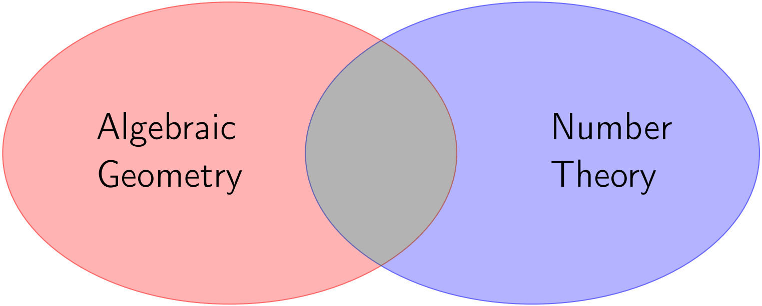
# Cohen-Macaulay type of endomorphism rings of abelian varieties over finite fields

Stefano Marseglia

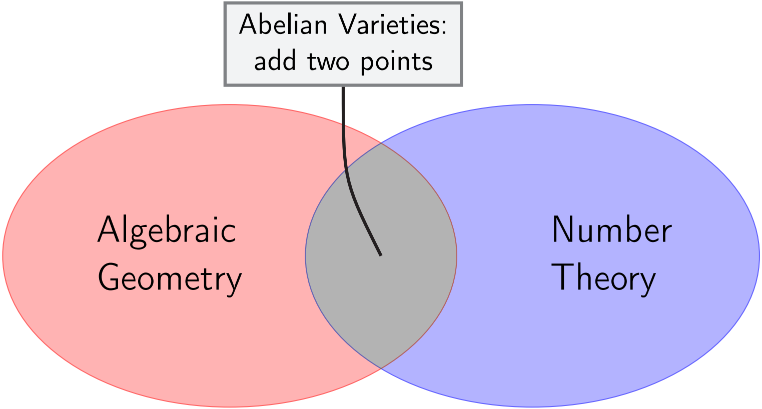
University of French Polynesia

Essen Oberseminar - 23 May 2024.

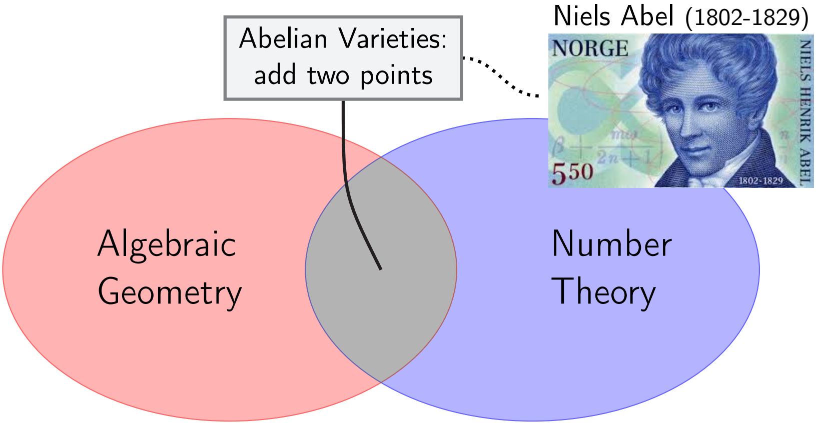
# What do I do for a living?



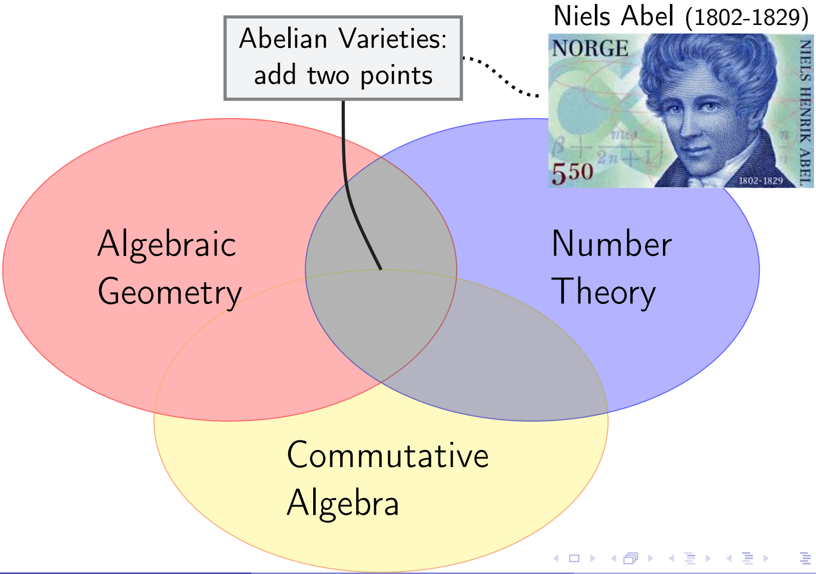
# What do I do for a living?



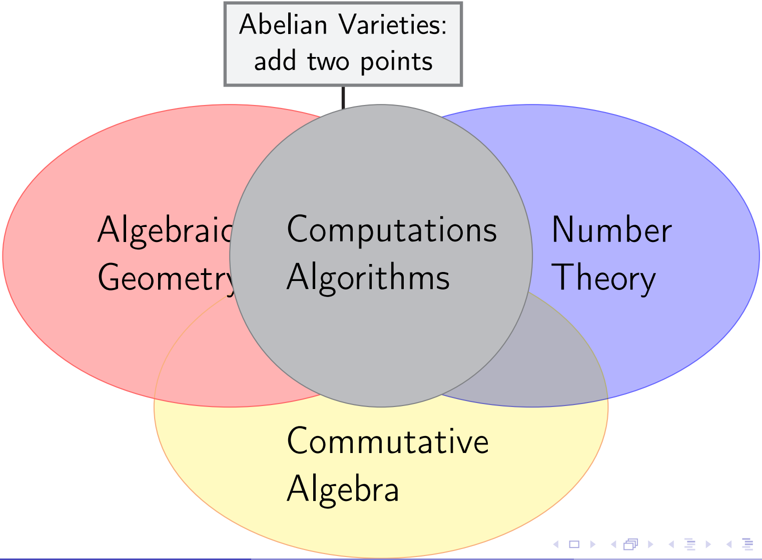
## What do I do for a living?



# What do I do for a living?



# What do I do for a living?



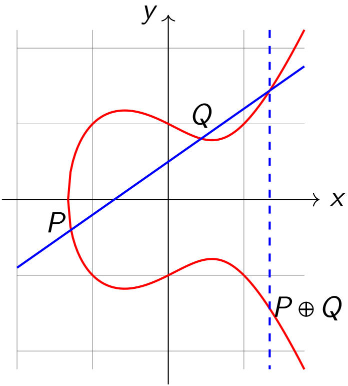
# Abelian varieties: what are they ?

Abelian varieties are connected projective group varieties.

## Abelian varieties: what are they ?

Abelian varieties are connected projective group varieties.

Abelian varieties of dim. 1 are called **elliptic curves**.
Eg: over $\mathbb{R}$, $y^2 = x^3 - x + 1$

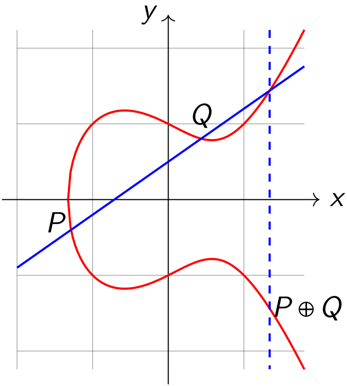


# Abelian varieties: what are they ?

Abelian varieties are connected projective group varieties.

Abelian varieties of dim. 1
are called **elliptic curves**.
Eg: over $\mathbb{R}$, $y^2 = x^3 - x + 1$

We can add points:
$P, Q \rightsquigarrow P \oplus Q$



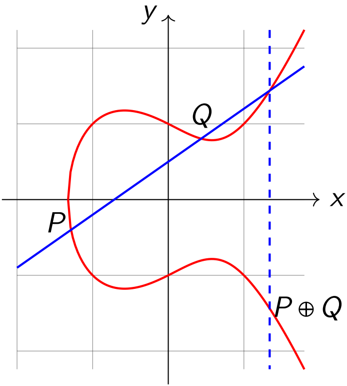
# Abelian varieties: what are they ?

Abelian varieties are connected projective group varieties.

Abelian varieties of dim. 1 are called **elliptic curves**.
Eg: over $\mathbb{R}$, $y^2 = x^3 - x + 1$

We can add points:
$P, Q \rightsquigarrow P \oplus Q$

Equations are impractical in dim $\geq 2$.
We need a better way to represent them...



# Abelian varieties over $\mathbb{C}$ vs $\mathbb{F}_q$

- Let $A/\mathbb{C}$ be an abelian variety of dimension $g$.

## Abelian varieties over $\mathbb{C}$ vs $\mathbb{F}_q$

- Let $A/\mathbb{C}$ be an abelian variety of dimension $g$.
- Then $A(\mathbb{C})$ is a **torus**: $T := \mathbb{C}^g/\Lambda$, where $\Lambda \simeq_{\mathbb{Z}} \mathbb{Z}^{2g}$.

# Abelian varieties over $\mathbb{C}$ vs $\mathbb{F}_q$

- Let $A/\mathbb{C}$ be an abelian variety of dimension $g$.
- Then $A(\mathbb{C})$ is a **torus**: $T := \mathbb{C}^g/\Lambda$, where $\Lambda \simeq_{\mathbb{Z}} \mathbb{Z}^{2g}$.
- $T$ admits a non-degenerate Riemann form $\longleftrightarrow$ polarization.

# Abelian varieties over $\mathbb{C}$ vs $\mathbb{F}_q$

- Let $A/\mathbb{C}$ be an abelian variety of dimension $g$.
- Then $A(\mathbb{C})$ is a **torus**: $T := \mathbb{C}^g/\Lambda$, where $\Lambda \simeq_{\mathbb{Z}} \mathbb{Z}^{2g}$.
- $T$ admits a non-degenerate Riemann form $\longleftrightarrow$ polarization.
- In fact, $A \mapsto A(\mathbb{C})$ induces an equivalence of categories:

$$\{\text{abelian varieties } /\mathbb{C}\} \longleftrightarrow \left\{ \begin{matrix} \mathbb{C}^g/\Lambda \text{ with } \Lambda \simeq \mathbb{Z}^{2g} \text{ admitting} \\ \text{a Riemann form} \end{matrix} \right\}.$$

## Abelian varieties over $\mathbb{C}$ vs $\mathbb{F}_q$

- Let $A/\mathbb{C}$ be an abelian variety of dimension $g$.
- Then $A(\mathbb{C})$ is a **torus**: $T := \mathbb{C}^g/\Lambda$, where $\Lambda \simeq_{\mathbb{Z}} \mathbb{Z}^{2g}$.
- $T$ admits a non-degenerate Riemann form $\longleftrightarrow$ polarization.
- In fact, $A \mapsto A(\mathbb{C})$ induces an equivalence of categories:

$$\{\text{abelian varieties } /\mathbb{C}\} \longleftrightarrow \left\{ \begin{matrix} \mathbb{C}^g/\Lambda \text{ with } \Lambda \simeq \mathbb{Z}^{2g} \text{ admitting} \\ \text{a Riemann form} \end{matrix} \right\}.$$

- In char. $p > 0$ such an equivalence cannot exist : there are (supersingular) elliptic curves with quaternionic endomorphism algebras.

## Abelian varieties over $\mathbb{C}$ vs $\mathbb{F}_q$

- Let $A/\mathbb{C}$ be an abelian variety of dimension $g$.
- Then $A(\mathbb{C})$ is a **torus**: $T := \mathbb{C}^g/\Lambda$, where $\Lambda \simeq_{\mathbb{Z}} \mathbb{Z}^{2g}$.
- $T$ admits a non-degenerate Riemann form $\longleftrightarrow$ polarization.
- In fact, $A \mapsto A(\mathbb{C})$ induces an equivalence of categories:

$$\{\text{abelian varieties } /\mathbb{C}\} \longleftrightarrow \left\{ \begin{matrix} \mathbb{C}^g/\Lambda \text{ with } \Lambda \simeq \mathbb{Z}^{2g} \text{ admitting} \\ \text{a Riemann form} \end{matrix} \right\}.$$

- In char. $p > 0$ such an equivalence cannot exist : there are (supersingular) elliptic curves with quaternionic endomorphism algebras.
- Nevertheless, as we will see later, over a finite field $\mathbb{F}_q$, we obtain analogous results if we restrict ourselves to certain **subcategories** of AVs.

## Abelian varieties over $\mathbb{C}$ vs $\mathbb{F}_q$

- Let $A/\mathbb{C}$ be an abelian variety of dimension $g$.
- Then $A(\mathbb{C})$ is a **torus**: $T := \mathbb{C}^g/\Lambda$, where $\Lambda \simeq_{\mathbb{Z}} \mathbb{Z}^{2g}$.
- $T$ admits a non-degenerate Riemann form $\longleftrightarrow$ polarization.
- In fact, $A \mapsto A(\mathbb{C})$ induces an equivalence of categories:

$$\{\text{abelian varieties } /\mathbb{C}\} \longleftrightarrow \left\{ \begin{matrix} \mathbb{C}^g/\Lambda \text{ with } \Lambda \simeq \mathbb{Z}^{2g} \text{ admitting} \\ \text{a Riemann form} \end{matrix} \right\}.$$

- In char. $p > 0$ such an equivalence cannot exist : there are (supersingular) elliptic curves with quaternionic endomorphism algebras.
- Nevertheless, as we will see later, over a finite field $\mathbb{F}_q$, we obtain analogous results if we restrict ourselves to certain **subcategories** of AVs.
- WARNING: all morphisms, endomorphisms, isogenies, etc. are defined over $\mathbb{F}_q$.

## Isogeny classification over $\mathbb{F}_q$

- An **isogeny** $A \to B$ is a surjective morphism with finite kernel.

## Isogeny classification over $\mathbb{F}_q$

- An **isogeny** $A \to B$ is a surjective morphism with finite kernel.
- $A/\mathbb{F}_q$ comes with a **Frobenius** endomorphism,

# Isogeny classification over $\mathbb{F}_q$

- An **isogeny** $A \to B$ is a surjective morphism with finite kernel.
- $A/\mathbb{F}_q$ comes with a **Frobenius** endomorphism, that induces an action

$$\mathrm{Frob}_A : T_\ell A \to T_\ell A \text{ for any } \ell \neq p,$$

where $T_\ell(A) = \varprojlim A[\ell^n] \simeq \mathbb{Z}_\ell^{2g}$.

# Isogeny classification over $\mathbb{F}_q$

- An **isogeny** $A \to B$ is a surjective morphism with finite kernel.
- $A/\mathbb{F}_q$ comes with a **Frobenius** endomorphism, that induces an action

$$\mathrm{Frob}_A : T_\ell A \to T_\ell A \text{ for any } \ell \neq p,$$

  where $T_\ell(A) = \varprojlim A[\ell^n] \simeq \mathbb{Z}_\ell^{2g}$.
- $h_A(x) := \mathrm{char}(\mathrm{Frob}_A)$ is a $q$-Weil polynomial.

# Isogeny classification over $\mathbb{F}_q$

- An **isogeny** $A \to B$ is a surjective morphism with finite kernel.
- $A/\mathbb{F}_q$ comes with a **Frobenius** endomorphism, that induces an action

$$\mathrm{Frob}_A : T_\ell A \to T_\ell A \text{ for any } \ell \neq p,$$

  where $T_\ell(A) = \varprojlim A[\ell^n] \simeq \mathbb{Z}_\ell^{2g}$.
- $h_A(x) := \mathrm{char}(\mathrm{Frob}_A)$ is a $q$-Weil polynomial.
- **Honda-Tate** theory:
  - $h_A(x)$ is *the* **isogeny invariant**

$$A \sim_{\mathbb{F}_q} B \text{ iff } h_A(x) = h_B(x),$$

# Isogeny classification over $\mathbb{F}_q$

- An **isogeny** $A \to B$ is a surjective morphism with finite kernel.
- $A/\mathbb{F}_q$ comes with a **Frobenius** endomorphism, that induces an action

$$\mathrm{Frob}_A : T_\ell A \to T_\ell A \text{ for any } \ell \neq p,$$

  where $T_\ell(A) = \varprojlim A[\ell^n] \simeq \mathbb{Z}_\ell^{2g}$.
- $h_A(x) := \mathrm{char}(\mathrm{Frob}_A)$ is a $q$-Weil polynomial.
- **Honda-Tate** theory:
  - $h_A(x)$ is *the* **isogeny invariant**

$$A \sim_{\mathbb{F}_q} B \text{ iff } h_A(x) = h_B(x),$$

  - the association

$$\text{isogeny class of } A \longmapsto h_A(x)$$

  allows us to enumerate all AVs up to isogeny.

# Endomorphism rings

- $\mathrm{End}(A)$ is a free $\mathbb{Z}$-module of finite rank ...

## Endomorphism rings

- $\mathrm{End}(A)$ is a free $\mathbb{Z}$-module of finite rank ...
- ... $\mathrm{End}(A) \subset \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$.

## Endomorphism rings

- $\mathrm{End}(A)$ is a free $\mathbb{Z}$-module of finite rank ...
- ... $\mathrm{End}(A) \subset \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$.
- Denote by $\pi_A \in \mathrm{End}(A)$ the Frobenius endomorphism of $A$.

# Endomorphism rings

- $\mathrm{End}(A)$ is a free $\mathbb{Z}$-module of finite rank ...
- ... $\mathrm{End}(A) \subset \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$.
- Denote by $\pi_A \in \mathrm{End}(A)$ the Frobenius endomorphism of $A$.
- Tate: $h_A(x)$ is squarefree $\iff$ $\mathrm{End}(A)$ is commutative.
  (We will assume this for the rest of the talk.)

# Endomorphism rings

- $\mathrm{End}(A)$ is a free $\mathbb{Z}$-module of finite rank ...
- ... $\mathrm{End}(A) \subset \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$.
- Denote by $\pi_A \in \mathrm{End}(A)$ the Frobenius endomorphism of $A$.
- Tate: $h_A(x)$ is squarefree $\iff$ $\mathrm{End}(A)$ is commutative.
  (We will assume this for the rest of the talk.)
- Set $K = \mathbb{Q}[x]/(h_A) = \mathbb{Q}[\pi]$. It is an **étale $\mathbb{Q}$-algebra**
  (i.e. a finite product of number fields).

# Endomorphism rings

- $\mathrm{End}(A)$ is a free $\mathbb{Z}$-module of finite rank ...
- ... $\mathrm{End}(A) \subset \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$.
- Denote by $\pi_A \in \mathrm{End}(A)$ the Frobenius endomorphism of $A$.
- Tate: $h_A(x)$ is squarefree $\iff$ $\mathrm{End}(A)$ is commutative.
  (We will assume this for the rest of the talk.)
- Set $K = \mathbb{Q}[x]/(h_A) = \mathbb{Q}[\pi]$. It is an **étale $\mathbb{Q}$-algebra**
  (i.e. a finite product of number fields).
- The association $\pi_A \mapsto \pi$ allows us to identify $\mathrm{End}(A)$ with a special kind of subring of $K$:

# Endomorphism rings

- $\mathrm{End}(A)$ is a free $\mathbb{Z}$-module of finite rank ...
- ... $\mathrm{End}(A) \subset \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$.
- Denote by $\pi_A \in \mathrm{End}(A)$ the Frobenius endomorphism of $A$.
- Tate: $h_A(x)$ is squarefree $\iff$ $\mathrm{End}(A)$ is commutative.
  (We will assume this for the rest of the talk.)
- Set $K = \mathbb{Q}[x]/(h_A) = \mathbb{Q}[\pi]$. It is an **étale $\mathbb{Q}$-algebra**
  (i.e. a finite product of number fields).
- The association $\pi_A \mapsto \pi$ allows us to identify $\mathrm{End}(A)$ with a special kind of subring of $K$:
- $\mathbb{Z}[\pi, q/\pi] \subseteq \mathrm{End}(A) \subseteq \mathcal{O}_K$ are orders in $K$
  (an **order** $R$ in $K$ is a subring $R \subset K$ such that $R \simeq_{\mathbb{Z}} \mathbb{Z}^{\dim_{\mathbb{Q}} K}$).

# Endomorphism rings

- $\mathrm{End}(A)$ is a free $\mathbb{Z}$-module of finite rank ...
- ... $\mathrm{End}(A) \subset \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$.
- Denote by $\pi_A \in \mathrm{End}(A)$ the Frobenius endomorphism of $A$.
- Tate: $h_A(x)$ is squarefree $\iff$ $\mathrm{End}(A)$ is commutative.
  (We will assume this for the rest of the talk.)
- Set $K = \mathbb{Q}[x]/(h_A) = \mathbb{Q}[\pi]$. It is an **étale $\mathbb{Q}$-algebra**
  (i.e. a finite product of number fields).
- The association $\pi_A \mapsto \pi$ allows us to identify $\mathrm{End}(A)$ with a special kind of subring of $K$:
- $\mathbb{Z}[\pi, q/\pi] \subseteq \mathrm{End}(A) \subseteq \mathcal{O}_K$ are orders in $K$
  (an **order** $R$ in $K$ is a subring $R \subset K$ such that $R \simeq_{\mathbb{Z}} \mathbb{Z}^{\dim_{\mathbb{Q}} K}$).
- Plan: study $A$ by studying some comm. algebra properties of $\mathrm{End}(A)$.

# Orders and fractional ideals in étale $\mathbb{Q}$-algebras

## Orders and fractional ideals in étale $\mathbb{Q}$-algebras

- Let $R$ be an order in a étale $\mathbb{Q}$-algebra $K$.

# Orders and fractional ideals in étale $\mathbb{Q}$-algebras

- Let $R$ be an order in a étale $\mathbb{Q}$-algebra $K$.
- A **fractional** $R$**-ideal** is a sub-$R$-module $I \subset K$ such that $I \simeq_{\mathbb{Z}} \mathbb{Z}^{\dim_{\mathbb{Q}} K}$.

# Orders and fractional ideals in étale $\mathbb{Q}$-algebras

- Let $R$ be an order in a étale $\mathbb{Q}$-algebra $K$.
- A **fractional** $R$**-ideal** is a sub-$R$-module $I \subset K$ such that $I \simeq_{\mathbb{Z}} \mathbb{Z}^{\dim_{\mathbb{Q}} K}$.
- Given fr. $R$-ideals $I, J$ then

$$(I : J) = \{a \in K : aJ \subseteq I\} \quad \text{and} \quad I^t = \left\{a \in K : \mathrm{Tr}_{K/\mathbb{Q}}(aI) \subseteq \mathbb{Z}\right\}$$

are also fr. $R$-ideals.

# Orders and fractional ideals in étale $\mathbb{Q}$-algebras

- Let $R$ be an order in a étale $\mathbb{Q}$-algebra $K$.
- A **fractional** $R$**-ideal** is a sub-$R$-module $I \subset K$ such that $I \simeq_{\mathbb{Z}} \mathbb{Z}^{\dim_{\mathbb{Q}} K}$.
- Given fr. $R$-ideals $I, J$ then

$$(I : J) = \{a \in K : aJ \subseteq I\} \quad \text{and} \quad I^t = \left\{a \in K : \mathrm{Tr}_{K/\mathbb{Q}}(aI) \subseteq \mathbb{Z}\right\}$$

  are also fr. $R$-ideals.
- The order $(I : I)$ is the **multiplicator ring** of $I$ and satisfies:

$$(I : I)^t = I \cdot I^t.$$

# Orders and fractional ideals in étale $\mathbb{Q}$-algebras

- Let $R$ be an order in a étale $\mathbb{Q}$-algebra $K$.
- A **fractional $R$-ideal** is a sub-$R$-module $I \subset K$ such that $I \simeq_{\mathbb{Z}} \mathbb{Z}^{\dim_{\mathbb{Q}} K}$.
- Given fr. $R$-ideals $I, J$ then

$$(I : J) = \{a \in K : aJ \subseteq I\} \quad \text{and} \quad I^t = \left\{a \in K : \mathrm{Tr}_{K/\mathbb{Q}}(aI) \subseteq \mathbb{Z}\right\}$$

  are also fr. $R$-ideals.
- The order $(I : I)$ is the **multiplicator ring** of $I$ and satisfies:

$$(I : I)^t = I \cdot I^t.$$

- A fr. $R$-ideal $I$ is invertible if $I(R : I) = R$ ...

# Orders and fractional ideals in étale $\mathbb{Q}$-algebras

- Let $R$ be an order in a étale $\mathbb{Q}$-algebra $K$.
- A **fractional** $R$**-ideal** is a sub-$R$-module $I \subset K$ such that $I \simeq_{\mathbb{Z}} \mathbb{Z}^{\dim_{\mathbb{Q}} K}$.
- Given fr. $R$-ideals $I, J$ then

$$(I : J) = \{a \in K : aJ \subseteq I\} \quad \text{and} \quad I^t = \left\{a \in K : \mathrm{Tr}_{K/\mathbb{Q}}(aI) \subseteq \mathbb{Z}\right\}$$

  are also fr. $R$-ideals.
- The order $(I : I)$ is the **multiplicator ring** of $I$ and satisfies:

$$(I : I)^t = I \cdot I^t.$$

- A fr. $R$-ideal $I$ is invertible if $I(R : I) = R$ ...
- ... or, equivalently, $I_{\mathfrak{m}} \simeq R_{\mathfrak{m}}$ as $R_{\mathfrak{m}}$-modules for every $\mathfrak{m}$ maximal $R$-ideal.
  ($R_{\mathfrak{m}}$ is the completion of $R$ at $\mathfrak{m}$)

# Orders and fractional ideals in étale $\mathbb{Q}$-algebras

- Let $R$ be an order in a étale $\mathbb{Q}$-algebra $K$.
- A **fractional** $R$**-ideal** is a sub-$R$-module $I \subset K$ such that $I \simeq_{\mathbb{Z}} \mathbb{Z}^{\dim_{\mathbb{Q}} K}$.
- Given fr. $R$-ideals $I, J$ then

  $$(I : J) = \{a \in K : aJ \subseteq I\} \quad \text{and} \quad I^t = \left\{a \in K : \mathrm{Tr}_{K/\mathbb{Q}}(aI) \subseteq \mathbb{Z}\right\}$$

  are also fr. $R$-ideals.
- The order $(I : I)$ is the **multiplicator ring** of $I$ and satisfies:

  $$(I : I)^t = I \cdot I^t.$$

- A fr. $R$-ideal $I$ is invertible if $I(R : I) = R$ ...
- ... or, equivalently, $I_{\mathfrak{m}} \simeq R_{\mathfrak{m}}$ as $R_{\mathfrak{m}}$-modules for every $\mathfrak{m}$ maximal $R$-ideal.
  ($R_{\mathfrak{m}}$ is the completion of $R$ at $\mathfrak{m}$)
- If $I$ is invertible, then $(I : I) = R$.

# Cohen-Macaulay type and Gorenstein orders

- Def: The **(Cohen-Macaulay) type** of $R$ at a maximal ideal $\mathfrak{m}$ is

$$\mathrm{type}_{\mathfrak{m}}(R) := \dim_{R/\mathfrak{m}} \frac{R^t}{\mathfrak{m}R^t}.$$

# Cohen-Macaulay type and Gorenstein orders

- Def: The **(Cohen-Macaulay) type** of $R$ at a maximal ideal $\mathfrak{m}$ is

$$\mathrm{type}_{\mathfrak{m}}(R) := \dim_{R/\mathfrak{m}} \frac{R^t}{\mathfrak{m}R^t}.$$

- Def: $R$ is **Gorenstein** at $\mathfrak{m}$ if $\mathrm{type}_{\mathfrak{m}}(R) = 1$.

# Cohen-Macaulay type and Gorenstein orders

- Def: The **(Cohen-Macaulay) type** of $R$ at a maximal ideal $\mathfrak{m}$ is
$$\mathrm{type}_{\mathfrak{m}}(R) := \dim_{R/\mathfrak{m}} \frac{R^t}{\mathfrak{m}R^t}.$$
- Def: $R$ is **Gorenstein** at $\mathfrak{m}$ if $\mathrm{type}_{\mathfrak{m}}(R) = 1$.
- Remark: these definitions coincides with the 'usual' ones.

# Cohen-Macaulay type and Gorenstein orders

- Def: The **(Cohen-Macaulay) type** of $R$ at a maximal ideal $\mathfrak{m}$ is

$$\mathrm{type}_{\mathfrak{m}}(R) := \dim_{R/\mathfrak{m}} \frac{R^t}{\mathfrak{m}R^t}.$$

- Def: $R$ is **Gorenstein** at $\mathfrak{m}$ if $\mathrm{type}_{\mathfrak{m}}(R) = 1$.
- Remark: these definitions coincides with the 'usual' ones.
- Ex: monogenic $\mathbb{Z}[\alpha]$ and maximal $\mathscr{O}_K$ orders are Gorenstein. (also $\mathbb{Z}[\pi, q/\pi]$ for AVs).

# Cohen-Macaulay type and Gorenstein orders

- Def: The **(Cohen-Macaulay) type** of $R$ at a maximal ideal $\mathfrak{m}$ is
$$\mathrm{type}_{\mathfrak{m}}(R) := \dim_{R/\mathfrak{m}} \frac{R^t}{\mathfrak{m}R^t}.$$
- Def: $R$ is **Gorenstein** at $\mathfrak{m}$ if $\mathrm{type}_{\mathfrak{m}}(R) = 1$.
- Remark: these definitions coincides with the 'usual' ones.
- Ex: monogenic $\mathbb{Z}[\alpha]$ and maximal $\mathcal{O}_K$ orders are Gorenstein. (also $\mathbb{Z}[\pi, q/\pi]$ for AVs).
- Ex: pick a prime $\ell \in \mathbb{Z}$. Then $\mathrm{type}_{\ell\mathcal{O}_K}(\mathbb{Z} + \ell\mathcal{O}_K) = \dim_{\mathbb{Q}} K - 1$.

# Classification for orders of type $\leq 2$

**Theorem**

*Let $\mathfrak{m}$ be a maximal ideal of $R$, and $I$ a fr. $R$-ideal with $(I : I) = R$.*

# Classification for orders of type $\leq 2$

**Theorem**

*Let $\mathfrak{m}$ be a maximal ideal of $R$, and $I$ a fr. $R$-ideal with $(I : I) = R$.*

1. *If* $\mathrm{type}_{\mathfrak{m}}(R) = 1$ *(Gorenstein) then $I_{\mathfrak{m}} \simeq R_{\mathfrak{m}}$ as $R_{\mathfrak{m}}$-modules.*

# Classification for orders of type $\leq 2$

**Theorem**

*Let $\mathfrak{m}$ be a maximal ideal of $R$, and $I$ a fr. $R$-ideal with $(I:I) = R$.*

1. *If* $\mathrm{type}_{\mathfrak{m}}(R) = 1$ *(Gorenstein) then $I_{\mathfrak{m}} \simeq R_{\mathfrak{m}}$ as $R_{\mathfrak{m}}$-modules.*
2. *If* $\mathrm{type}_{\mathfrak{m}}(R) = 2$ *then either $I_{\mathfrak{m}} \simeq R_{\mathfrak{m}}$ or $I_{\mathfrak{m}} \simeq R^t_{\mathfrak{m}}$ as $R_{\mathfrak{m}}$-modules.*

## Classification for orders of type $\leq 2$

**Theorem**

*Let $\mathfrak{m}$ be a maximal ideal of $R$, and $I$ a fr. $R$-ideal with $(I : I) = R$.*

1. *If $\mathrm{type}_{\mathfrak{m}}(R) = 1$ (Gorenstein) then $I_{\mathfrak{m}} \simeq R_{\mathfrak{m}}$ as $R_{\mathfrak{m}}$-modules.*
2. *If $\mathrm{type}_{\mathfrak{m}}(R) = 2$ then either $I_{\mathfrak{m}} \simeq R_{\mathfrak{m}}$ or $I_{\mathfrak{m}} \simeq R_{\mathfrak{m}}^t$ as $R_{\mathfrak{m}}$-modules.*

Part 1 is contained (in a much more general form) in the "Ubiquity" paper by H. Bass.
Part 2 is new, and we give a proof.

# Classification for orders of type $\leq 2$

**Theorem**

*Let $\mathfrak{m}$ be a maximal ideal of $R$, and $I$ a fr. $R$-ideal with $(I:I) = R$.*

1. *If $\mathrm{type}_{\mathfrak{m}}(R) = 1$ (Gorenstein) then $I_{\mathfrak{m}} \simeq R_{\mathfrak{m}}$ as $R_{\mathfrak{m}}$-modules.*
2. *If $\mathrm{type}_{\mathfrak{m}}(R) = 2$ then either $I_{\mathfrak{m}} \simeq R_{\mathfrak{m}}$ or $I_{\mathfrak{m}} \simeq R_{\mathfrak{m}}^t$ as $R_{\mathfrak{m}}$-modules.*

Part 1 is contained (in a much more general form) in the "Ubiquity" paper by H. Bass.
Part 2 is new, and we give a proof.

**Lemma**

*Let $U, V, W$ be vectors spaces (over some field). Assume that $\dim W \geq 2$, and let $m : U \otimes V \to W$ be a surjective map. Then:*

# Classification for orders of type $\leq 2$

**Theorem**

*Let $\mathfrak{m}$ be a maximal ideal of $R$, and $I$ a fr. $R$-ideal with $(I:I) = R$.*

1. *If $\operatorname{type}_{\mathfrak{m}}(R) = 1$ (Gorenstein) then $I_{\mathfrak{m}} \simeq R_{\mathfrak{m}}$ as $R_{\mathfrak{m}}$-modules.*
2. *If $\operatorname{type}_{\mathfrak{m}}(R) = 2$ then either $I_{\mathfrak{m}} \simeq R_{\mathfrak{m}}$ or $I_{\mathfrak{m}} \simeq R_{\mathfrak{m}}^t$ as $R_{\mathfrak{m}}$-modules.*

Part 1 is contained (in a much more general form) in the "Ubiquity" paper by H. Bass.
Part 2 is new, and we give a proof.

**Lemma**

*Let $U, V, W$ be vectors spaces (over some field). Assume that $\dim W \geq 2$, and let $m : U \otimes V \to W$ be a surjective map. Then:*

1. *$\exists u \in U$ such that $\dim(m(u \otimes V)) \geq 2$, or*

# Classification for orders of type $\leq 2$

### Theorem

*Let $\mathfrak{m}$ be a maximal ideal of $R$, and $I$ a fr. $R$-ideal with $(I : I) = R$.*

1. *If $\operatorname{type}_{\mathfrak{m}}(R) = 1$ (Gorenstein) then $I_{\mathfrak{m}} \simeq R_{\mathfrak{m}}$ as $R_{\mathfrak{m}}$-modules.*
2. *If $\operatorname{type}_{\mathfrak{m}}(R) = 2$ then either $I_{\mathfrak{m}} \simeq R_{\mathfrak{m}}$ or $I_{\mathfrak{m}} \simeq R^t_{\mathfrak{m}}$ as $R_{\mathfrak{m}}$-modules.*

Part 1 is contained (in a much more general form) in the "Ubiquity" paper by H. Bass.
Part 2 is new, and we give a proof.

### Lemma

*Let $U, V, W$ be vectors spaces (over some field). Assume that $\dim W \geq 2$, and let $m : U \otimes V \to W$ be a surjective map. Then:*

1. *$\exists u \in U$ such that $\dim(m(u \otimes V)) \geq 2$, or*
2. *$\exists v \in V$ such that $\dim(m(U \otimes v)) \geq 2$.*

# Proof of Part 2

## Proof of Part 2

- Put $U = I/\mathfrak{m}I$, $V = I^t/\mathfrak{m}I^t$ and $W = R^t/\mathfrak{m}R^t$.

## Proof of Part 2

- Put $U = I/\mathfrak{m}I$, $V = I^t/\mathfrak{m}I^t$ and $W = R^t/\mathfrak{m}R^t$.
- By assumption $R^t = I \cdot I^t$, so the map $m : U \otimes V \to W$ induced by multiplication $I \times I^t \to R^t$ is surjective.

# Proof of Part 2

- Put $U = I/\mathfrak{m}I$, $V = I^t/\mathfrak{m}I^t$ and $W = R^t/\mathfrak{m}R^t$.
- By assumption $R^t = I \cdot I^t$, so the map $m : U \otimes V \to W$ induced by multiplication $I \times I^t \to R^t$ is surjective.
- Moreover, $\dim W = 2$ (because of the assumption on the type).

# Proof of Part 2

- Put $U = I/\mathfrak{m}I$, $V = I^t/\mathfrak{m}I^t$ and $W = R^t/\mathfrak{m}R^t$.
- By assumption $R^t = I \cdot I^t$, so the map $m : U \otimes V \to W$ induced by multiplication $I \times I^t \to R^t$ is surjective.
- Moreover, $\dim W = 2$ (because of the assumption on the type).
- By the Lemma:
  1. $\exists x \in I$ such that $m((x+\mathfrak{m}I)\otimes V) = \frac{xI^t+\mathfrak{m}R^t}{\mathfrak{m}R^t}$ equals $W$.
     By Nakayama's lemma: $I^t_{\mathfrak{m}} \simeq R^t_{\mathfrak{m}} \iff R_{\mathfrak{m}} \simeq I_{\mathfrak{m}}, \ldots$

## Proof of Part 2

- Put $U = I/\mathfrak{m}I$, $V = I^t/\mathfrak{m}I^t$ and $W = R^t/\mathfrak{m}R^t$.
- By assumption $R^t = I \cdot I^t$, so the map $m : U \otimes V \to W$ induced by multiplication $I \times I^t \to R^t$ is surjective.
- Moreover, $\dim W = 2$ (because of the assumption on the type).
- By the Lemma:
  1. $\exists x \in I$ such that $m((x + \mathfrak{m}I) \otimes V) = \frac{xI^t + \mathfrak{m}R^t}{\mathfrak{m}R^t}$ equals $W$.
     By Nakayama's lemma: $I^t_{\mathfrak{m}} \simeq R^t_{\mathfrak{m}} \iff R_{\mathfrak{m}} \simeq I_{\mathfrak{m}}, \ldots$
  2. ...or, $\exists y \in I^t$ such that $U \otimes m(U \otimes (y + \mathfrak{m})I^t) = W$ implying $I^t_{\mathfrak{m}} \simeq R_{\mathfrak{m}} \iff I_{\mathfrak{m}} \simeq R^t_{\mathfrak{m}}$.

# Back to AVs: Categorical equivalence(s)

# Back to AVs: Categorical equivalence(s)

Fix a squarefree characteristic poly $h(x)$ of Frobenius $\pi$ over $\mathbb{F}_q$.
Put $K = \mathbb{Q}[x]/h = \mathbb{Q}[\pi]$. Let $\mathscr{I}_h$ be the corresponding isogeny class.

# Back to AVs: Categorical equivalence(s)

Fix a squarefree characteristic poly $h(x)$ of Frobenius $\pi$ over $\mathbb{F}_q$.
Put $K = \mathbb{Q}[x]/h = \mathbb{Q}[\pi]$. Let $\mathscr{I}_h$ be the corresponding isogeny class.

**Theorem**

*If $q = p$ is prime or that $\mathscr{I}_h$ is ordinary (coeff. of $x^g$ in $h(x)$ is $\not\equiv 0 \bmod p$)*

# Back to AVs: Categorical equivalence(s)

Fix a squarefree characteristic poly $h(x)$ of Frobenius $\pi$ over $\mathbb{F}_q$.
Put $K = \mathbb{Q}[x]/h = \mathbb{Q}[\pi]$. Let $\mathscr{I}_h$ be the corresponding isogeny class.

**Theorem**

*If $q = p$ is prime or that $\mathscr{I}_h$ is ordinary (coeff. of $x^g$ in $h(x)$ is $\not\equiv 0 \bmod p$) then there is an* **equivalence** *of categories*

$$\{\ \mathscr{I}_h \text{ with } \mathbb{F}_q\text{–morphisms}\ \}$$
$$\updownarrow$$
$$\{\text{fr. } \mathbb{Z}[\pi, q/\pi]\text{-ideals with linear morphisms}\}$$

# Back to AVs: Categorical equivalence(s)

Fix a squarefree characteristic poly $h(x)$ of Frobenius $\pi$ over $\mathbb{F}_q$.
Put $K = \mathbb{Q}[x]/h = \mathbb{Q}[\pi]$. Let $\mathscr{I}_h$ be the corresponding isogeny class.

### Theorem

*If $q = p$ is prime or that $\mathscr{I}_h$ is ordinary (coeff. of $x^g$ in $h(x)$ is $\not\equiv 0 \bmod p$) then there is an* **equivalence** *of categories*

$$\{\ \mathscr{I}_h \text{ with } \mathbb{F}_q\text{–morphisms}\ \}$$
$$\updownarrow$$
$$\{\text{fr. } \mathbb{Z}[\pi, q/\pi]\text{-ideals with linear morphisms}\}$$

*Moreover, if $A \mapsto I$ then $A^\vee \mapsto \overline{I}^t$, where $\bar{\cdot}$ is defined by $\overline{\pi} = q/\pi$ (the CM-involution).*

# Back to AVs: Categorical equivalence(s)

Fix a squarefree characteristic poly $h(x)$ of Frobenius $\pi$ over $\mathbb{F}_q$.
Put $K = \mathbb{Q}[x]/h = \mathbb{Q}[\pi]$. Let $\mathscr{I}_h$ be the corresponding isogeny class.

**Theorem**

*If $q = p$ is prime or that $\mathscr{I}_h$ is ordinary (coeff. of $x^g$ in $h(x)$ is $\not\equiv 0 \bmod p$) then there is an* **equivalence** *of categories*

$$\{\ \mathscr{I}_h \text{ with } \mathbb{F}_q\text{–morphisms}\ \}$$
$$\updownarrow$$
$$\{\text{fr. } \mathbb{Z}[\pi, q/\pi]\text{-ideals with linear morphisms}\}$$

*Moreover, if $A \mapsto I$ then $A^\vee \mapsto \overline{I}^t$, where $\bar{\cdot}$ is defined by $\overline{\pi} = q/\pi$ (the CM-involution).*

References: Deligne, Howe, Centeleghe-Stix, Bergström-Karemaker-M.

# AVs: Isomorphism classes

- We get a bijection

$$\{ \text{ isom. classes of AVs in } \mathscr{I}_h \} \longleftrightarrow \{\text{isom. classes of fr. } \mathbb{Z}[\pi, q/\pi]\text{-ideals} \}$$
$$:= \mathrm{ICM}(\mathbb{Z}[\pi, q/\pi]) \text{ ideal class monoid}$$

- If $\mathbb{Z}[\pi, q/\pi] = \mathscr{O}_K$ is the maximal order then $\mathrm{ICM}(\mathbb{Z}[\pi, q/\pi]) = \mathrm{Pic}(\mathscr{O}_K)$ is a product of class groups of number fields and we are good.
- Problem: $\mathbb{Z}[\pi, q/\pi]$ might not be a Dedekind ring $\rightsquigarrow$ non-invertible ideals.

# ICM : Ideal Class Monoid

Let $R$ be an **order** in an étale $\mathbb{Q}$-algebra $K$.

## ICM : Ideal Class Monoid

Let $R$ be an **order** in an étale $\mathbb{Q}$-algebra $K$.

- Recall: for **fractional** $R$**-ideals** $I$ and $J$

$$I \simeq_R J \Longleftrightarrow \exists x \in K^\times \text{ s.t. } xI = J.$$

# ICM : Ideal Class Monoid

Let $R$ be an **order** in an étale $\mathbb{Q}$-algebra $K$.

- Recall: for **fractional** $R$**-ideals** $I$ and $J$

$$I \simeq_R J \iff \exists x \in K^\times \text{ s.t. } xI = J.$$

- We have

$$\mathrm{ICM}(R) \supseteq \mathrm{Pic}(R) = {}^{\{\text{invertible fractional } R\text{-ideals}\}}\big/_{\simeq_R}$$

with equality ⇕ iff $R = \mathcal{O}_K$

# ICM : Ideal Class Monoid

Let $R$ be an **order** in an étale $\mathbb{Q}$-algebra $K$.

- Recall: for **fractional $R$-ideals** $I$ and $J$
$$I \simeq_R J \iff \exists x \in K^\times \text{ s.t. } xI = J.$$
- We have
$$\mathrm{ICM}(R) \supseteq \mathrm{Pic}(R) = {\{\text{invertible fractional } R\text{-ideals}\}}\big/{\simeq_R}$$
with equality $\updownarrow$ iff $R = \mathcal{O}_K$
- Simplify the problem by localizing: **weak equivalence** (Dade, Taussky, Zassenhaus '62)
$$I_\mathfrak{m} \simeq_{R_\mathfrak{m}} J_\mathfrak{m} \text{ for every } \mathfrak{m} \in \mathrm{mSpec}(R)$$

# ICM : Ideal Class Monoid

Let $R$ be an **order** in an étale $\mathbb{Q}$-algebra $K$.

- Recall: for **fractional $R$-ideals** $I$ and $J$

$$I \simeq_R J \iff \exists x \in K^\times \text{ s.t. } xI = J.$$

- We have

$$\mathrm{ICM}(R) \supseteq \mathrm{Pic}(R) = {}^{\{\text{invertible fractional } R\text{-ideals}\}}\!\big/_{\simeq_R}$$

with equality $\rightsquigarrow$ iff $R = \mathcal{O}_K$

- Simplify the problem by localizing: **weak equivalence** (Dade, Taussky, Zassenhaus '62)

$$I_\mathfrak{m} \simeq_{R_\mathfrak{m}} J_\mathfrak{m} \text{ for every } \mathfrak{m} \in \mathrm{mSpec}(R)$$

$$\Updownarrow$$

$$1 \in (I : J)(J : I)$$ easy to check!

# Compute ICM($R$)

Let $\mathscr{W}(R)$ be the set of weak eq. classes.

# Compute $\mathrm{ICM}(R)$

Let $\mathscr{W}(R)$ be the set of weak eq. classes. Partition w.r.t. the multiplicator ring:

$$\mathscr{W}(R) = \bigsqcup_{R \subseteq S \subseteq \mathscr{O}_K} \mathscr{W}_S(R)$$

$$\mathrm{ICM}(R) = \bigsqcup_{R \subseteq S \subseteq \mathscr{O}_K} \mathrm{ICM}_S(R)$$

# Compute $\mathrm{ICM}(R)$

Let $\mathscr{W}(R)$ be the set of weak eq. classes. Partition w.r.t. the multiplicator ring:

$$\mathscr{W}(R) = \bigsqcup_{R \subseteq S \subseteq \mathcal{O}_K} \mathscr{W}_S(R)$$

$$\mathrm{ICM}(R) = \bigsqcup_{R \subseteq S \subseteq \mathcal{O}_K} \mathrm{ICM}_S(R)$$

the "pedix" $-_S$ means "only classes with multiplicator ring S"

# Compute $\mathrm{ICM}(R)$

Let $\mathscr{W}(R)$ be the set of weak eq. classes. Partition w.r.t. the multiplicator ring:

$$\mathscr{W}(R) = \bigsqcup_{R\subseteq S\subseteq \mathscr{O}_K} \mathscr{W}_S(R)$$

$$\mathrm{ICM}(R) = \bigsqcup_{R\subseteq S\subseteq \mathscr{O}_K} \mathrm{ICM}_S(R)$$

the "pedix" $-_S$ means "only classes with multiplicator ring S"

Theorem (M.)

*For every over-order $S$ of $R$, $\mathrm{Pic}(S)$ acts freely on $\mathrm{ICM}_S(R)$ and*

$$\mathscr{W}_S(R) = \mathrm{ICM}_S(R)/\mathrm{Pic}(S).$$

# Compute $\mathrm{ICM}(R)$

Let $\mathscr{W}(R)$ be the set of weak eq. classes. Partition w.r.t. the multiplicator ring:

$$\mathscr{W}(R) = \bigsqcup_{R \subseteq S \subseteq \mathscr{O}_K} \mathscr{W}_S(R)$$

$$\mathrm{ICM}(R) = \bigsqcup_{R \subseteq S \subseteq \mathscr{O}_K} \mathrm{ICM}_S(R)$$

the "pedix" $-_S$ means "only classes with multiplicator ring S"

Theorem (M.)

*For every over-order $S$ of $R$, $\mathrm{Pic}(S)$ acts freely on $\mathrm{ICM}_S(R)$ and*

$$\mathscr{W}_S(R) = \mathrm{ICM}_S(R)/\mathrm{Pic}(S).$$

*Repeat for every $R \subseteq S \subseteq \mathscr{O}_K \rightsquigarrow \mathrm{ICM}(R)$.*

## Compute ICM($R$)

- To compute the overorders: see Hoffman-Sircana.

## Compute $\mathrm{ICM}(R)$

- To compute the overorders: see Hoffman-Sircana.
- To compute $\mathrm{Pic}(S)$: see Klüners-Pauli.

# Compute $\mathrm{ICM}(R)$

- To compute the overorders: see Hoffman-Sircana.
- To compute $\mathrm{Pic}(S)$: see Klüners-Pauli.
- To compute $W(R) = \sqcup W_S(R)$:

# Compute ICM($R$)

- To compute the overorders: see Hoffman-Sircana.
- To compute Pic($S$): see Klüners-Pauli.
- To compute $W(R) = \sqcup W_S(R)$:
- all representatives can be found in

$$\left\{ \text{sub-}R\text{-modules of } {}^{\mathcal{O}_K}\!\big/_{\mathfrak{f}_R} \right\} \quad \text{finite}$$

where $\mathfrak{f}_R = (R : \mathcal{O}_K)$ is the conductor of $R$.

# Compute $\mathrm{ICM}(R)$

- To compute the overorders: see Hoffman-Sircana.
- To compute $\mathrm{Pic}(S)$: see Klüners-Pauli.
- To compute $W(R) = \sqcup W_S(R)$:
- all representatives can be found in

$$\left\{ \text{sub-}R\text{-modules of } {}^{\mathcal{O}_K}\!/\!_{\mathfrak{f}_R} \right\} \quad \text{finite}$$

where $\mathfrak{f}_R = (R : \mathcal{O}_K)$ is the conductor of $R$.
- Can we use the type? Write $W_S(R) = \prod_{\mathfrak{m} \subset S} (W_S(R))_{\mathfrak{m}}$.

# Compute $\mathrm{ICM}(R)$

- To compute the overorders: see Hoffman-Sircana.
- To compute $\mathrm{Pic}(S)$: see Klüners-Pauli.
- To compute $W(R) = \sqcup W_S(R)$:
- all representatives can be found in

$$\left\{ \text{sub-}R\text{-modules of } {}^{\mathscr{O}_K}\!\big/_{\mathfrak{f}_R} \right\} \quad \textcolor{blue}{\text{finite}}$$

  where $\mathfrak{f}_R = (R : \mathscr{O}_K)$ is the conductor of $R$.
- Can we use the type? Write $W_S(R) = \prod_{\mathfrak{m} \subset S} (W_S(R))_{\mathfrak{m}}$.
- We have proven that:
  if the type of $S$ at $\mathfrak{m}$ is 1 then $(W_S(R))_{\mathfrak{m}} = \{[S_{\mathfrak{m}}]\}$, while
  if the type of $S$ at $\mathfrak{m}$ is 2 then $(W_S(R))_{\mathfrak{m}} = \{[S_{\mathfrak{m}}], [S^t_{\mathfrak{m}}]\}$

# AVs: Group of rational points

Theorem ( Springer-M. )

*$\mathscr{I}_h$ and $K = \mathbb{Q}[\pi] = \mathbb{Q}[x]/h$ as before.*

# AVs: Group of rational points

Theorem ( Springer-M. )

*$\mathscr{I}_h$ and $K = \mathbb{Q}[\pi] = \mathbb{Q}[x]/h$ as before.*
*Let $R$ be an order in $K$ and $\mathfrak{m}$ a maximal ideal of $R$ (possibly but not necessarily above $p$).*

# AVs: Group of rational points

**Theorem ( Springer-M. )**

*$\mathscr{I}_h$ and $K = \mathbb{Q}[\pi] = \mathbb{Q}[x]/h$ as before.*
*Let $R$ be an order in $K$ and $\mathfrak{m}$ a maximal ideal of $R$ (possibly but not necessarily above $p$). Assume:*

$$\mathrm{type}_{\mathfrak{m}}(R) \leq 2 \textit{ for every } \mathfrak{m} \supseteq (1-\pi)R.$$

# AVs: Group of rational points

**Theorem ( Springer-M. )**

*$\mathscr{I}_h$ and $K = \mathbb{Q}[\pi] = \mathbb{Q}[x]/h$ as before.*
*Let $R$ be an order in $K$ and $\mathfrak{m}$ a maximal ideal of $R$ (possibly but not necessarily above $p$). Assume:*

$$\mathrm{type}_{\mathfrak{m}}(R) \leq 2 \textit{ for every } \mathfrak{m} \supseteq (1-\pi)R.$$

*Then for every $A \in \mathscr{I}_h$ such that $\mathrm{End}(A) = R$ we have that $A(\mathbb{F}_q) = R/(1-\pi)R$.*

## AVs: Group of rational points

Theorem ( Springer-M. )

*$\mathscr{I}_h$ and $K = \mathbb{Q}[\pi] = \mathbb{Q}[x]/h$ as before.*
*Let $R$ be an order in $K$ and $\mathfrak{m}$ a maximal ideal of $R$ (possibly but not necessarily above $p$). Assume:*

$$\mathrm{type}_{\mathfrak{m}}(R) \leq 2 \text{ for every } \mathfrak{m} \supseteq (1-\pi)R.$$

*Then for every $A \in \mathscr{I}_h$ such that $\mathrm{End}(A) = R$ we have that $A(\mathbb{F}_q) = R/(1-\pi)R$.*

Proof: Say that $A \mapsto I$. Then $A(\mathbb{F}_q) = \ker(1-\pi_A) = \frac{I}{(1-\pi)I} =: M$.

# AVs: Group of rational points

**Theorem ( Springer-M. )**

*$\mathscr{I}_h$ and $K = \mathbb{Q}[\pi] = \mathbb{Q}[x]/h$ as before.
Let $R$ be an order in $K$ and $\mathfrak{m}$ a maximal ideal of $R$ (possibly but not necessarily above $p$). Assume:*

$$\mathrm{type}_{\mathfrak{m}}(R) \leq 2 \text{ for every } \mathfrak{m} \supseteq (1-\pi)R.$$

*Then for every $A \in \mathscr{I}_h$ such that $\mathrm{End}(A) = R$ we have that $A(\mathbb{F}_q) = R/(1-\pi)R$.*

Proof: Say that $A \mapsto I$. Then $A(\mathbb{F}_q) = \ker(1-\pi_A) = \frac{I}{(1-\pi)I} =: M$.
$M$ is finite: $M = \oplus_{\mathfrak{m}\supset(1-\pi)R} M_{\mathfrak{m}}$.

# AVs: Group of rational points

**Theorem (Springer-M.)**

*$\mathscr{I}_h$ and $K = \mathbb{Q}[\pi] = \mathbb{Q}[x]/h$ as before.*
*Let $R$ be an order in $K$ and $\mathfrak{m}$ a maximal ideal of $R$ (possibly but not necessarily above $p$). Assume:*

$$\mathrm{type}_{\mathfrak{m}}(R) \leq 2 \textit{ for every } \mathfrak{m} \supseteq (1-\pi)R.$$

*Then for every $A \in \mathscr{I}_h$ such that $\mathrm{End}(A) = R$ we have that $A(\mathbb{F}_q) = R/(1-\pi)R$.*

Proof: Say that $A \mapsto I$. Then $A(\mathbb{F}_q) = \ker(1-\pi_A) = \frac{I}{(1-\pi)I} =: M$.
$M$ is finite: $M = \oplus_{\mathfrak{m}\supset(1-\pi)R} M_{\mathfrak{m}}$.
If $I_{\mathfrak{m}} \simeq R_{\mathfrak{m}}$ then $M_{\mathfrak{m}} \simeq_R \frac{R_{\mathfrak{m}}}{(1-\pi)R_{\mathfrak{m}}}$.

# AVs: Group of rational points

**Theorem ( Springer-M. )**

*$\mathscr{I}_h$ and $K = \mathbb{Q}[\pi] = \mathbb{Q}[x]/h$ as before.*
*Let $R$ be an order in $K$ and $\mathfrak{m}$ a maximal ideal of $R$ (possibly but not necessarily above $p$). Assume:*

$$\mathrm{type}_{\mathfrak{m}}(R) \leq 2 \text{ for every } \mathfrak{m} \supseteq (1-\pi)R.$$

*Then for every $A \in \mathscr{I}_h$ such that $\mathrm{End}(A) = R$ we have that $A(\mathbb{F}_q) = R/(1-\pi)R$.*

Proof: Say that $A \mapsto I$. Then $A(\mathbb{F}_q) = \ker(1-\pi_A) = \frac{I}{(1-\pi)I} =: M$.
$M$ is finite: $M = \oplus_{\mathfrak{m} \supset (1-\pi)R} M_{\mathfrak{m}}$.
If $I_{\mathfrak{m}} \simeq R_{\mathfrak{m}}$ then $M_{\mathfrak{m}} \simeq_R \frac{R_{\mathfrak{m}}}{(1-\pi)R_{\mathfrak{m}}}$.
If $I_{\mathfrak{m}} \simeq R_{\mathfrak{m}}^t$ then $M_{\mathfrak{m}} \simeq_R \frac{R_{\mathfrak{m}}^t}{(1-\pi)R_{\mathfrak{m}}^t} \simeq_{\mathbb{Z}} \frac{R_{\mathfrak{m}}}{(1-\pi)R_{\mathfrak{m}}}$.

## AVs: self-duality

**Theorem ( Springer-M. )**

*$\mathscr{I}_h$ and $K = \mathbb{Q}[\pi] = \mathbb{Q}[x]/h$ as before.*

# AVs: self-duality

**Theorem ( Springer-M. )**

*$\mathscr{I}_h$ and $K = \mathbb{Q}[\pi] = \mathbb{Q}[x]/h$ as before.*
*Let $R$ be an order in $K$ and $\mathfrak{m}$ a maximal ideal of $R$.*

## AVs: self-duality

**Theorem ( Springer-M. )**

*$\mathscr{I}_h$ and $K = \mathbb{Q}[\pi] = \mathbb{Q}[x]/h$ as before.*
*Let $R$ be an order in $K$ and $\mathfrak{m}$ a maximal ideal of $R$. Assume:*

$$R = \overline{R}, \quad \mathfrak{m} = \overline{\mathfrak{m}}, \quad \textit{and} \quad \mathrm{type}_{\mathfrak{m}}(R) = 2.$$

## AVs: self-duality

**Theorem ( Springer-M. )**

*$\mathscr{I}_h$ and $K = \mathbb{Q}[\pi] = \mathbb{Q}[x]/h$ as before.*
*Let $R$ be an order in $K$ and $\mathfrak{m}$ a maximal ideal of $R$. Assume:*

$$R = \overline{R}, \quad \mathfrak{m} = \overline{\mathfrak{m}}, \quad \textit{and} \quad \mathrm{type}_{\mathfrak{m}}(R) = 2.$$

*Then for every $A \in \mathscr{I}_h$ such that $\mathrm{End}(A) = R$ we have that $A \not\simeq A^\vee$.*

## AVs: self-duality

**Theorem ( Springer-M. )**

*$\mathscr{I}_h$ and $K = \mathbb{Q}[\pi] = \mathbb{Q}[x]/h$ as before.*
*Let $R$ be an order in $K$ and $\mathfrak{m}$ a maximal ideal of $R$. Assume:*

$$R = \overline{R}, \quad \mathfrak{m} = \overline{\mathfrak{m}}, \quad \textit{and} \quad \mathrm{type}_{\mathfrak{m}}(R) = 2.$$

*Then for every $A \in \mathscr{I}_h$ such that $\mathrm{End}(A) = R$ we have that $A \not\simeq A^\vee$. In particular, such an $A$ cannot be principally polarized nor a Jacobian.*

# AVs: self-duality

**Theorem ( Springer-M. )**

*$\mathscr{I}_h$ and $K = \mathbb{Q}[\pi] = \mathbb{Q}[x]/h$ as before.*
*Let $R$ be an order in $K$ and $\mathfrak{m}$ a maximal ideal of $R$. Assume:*

$$R = \overline{R}, \quad \mathfrak{m} = \overline{\mathfrak{m}}, \quad \textit{and} \quad \mathrm{type}_{\mathfrak{m}}(R) = 2.$$

*Then for every $A \in \mathscr{I}_h$ such that $\mathrm{End}(A) = R$ we have that $A \not\simeq A^\vee$. In particular, such an $A$ cannot be principally polarized nor a Jacobian.*

Proof: Say that $A \mapsto I$. Hence $A^\vee \mapsto \overline{I}^t$.

# AVs: self-duality

**Theorem ( Springer-M. )**

*$\mathscr{I}_h$ and $K = \mathbb{Q}[\pi] = \mathbb{Q}[x]/h$ as before.*
*Let $R$ be an order in $K$ and $\mathfrak{m}$ a maximal ideal of $R$. Assume:*

$$R = \overline{R}, \quad \mathfrak{m} = \overline{\mathfrak{m}}, \quad \textit{and} \quad \mathrm{type}_{\mathfrak{m}}(R) = 2.$$

*Then for every $A \in \mathscr{I}_h$ such that $\mathrm{End}(A) = R$ we have that $A \not\simeq A^\vee$. In particular, such an $A$ cannot be principally polarized nor a Jacobian.*

Proof: Say that $A \mapsto I$. Hence $A^\vee \mapsto \overline{I}^t$.
By the Classification: either $I_{\mathfrak{m}} \simeq R_{\mathfrak{m}}$ or $I_{\mathfrak{m}} \simeq R^t_{\mathfrak{m}}$.

# AVs: self-duality

**Theorem ( Springer-M. )**

*$\mathscr{I}_h$ and $K = \mathbb{Q}[\pi] = \mathbb{Q}[x]/h$ as before.*
*Let $R$ be an order in $K$ and $\mathfrak{m}$ a maximal ideal of $R$. Assume:*

$$R = \overline{R}, \quad \mathfrak{m} = \overline{\mathfrak{m}}, \quad \textit{and} \quad \mathrm{type}_{\mathfrak{m}}(R) = 2.$$

*Then for every $A \in \mathscr{I}_h$ such that $\mathrm{End}(A) = R$ we have that $A \not\simeq A^\vee$. In particular, such an $A$ cannot be principally polarized nor a Jacobian.*

Proof: Say that $A \mapsto I$. Hence $A^\vee \mapsto \overline{I}^t$.
By the Classification: either $I_{\mathfrak{m}} \simeq R_{\mathfrak{m}}$ or $I_{\mathfrak{m}} \simeq R^t_{\mathfrak{m}}$.
In the first case: $\overline{I}^t_{\mathfrak{m}} = \overline{I}^t_{\overline{\mathfrak{m}}} \simeq R^t_{\mathfrak{m}} \not\simeq R_{\mathfrak{m}}$.

## AVs: self-duality

**Theorem ( Springer-M. )**

*$\mathscr{I}_h$ and $K = \mathbb{Q}[\pi] = \mathbb{Q}[x]/h$ as before.*
*Let $R$ be an order in $K$ and $\mathfrak{m}$ a maximal ideal of $R$. Assume:*

$$R = \overline{R}, \quad \mathfrak{m} = \overline{\mathfrak{m}}, \quad \textit{and} \quad \mathrm{type}_{\mathfrak{m}}(R) = 2.$$

*Then for every $A \in \mathscr{I}_h$ such that $\mathrm{End}(A) = R$ we have that $A \not\simeq A^\vee$. In particular, such an $A$ cannot be principally polarized nor a Jacobian.*

Proof: Say that $A \mapsto I$. Hence $A^\vee \mapsto \overline{I}^t$.
By the Classification: either $I_{\mathfrak{m}} \simeq R_{\mathfrak{m}}$ or $I_{\mathfrak{m}} \simeq R^t_{\mathfrak{m}}$.
In the first case: $\overline{I}^t_{\mathfrak{m}} = \overline{I}^t_{\overline{\mathfrak{m}}} \simeq R^t_{\mathfrak{m}} \not\simeq R_{\mathfrak{m}}$.
Similarly, in the second: $\overline{I}^t_{\mathfrak{m}} = \overline{I}^t_{\overline{\mathfrak{m}}} \simeq R_{\mathfrak{m}} \not\simeq R^t_{\mathfrak{m}}$.

# AVs: self-duality

**Theorem ( Springer-M. )**

*$\mathscr{I}_h$ and $K = \mathbb{Q}[\pi] = \mathbb{Q}[x]/h$ as before.*
*Let $R$ be an order in $K$ and $\mathfrak{m}$ a maximal ideal of $R$. Assume:*

$$R = \overline{R}, \quad \mathfrak{m} = \overline{\mathfrak{m}}, \quad \textit{and} \quad \mathrm{type}_{\mathfrak{m}}(R) = 2.$$

*Then for every $A \in \mathscr{I}_h$ such that $\mathrm{End}(A) = R$ we have that $A \not\simeq A^\vee$. In particular, such an $A$ cannot be principally polarized nor a Jacobian.*

Proof: Say that $A \mapsto I$. Hence $A^\vee \mapsto \overline{I}^t$.
By the Classification: either $I_\mathfrak{m} \simeq R_\mathfrak{m}$ or $I_\mathfrak{m} \simeq R^t_\mathfrak{m}$.
In the first case: $\overline{I}^t_\mathfrak{m} = \overline{I}^t_{\overline{\mathfrak{m}}} \simeq R^t_\mathfrak{m} \not\simeq R_\mathfrak{m}$.
Similarly, in the second: $\overline{I}^t_\mathfrak{m} = \overline{I}^t_{\overline{\mathfrak{m}}} \simeq R_\mathfrak{m} \not\simeq R^t_\mathfrak{m}$.
In both cases: $I \not\simeq \overline{I}^t \iff A \not\simeq A^\vee$.

# Some stats and refs

How often do the hypothesis of the previous theorem ($R = \overline{R}$, exists $\mathfrak{m} = \overline{\mathfrak{m}}$ with $\mathrm{type}_{\mathfrak{m}}(R) = 2$) do occur?
We computed the isomorphism classes of AVs$/\mathbb{F}_q$ (see LMFDB xyz) for 615.269 isogeny classes (for $1 \leq g \leq 5$ and various $q$).
We encountered

- 3.914.908 commutative endomorphism rings, of which:

# Some stats and refs

How often do the hypothesis of the previous theorem ($R = \overline{R}$, exists $\mathfrak{m} = \overline{\mathfrak{m}}$ with $\mathrm{type}_{\mathfrak{m}}(R) = 2$) do occur?
We computed the isomorphism classes of AVs/$\mathbb{F}_q$ (see LMFDB xyz) for 615.269 isogeny classes (for $1 \leq g \leq 5$ and various $q$).
We encountered

- 3.914.908 commutative endomorphism rings, of which:
- 72.6% satisfy $R = \overline{R}$;

## Some stats and refs

How often do the hypothesis of the previous theorem ($R = \overline{R}$, exists $\mathfrak{m} = \overline{\mathfrak{m}}$ with $\mathrm{type}_{\mathfrak{m}}(R) = 2$) do occur?
We computed the isomorphism classes of AVs/$\mathbb{F}_q$ (see LMFDB xyz) for 615.269 isogeny classes (for $1 \le g \le 5$ and various $q$).
We encountered

- 3.914.908 commutative endomorphism rings, of which:
- 72.6% satisfy $R = \overline{R}$;
- 10.3% satisfy $R = \overline{R}$ and are non-Gorenstein;

# Some stats and refs

How often do the hypothesis of the previous theorem ($R = \overline{R}$, exists $\mathfrak{m} = \overline{\mathfrak{m}}$ with $\mathrm{type}_{\mathfrak{m}}(R) = 2$) do occur?
We computed the isomorphism classes of AVs/$\mathbb{F}_q$ (see LMFDB xyz) for 615.269 isogeny classes (for $1 \leq g \leq 5$ and various $q$).
We encountered

- 3.914.908 commutative endomorphism rings, of which:
- 72.6% satisfy $R = \overline{R}$;
- 10.3% satisfy $R = \overline{R}$ and are non-Gorenstein;
- 7.4% satisfy $R = \overline{R}$, are non-Gorenstein and $\exists \mathfrak{m} = \overline{\mathfrak{m}}$ s.t. with $\mathrm{type}_{\mathfrak{m}}(R) = 2$.

Thank you!

# Thank you!

Main references:

- *Cohen-Macaulay type of orders, generators and ideal classes*
  `https://arxiv.org/abs/2206.03758`
- *Abelian varieties over finite fields and their groups of rational points*
  with Caleb Springer, to appear in Algebra&Number Theory
  `https://arxiv.org/abs/2211.15280`
- Magma package for étale $\mathbb{Q}$-algebras
  `https://github.com/stmar89/AlgEt` (also in Magma 2-28.1)