My journey in Kummer theory

Sebastiano Tronto

Kummer theory

Fix:

- K a field
- $n > 0$ intger $n \nmid \operatorname{char} K$
- $\zeta_n \in \overline{K}$ root of unity of order n
- $a_1, \dots, a_r \in K^\times$

We have:

- Cyclotomic-Kummer extension $K(\zeta_n, \sqrt[n]{a_1}, \dots, \sqrt[n]{a_r})$
- Galois over K, abelian over $K(\zeta_n)$
- If $\zeta_n \in K$, **all** abelian extensions of K are of this form

Kummer degrees

- Assume K is a number field. For varying n, the degrees

$$\left[K\left(\zeta_n, \sqrt[n]{a_1}, \ldots, \sqrt[n]{a_r}\right) : K\left(\zeta_n\right)\right]$$

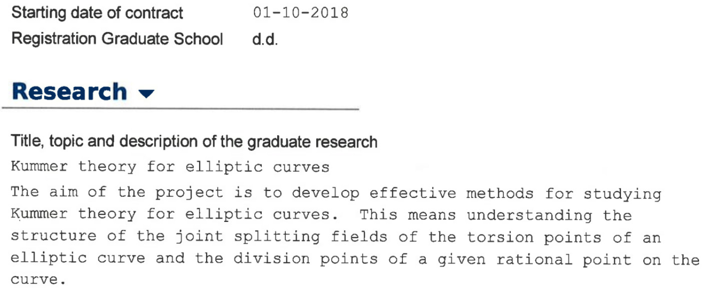
are related to *Artin's primitive root conjecture*.

- If $\langle a_1, \ldots, a_r \rangle \subseteq K^\times$ is torsion-free of rank r, there is a positive constant $c = c(K, a_1, \ldots, a_r)$ such that

$$\frac{n^r}{\left[K\left(\zeta_n, \sqrt[n]{a_1}, \ldots, \sqrt[n]{a_r}\right) : K\left(\zeta_n\right)\right]} \quad \text{divides} \quad c$$

for every $n \geq 1$.

The beginning



Starting date of contract	01-10-2018
Registration Graduate School	d.d.

Research ▾

Title, topic and description of the graduate research

Kummer theory for elliptic curves

The aim of the project is to develop effective methods for studying Kummer theory for elliptic curves. This means understanding the structure of the joint splitting fields of the torsion points of an elliptic curve and the division points of a given rational point on the curve.

Kummer theory for elliptic curves

Fix

- K number field, $n > 0$ integer
- E elliptic curve over K
- $P_1, \dots, P_r \in E(K)$, let $n^{-1}P_i = \{Q \in E(\overline{K}) \mid nQ = P_i\}$

We have:

- Torsion-Kummer extension $K(E[n](\overline{K}), n^{-1}P_1, \dots, n^{-1}P_r)$
- Galois over K, abelian over $K(E[n](\overline{K}))$
- Related to problems similar to Artin's conjecture

First assignment

Prove the following:

Theorem

Let K, E, P_i be as in the previous slide. Assume that E has no CM and that $\mathrm{rk}_{\mathbb{Z}}\langle P_1, \ldots, P_r\rangle = r$. There is a positive constant c such that for every positive integer n the ratio

$$\frac{n^{2r}}{\left[K\left(E[n](\overline{K}), n^{-1}P_1, \ldots, n^{-1}P_r\right)\right]} \quad \textit{divides} \quad c$$

First assignment

Prove the following:

Theorem (Ribet, 1979)

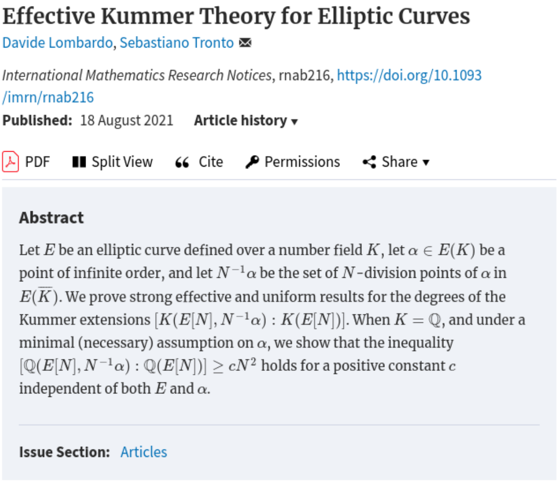
Let K, E, P_i be as in the previous slide. Assume that E has no CM and that $\mathrm{rk}_{\mathbb{Z}}\langle P_1, \ldots, P_r\rangle = r$. There is a positive constant c such that for every positive integer n the ratio

$$\frac{n^{2r}}{\left[K\left(E[n](\overline{K}), n^{-1}P_1, \ldots, n^{-1}P_r\right)\right]} \quad \textit{divides} \quad c$$

First assignment

- Actual task: relate c explicitly to certain properties of E
- Main background needed: Galois representations
- Jones and Rouse, 2007: surjective p-adic Galois representation (“nice” $\implies$ “nice”)
- Me: “not that bad” $\implies$ “not that bad” (quantitatively)

First paper



Effective Kummer Theory for Elliptic Curves

Davide Lombardo, Sebastiano Tronto ✉

International Mathematics Research Notices, rnab216, https://doi.org/10.1093/imrn/rnab216

Published: 18 August 2021 **Article history** ▾

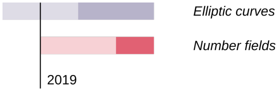
Abstract

Let E be an elliptic curve defined over a number field K, let $\alpha \in E(K)$ be a point of infinite order, and let $N^{-1}\alpha$ be the set of N-division points of α in $E(\overline{K})$. We prove strong effective and uniform results for the degrees of the Kummer extensions $[K(E[N], N^{-1}\alpha) : K(E[N])]$. When $K = \mathbb{Q}$, and under a minimal (necessary) assumption on α, we show that the inequality $[\mathbb{Q}(E[N], N^{-1}\alpha) : \mathbb{Q}(E[N])] \geq cN^2$ holds for a positive constant c independent of both E and α.

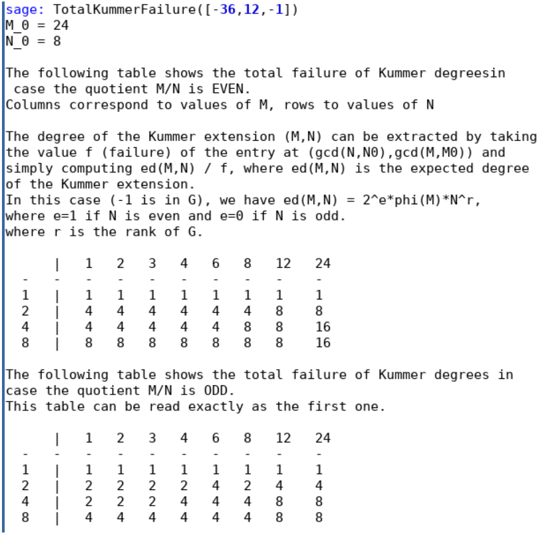
Issue Section: Articles

Side project(s) - number fields

- Collaboration with Antonella Perucca and Pietro Sgobba
- Implementation of software for computing degrees over $\mathbb{Q}$
- Explicit work over quadratic fields and other number fields



Computing Kummer degrees with Sage

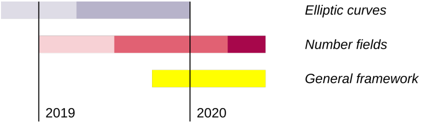


```
sage: TotalKummerFailure([-36,12,-1])
M_0 = 24
N_0 = 8

The following table shows the total failure of Kummer degreesin
 case the quotient M/N is EVEN.
Columns correspond to values of M, rows to values of N

The degree of the Kummer extension (M,N) can be extracted by taking
the value f (failure) of the entry at (gcd(N,N0),gcd(M,M0)) and
simply computing ed(M,N) / f, where ed(M,N) is the expected degree
of the Kummer extension.
In this case (-1 is in G), we have ed(M,N) = 2^e*phi(M)*N^r,
where e=1 if N is even and e=0 if N is odd.
where r is the rank of G.

        |   1   2   3   4   6   8   12   24
  -     -   -   -   -   -   -   -   -    -
  1     |   1   1   1   1   1   1   1    1
  2     |   4   4   4   4   4   4   8    8
  4     |   4   4   4   4   4   8   8    16
  8     |   8   8   8   8   8   8   8    16

The following table shows the total failure of Kummer degrees in
case the quotient M/N is ODD.
This table can be read exactly as the first one.

        |   1   2   3   4   6   8   12   24
  -     -   -   -   -   -   -   -   -    -
  1     |   1   1   1   1   1   1   1    1
  2     |   2   2   2   2   4   2   4    4
  4     |   2   2   2   4   4   4   8    8
  8     |   4   4   4   4   4   4   8    8
```

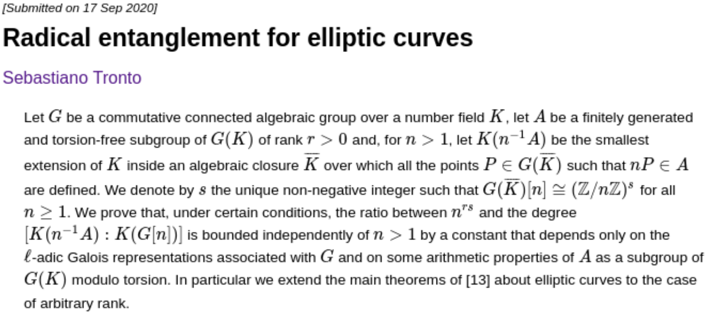
Solo project - general framework

Motivation: the relevant properties of the curve. Can I get a general result of the form “if this and this hold, the result for Kummer theory also holds”?

- Inspired by work of W. J. Palenstijn
- Limitation: endomorphism ring!



Solo project - general framework



[Submitted on 17 Sep 2020]

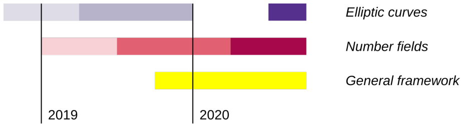
Radical entanglement for elliptic curves

Sebastiano Tronto

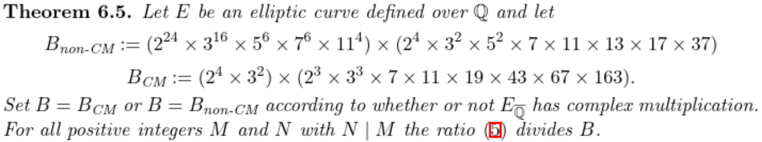
Let G be a commutative connected algebraic group over a number field K, let A be a finitely generated and torsion-free subgroup of $G(K)$ of rank $r > 0$ and, for $n > 1$, let $K(n^{-1}A)$ be the smallest extension of K inside an algebraic closure $\overline{K}$ over which all the points $P \in G(\overline{K})$ such that $nP \in A$ are defined. We denote by s the unique non-negative integer such that $G(\overline{K})[n] \cong (\mathbb{Z}/n\mathbb{Z})^s$ for all $n \geq 1$. We prove that, under certain conditions, the ratio between n^{rs} and the degree $[K(n^{-1}A) : K(G[n])]$ is bounded independently of $n > 1$ by a constant that depends only on the ℓ-adic Galois representations associated with G and on some arithmetic properties of A as a subgroup of $G(K)$ modulo torsion. In particular we extend the main theorems of [13] about elliptic curves to the case of arbitrary rank.

Elliptic curve - uniform results over $\mathbb{Q}$

- Continuation of work with Lombardo
- Found explicit value for c independent of E



Elliptic curve - uniform results over $\mathbb{Q}$



Theorem 6.5. *Let E be an elliptic curve defined over $\mathbb{Q}$ and let*

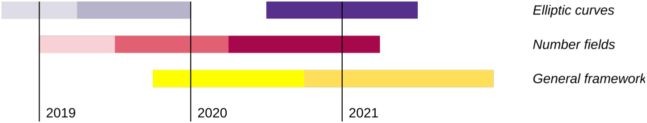
$$B_{non\text{-}CM} := (2^{24} \times 3^{16} \times 5^{6} \times 7^{6} \times 11^{4}) \times (2^{4} \times 3^{2} \times 5^{2} \times 7 \times 11 \times 13 \times 17 \times 37)$$

$$B_{CM} := (2^{4} \times 3^{2}) \times (2^{3} \times 3^{3} \times 7 \times 11 \times 19 \times 43 \times 67 \times 163).$$

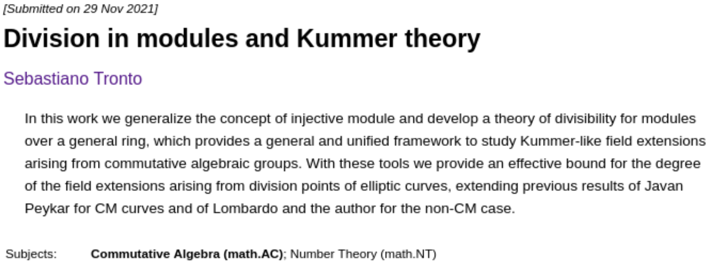
Set $B = B_{CM}$ or $B = B_{non\text{-}CM}$ according to whether or not $E_{\overline{\mathbb{Q}}}$ has complex multiplication. For all positive integers M and N with $N \mid M$ the ratio (5) *divides B.*

General framework - part 2

- Solving the limitations of my previous solo work
- Need to work over a general ring
- Ideas from thesis of Abtien Javan Peykar
- Long digression in commutative algebra



General framework - part 2



[Submitted on 29 Nov 2021]

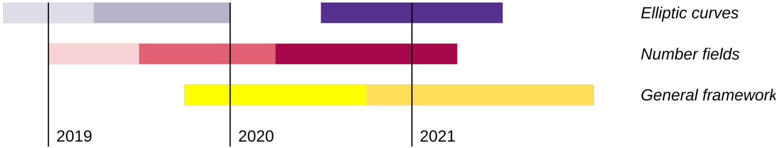
Division in modules and Kummer theory

Sebastiano Tronto

In this work we generalize the concept of injective module and develop a theory of divisibility for modules over a general ring, which provides a general and unified framework to study Kummer-like field extensions arising from commutative algebraic groups. With these tools we provide an effective bound for the degree of the field extensions arising from division points of elliptic curves, extending previous results of Javan Peykar for CM curves and of Lombardo and the author for the non-CM case.

Subjects: **Commutative Algebra (math.AC)**; Number Theory (math.NT)

Timeline


Elliptic curves
Number fields
General framework
2019
2020
2021