Real multiplication on superspecial abelian varieties and the strict class group

Mickaël Montessinos

Eötvös Loránd University, Hungary

Friday 18$^{\text{th}}$ September, 2026

Leuven Isogeny Days 7

Real multiplication with trivial strict class group

Fix a totally real number field K of degree n with trivial strict class group.

Optimistic promises

- Algebraically speaking, principally polarised superspecial abelian varieties with real multiplication by $\mathbb{Z}_K$ behave remarkably like supersingular elliptic curve.
- We have a Deuring correspondence.
- The $\mathfrak{l}$-isogeny graph is connected.
- We have KLPT! (for $n = 2$ and K with small discriminant).
- We could just pretend that these are supersingular elliptic curves and replicate the schemes we know and love with smaller primes.[a]

[a] Difficulties may arise for representing isogenies on the geometric side of things.

Real multiplication with arbitrary strict class group

Fix a totally real number field K of degree n with arbitrary strict class group.

The end of innocence

1. The $\mathfrak{l}$-isogeny graph may not be connected.
2. Many isomorphy classes of varieties with RM may have isomorphic endomorphism rings.
3. Polarisations and real multiplications are slightly decorrelated.
4. KLPT is not so straightforward.

Silver lining

- All the issues above can be described precisely.
- New toys to play with!

Superspecial abelian varieties with real multiplication

Fix a supersingular elliptic curve E_0 over $\mathbb{F}_{p^2}$, $n \in \mathbb{N}$ and K a totally real number field of degree n unramified at p. Set $\mathrm{End}(E_0) = \mathcal{O}_0$.

Definition

A *real multiplication* on E_0^n is an embedding

$$\iota\colon \mathbb{Z}_K \to \mathrm{End}(E_0^n) = M_n(\mathcal{O}_0).$$

Since all superspecial abelian varieties of dimension n are isomorphic, we may restrict to studying real multiplications on E_0^n.

$$\begin{tikzcd} & \mathbb{Z}_K \arrow[dl, "\iota_A"'] \arrow[dr, "\iota_{E_0}"] & \\ A \arrow[rr, "\sim"] & & E_0^g \end{tikzcd}$$

Homomorphisms and endomorphisms

Definition (The module of homomorphisms)

Let ι_1, ι_2 be real multiplications. A homomorphism

$$\gamma \colon \iota_1 \to \iota_2$$

is a matrix $\gamma \in M_n(\mathcal{O}_0)$ such that

$$\forall \alpha \in \mathbb{Z}_K, \ \iota_2(\alpha)\gamma = \gamma\iota_1(\alpha).$$

We write $\mathrm{Hom}(\iota_1, \iota_2)$ for the $\mathbb{Z}_K$-module of such homomorphisms.

Theorem ([Nic05, Theorem 2.5.27] generalised)

Let ι be a real multiplication. The module $\mathrm{End}(\iota) = \mathrm{Hom}(\iota, \iota)$ *is an Eichler order of discriminant p in*

$$\mathrm{End}^0(\iota) := \mathbb{Q}\,\mathrm{End}(\iota) \simeq B_{p,\infty} \otimes_{\mathbb{Q}} K.$$

The Deuring correspondence

Fix a real multiplication ι_0.

Definition (The ideal of a homomorphism)

Let ι be a real multiplication, and let $\gamma \in \mathrm{Hom}(\iota_1, \iota_2)$. We set

$$I_\gamma = \mathrm{Hom}(\iota_2, \iota_1)\gamma.$$

I_γ is a left ideal in $\mathrm{End}(\iota_1)$ whose right order is isomorphic to $\mathrm{End}(\iota_2)$.

Not quite a theorem but I'm pretty sure. I just need to write down the proof. Really, how hard can it be? Ok, fine, let's call it a conjecture. But you're killing me!

For a real multiplication ι, pick any $\gamma \in \mathrm{Hom}(\iota_0, \iota)$ and associate ι to I_γ. This defines a bijection

$$\{\text{Real multiplications}\}/\{\sim\} \to \{\text{left ideal classes in } \mathrm{End}(\iota_0)\}.$$

The Deuring correspondence is well behaved

Theorem

- *If* $\gamma_1 \in \mathrm{End}(\iota_1, \iota_2)$ *and* $\gamma_2 \in \mathrm{End}(\iota_2, \iota_3)$, *then*

$$I_{\gamma_1}(\gamma_1^{-1} I_{\gamma_2} \gamma_1) = I_{\gamma_1 \gamma_2}.$$

- *If* $\gamma : \gamma_1 \to \gamma_2$, *we have*

$$N_{K/\mathbb{Q}}(N(I_\gamma)) = \mathrm{nrd}(\gamma).$$

Takeaway

The Deuring correspondence is well behaved regarding the composition and the degree of homomorphisms.

A primer on the strict class group

Definition

The strict class group $\mathrm{Cl}^+(K)$ of K is the group

$$\{\text{ideals of } \mathbb{Z}_K\} \,/\, \{\text{principal ideals with a totally positive generator}\}$$

Definition (Invertible modules with a notion of positivity)

An *invertible $\mathbb{Z}_K$-module with a notion of positivity* is the data (M, M^+) of

1. An invertible $\mathbb{Z}_K$-module M;
2. An orientation on the real line $M \otimes_{\mathbb{Z}_K} \sigma$ for σ going over the embeddings of K into $\mathbb{R}$.

Fact

There is a bijection between $\mathrm{Cl}^+(K)$ and the set of isomorphy classes of invertible $\mathbb{Z}_K$-modules with a notion of positivity.

Isogeny paths

Theorem ([Vig80, Theorem III.4.3])

The set of left ideal classes of $\mathcal{O}$ is supported by ideals with norm supported in any set of ideals whose classes generate $\mathrm{Cl}^+(K)$.

Consequence

While the ℓ-isogeny graph fails to be connected, smooth isogeny paths may exist depending on the generators of the strict class group.

Theorem ([Wes19])

Under ERH, the strict class group of K is generated by primes ideals coprime to p with norm bounded from above by

$$B = (2.71 \log(p^2 \Delta_K) + 2.67n + 4.13)^2$$

Real multiplications with isomorphic End rings

Some quaternion facts ([KV10])

Let $\mathcal{O}$ be an Eichler of discriminant p in $B_{p,\infty} \otimes K$.

1. Let I be a left ideal in $\mathcal{O}$, let $\mathcal{O}'$ be the right order of I. There is a bijection between the set of left ideal classes in $\mathcal{O}$ with $\mathcal{O}'$ as a right order and the set of two-sided ideal classes in $\mathcal{O}'$.
2. If $\mathcal{O}'$ is an Eichler order of discriminant p, the set of two-sided ideal classes of $\mathcal{O}'$ is generated by

$$\left\{\mathcal{O}'I, [I] \in \mathrm{Cl}(K)\right\} \cup \left\{[\mathcal{O}', \mathcal{O}'] + \mathcal{O}'\mathfrak{p}, \mathfrak{p} \mid p\right\}.$$

Consequence

A real multiplication ι shares an endomorphism ring with its Frobenius conjugateS and some conjugates induced by a class group action.

Definition (The conjugated real multiplication)

Let ι be a real multiplication. The *conjugate* real multiplication is the embedding

$$\begin{array}{cccc} \iota^* & \mathbb{Z}_K & \to & M_n(\mathcal{O}_0) \\ & \alpha & \mapsto & \iota(\alpha)^* \end{array}$$

Definition (K-linear polarisations)

Define

$$\mathcal{M}_\iota = \{g \in \mathrm{Hom}(\iota, \iota^*) \colon \; g = g^*\}$$
$$\mathcal{M}_\iota^+ = \{g \in \mathcal{M}(\iota) \colon \; g \text{ is positive definite}\}\,.$$

A K-linear polarisation of ι is an element of $\mathcal{M}^+(\iota)$.

Polarisations and the strict class group

Let ι be a real multiplication.

1. $\mathcal{M}_\iota$ is a $\mathbb{Z}_K$ module via multiplication by $\iota(\alpha)$ on the right.
2. This makes $(\mathcal{M}_\iota, \mathcal{M}_\iota^+)$ into an invertible $\mathbb{Z}_K$-module with notion of positivity.
3. There is a map from the set of isomorphy classes of real multiplication to $\mathrm{Cl}^+(K)$.
4. The real multiplication ι admits a K-linear principal polarisation if and only if $(\mathcal{M}_\iota, \mathcal{M}_\iota^+)$ is isomorphic to $(\mathbb{Z}_K, \mathbb{Z}_K^+)$.
5. If $\gamma\colon \iota_1 \to \iota_2$, we have

$$[(\mathcal{M}_{\iota_2}, \mathcal{M}_{\iota_2}^+)] = [(\mathcal{M}_{\iota_1}, \mathcal{M}_{\iota_1}^+) N(I_\gamma)]$$

And now, a fun construction

Theorem ([LM33, Tau49, Ben67])

There is a bijection

$$\begin{array}{ccc} \mathrm{Cl}(K) & \to & \{\textit{Embeddings } \mathbb{Z}_K \hookrightarrow M_n(\mathbb{Z})\}/\{\sim\} \\ I & \mapsto & \iota_I = \textit{Regular representation of } \mathbb{Z}_K \textit{ with} \\ & & \textit{respect to a basis of } I \end{array}$$

Fun facts

1. $\mathrm{End}(\iota_I) \simeq \mathcal{O}_0 \otimes \mathbb{Z}_K$.
2. $\mathrm{Hom}(\iota, \iota_{\mathbb{Z}_K}) \simeq \mathrm{End}(\iota_{\mathbb{Z}_K}) I$.
3. $(\mathcal{M}_{\iota_I}, \mathcal{M}^+_{\iota_I}) \simeq (\mathcal{M}_{\iota_{\mathbb{Z}_K}}, \mathcal{M}^+_{\iota_{\mathbb{Z}_K}})(I, I^+)^2$.

Some open questions

1. Give a geometric interpretation of these algebraic phenomena.
2. Are these phenomena applicable to cryptography?
3. Computing isogenies induced by the class group of the RM without knowing the endomorphism ring.
4. Generalised RM-KLPT
5. Invent your own open question

Play with RM in Sage!

https://gitlab.com/Mickanos/real-multiplication

Edward A. Bender.
Classes of matrices over an integral domain.
Ill. J. Math., 11:697–702, 1967.

Markus Kirschmer and John Voight.
Algorithmic enumeration of ideal classes for quaternion orders.
SIAM J. Comput., 39(5):1714–1747, 2010.

Claiborne G. Latimer and C. C. MacDuffee.
A correspondence between classes of ideals and classes of matrices.
Ann. Math. (2), 34:313–316, 1933.

Marc-Hubert Nicole.
Superspecial abelian varieties, theta series and the Jacquet–Langlands correspondence.
PhD thesis, McGillUniversity, 2005.

References II

Olga Taussky.
On a theorem of Latimer and MacDuffee.
Can. J. Math., 1:300–302, 1949.

Marie-France Vignéras.
Arithmétique des algèbres de quaternions, volume 800 of *Lect. Notes Math.*
Springer, Cham, 1980.

Benjamin Wesolowski.
Generating subgroups of ray class groups with small prime ideals.
In *ANTS XIII. Proceedings of the thirteenth algorithmic number theory symposium, University of Wisconsin-Madison, WI, USA, July 16–20, 2018*, pages 461–478. Berkeley, CA: Mathematical Sciences Publishers (MSP), 2019.