Kummer theory for commutative algebraic groups

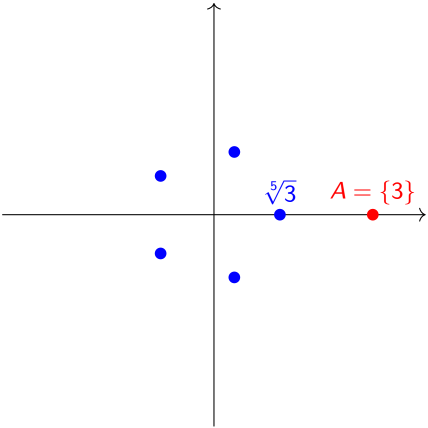
Sebastiano Tronto

6 September 2022

Universiteit Leiden

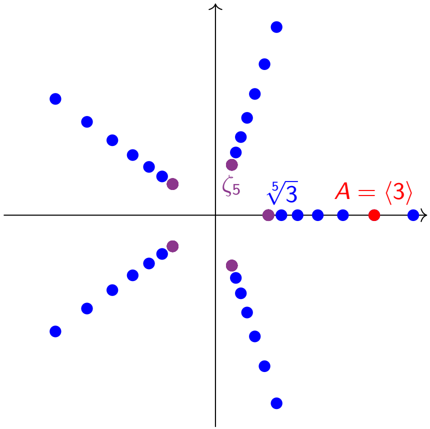
UNIVERSITÉ DU LUXEMBOURG

Kummer theory



- K number field, $\overline{K}$ algebraic closure
- $A \subseteq K^\times$, $\sqrt[n]{A} = \{x \in \overline{K} \mid x^n \in A\}$
- *Kummer extension* $K(\sqrt[n]{A})$
- Galois over K, abelian over $K(\zeta_n)$

Kummer theory



- K number field, $\overline{K}$ algebraic closure
- $A \leq K^\times$, $\sqrt[n]{A} = \{x \in \overline{K} \mid x^n \in A\}$
- *Kummer extension* $K(\sqrt[n]{A})$
- Galois over K, abelian over $K(\zeta_n)$

Kummer degrees

$\mathrm{rk}_{\mathbb{Z}} A = r$, torsion-free

- Degrees $[K(\sqrt[n]{A}) : K(\zeta_n)]$: applications in *density problems*
- Always divide n^r
- $n^r/[K(\sqrt[n]{A} : K(\zeta_n)]$ is bounded

Explicit computation of Kummer degrees

```
sage: G = [-2^3, (2/3)^27, -1/5]
sage: TotalKummerFailure(G)
M_0 = 120
N_0 = 216

         |   1     2     3     4     5     6     8     10    12    15    20    24    30    40    60    120
  -      -   -     -     -     -     -     -     -     -     -     -     -     -     -     -     -     -
  1      |   1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1
  2      |   1     1     1     1     1     2     2     1     2     1     2     4     2     4     4     8
  3      |   9     9     9     9     9     9     9     9     9     9     9     9     9     9     9     9
  4      |   1     1     1     1     1     1     2     1     2     1     2     4     1     4     4     8
  6      |   9     9     9     9     9     18    18    9     18    9     18    36    18    36    36    72
  8      |   2     2     2     2     2     2     2     2     2     2     2     4     2     4     2     8
  9      |   27    27    27    27    27    27    27    27    27    27    27    27    27    27    27    27
  12     |   9     9     9     9     9     9     18    9     18    9     18    36    9     36    36    72
  18     |   27    27    27    27    27    54    54    27    54    27    54    108   54    108   108   216
  24     |   18    18    18    18    18    18    18    18    18    18    18    36    18    36    18    72
  27     |   81    81    81    81    81    81    81    81    81    81    81    81    81    81    81    81
  36     |   27    27    27    27    27    27    54    27    54    27    54    108   27    108   108   216
  54     |   81    81    81    81    81    162   162   81    162   81    162   324   162   324   324   648
  72     |   54    54    54    54    54    54    54    54    54    54    54    108   54    108   54    216
  108    |   81    81    81    81    81    81    162   81    162   81    162   324   81    324   324   648
  216    |   162   162   162   162   162   162   162   162   162   162   162   324   162   324   162   648
```

Kummer theory for algebraic groups

G commutative algebraic group over K number field

- $A \leq G(K)$, $n^{-1}A = \{P \in G(\overline{K}) \mid nP \in A\}$
- "Kummer extension" $K(n^{-1}A)$
- Galois over K, abelian over $K(G(\overline{K})[n])$
- Classical Kummer theory when $G = \mathbb{G}_m$

Classical results

Theorem (Ribet, 1979)

Let G be the extension of an abelian variety of dimension d by a torus of dimension e over a number field K. Let $P_1, \ldots, P_r \in G(K)$ be linearly independent over the ring $\mathrm{End}_K(G)$. Then there exists a constant C, depending only on G and on $P_1, \ldots, P_r$, such that for every positive integer n

$$\frac{n^{r(2d+e)}}{[K(n^{-1}\langle P_1, \ldots, P_r\rangle) : K(G(\overline{K})[n])]} \quad \textit{divides} \quad C$$

Towards effective results for elliptic curves

Theorem (Jones, Rouse - 2010)

Let E be a non-CM elliptic curve over a number field K. Let $P \in E(K)$ be a non-torsion point and let ℓ be a prime different from 2. If $P \notin \ell E(K)$ and the ℓ-adic Galois representation associated with E is surjective, then for every integer $k \geq 0$

$$[K(\ell^{-k}P) : K(E(\overline{K})[\ell^k])] = \ell^{2k}$$

Towards effective results for elliptic curves

- Idea: "nice" Galois representation $\implies$ "nice" Kummer part
- My task: "*this* bad" $\implies$ "$f($*this*$)$ bad"
- Do this for every n

Example: curve 17739g1

Consider

$$E : y^2 + y = x^3 - 216 - 1861, \qquad P = \left(\frac{23769}{400}, \frac{3529853}{8000}\right)$$

- $P \in E(\mathbb{Q})$ and $P \notin 3E(\mathbb{Q})$
- The mod 3 Galois representation of E is *not* surjective
- $P \in 3E(\mathbb{Q}(E[3]))$

Effective results for elliptic curves

Theorem (Lombardo, T. - 2019)

Let E be an elliptic curve over a number field K with $\mathrm{End}_K(E) = \mathbb{Z}$. Let $P \in E(K)$ be a non-torsion point. There is an explicit constant C, depending only on P, E, K and the ℓ-adic torsion representations associated with E for all primes ℓ, such that for all positive integers n

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

Effective results for elliptic curves

Theorem (Lombardo, T. - 2021)

Let E be an elliptic curve over $\mathbb{Q}$ and let $P \in E(\mathbb{Q})$ be a non-torsion point whose image in $E(\mathbb{Q})/E(\mathbb{Q})_{\mathrm{tors}}$ is not divisible by any positive integer n. Then for every positive integer n the ratio

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

divides

$$C_{non\text{-}CM} = 2^{28} \times 3^{18} \times 5^8 \times 7^7 \times 11^5 \times 13 \times 17 \times 37$$

if E does not have complex multiplication and

$$C_{CM} = 2^7 \times 3^5 \times 7 \times 11 \times 19 \times 43 \times 67 \times 163$$

if E has complex multiplication.

Related objects

G_{ℓ^∞} = image of ℓ-adic Galois representation

- Exponenent of cohomology group

$$H^1\left(\mathrm{Gal}(K(E(\overline{K})_{\mathrm{tors}}) \mid K), E(K)_{\mathrm{tors}}\right)$$

- Index of the $\mathbb{Z}_\ell$-algebra generated by G_{ℓ^∞}, for every ℓ

$$[\mathrm{Mat}_{2\times 2}(\mathbb{Z}_\ell) : \mathbb{Z}_\ell(G_{\ell^\infty})]$$

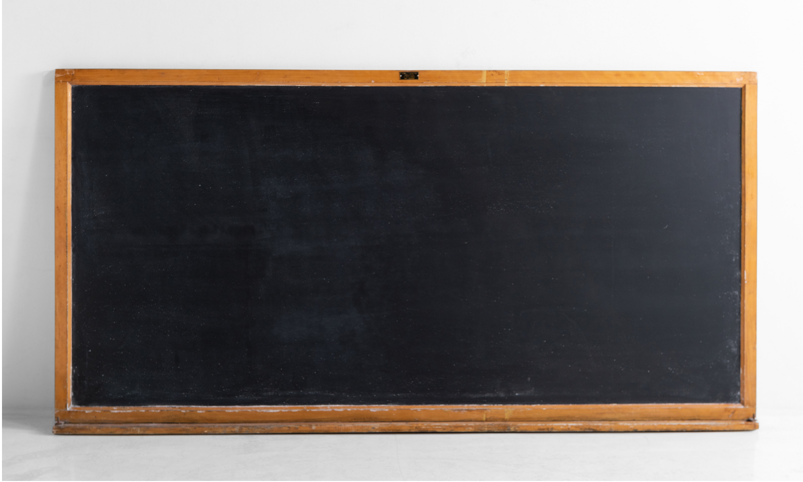
Complex multiplication

- Independent work by Javan Peykar (2021)
- Some assumptions on $\mathrm{End}_K(E)$: Dedekind domain
- Main idea: work with A and $n^{-1}A$ as $\mathrm{End}_K(E)$-modules

Question

Can we do this more generally?

Blackboard time!



Elliptic curves - unified theory

- E any elliptic curve over a number field K
- $R = \mathrm{End}_K(E)$ is either $\mathbb{Z}$ or and order $\mathcal{O}$ in a number field F
- $A \subseteq E(K)$ any R-submodule
- E_{tors} is an injective R-module (Lenstra, 1996)

Elliptic curves - unified theory

- Since $E(K)$ has finite rank, there exists $d > 0$ such that

$$d \cdot \{P \in E(K) + E_{\text{tors}} \mid nP \in A + E_{tors} \text{ for some } n \in \mathbb{Z}_{\geq 1}\} \subseteq A + E_{\text{tors}}$$

- By (Lombardo, T - 2019), there exists $n > 0$ such that

$$n \cdot H^1\left(\mathrm{Gal}(K(E(\overline{K})_{\text{tors}}) \mid K), E(K)_{\text{tors}}\right) = 0$$

- By (Lombardo, T - 2019), there exists $m > 0$ such that

$$m \cdot \mathbb{Z}(\mathrm{Im}(\tau)) \supseteq \mathrm{End}_R(E_{\text{tors}})$$

Elliptic curves - main theorem

Theorem (T. - 2021)

Let E be an elliptic curve over a number field K. Let $A \subseteq E(K)$ be an $\mathrm{End}_K(E)$-submodule of rank r. There is an explicit constant C, depending only on A, E, K and the ℓ-adic torsion representations associated with E for all primes ℓ, such that for all positive integers n

$$\frac{n^{2r}}{[K(n^{-k}A) : K(E(\overline{K})[n])]} \quad \textit{divides} \quad C$$