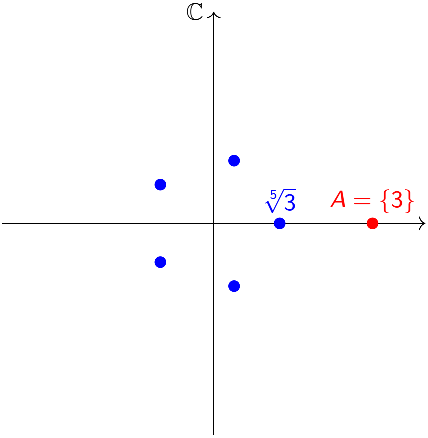
Division in modules and Kummer theory

Sebastiano Tronto

Universiteit Leiden

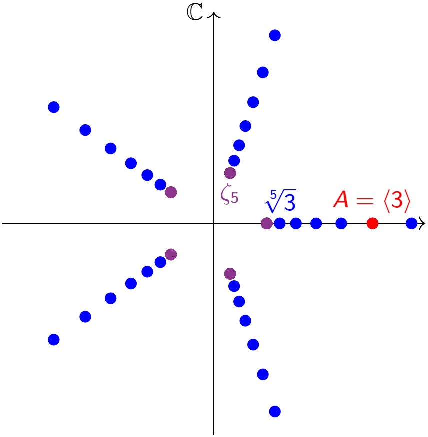
UNIVERSITÉ DU LUXEMBOURG

Kummer theory



- $A \subseteq \mathbb{Q}^\times$, $\sqrt[n]{A} = \{x \in \mathbb{C} \mid x^n \in A\}$
- *Kummer extension* $\mathbb{Q}(\sqrt[n]{A})$
- Galois over $\mathbb{Q}$, contains $\mathbb{Q}(\zeta_n)$

Kummer theory



- $A \leq \mathbb{Q}^\times$, $\sqrt[n]{A} = \{x \in \mathbb{C} \mid x^n \in A\}$
- *Kummer extension* $\mathbb{Q}(\sqrt[n]{A})$
- Galois over $\mathbb{Q}$, contains $\mathbb{Q}(\zeta_n)$

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 $\mathbb{Q}$, contains $\mathbb{Q}(G(\overline{K})[n])$
- Classical Kummer theory when $G = \mathbb{G}_m$

Results for elliptic curves

$G = E$ elliptic curve, $A = \langle \alpha \rangle$

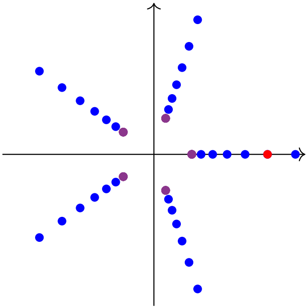
- Ribet, 1979: $cn^2 \leq [K(n^{-1}A) : K(E(\overline{K})[n])] \leq n^2$
- Lombardo-T., 2020: Effective $c = c(E, K, \alpha)$ if no CM
- Lombardo-T., 2021: over $K = \mathbb{Q}$

  $$c^{-1} \leq 2^{28} \cdot 3^{18} \cdot 5^{8} \cdot 7^{7} \cdot 11^{5} \cdot 13 \cdot 17 \cdot 19 \cdot 37 \cdot 43 \cdot 67 \cdot 163$$

- A. Javan Peykar, 2021: CM case

Endomorphism rings

A. Javan Peykar, 2021: CM case $\to$ take $\color{red}{A}$ an $\mathrm{End}_K(E)$-module



Over $\mathbb{Z}$

$\rightsquigarrow$

?

Over $\mathrm{End}_K(E)$

Division modules

R ring, $M \subseteq N$ (left) modules, I (right) ideal

$$(M :_N I) := \{x \in N \mid Ix \subseteq M\}$$

For $M = 0$ we have the I-torsion

$$N[I] := (0 :_N I)$$

Division in modules

Facts

- $(M :_N 0) = N$ *and* $(M :_N R) = M$
- *If* $I \subseteq I'$ *we have* $(M :_N I) \supseteq (M :_N I')$

We want to work with **infinite unions** like $\bigcup_{n\geq 1} n^{-1}A$

Ideal filters

An **ideal filter** $\mathcal{J}$ on R is a set of right ideals such that:

1. If I and I' are in $\mathcal{J}$, then $I \cap I' \in \mathcal{J}$
2. If $I \in \mathcal{J}$ and I' is a right ideal with $I' \supseteq I$, then $I' \in \mathcal{J}$

We let

$$(M :_N \mathcal{J}) = \bigcup_{I \in \mathcal{J}} (M :_N I) \qquad \text{and} \qquad N[\mathcal{J}] = (0 :_N \mathcal{J})$$

Ideal filters

Examples

$$\infty := \{I \textit{ ideal of } R \mid I \supseteq nR \textit{ for some } n \geq 1\}$$

$$\mathfrak{p}^\infty := \{I \textit{ ideal of } R \mid I \supseteq p^k R \textit{ for some } k \geq 0\} \quad (p \textit{ prime})$$

$\mathcal{J}$-injectivity

$$
\begin{tikzcd}
\Gamma & \\
M \arrow[u] \arrow[r, hook, "f"'] & N \arrow[ul, dashed, "\exists g"']
\end{tikzcd}
$$

$$(f(M) :_N \mathcal{J}) = N$$

Γ is $\mathcal{J}$-injective if maps to Γ lift over "$\mathcal{J}$-extensions"

$\mathcal{J}$-injectivity

- Injective $\iff$ $\mathcal{J}$-injective for $\mathcal{J} = \{\text{all ideals}\}$
- Over $\mathbb{Z}$: injective $\iff$ ∞-injective, and $M[\infty] = M_{\text{tors}}$
- Over $\mathbb{Z}$: p-divisible $\iff$ $\mathfrak{p}^\infty$-injective
- Baer's criterion
- Existence of "$\mathcal{J}$-hull" (smallest $\mathcal{J}$-injective extension)

$(\mathcal{J}, T)$-extensions

Definition

Fix an ideal filter $\mathcal{J}$ and a $\mathcal{J}$-injective module T with $T = T[\mathcal{J}]$.
A $(\mathcal{J}, T)$-extension of M is a module $N \supseteq M$ such that:

1. $(M :_N \mathcal{J}) = N$
2. $N[\mathcal{J}] \hookrightarrow T$

Example ($\mathcal{J} = \infty$, $T = E(\overline{K})_{\text{tors}}$)

For $M \leq E(K)$, the modules $N = n^{-1}M$ are $(\mathcal{J}, T)$-extensions.

$(\mathcal{J}, T)$-extensions

- Abstraction for division modules of Kummer theory
- Maximal $(\mathcal{J}, T)$-extension: $\mathcal{J}$-hull of $M + T$
- Behave like field extensions (Galois-like category)
- Pullback and pushforward along certain maps ($\varphi_* \dashv \varphi^*$)

Galois representations

$A \leq G(K) \qquad \Gamma = \bigcup_{n \geq 1} n^{-1} A \subseteq G(\overline{K}) \qquad T = G(\overline{K})_{\mathrm{tors}}$

$$\begin{array}{c} \mathrm{Gal}(K(\Gamma) \mid K) \\ \big\downarrow \\ \mathrm{Aut}_A(\Gamma) \end{array}$$

Galois representations

$$A \leq G(K) \qquad \Gamma = \bigcup_{n\geq 1} n^{-1}A \subseteq G(\overline{K}) \qquad T = G(\overline{K})_{\mathrm{tors}}$$

$$\begin{tikzcd}
 & \mathrm{Gal}(K(\Gamma) \mid K) \arrow[d, hook] & \\
\mathrm{Aut}_{A+T}(\Gamma) \arrow[r, hook] & \mathrm{Aut}_A(\Gamma) \arrow[r, two heads] & \mathrm{Aut}_{A_{\mathrm{tors}}}(T)
\end{tikzcd}$$

Galois representations

$$A \leq G(K) \qquad \Gamma = \bigcup_{n\geq 1} n^{-1}A \subseteq G(\overline{K}) \qquad T = G(\overline{K})_{\mathrm{tors}}$$

$$\begin{tikzcd}
\mathrm{Gal}(K(\Gamma) \mid K(T)) \arrow[r, hook] \arrow[d, hook] & \mathrm{Gal}(K(\Gamma) \mid K) \arrow[r, two heads] \arrow[d, hook] & \mathrm{Gal}(K(T) \mid K) \arrow[d, hook] \\
\mathrm{Aut}_{A+T}(\Gamma) \arrow[r, hook] & \mathrm{Aut}_A(\Gamma) \arrow[r, two heads] & \mathrm{Aut}_{A_{\mathrm{tors}}}(T)
\end{tikzcd}$$

Final tools

- $\mathrm{Gal}(K(T) \mid K) \hookrightarrow \mathrm{Aut}_{A_{\mathrm{tors}}}(T) \hookrightarrow \mathrm{Aut}(T)$: classic Glaois rep.
- $\mathrm{Aut}_{A+T}(\Gamma)$ abelian with action of $\mathrm{Aut}_{A_{\mathrm{tors}}}(T)$
- Bounds on exponent of $H^1(\mathrm{Gal}(K(T) \mid K), T)$
- Morita duality

New results

- General “open image framework” for Kummer extensions
- Completed and unified CM and non-CM cases
- Better understanding of Kummer theory for algebraic groups
- In progress: higher-dimensional abelian varieties

Thank you for your attention