ENS DE LYON

Entanglement in the family of division fields of a CM elliptic curve

Riccardo Pengo (based on joint work with Francesco Campagna)

- arXiv:2006.00883
- Unité des mathématiques pures et appliquées, École normale supérieure de Lyon
- riccardo.pengo@ens-lyon.fr, riccardopengo@gmail.com
- https://sites.google.com/view/riccardopengo/

French-Korean International Research Laboratory in Mathematics
Webinar in Number theory, 17 May 2021

The plan

The plan

Basic definitions

Fix a number field F with algebraic closure $\overline{F}$, and let $\mathscr{F} = \{F_s\}_{s \in S}$ be a family of Galois extensions $F \subseteq F_s \subseteq \overline{F}$.

- $\mathscr{F}$ is **linearly disjoint** (over F) if the map:

$$\iota_{\mathscr{F}} \colon \mathrm{Gal}\left(\prod_{s \in S} F_s \middle/ F \right) \hookrightarrow \prod_{s \in S} \mathrm{Gal}(F_s/F)$$

is an isomorphism;

- **Lenstra (2006):** $\mathscr{F}$ is **entangled** (over F), otherwise.

Problem: Study the **entanglement** in the family $\mathscr{F}$.

Radical families

Artin (1927), Lehmer & Lehmer (1957): For any number field F, any $a \in F^\times$ and $N \in \mathbb{N}$, set:

$$F_N^{(a)} := F(\zeta_N, \sqrt[N]{a})$$ splitting field of $x^N - a$

and study the entanglement of $\mathscr{F}^{(a)} := \{F_p^{(a)}\}_{p \in \mathscr{P}}$ (connected to **Artin's primitive root conjecture**).

Some entanglement: Suppose $F = \mathbb{Q}$. For any $a \in \mathbb{Q}^\times$, one has:

$$F_2^{(a)} \subseteq \prod_{p \mid \Delta_{\mathbb{Q}(\sqrt{a})}} F_p^{(a)}$$

and in particular we have entanglement if $\Delta_{\mathbb{Q}(\sqrt{a})}$ is odd.

Cyclotomic fields: The family $\mathscr{F}_{\mathbb{G}_m} = \{\mathbb{Q}(\zeta_{p^\infty})\}_{p \in \mathscr{P}}$, where:

$$\mathbb{Q}(\zeta_{p^\infty}) := \varinjlim_{n \in \mathbb{N}} \mathbb{Q}(\zeta_{p^n})$$

is linearly disjoint over $\mathbb{Q}$, as follows from **ramification theory**.

Division fields

Fix a number field F, an elliptic curve $E_{/F}$ and an ideal $I \subseteq \mathrm{End}_{\overline{F}}(E)$. Then, define:

$$E[I] := \bigcap_{\alpha \in I} \ker(E(\overline{F}) \xrightarrow{[\alpha]} E(\overline{F})) \qquad E_{\mathrm{tors}} := E(\overline{F})_{\mathrm{tors}}$$

$$E[I^\infty] := \varinjlim_{n \in \mathbb{N}} E[I^n] \qquad \mathscr{F}_E := \{F(E[p^\infty])\}_{p \in \mathscr{P}}$$

Serre (1971): If $\mathrm{End}_{\overline{F}}(E) \cong \mathbb{Z}$, there exists a finite set $S \subseteq \mathscr{P}$ such that $\mathscr{F}_E \setminus \{F(E[p^\infty])\}_{p \in S}$ is linearly disjoint.

Campagna & Stevenhagen (2018), **Lombardo & Tronto** (2019)**:** S can be taken to be any set of primes containing the divisors of $B_E := 2 \cdot 3 \cdot 5 \cdot \Delta_F \cdot \mathrm{N}_{F/\mathbb{Q}}(\mathfrak{f}_E)$ and those $p \in \mathscr{P}$ for which $F(E[p])$ is not **maximal**.

Brau & Jones (2016), Morrow (2019), Daniels & Lozano-Robledo (2019), Jones & McMurdy (2020), Daniels & Morrow (2020), Daniels & Lozano-Robledo & Morrow (2021): One can classify the entanglement in the family $\mathscr{F}_E$ by determining the F-rational points of certain modular curves of composite level.

Galois representations

Fix a number field F, an elliptic curve $E_{/F}$ and an ideal $I \subseteq \mathrm{End}_F(E)$. Then, considering the diagram:

$$\begin{array}{ccc} & \xrightarrow{\rho_E} & \mathrm{Aut}_{\mathbb{Z}}(E_{\mathrm{tors}}) \cong \mathrm{GL}_2(\widehat{\mathbb{Z}}) \\ & & \downarrow\!\!\downarrow \\ G_F := \mathrm{Gal}(\overline{F}/F) & \xrightarrow{\rho_{E,I^\infty}} & \mathrm{Aut}_{\mathbb{Z}}(E[I^\infty]) \\ & & \downarrow\!\!\downarrow \\ & \xrightarrow{\rho_{E,I}} & \mathrm{Aut}_{\mathbb{Z}}(E[I]) \end{array}$$

the extension $F \subseteq F(E[I])$ is said to be **maximal** if $\rho_{E,I}$ is surjective.

Serre (1971): If $\mathrm{End}_{\overline{F}}(E) \cong \mathbb{Z}$, the image of ρ_E has finite index in $\mathrm{Aut}_{\mathbb{Z}}(E_{\mathrm{tors}}) \cong \mathrm{GL}_2(\widehat{\mathbb{Z}})$. In particular, the extension $F \subseteq F(E[p])$ is maximal for all but finitely many $p \in \mathscr{P}$.

The plan

Complex multiplication

Fix a number field F and an elliptic curve $E_{/F}$. Then:

- **Shimura (1998):** If $\mathrm{End}_F(E) \not\cong \mathbb{Z}$ then $\mathrm{End}_F(E) \cong \mathcal{O} \subseteq K \subseteq F$;
- **Bourdon & Clark (2020):** If $\mathrm{End}_F(E) \cong \mathcal{O}$ and $I \subseteq \mathcal{O}$ is invertible, $E[I]$ is a free $\mathcal{O}/I$-module of rank one;
- **Serre (1971):** If $\mathrm{End}_F(E) \cong \mathcal{O}$, the image of ρ_E has finite index inside $\mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tors}}) \cong \widehat{\mathcal{O}}^\times \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}}) \cong \mathrm{Aut}_{\mathbb{Z}}(E_{\mathrm{tors}})$. In particular, there exists a finite set $S \subseteq \mathscr{P}$ such that the family

$$\mathscr{F}_{E,S} := \{F(E[p^\infty])\}_{p \in \mathscr{P} \setminus S}$$

is linearly disjoint over F.

- For any invertible ideal $I \subseteq \mathcal{O}$, the extension $F \subseteq F(E[I])$ is said to be **maximal** if $\rho_{E,I}(G_F) = \mathrm{Aut}_{\mathcal{O}}(E[I]) \cong (\mathcal{O}/I)^\times$.

ENS DE LYON

Effective linear disjointness

Fix a number field F and an elliptic curve $E_{/F}$.

Campagna & P. (2020):

If $\mathrm{End}_F(E) \cong \mathscr{O} \subseteq K \subseteq F$, and $S \subseteq \mathscr{P}$ is any set containing the prime divisors of

$$\boxed{B_E := \mathfrak{f}_{\mathscr{O}} \cdot \Delta_F \cdot \mathrm{N}_{F/\mathbb{Q}}(\mathfrak{f}_E)}$$

the family $\mathscr{F}_{E,S}$ is linearly disjoint over F.

Sketch of proof: We use ramification theory, as follows:

1. the extension $F \subseteq F(E[I])$ is unramified outside $(I \cdot \mathscr{O}_F) \cdot \mathfrak{f}_E$, for every ideal $I \subseteq \mathscr{O}$ coprime to $\mathfrak{f}_{\mathscr{O}}$;
2. the extension $F \subseteq F(E[\mathfrak{p}^n])$ is maximal and totally ramified at each prime dividing $\mathfrak{p} \cdot \mathscr{O}_F$, for every prime ideal $\mathfrak{p} \nmid B_E \cdot \mathscr{O}$ and every $n \in \mathbb{N}$. A different proof is provided by **Lozano-Robledo (2018)**;
3. every sub-extension of $F \subseteq F(E[p^n])$ ramifies at some prime dividing $p \cdot \mathscr{O}_F$, for every rational prime $p \nmid B_E$ and every $n \in \mathbb{Z}_{\geq 1}$.

The plan

$F^{ab} \supseteq F(E_{tors}) \supseteq F \cdot K^{ab}$

Two natural problems

Fix a number field F and an elliptic curve $E_{/F}$. We have two related problems:

- find the smallest sets $S \subseteq \mathscr{P}$ such that the family $\mathscr{F}_{E,S} := \{F(E[p^\infty])\}_{p \in \mathscr{P} \setminus S}$ is **linearly disjoint**;
- find the smallest sets $S' \subseteq \mathscr{P}$ such that $F \subseteq F(E[p^n])$ is **maximal** for every $p \in \mathscr{P} \setminus S'$ and $n \in \mathbb{N}$.

Suppose now that $\mathrm{End}_F(E) \cong \mathscr{O} \subseteq K \subseteq F$ and $F = H_{\mathscr{O}} := K(j(E))$ is the **ring class field** of $\mathscr{O}$.

Campagna & P. (2020): If $H_{\mathscr{O}}(E_{\mathrm{tors}}) \neq K^{\mathrm{ab}}$, then $\mathrm{Pic}(\mathscr{O}) \neq \{1\}$ and:

- the family $\mathscr{F}_E = \mathscr{F}_{E,\emptyset}$ is **linearly disjoint**;
- the extension $F \subseteq F(E[p^n])$ is **maximal**, for every $p \in \mathscr{P}$ and $n \in \mathbb{N}$.

Moreover, if $\mathrm{Pic}(\mathscr{O}) \neq \{1\}$ there exist **infinitely many** elliptic curves $E_{/H_{\mathscr{O}}}$ such that $H_{\mathscr{O}}(E_{\mathrm{tors}}) \neq K^{\mathrm{ab}}$.

Sketch of proof: We divide it in two steps:

- if $F \subseteq F(E[N])$ is not maximal for some $N > 3$, then we show that $H_{\mathscr{O}}(E_{\mathrm{tors}}) = K^{\mathrm{ab}}$;
- we use the existence of infinitely many quadratic extensions of $H_{\mathscr{O}}$ which are not abelian over K, to construct the elliptic curves $E_{/H_{\mathscr{O}}}$ by twisting a given one.

$K \subseteq H_{\mathcal{O}} \subseteq H_{I,\mathcal{O}}$

Ray class fields for orders

Fix a number field K, an order $\mathcal{O} \subseteq K$ and a non-zero ideal $I \subseteq \mathcal{O}$. Let $\mathcal{O}_p := \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ for any $p \in \mathscr{P}$.

Söhngen (1935), Stevenhagen (2001), Lv & Deng (2015), Yi & Lv (2018), Campagna & P. (2020): The **ray class field** of K modulo $(I, \mathcal{O})$ is the abelian extension $K \subseteq H_{I,\mathcal{O}} := (K^{\mathrm{ab}})^{[U_{I,\mathcal{O}}, K]}$, where:

$$U_{I,\mathcal{O}} := \prod_{p \in \mathscr{P}} (\mathcal{O}_p^\times \cap (1 + I \cdot \mathcal{O}_p)) \subseteq \prod_{p \in \mathscr{P}}{}' (K \otimes_{\mathbb{Q}} \mathbb{Q}_p)^\times = (\mathbb{A}_{\mathbb{Q}} \otimes_{\mathbb{Q}} K)^\times \cong \mathbb{A}_K^\times$$

and $[\cdot, K] \colon \mathbb{A}_K^\times \twoheadrightarrow G_K^{\mathrm{ab}}$ is the Artin map. In particular, $H_{\mathcal{O}} := H_{1,\mathcal{O}}$ is the **ring class field** of $\mathcal{O}$.

Yi & Lv (2018), Campagna & P. (2020, ≥ 2021): We have the isomorphisms:

$$\boxed{\mathrm{Gal}(H_{I,\mathcal{O}}/K) \cong \frac{\mathbb{A}_K^\times}{K^\times \cdot U_{I,\mathcal{O}}} \cong \frac{\mathscr{I}_{I,\mathcal{O}}}{\mathscr{P}_{I,\mathcal{O}}}} \Rightarrow \boxed{\mathrm{Gal}(H_{\mathcal{O}}/K) \cong \mathrm{Pic}(\mathcal{O})} \quad \text{and} \quad \boxed{\mathrm{Gal}(H_{I,\mathcal{O}}/H_{\mathcal{O}}) \cong \frac{(\mathcal{O}/I)^\times}{\pi_I(\mathcal{O}^\times)}}$$

where $\pi_I \colon \mathcal{O} \twoheadrightarrow \mathcal{O}/I$ is the canonical quotient map, $\mathscr{I}_{I,\mathcal{O}}$ is the group of invertible ideals $\mathfrak{a} \subseteq \mathcal{O}$ such that $\mathfrak{a} + I = \mathcal{O}$, and $\mathscr{P}_{I,\mathcal{O}} \subseteq \mathscr{I}_{I,\mathcal{O}}$ is the "ray" of principal ideals generated by those $\alpha \in \mathcal{O}$ such that $\pi_I(\alpha) = 1$.

Minimality of division fields

Fix a number field F and an elliptic curve $E_{/F}$. **Weil's pairing** gives the "lower bound" $F \cdot \mathbb{Q}(\zeta_N) \subseteq F(E[N])$.

Söhngen (1935), Stevenhagen (2001), Campagna & P. (2020):

If $\mathrm{End}_F(E) \cong \mathscr{O} \subseteq K \subseteq F$, and $I \subseteq \mathscr{O}$ is invertible, then we have the "lower bound":

$$\boxed{F \cdot H_{I,\mathscr{O}} \subseteq F(E[I])}$$

where $K \subseteq H_{I,\mathscr{O}}$ is the ray class field of K modulo $(I, \mathscr{O})$.

Sketch of proof: Use the **adelic description** of the abelian extension $K \subseteq H_{I,\mathscr{O}}$, together with a general result of **Shimura (1971)**, which follows from the **main theorem of complex multiplication**.

Coates & Wiles (1977), Kuhman (1978), Campagna & P. (2020): If $F(E_{\mathrm{tors}}) = F \cdot K^{\mathrm{ab}}$, then:

$$\boxed{F \cdot H_{I,\mathscr{O}} = F(E[I])}$$

for every invertible ideal $I \subseteq \mathfrak{f}_\varphi \cap \mathscr{O}$, where $\varphi \colon \mathbb{A}_K^\times \to \mathbb{C}^\times$ is any Hecke character factorising $\psi_E \colon \mathbb{A}_F^\times \to \mathbb{C}^\times$ via the norm map $\mathrm{N}_{F/K} \colon \mathbb{A}_F^\times \to \mathbb{A}_K^\times$. In particular, if $\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{f}_\varphi \cap \mathscr{O})$ has at least two prime divisors, the family $\mathscr{F}_E$ is **entangled** over F.

Indices of Galois representations

Fix a number field F and an elliptic curve $E_{/F}$, such that $\mathrm{End}_F(E) \cong \mathcal{O} \subseteq K \subseteq F$.

Lombardo (2017), Bourdon & Clark (2020), Campagna & P. (≥ 2021): We have:

$$\left|\mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tors}}) : \rho_E(G_F)\right| = \frac{[F \cap K^{\mathrm{ab}} : H_{\mathcal{O}}] \cdot |\mathcal{O}^\times|}{[F(E_{\mathrm{tors}}) : F \cdot K^{\mathrm{ab}}]} \leq [F \cap K^{\mathrm{ab}} : H_{\mathcal{O}}] \cdot |\mathcal{O}^\times|$$

and in particular $\left|\mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tors}}) : \rho_E(G_F)\right| = [F \cap K^{\mathrm{ab}} : H_{\mathcal{O}}] \cdot |\mathcal{O}^\times|$ if $F(E_{\mathrm{tors}}) = F \cdot K^{\mathrm{ab}}$.

Shimura (1971), Robert (1983), Gurney (2019), Campagna & P. (2020): If $K \neq \mathbb{Q}(i)$, there exist infinitely many elliptic curves $\boxed{E_{/H_{\mathcal{O}}}}$ such that $H_{\mathcal{O}}(E_{\mathrm{tors}}) = K^{\mathrm{ab}}$.

Sketch of proof: Start from E_0 such that $H_{\mathcal{O}}((E_0)_{\mathrm{tors}}) \neq K^{\mathrm{ab}}$, and twist it. More precisely:

- there exist infinitely many primes $p \in \mathcal{P}$ which split as $p \cdot \mathcal{O} = \mathfrak{p} \cdot \overline{\mathfrak{p}}$ and are inert in $\mathbb{Q}(i)$;
- if $p \nmid \mathrm{N}_{H_{\mathcal{O}}/\mathbb{Q}}(\mathfrak{f}_{E_0})$ then $H_{\mathcal{O}}(E_0[\mathfrak{p}]) = H_{\mathfrak{p},\mathcal{O}}(\sqrt{\alpha_{\mathfrak{p}}})$ for some $\alpha_{\mathfrak{p}} \in H_{\mathcal{O}}$ which is not a square;
- we set $E_{\mathfrak{p}} := E_0^{(\alpha_{\mathfrak{p}})}$. All these curves are twists of E_0, but pairwise non-isomorphic over $H_{\mathcal{O}}$.

The plan

Deuring's formula and twisting

Fix an elliptic curve $E_{/\mathbb{Q}}$ such that $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \cong \mathcal{O} \subseteq K$. Note that $K \subseteq \mathbb{Q}(E[I])$ if $|\mathcal{O}/I| > 2$.
Let $\psi_E \colon \mathbb{A}_K^\times \to \mathbb{C}^\times$ be the Hecke character associated to $E_{/K}$.

Deuring (~1955), Milne (1972): $\mathfrak{f}_E = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{f}_{\psi_E}) \cdot \Delta_K$.

Fix $p \in \mathscr{P}$ and $n \in \mathbb{N}$. We consider the maximality of the division fields $K(E^{(\alpha)}[p^n])$, for $\alpha \in \mathbb{Q}^\times$.

Campagna & P. (2020): If $\Delta_{\mathcal{O}} < -4$, we can reduce to the following cases:

- if $\alpha = (-1)^{(q-1)/2} q$ for some odd $q \in \mathscr{P}$ such that $q \nmid p \cdot \mathfrak{f}_E$, the field $K(E^{(\alpha)}[p^n])$ is always maximal;
- if $\alpha \in \{-2,-1,2\}$ and $2 \nmid p \cdot \mathfrak{f}_E$, the field $K(E^{(\alpha)}[p^n])$ is always maximal;
- if $\alpha = (-1)^{(p-1)/2} p$ and $p \geq 3$, then $K(E^{(\alpha)}[p^n])$ is maximal $\Leftrightarrow$ $K(E[p^n])$ is maximal;
- if $\alpha \in \{-2,-1,2\}$ and $p^n = 2^n \geq |\alpha|$, then $K(E^{(\alpha)}[2^n])$ is maximal $\Leftrightarrow$ $K(E[2^n])$ is maximal.

Sketch of proof: Use Deuring's formula, and general facts about twisting of Galois representations.

Entanglements over the rationals

Fix an imaginary quadratic field K and an order $\mathscr{O} \subseteq K$ such that $\mathrm{Pic}(\mathscr{O}) = \{1\}$ and $\Delta_{\mathscr{O}} < -4$.
Let $p \in \mathscr{P}$ be the unique prime ramifying in $\mathbb{Q} \subseteq K$.
Label all the elliptic curves over $\mathbb{Q}$ which have CM by $\mathscr{O}$ as $\{A_r\}_{r=1}^{+\infty}$, in such a way that $|\mathfrak{f}_{A_r}| \leq |\mathfrak{f}_{A_{r+1}}|$.

Campagna & P. (2020): Let $r_0 := 4$ if $\mathscr{O} \in \{\mathbb{Z}[2i], \mathbb{Z}[\sqrt{-2}]\}$, and $r_0 := 2$ otherwise. Then:

$r \leq r_0$ the family $\mathscr{F}_{A_r}$ is linearly disjoint over K. Moreover:

- the division fields $K(A_r[q^n])$ are maximal if $q \neq p$;
- the division fields $K(A_r[p^n])$ are minimal, if $n \geq r_0 - 1$.

$r > r_0$ we have $A_r = A_{r'}^{(\Delta_r)}$, for a unique $r' \leq r_0$ and a unique discriminant $\Delta_r \in \mathbb{Z}$ such that $p \nmid \Delta_r$.
Moreover, the family $\mathscr{F}_{A_r,S}$ is linearly disjoint over K, for every $S \subseteq \mathscr{P}$ containing each $q \mid p \cdot \Delta_r$.
Finally, we have that:

- the division fields $K(A_r[q^n])$ are maximal, for every $q \in \mathscr{P}$ and $n \in \mathbb{N}$;
- if $n \geq r_0 - 1$, then $K(A_r[p^n]) = H_{p^n,\mathscr{O}}(\sqrt{\Delta_r})$ and $K(A_r[p^n]) \cap K(A_r[\Delta_r]) = K(\sqrt{\Delta_r})$.

ENS DE LYON

Thank you very much for your attention!

고생 끝에 낙이 온다

« À la fin des épreuves vient le bonheur »