# Coincidences of an elliptic curve over a number field

Zoé Yvon

Aix-Marseille Université

July 4th, 2025

# Context: Inverse Galois problem

Let $F$ be a number field. We say that a (finite) group $G$ is *realizable as Galois group over $F$* if

$$G \simeq \mathrm{Gal}(L/F)$$

for some Galois extension $L/F$.

**Inverse Galois problem**

Which groups are realizable as Galois group over $F$?

**Theorem (Dirichlet, Hilbert)**

*Finite abelian groups, symmetric groups, alternating groups are realizable as Galois group over $\mathbb{Q}$.*

This talk: subgroups of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$, over a general number field.

# Torsion points of an elliptic curve

Let $m$ be a positive integer. Let $E/F$ be an elliptic curve defined over $F$.

**Definition (Group of $m$-torsion points)**

$$E[m] := \{P \in E(\overline{F}) \mid mP = \underbrace{P + \cdots + P}_{m \text{ times}} = \mathrm{O}\}.$$

**Proposition**

$$E[m] \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}, \quad \mathrm{Aut}(E[m]) \simeq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}).$$

**Definition ($m$-division field)**

$$F(E[m]) := F(\{x, y \mid (x, y) \in E[m]\})$$

# Galois representations of elliptic curves

For $(x_0, y_0) \in E[m]$ and $\sigma \in \mathrm{Gal}(\overline{F}/F)$, we have $(\sigma(x_0), \sigma(y_0)) \in E[m]$.

Hence $\mathrm{Gal}(\overline{F}/F) \circlearrowright E[m]$.

**Definition (Galois representations associated to $E/F$)**

$$\rho_{E,m} : \mathrm{Gal}(\overline{F}/F) \to \mathrm{Aut}(E[m]) \simeq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) \qquad \text{(mod } m\text{)}$$

$$\rho_{E,p^\infty} : \mathrm{Gal}(\overline{F}/F) \to \mathrm{Aut}(\varprojlim E[p^k]) \simeq \mathrm{GL}_2(\mathbb{Z}_p) \qquad (p\text{-adic, } p \text{ prime})$$

$$\rho_E : \mathrm{Gal}(\overline{F}/F) \to \mathrm{Aut}(\varprojlim E[m]) \simeq \mathrm{GL}_2(\hat{\mathbb{Z}}) \qquad \text{(adelic)}$$

$$\begin{array}{ccc} \mathrm{Gal}(\overline{F}/F)/\ker(\rho_{E,m}) & = & \mathrm{Gal}(\overline{F}/F)/\mathrm{Gal}(\overline{F}/F(E[m])) \\ \wr\| & & \wr\| \\ \mathrm{Im}(\rho_{E,m}) & \simeq & \mathrm{Gal}(F(E[m])/F) \end{array}$$

# Cyclotomic character

Let $(\zeta_m)$ be a compatible system of $m$-th roots of unity *i.e.* $\zeta_{km}^k = \zeta_m$.

For any $\sigma \in \mathrm{Gal}(\overline{F}/F)$, there is a unique $\chi_m(\sigma) \in (\mathbb{Z}/m\mathbb{Z})^*$ such that

$$\sigma(\zeta_m) = \zeta_m^{\chi_m(\sigma)}.$$

**Definition (cyclotomic character mod $m$)**

$$\chi_m : \mathrm{Gal}(\overline{F}/F) \to (\mathbb{Z}/m\mathbb{Z})^* \quad \sigma \mapsto \chi_m(\sigma).$$

$$\begin{array}{ccc} \mathrm{Gal}(\overline{F}/F)/\ker(\chi_m) & = & \mathrm{Gal}(\overline{F}/F)/\mathrm{Gal}(\overline{F}/F(\zeta_m)) \\ \wr\| & & \wr\| \\ \mathrm{Im}(\chi_m) & \simeq & \mathrm{Gal}(F(\zeta_m)/F) \end{array}$$

# Weil pairing

**Proposition**

$$\det \circ \rho_{E,m} = \chi_m$$

**Corollary**

$$\mathrm{Im}(\det \circ \rho_{E,m}) \simeq \mathrm{Gal}(F(\zeta_m)/F) \quad \textit{and} \quad F(\zeta_m) \subseteq F(E[m])$$

**Definition**

We say that $\mathrm{Im}(\rho_{E,m})$ is **maximal** if it is equal to the largest subgroup $G$ of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ such that $\det(G) = \mathrm{Im}(\chi_m)$.

# Some results

**Theorem (Serre's open image theorem, 1972)**

*If $E/F$ does not have complex multiplication (CM), then it has maximal $p$-adic images for almost all prime $p$.*

**Theorem (Jones and Zywina, 2010)**

*Almost all* elliptic curves over $F$ have maximal $p$-adic images for any $p$.*

**Theorem (Jones and Zywina, 2010)**

*For almost all elliptic curves $E/\mathbb{Q}$, $\mathrm{Im}(\rho_E)$ has index 2 in $\mathrm{GL}_2(\hat{\mathbb{Z}})$.*
*If $F \neq \mathbb{Q}$, then almost all elliptic curves over $F$ have maximal adelic image.*

# $\hat{\mathbb{Z}}$

$$\hat{\mathbb{Z}} \simeq \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_7 \times \mathbb{Z}_{11} \times \cdots$$

$$\begin{array}{cccccc}
\vdots & \vdots & \cdots & \cdots & \cdots & \cdots \\
\downarrow & \downarrow & & & & \\
\mathbb{Z}/2^4\mathbb{Z} & \mathbb{Z}/3^4\mathbb{Z} & \vdots & \cdots & \cdots & \cdots \\
\downarrow & \downarrow & \downarrow & & & \\
\mathbb{Z}/2^3\mathbb{Z} & \mathbb{Z}/3^3\mathbb{Z} & \mathbb{Z}/5^3\mathbb{Z} & \vdots & \cdots & \cdots \\
\downarrow & \downarrow & \downarrow & \downarrow & & \\
\mathbb{Z}/2^2\mathbb{Z} & \mathbb{Z}/3^2\mathbb{Z} & \mathbb{Z}/5^2\mathbb{Z} & \mathbb{Z}/7^2\mathbb{Z} & \vdots & \cdots \\
\downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\
\mathbb{Z}/2\mathbb{Z} & \mathbb{Z}/3\mathbb{Z} & \mathbb{Z}/5\mathbb{Z} & \mathbb{Z}/7\mathbb{Z} & \mathbb{Z}/11\mathbb{Z} & \cdots
\end{array}$$

# $\mathrm{GL}_2(\hat{\mathbb{Z}})$

$$
\begin{array}{ccccccccccc}
\mathrm{GL}_2(\hat{\mathbb{Z}}) \simeq & \mathrm{GL}_2(\mathbb{Z}_2) & \times & \mathrm{GL}_2(\mathbb{Z}_3) & \times & \mathrm{GL}_2(\mathbb{Z}_5) & \times & \mathrm{GL}_2(\mathbb{Z}_7) & \times & \mathrm{GL}_2(\mathbb{Z}_{11}) & \times \cdots \\
& \vdots & & \vdots & & \cdots & & \cdots & & \cdots & \cdots \\
& \twoheaddownarrow & & \twoheaddownarrow & & & & & & & \\
& \mathrm{GL}_2(\mathbb{Z}/2^4\mathbb{Z}) & & \mathrm{GL}_2(\mathbb{Z}/3^4\mathbb{Z}) & & \vdots & & \cdots & & \cdots & \cdots \\
& \twoheaddownarrow & & \twoheaddownarrow & & \twoheaddownarrow & & & & & \\
& \mathrm{GL}_2(\mathbb{Z}/2^3\mathbb{Z}) & & \mathrm{GL}_2(\mathbb{Z}/3^3\mathbb{Z}) & & \mathrm{GL}_2(\mathbb{Z}/5^3\mathbb{Z}) & & \vdots & & \cdots & \cdots \\
& \twoheaddownarrow & & \twoheaddownarrow & & \twoheaddownarrow & & \twoheaddownarrow & & & \\
& \mathrm{GL}_2(\mathbb{Z}/2^2\mathbb{Z}) & & \mathrm{GL}_2(\mathbb{Z}/3^2\mathbb{Z}) & & \mathrm{GL}_2(\mathbb{Z}/5^2\mathbb{Z}) & & \mathrm{GL}_2(\mathbb{Z}/7^2\mathbb{Z}) & & \vdots & \cdots \\
& \twoheaddownarrow & & \twoheaddownarrow & & \twoheaddownarrow & & \twoheaddownarrow & & \twoheaddownarrow & \\
& \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) & & \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}) & & \mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z}) & & \mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z}) & & \mathrm{GL}_2(\mathbb{Z}/11\mathbb{Z}) & \cdots
\end{array}
$$

# Entanglement

$$\mathrm{Im}(\rho_E) \hookrightarrow \mathrm{Im}(\rho_{E,2^\infty}) \times \mathrm{Im}(\rho_{E,3^\infty}) \times \mathrm{Im}(\rho_{E,5^\infty}) \times \mathrm{Im}(\rho_{E,7^\infty}) \times \mathrm{Im}(\rho_{E,11^\infty}) \times \cdots$$

$$\begin{array}{cccccc}
\vdots & \vdots & \cdots & \cdots & \cdots & \cdots \\
\downarrow & \downarrow & & & & \\
\mathrm{Im}(\rho_{E,2^4}) & \mathrm{Im}(\rho_{E,3^4}) & \vdots & \cdots & \cdots & \cdots \\
\downarrow & \downarrow & \downarrow & & & \\
\mathrm{Im}(\rho_{E,2^3}) & \mathrm{Im}(\rho_{E,3^3}) & \mathrm{Im}(\rho_{E,5^3}) & \vdots & \cdots & \cdots \\
\downarrow & \downarrow & \downarrow & \downarrow & & \\
\mathrm{Im}(\rho_{E,2^2}) & \mathrm{Im}(\rho_{E,3^2}) & \mathrm{Im}(\rho_{E,5^2}) & \mathrm{Im}(\rho_{E,7^2}) & \vdots & \cdots \\
\downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\
\mathrm{Im}(\rho_{E,2}) & \mathrm{Im}(\rho_{E,3}) & \mathrm{Im}(\rho_{E,5}) & \mathrm{Im}(\rho_{E,7}) & \mathrm{Im}(\rho_{E,11}) & \cdots
\end{array}$$

# Linearly disjoint extension

Two Galois extensions $L/F$ and $M/F$ are *linearly disjoint* if the injective morphism

$$\mathrm{Gal}(LM/F) \hookrightarrow \mathrm{Gal}(L/F) \times \mathrm{Gal}(M/F)$$

is an isomorphism, equivalently $L \cap M = F$.

The non-linear disjointness of the family $(F(E[p^\infty])/F)$ is the cause of the non-surjectivity of

$$\mathrm{Im}(\rho_E) \hookrightarrow \prod_{p \text{ prime}} \mathrm{Im}(\rho_{E,p^\infty}).$$

# Entanglement and Coincidence

## Definition

Let $m, n$ be coprime integers. We say that $E/F$ has **$(m,n)$-entanglement** if one of the following equivalent conditions hold

- $\mathrm{Im}(\rho_{E,mn}) \hookrightarrow \mathrm{Im}(\rho_{E,m}) \times \mathrm{Im}(\rho_{E,n})$ is not an isomorphism
- $\mathrm{Gal}(F(E[mn])/F) \hookrightarrow \mathrm{Gal}(F(E[m])/F) \times \mathrm{Gal}(F(E[n])/F)$ is not an isomorphism
- $\boldsymbol{F(E[m]) \cap F(E[n]) \neq F}$.

## Definition

Let $m, n$ be integers. We say that $E/F$ has an **$(m,n)$-coincidence** if $\boldsymbol{F(E[m]) = F(E[n])}$.

# Example

**Example: $E : y^3 = x^3 - 36x + 84$**

$$\mathrm{Im}(\rho_{E,6}) \underset{\text{index } 6}{\hookrightarrow} \mathrm{GL}_2(\mathbb{Z}/6\mathbb{Z}) \simeq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$$

$$\mathrm{Gal}(\mathbb{Q}(E[6])/\mathbb{Q}) \underset{\text{index } 6}{\hookrightarrow} \mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(E[3])/\mathbb{Q})$$

Thus $[\mathbb{Q}(E[6]) : \mathbb{Q}] = [\mathbb{Q}(E[3]) : \mathbb{Q}]$ and, since $\mathbb{Q}(E[6]) = \mathbb{Q}(E[2])\mathbb{Q}(E[3])$, we have

$$\mathbb{Q}(E[3]) = \mathbb{Q}(E[6]) \quad \textit{i.e.} \quad \mathbb{Q}(E[2]) \cap \mathbb{Q}(E[3]) = \mathbb{Q}(E[2]) \neq \mathbb{Q}.$$

Thus $E/F$ has a $(2,3)$-entanglement and a $(3,6)$-coincidence.

# Over $\mathbb{Q}$

Brau&Jones (2016), Daniels&Lozano-Robledo&Morrow (2021): classified $(2,3)$, $(2,4)$ and $(3,6)$-coincidence.
It is expected that these are the only possible coincidences over $\mathbb{Q}$.

# Over a general number field: aim of my thesis

If $F(E[n]) = F(E[m])$ then $F(\zeta_n) \subseteq F(E[m])$.

1. They do not require any assumption on the ground field,
2. There is no distinction between CM and non-CM case.

# Maximal image

If $F(\zeta_n) \subseteq F(E[m])$ then $F(\zeta_n) \subseteq F(E[m]) \cap F^{\mathrm{ab}}$. We have

$$\mathrm{Gal}(F(\zeta_m)/F) \simeq \det(\mathrm{Im}(\rho_{E,m})) \simeq \mathrm{Im}(\rho_{E,m})/(\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z}) \cap \mathrm{Im}(\rho_{E,m}))$$

and

$$\mathrm{Gal}(F(E[m]) \cap F^{\mathrm{ab}}/F) \simeq \mathrm{Im}(\rho_{E,m})/D(\mathrm{Im}(\rho_{E,m})).$$

$\rightarrow$ study of the **derived group** $D(\mathrm{Im}(\rho_{E,m}))$.

**Theorem (Y., 2025)**

*Suppose that $72 \mid m$ and $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z}) \leq \mathrm{Im}(\rho_{E,m})$. Then*

$$F(E[m]) \cap F^{\mathrm{ab}} = F(\zeta_m).$$

*In particular, if $E/F$ has an $(m,n)$-coincidence, then $F(\zeta_n) \subseteq F(\zeta_m)$.*

# Prime divisors

Let $\mathfrak{f}_E$ be the conductor ideal of $E$, and $\mathrm{N}(\mathfrak{f}_E)$ be its norm.

**Theorem (Y., 2024)**

*If $F(\zeta_n) \subseteq F(E[m])$ then, for all primes $p$ such that $v_p(m) < v_p(n)$:*

$$p \mid 2 \cdot \Delta_F \cdot \mathrm{N}(\mathfrak{f}_E).$$

If $p \mid m, n$: other part of my thesis.

If $p \mid n$ and $p \nmid m$, ramification considerations: we must have, for $\mathfrak{p} \mid p$,

$$e_{\mathfrak{p}}(F(\zeta_{p^{v_p(n)}})/F) \mid e_{\mathfrak{p}}(F(E[m])/F).$$

# Ramification tables

| Sufficient condition on $E/F$ | $t = e_{\mathfrak{p}}(F(E[m])/F)$ |
|---|---|
| good red. at $\mathfrak{p}$ | $t = 1$ |
| mult. red. at $\mathfrak{p}$ with $p$ odd<br>split mult. red. at $\mathfrak{p}$ with $p = 2$<br>add. red. at $\mathfrak{p}$, $p > 3$<br>add., no pot. good red. at $\mathfrak{p}$ with $p = 3$ | $v_p(t) = 0$ |
| (non split) mult. red. at $\mathfrak{p}$ with $p = 2$<br>add., pot. good red. at $\mathfrak{p}$ with $p = 3$ | $v_p(t) \leq 1$ |
| add. red. at $\mathfrak{p}$ with $p = 2$ | $v_p(t) \leq 3$ |

| $s = e_{\mathfrak{p}}(F(\zeta_{p^k})/F)$ | Necessary condition on $e_{\mathfrak{p}}(F/\mathbb{Q})$ |
|---|---|
| $s = 1$ | $\varphi(p^k) \mid e_{\mathfrak{p}}(F/\mathbb{Q})$ |
| $v_p(s) = 0$ | $v_p(e_{\mathfrak{p}}(F/\mathbb{Q})) \geq k - 1$ |
| $v_p(s) \leq 1$ | $v_p(e_{\mathfrak{p}}(F/\mathbb{Q})) \geq k - 2$ |
| $v_p(s) \leq 3$ | $v_p(e_{\mathfrak{p}}(F/\mathbb{Q})) \geq k - 4$ |

**Theorem (Campagna-Stevenhagen, 2022)**

*Suppose $E/F$ is non-CM and $S$ is the set of primes $p$ dividing $2 \cdot 3 \cdot 5 \cdot \Delta_F \cdot \mathrm{N}(\mathfrak{f}_E)$, then $(F(E[p^\infty]))_{p \notin S}$ is linearly disjoint over $F$.*

**Corollary**

*Suppose $E/F$ is non-CM and has an $(m, n)$-coincidence. If $p \mid m$ and $p \nmid n$ then $p \mid 2 \cdot 3 \cdot 5 \cdot \Delta_F \cdot \mathrm{N}(\mathfrak{f}_E)$.*

**Theorem (Y., 2024)**

*If $F(E[m]) = F(E[n])$ then, for all primes $p$ such that $v_p(m) \neq v_p(n)$:*

$$p \mid 2 \cdot \Delta_F \cdot \mathrm{N}(\mathfrak{f}_E).$$

## Theorem (Campagna-Stevenhagen, 2022)

*Suppose $E/F$ is non-CM and $S$ is the set of primes $p$ dividing $2 \cdot 3 \cdot 5 \cdot \Delta_F \cdot \mathrm{N}(\mathfrak{f}_E)$, then $(F(E[p^\infty]))_{p \notin S}$ is linearly disjoint over $F$.*

## Corollary

*Suppose $E/F$ is non-CM and has an $(m, n)$-coincidence. If $p \mid m$ and $p \nmid n$ then $p \mid 2 \cdot 3 \cdot 5 \cdot \Delta_F \cdot \mathrm{N}(\mathfrak{f}_E)$.*

## Theorem (Y., 2024)

*If $F(E[m]) = F(E'[n])$ then, for all primes $p$ such that $v_p(m) \neq v_p(n)$:*

$$p \mid 2 \cdot \Delta_F \cdot \mathrm{N}(\mathfrak{f}_E) \cdot \mathrm{N}(\mathfrak{f}_{E'}).$$

# Generalisations to abelian varieties

We can state analogous results replacing $E/F$ by a principally polarized abelian variety $A/F$: there are relations between the ramification of $F(A[m])/F$ and the reduction type of $A$ at $p \nmid m$, and we also have $F(\zeta_m) \subseteq F(A[m])$.

# The end

Thank you everyone !

Merci à tous !