in polynomial time
- Still many issues to make it into a signature scheme, but at least one has an explicit Deuring correspondence, which is the big first step
- Many technical improvements emerged with the introduction of HD techniques, which led to the evolution of SQIsign

The evolution of SQIsign

Australopithecus *Homo habilis* *Homo erectus* *Homo neanderthalensis* *Homo sapiens*



Superspecial abelian surfaces

- Endomorphism rings of superspecial abelian surfaces are maximal orders in $M_2(B_{p,\infty})$

Superspecial abelian surfaces

- Endomorphism rings of superspecial abelian surfaces are maximal orders in $M_2(B_{p,\infty})$
- Eichler's theorem: all maximal orders in $M_2(B_{p,\infty})$ are conjugate to each other (isomorphic as rings)

Superspecial abelian surfaces

- Endomorphism rings of superspecial abelian surfaces are maximal orders in $M_2(B_{p,\infty})$
- Eichler's theorem: all maximal orders in $M_2(B_{p,\infty})$ are conjugate to each other (isomorphic as rings)
- Main point: endomorphism rings are **rings with an involution**, which is fundamental to their structure!

Superspecial abelian surfaces

- Endomorphism rings of superspecial abelian surfaces are maximal orders in $M_2(B_{p,\infty})$
- Eichler's theorem: all maximal orders in $M_2(B_{p,\infty})$ are conjugate to each other (isomorphic as rings)
- Main point: endomorphism rings are **rings with an involution**, which is fundamental to their structure!
- How can one properly have an algebraic correspondence for superspecial surfaces?

Ibukiyama–Katsura–Oort

- Since all maximal orders are isomorphic, it is enough to fix one that is easy to work with
- Take $M_2(O_0)$ where O_0 is a maximal order in $B_{p,\infty}$
- IKO: parametrize surfaces by varying the involutions on $M_2(O_0)$
- Each positive involution will be

$$x^\dagger = g^{-1}x^*g,$$

where $*$ is conjugate transpose and

$$g = \begin{pmatrix} s & r \\ \bar{r} & t \end{pmatrix},$$

with $s, t > 0$ integers, $r \in O_0$, and $st - N(r) > 0$

- Two matrices g_1, g_2 are equivalent if $g_2 = u^*g_1u$ where $u \in \mathrm{GL}_2(O_0)$
- What about isogenies?

Ibukiyama–Katsura–Oort II

- A polarized isogeny will be represented by a $\gamma \in M_2(O_0)$ if

$$\gamma^* g_2 \gamma = N g_1,$$

where N is an integer

- While this definition is nice and simple, it is not so natural from an algebraic point of view
- Question: could you have a version of IKO where you keep the involution to be $*$ and vary the maximal order?
- Ongoing work: yes

Base-point free IKO

- Important fact: not all maximal orders are stable under conjugate transpose! So we take exactly those that are as our objects
- Isogenies will naturally correspond to conjugations $(\gamma^{-1}\Lambda\gamma)$, as all one-sided ideals of maximal orders are principal
- You can't take any conjugation, as you need the new order to be stable under conjugate transpose. A simple calculation shows that $\gamma \in \Lambda$ represents polarized conjugation if $\gamma^*\gamma$ generates a two-sided ideal of Λ (whose classification is known)
- How can you get from IKO to this version? Write $g = u^*u$ with $u \in M_2(B_{p,\infty})$, and then $uM_2(O_0)u^{-1}$ will be a maximal order stable under $*$
- Summary: all of this explains why you have to care about polarizations and polarized isogenies in higher dimensions. What else is this good for?

KLPT2

- KLPT2 (Castryck, Decru, K, Laval, Petit, Ti): given g_1 and g_2 , you can actually find a γ such that $\gamma^* g_2 \gamma = 2^k g_1$ in polynomial time, which is a first step in generalizing SQIsign to higher dimensions (don't believe isogenists — current versions are not higher-dimensional)
- The main issue with KLPT2 and its improvements is that the path is very long (even in improved versions), and other ideas currently run into some issues
- Problem: because of the appearance of polarizations, isogenies between surfaces have no lattice structure, hence short isogenies are hard to find
- Methods in dimension 1 do not immediately generalize to dimension 2, because the underlying algebra is **not a quaternion algebra**
- **We want quaternions!!**

Along came real multiplications

Definition 2

Let A be a superspecial surface and let R be the ring of integers of a totally real quadratic field. We say A has RM by R if there exists an embedding $\iota: R \hookrightarrow \text{End}(A)$ such that the image of ι is symmetric with respect to the Rosati involution elementwise.

What does the RM-preserving part of the endomorphism ring look like? What do KLPT-like problems look like?

RM-KLPT

- Take $a \in M_2(O_0)$ that is symmetric with respect to the $(g-)$ Rosati involution, denoted †
- What is the centralizer of a in $B_{p,\infty}$?
- A short lemma shows that it is $B_{p,\infty} \otimes \mathbb{Q}(a)$, and Rosati acts as quaternion conjugation on this quaternion algebra
- A KLPT problem: one is given two matrices with real multiplication $(g_1, a_1), (g_2, a_2)$ and has to find a $\gamma \in M_2(O_0)$ such that

$$\gamma^* g_2 \gamma = g_1 N, \quad \gamma a_1 = a_2 \gamma$$

- Even more constraints than in KLPT2 — what can we do?
- Joint work with Chen, Decru, Montessinos, Spindler and Swanson
- One can reduce this problem to finding connecting ideals between “maximal orders” in $B_{p,\infty} \otimes \mathbb{Q}(\sqrt{d})$ and really follow all the steps of 1-dimensional KLPT!

RM-KLPT II

- We want to solve

$$\gamma^* g_2 \gamma = g_1 2^l, \quad \gamma a_1 = a_2 \gamma$$

- We find an initial solution δ for which $\delta^* g_2 \delta = g_1 N$, $\delta a_1 = a_2 \delta$, and we have no control on how big N is (in fact N won't even be an integer in our algorithm)
- One can show that finding an element of norm $N 2^k$ in the ideal $\text{Cent}(a_2) \cap \delta^* M_2(O_0)$ will provide a solution to the original equation with 2^k
- While this can be shown by a calculation, the reason it works is that you have the exact geometric picture as in the case of the Deuring correspondence

RM-KLPT III

- For reasons mentioned in the open-problem section, we currently restrict to RM by a very small field ($\mathbb{Q}(\sqrt{5})$)
- KLPT2 does not look like KLPT1 at all, and it has many limitations (paths are around p^{18})
- RM-KLPT returns a path of length $p^{5.5}$ ($p^{4.5}$ after incorporating the Petit–Smith improvement)
- Everything you have seen in dimension 1 more or less immediately generalizes to this setting with good bounds
- Why should cryptographers care?

Higher dimensional isogeny problems

- Is the endomorphism ring problem harder in higher dimensions?
- A recent attack generalizes to the RM setting, but its cost is $p^{2/3+o(1)}$ with memory scaling quadratically as well
- Big ongoing project started with Damien Robert (involving many people): generalize all SQIsign variants to the RM setting
- Advantages: no problem doing this in dimension 2, the bounds are pretty much the same, and generalization to higher dimensions is also very easy
- In dimension 2 you can use half the field characteristic, and Qlapoti generalizes in a straightforward way
- Hope: RM-SQIsign will be faster

Higher dimensional isogeny problems II

- Preliminary results: the new attack also generalizes to the general case, but right now it seems to give no advantage
- The general endomorphism ring problem has $O(p)$ complexity
- It is still an important question how to do SQIsign without the small RM
- The RM viewpoint is still helpful: many isogenies between surfaces can be viewed as RM-preserving isogenies for some RM, and RM isogenies are automatically polarized! (that is why we love quaternions!)
- A small observation: an endomorphism b is RM-preserving for some RM if and only if $bb^\dagger = b^\dagger b$

Orientations

- We have seen attempts at higher-dimensional SQIsign. What about CSIDH?
- CSIDH for non-isogenists: one can look at supersingular elliptic curves over $\mathbb{F}_p$, and then there is a commutative group action of the class group of $\mathbb{Z}[\sqrt{-p}]$ on the set of these curves
- This enables many, many cryptographic constructions
- The situation is a bit more general: an orientation of a supersingular elliptic curve (probably a bad name — it should be called CM?) is a quadratic subring of the endomorphism ring
- The class group of this ring acts naturally on the set of oriented supersingular elliptic curves
- Class group actions other than CSIDH exist, e.g., SCALLOP, Orient Express

Surfaces with CM

- What about higher dimensions?

Definition 3

A surface A has CM by a quartic CM order R if R embeds into the endomorphism ring of A in a way that **Rosati acts as complex conjugation** (this is automatic in dimension 1 but NOT in higher dimensions).

- Is the class group acting on these CM surfaces? NO — it has to be refined (Shimura class group) to incorporate principal polarizations
- Castryck, Dina, K, Lorenzon: we investigated this Shimura action for superspecial surfaces, and I will just quickly list some fun facts

Surfaces with CM II

- CSIDH does not generalize to this setting, but there are versions which resemble CSIDH
- Orbits are more complicated as the action is not transitive: you can have 1, 2, or 4 orbits depending on the CM
- If your surface has CM by an order with a small Shimura class group, then you can compute the full endomorphism ring in polynomial time
- If your surface has a known endomorphism ring, you can evaluate the Shimura class group action for ideals that DO NOT give you an N -isogeny

Conclusion

- Understanding phenomena is often easier on the algebra side (even doing experiments is)
- Involutions are much more important for higher dimensions and are very closely related to polarizations
- Varieties with RM are the good analogues of the 1 dimensional picture
- It is to view higher dimensional isogenies as a collection of RM preserving isogenies (you can view the Hom set as an infinite collection of lattices)
- If you feel that the higher dimensional scene is impossible to learn at this stage, do not worry, you can jump on the isogeny train if you like quaternions!