Kummer Theory for Elliptic Curves

Sebastiano Tronto

joint work with Davide Lombardo

2020-02-06

UNIVERSITÉ DU LUXEMBOURG

Let K be a number field; let $\alpha \in K^\times$ not a root of unity.

UNIVERSITÉ DU LUXEMBOURG

Kummer Theory

Let K be a number field; let $\alpha \in K^\times$ not a root of unity.

- Consider the splitting field L of $X^n - \alpha$

Let K be a number field; let $\alpha \in K^\times$ not a root of unity.

- Consider the splitting field L of $X^n - \alpha$
- L contains the n-th cyclotomic extension $K(\zeta_n)$

UNIVERSITÉ DU LUXEMBOURG

Let K be a number field; let $\alpha \in K^\times$ not a root of unity.

- Consider the splitting field L of $X^n - \alpha$
- L contains the n-th cyclotomic extension $K(\zeta_n)$
- $L \mid K$ and $L \mid K(\zeta_n)$ are Galois

UNIVERSITÉ DU LUXEMBOURG

Kummer Theory - Computing Degrees

The degree $[L : K(\zeta_n)]$ is very close to n.

Kummer Theory - Computing Degrees

The degree $[L : K(\zeta_n)]$ is very close to n.

For explicit computations:

The degree $[L : K(\zeta_n)]$ is very close to n.

For explicit computations:

- Properties of $K(\zeta_n) \mid K$ (does K intersect $\mathbb{Q}(\zeta_n)$?)

The degree $[L : K(\zeta_n)]$ is very close to n.

For explicit computations:

- Properties of $K(\zeta_n) \mid K$ (does K intersect $\mathbb{Q}(\zeta_n)$?)
- Divisibility properties of α in K (is it an n-th power?)

Kummer Theory - Computing Degrees

The degree $[L : K(\zeta_n)]$ is very close to n.

For explicit computations:

- Properties of $K(\zeta_n) \mid K$ (does K intersect $\mathbb{Q}(\zeta_n)$?)
- Divisibility properties of α in K (is it an n-th power?)
- Relations between $\sqrt[n]{\alpha}$ and ζ_n

E elliptic curve over a number field K; let $P \in E(K)$ not torsion.

E elliptic curve over a number field K; let $P \in E(K)$ not torsion.

- There are n^2 points $Q_1, \ldots, Q_{n^2} \in E(\overline{K})$ such that $nQ_i = P$

$$n^{-1}P := \{Q_1, \ldots, Q_{n^2}\}$$

E elliptic curve over a number field K; let $P \in E(K)$ not torsion.

- There are n^2 points $Q_1, \dots, Q_{n^2} \in E(\overline{K})$ such that $nQ_i = P$

$$n^{-1}P := \{Q_1, \dots, Q_{n^2}\}$$

- Consider $L := K(n^{-1}P)$

UNIVERSITÉ DU LUXEMBOURG

E elliptic curve over a number field K; let $P \in E(K)$ not torsion.

- There are n^2 points $Q_1, \ldots, Q_{n^2} \in E(\overline{K})$ such that $nQ_i = P$

$$n^{-1}P := \{Q_1, \ldots, Q_{n^2}\}$$

- Consider $L := K(n^{-1}P)$
- L contains the n-th torsion field $K(E[n])$

E elliptic curve over a number field K; let $P \in E(K)$ not torsion.

- There are n^2 points $Q_1, \ldots, Q_{n^2} \in E(\overline{K})$ such that $nQ_i = P$

$$n^{-1}P := \{Q_1, \ldots, Q_{n^2}\}$$

- Consider $L := K(n^{-1}P)$
- L contains the n-th torsion field $K(E[n])$
- $L \mid K$ and $L \mid K(E[n])$ are Galois

Kummer Theories - comparison

Classical	Elliptic Curves
$\mathbb{G}_m$	E
roots of unity $\zeta_n \in \mu_n$	torsion points $T \in E[n]$
$K(\zeta_n)$	$K(E[n])$
$\alpha \in K^\times$ not root of unity	$P \in E(K)$ not torsion
$\{\beta \in \overline{K}^\times \mid \beta^n = \alpha\}$	$\{Q \in E(\overline{K}) \mid nQ = P\}$
$K(\sqrt[n]{a}, \zeta_n)$	$K(n^{-1}P)$
$[K(\sqrt[n]{a}, \zeta_n) : K(\zeta_n)] \sim n$	$[K(n^{-1}P) : K(E[n])] \sim n^2$

UNIVERSITÉ DU LUXEMBOURG

Main result

Theorem

Assume that $\mathrm{End}_K(E) = \mathbb{Z}$. *There is an explicit constant* C, *depending only on* P *and on the torsion Galois representations associated with* E, *such that*

$$\frac{n^2}{[K(n^{-1}P) : K(E[n])]} \qquad \textit{divides} \qquad C$$

for all $n \geq 1$.

Main result

Theorem

Assume that $\mathrm{End}_K(E) = \mathbb{Z}$. *There is an explicit constant* C, *depending only on* P *and on the torsion Galois representations associated with* E, *such that*

$$\frac{n^2}{[K(n^{-1}P) : K(E[n])]} \qquad \textit{divides} \qquad C$$

for all $n \geq 1$.

Previously known with a non-explicit constant.

Main result - idea of proof

Elementary field theory gives

$$\frac{n^2}{[K(n^{-1}P) : K(E[n])]} =$$

$$= \prod_{\substack{\ell \mid n \\ \ell \text{ prime}}} \underbrace{\frac{\ell^{2e_\ell}}{[K(\ell^{-e_\ell}P) : K(E[\ell^{e_\ell}])]}}_{A_\ell(n)} \cdot \underbrace{[K(\ell^{-e_\ell}P) \cap K(E[n]) : K(E[\ell^{e_\ell}])]}_{B_\ell(n)}$$

where $e_\ell = v_\ell(n)$.

Elementary field theory gives

$$\frac{n^2}{[K(n^{-1}P) : K(E[n])]} =$$

$$= \prod_{\substack{\ell \mid n \\ \ell \text{ prime}}} \underbrace{\frac{\ell^{2e_\ell}}{[K(\ell^{-e_\ell}P) : K(E[\ell^{e_\ell}])]}}_{A_\ell(n)} \cdot \underbrace{[K(\ell^{-e_\ell}P) \cap K(E[n]) : K(E[\ell^{e_\ell}])]}_{B_\ell(n)}$$

where $e_\ell = v_\ell(n)$.

We call $A_\ell(n)$ the ℓ-adic failure and $B_\ell(n)$ the adelic failure.

UNIVERSITÉ DU LUXEMBOURG

Goals:

- Show that $A_\ell(n)$ is bounded as a function of n

Main result - idea of proof

Goals:

- Show that $A_\ell(n)$ is bounded as a function of n
- $A_\ell = 1$ for almost all primes

Goals:

- Show that $A_\ell(n)$ is bounded as a function of n
- $A_\ell = 1$ for almost all primes
- Same for B_ℓ

Main result - idea of proof

Goals:

- Show that $A_\ell(n)$ is bounded as a function of n
- $A_\ell = 1$ for almost all primes
- Same for B_ℓ
- Everything explicitly!

UNIVERSITÉ DU LUXEMBOURG

Proof idea - ℓ-adic failure

Assume that E has no CM and fix a prime ℓ.

Proof idea - ℓ-adic failure

Assume that E has no CM and fix a prime ℓ.

- Write $P = \ell^{d_\ell} Q + T$ in $E(K)$, with T torsion and d_ℓ maximal

Proof idea - ℓ-adic failure

Assume that E has no CM and fix a prime ℓ.

- Write $P = \ell^{d_\ell} Q + T$ in $E(K)$, with T torsion and d_ℓ maximal

Theorem (Jones, Rouse (2007))

Assume $\ell > 2$. If $d_\ell = 0$ and the ℓ-adic Galois representation associated with E is surjective, then $A_\ell(n) = 1$ for every $n > 1$.

UNIVERSITÉ DU LUXEMBOURG

Assume that E has no CM and fix a prime ℓ.

- Write $P = \ell^{d_\ell} Q + T$ in $E(K)$, with T torsion and d_ℓ maximal

Theorem (Jones, Rouse (2007))

Assume $\ell > 2$. If $d_\ell = 0$ and the ℓ-adic Galois representation associated with E is surjective, then $A_\ell(n) = 1$ for every $n > 1$.

- Serre's open image theorem $\Longrightarrow$ finitely many primes left

UNIVERSITÉ DU LUXEMBOURG

Proof idea - ℓ-adic failure (an example)

Problem: d_ℓ may increase when we work over $K(E[\ell^e])$

Proof idea - ℓ-adic failure (an example)

Problem: d_ℓ may increase when we work over $K(E[\ell^e])$

Example

The curve

$$E/\mathbb{Q}: \qquad y^2+y = x^3-216x-1861 \qquad \textit{(Cremona 17739g1)}$$

has a point

$$P = \left(\frac{23769}{400}, \frac{3529853}{8000}\right) \in E(\mathbb{Q})$$

with $d_3 = 0$.
However, there is a point $Q \in \mathbb{Q}(E[3])$ *such that* $P = 3Q$.

Proof idea - ℓ-adic failure

Using Galois cohomology, we bound A_ℓ in terms of:

- the divisibility parameter d_ℓ
- "how much" ρ_{ℓ^∞} is not surjective

Proof idea - ℓ-adic failure

Using Galois cohomology, we bound A_ℓ in terms of:

- the divisibility parameter d_ℓ
- "how much" ρ_{ℓ^∞} is not surjective

Proposition

There is an explicit integer c_ℓ, depending only on the ℓ-adic Galois representation associated with E, such that $A_\ell(n)$ divides $\ell^{4c_\ell+2d_\ell}$ for every $n > 1$.

Proof idea - adelic failure

Let $e_\ell = v_\ell(n)$ and $r = n/\ell^{e_\ell}$.

Let $e_\ell = v_\ell(n)$ and $r = n/\ell^{e_\ell}$.

$$B_\ell(n) = [K(\ell^{-e_\ell} P) \cap K(E[n]) : K(E[\ell^{e_\ell}])]$$

Proof idea - adelic failure

Let $e_\ell = v_\ell(n)$ and $r = n/\ell^{e_\ell}$.

$$B_\ell(n) = [K(\ell^{-e_\ell}P) \cap K(E[n]) : K(E[\ell^{e_\ell}])]$$

- One can show that

$$B_\ell(n) = [\underbrace{K(\ell^{-e_\ell}P) \cap K(E[r])}_{F} : \underbrace{K(E[\ell^{e_\ell}]) \cap K(E[r])}_{M}]$$

Proof idea - adelic failure

Let $e_\ell = v_\ell(n)$ and $r = n/\ell^{e_\ell}$.

$$B_\ell(n) = [K(\ell^{-e_\ell}P) \cap K(E[n]) : K(E[\ell^{e_\ell}])]$$

- One can show that

$$B_\ell(n) = [\underbrace{K(\ell^{-e_\ell}P) \cap K(E[r])}_{F} : \underbrace{K(E[\ell^{e_\ell}]) \cap K(E[r])}_{M}]$$

- If $M = K$ then $B_\ell(n) = 1$

UNIVERSITÉ DU LUXEMBOURG

Proof idea - adelic failure

$$M := K(E[\ell^{e_\ell}]) \cap K(E[r])$$

Theorem (Campagna, Stevenhagen (2019))

There is a finite and explicit set of primes S, depending only on E, such that if $\ell \notin S$, then $M = K$.

Proof idea - adelic failure

$$M := K(E[\ell^{e_\ell}]) \cap K(E[r])$$

Theorem (Campagna, Stevenhagen (2019))

There is a finite and explicit set of primes S, depending only on E, such that if $\ell \notin S$, then $M = K$.

For the other primes:

Proof idea - adelic failure

$$M := K(E[\ell^{e_\ell}]) \cap K(E[r])$$

Theorem (Campagna, Stevenhagen (2019))

There is a finite and explicit set of primes S, depending only on E, such that if $\ell \notin S$, then $M = K$.

For the other primes:

- There is a finite extension $\tilde{K} \mid K$, depending only on S, such that working over $\tilde{K}$ we have $\tilde{M} = \tilde{K}$

Proof idea - adelic failure

$$M := K(E[\ell^{e_\ell}]) \cap K(E[r])$$

Theorem (Campagna, Stevenhagen (2019))

There is a finite and explicit set of primes S, depending only on E, such that if $\ell \notin S$, then $M = K$.

For the other primes:

- There is a finite extension $\tilde{K} \mid K$, depending only on S, such that working over $\tilde{K}$ we have $\tilde{M} = \tilde{K}$
- We have the bound

$$B_\ell(n) \mid \ell^{2c_\ell + 3v_\ell([\tilde{K}:K])}$$

UNIVERSITÉ DU LUXEMBOURG

Proof idea - summary

1. Split the "failure of maximality" in ℓ-adic and adelic failures

Proof idea - summary

1. Split the "failure of maximality" in ℓ-adic and adelic failures
2. For most primes things are nice and $A_\ell = B_\ell = 1$ (direct application of older results)

Proof idea - summary

1. Split the "failure of maximality" in ℓ-adic and adelic failures
2. For most primes things are nice and $A_\ell = B_\ell = 1$ (direct application of older results)
3. For the other primes, things don't go too bad (some extra work to do)

Main result

Theorem

Assume that $\mathrm{End}_K(E) = \mathbb{Z}$. *There is an explicit constant* C, *depending only on* P *and on the torsion Galois representations associated with* E *such that*

$$\frac{n^2}{[K(n^{-1}P) : K(E[n])]} \qquad \textit{divides} \qquad C$$

for all $n \geq 1$.

UNIVERSITÉ DU LUXEMBOURG

Thank you for your attention!

UNIVERSITÉ DU LUXEMBOURG