Kummer theory for algebraic groups

Sebastiano Tronto

2020-10-28

Setting

Fix:

- K number field with algebraic closure $\overline{K}$
- G commutative, connected algebraic group over K
- $A \subseteq G(K)$ finitely generated, torsion-free subgroup

Notation:

- $G[n] = G(\overline{K})[n]$ and $G_{\text{tors}} = \bigcup_{n \geq 1} G[n]$
- $s \geq 1$ such that $G[n] \cong (\mathbb{Z}/n\mathbb{Z})^s$ for all n
- $r = \text{rk}(A)$

Division points

For every positive integer n we consider the n-division points of A

$$n^{-1}A := \left\{P \in G(\overline{K}) \mid nP \in A\right\}$$

and we let $\Gamma_A := \bigcup_{n\geq 1} n^{-1}A$.

Division points

Example

If $A = 0$ then $n^{-1}A = G[n]$ and $\Gamma_A = G_{\text{tors}}$

Example

If $G = \mathbb{G}_m$ (so $G(K) = K^\times$ and $G(\overline{K}) = \overline{K}^\times$) and $A = \langle a \rangle$ with $a \in K^\times$ not a root of unity, then $n^{-1}A$ is the group generated by all n-th roots of a. It contains the n-th roots of unity of $\overline{K}$.

Kummer extensions

The field $K(n^{-1}A)$:

- Galois over K, contains $K(G[n])$.
- Generalization of classical Kummer extensions.

Goal

Studying the extensions $K \subseteq K(G[n]) \subseteq K(n^{-1}A)$, in particular the degree of $K(n^{-1}A)$ over $K(G[n])$.

Why is this interesting?

- Interesting objects in their own right.
- Related to torsion fields and Galois representations.
- Density problems: $\{\mathfrak{p} \text{ prime of } K \mid \ell \nmid \#(A \bmod \mathfrak{p})\}$ for ℓ fixed prime.

Basic properties

Consider $A = \langle P \rangle$, fix $Q \in G(\overline{K})$ with $nQ = P$.

- if $nQ_1 = nQ_2 = P$ then $Q_1 - Q_2 \in G[n]$, so $\{q \in G(\overline{K}) \mid nq = P\} = Q + G[n]$, which generates $n^{-1}A$.
- The **Kummer map**

$$\begin{aligned} \mathrm{Gal}(K(n^{-1}A) \mid K(G[n])) &\to G[n] \\ \sigma &\to \sigma(Q) - Q \end{aligned}$$

  is an injective homomorphism.
- $\implies$ in general $[K(n^{-1}A) : K(G[n])]$ divides $(\#G[n])^{\mathrm{rk}(A)} = n^{rs}$.

Classical results

Theorem (Ribet 1979)

Assume that G is the product of an abelian variety and a torus.
Suppose that $A = \langle P_1, \dots, P_r \rangle$ and that $P_1, \dots, P_t$ are $\mathrm{End}_K(G)$-linearly independent modulo $P_{t+1}, \dots, P_r$.
Then there is a positive integer $C = C(K, G, A)$ such that for every $n \geq 1$

$$\frac{n^{ts}}{[K(n^{-1}A) : K(G[n])]} \quad \text{divides} \quad C$$

Classical results

- Ribet's theorem:
  - Open image theorem for $K(\Gamma_A)$.
  - Not effective.
- Key objects and properties:
  - Properties of the $\mathrm{End}_K(G)$-module generated by A.
  - Galois representations associated with G.
  - Cohomology group $H^1(\mathrm{Gal}(K(G_{\mathrm{tors}}) \mid K), G_{\mathrm{tors}})$.

A general framework

Fixing a compatible basis for G_{tors} we have a representation

$$\rho : \mathrm{Gal}(\overline{K} \mid K) \to \mathrm{GL}_s(\hat{\mathbb{Z}})$$

Some notation:

- $H := \rho(\mathrm{Gal}(\overline{K} \mid K))$
- H_ℓ projection of H in $\mathrm{GL}_s(\mathbb{Z}_\ell)$
- $\mathbb{Z}_\ell[H_\ell]$ closed $\mathbb{Z}_\ell$-subalgebra of $\mathrm{Mat}_{s\times s}(\mathbb{Z}_\ell)$ generated by H_ℓ

A general framework

Theorem

If there are positive integers d_A, N_G and M_G such that

1. $d_A(\Gamma_A \cap G(K)) \subseteq A + G(K)_{\mathrm{tors}}$,
2. *for every prime ℓ we have $\mathbb{Z}_\ell[H_\ell] \supseteq N_G \operatorname{Mat}_{s\times s}(\mathbb{Z}_\ell)$ and*
3. *the exponent of $H^1(\mathrm{Gal}(K(G_{\mathrm{tors}}) \mid K), G_{\mathrm{tors}})$ divides M_G;*

then for every $n \geq 1$:

$$\frac{n^{rs}}{[K(n^{-1}A) : K(G[n])]} \quad \text{divides} \quad (d_A N_G M_G)^{rs}$$

The parameter d_A

Example

Let $P \in G(K) \setminus G(K)_{\mathrm{tors}}$ and, for $n \geq 1$, let $A(n) = \langle nP \rangle$.
Then $K(n^{-1}A(n)) = K(G[n])$ and $d_{A(n)} \geq n$.

Elliptic curves - maximal growth

- Let $G = E$ be an elliptic curve with $\mathrm{End}_K(E) = \mathbb{Z}$.
- Let n_ℓ be the smallest integer such that

$$\#(H_\ell \bmod \ell^{n+1})/\#(H_\ell \bmod \ell^n) = \begin{cases} \ell^4 & \text{if } E \text{ does not have CM} \\ \ell^2 & \text{if } E \text{ has CM} \end{cases}$$

  for all $n \geq n_\ell$.
- n_ℓ is effectively computable.

Elliptic curves - bad primes

Let $S(E)$ be the set of primes ℓ such that:

- If E does not have CM, one of the following holds:
  1. $\ell \mid 2 \cdot 3 \cdot 5 \cdot \Delta_{K/\mathbb{Q}}$;
  2. $(H_\ell \bmod \ell) \ncong \mathrm{GL}_2(\mathbb{F}_\ell)$;
  3. E has bad reduction at some prime of K above ℓ.
- If E has CM (by $\mathcal{O}$, $F = \mathrm{Frac}(\mathcal{O})$), one of the following holds:
  1. ℓ divides the conductor of $\mathcal{O}$;
  2. ℓ ramifies in $K \cdot F$;
  3. E has bad reduction at some prime of K above ℓ.

In both cases $S(E)$ is finite and effectively computable.

Elliptic curves - parameters for Cartan subgroups

If E has CM:

- H_ℓ is contained in the normaliser of a Cartan subgroup C_ℓ of $\mathrm{GL}_2(\mathbb{Z}_\ell)$;
- C_ℓ is determined by parameters $(\gamma_\ell, \delta_\ell) \in \mathbb{Z}_\ell^2$;
- $(\gamma_\ell, \delta_\ell)$ are computable.

Elliptic curves - results

Theorem (D. Lombardo, S. T.)

Let E be an elliptic curve over K with $\mathrm{End}_K(E) = \mathbb{Z}$ and let $A \subseteq E(K)$ be a torsion-free subgroup of rank r. Define N and M as follows:

- *If E does not have CM, let*

$$N = \prod_{\ell \in S(E)} \ell^{2n_\ell}, \quad M = \prod_{\ell \in S(E)} (\ell^2 - 1)(\ell^2 - \ell)$$

- *If E has CM, let*

$$N = \prod_{\ell \in S(E)} \ell^{n_\ell + v_\ell(4\delta_\ell)}, \quad M = 2^{24[K:\mathbb{Q}]} \cdot \prod_{\substack{\ell \text{ odd prime,} \\ (\ell-1) \mid 3[K:\mathbb{Q}]}} \ell^{12[K:\mathbb{Q}]}$$

Then for every $n \geq 1$ the ratio $\frac{n^{2r}}{[K(n^{-1}A):K(E[n])]}$ divides $(d_A NM)^{2r}$.

Elliptic curves - results

Theorem (D. Lombardo, S. T.)

There is a universal constant $C \geq 1$ such that, for every elliptic curve E over $\mathbb{Q}$ and every torsion-free subgroup $A \subseteq E(K)$ of rank r, for every $n \geq 1$ the ratio $\frac{n^{2r}}{[K(n^{-1}A):K(E[n])]}$ divides $(d_A C)^{2r}$.

What about CM?

Assume that $\mathcal{O} := \mathrm{End}_K(E) \neq \mathbb{Z}$.

- Let $P \in E(K)$ non-torsion, fix $Q \in E(\overline{K})$ with $nQ = P$.
- Let $A := \mathcal{O}P$ and $A' = \mathbb{Z}P$.
- $n^{-1}\sigma(P) = \sigma(Q) + E[n]$ for every $\sigma \in \mathcal{O}$.
- Then $n^{-1}A = \langle n^{-1}\sigma(P) \mid \sigma \in \mathcal{O} \rangle = \langle \mathcal{O}Q + E[n] \rangle$.
- In particular $K(n^{-1}A) \subseteq K(n^{-1}A')$, so

$$\frac{n^4}{[K(n^{-1}A) : K(E[n])]} = \frac{n^4}{[K(n^{-1}A') : K(E[n])]} \geq n^2$$

General framework - sketch of proof

- Focus on $K(\Gamma_A) = \bigcup_{n\geq 1} K(n^{-1}A)$

$$1 \longrightarrow \mathrm{Gal}(K(\Gamma_A) \mid K(G_{\mathrm{tors}})) \longrightarrow \mathrm{Gal}(K(\Gamma_A) \mid K) \longrightarrow \mathrm{Gal}(K(G_{\mathrm{tors}}) \mid K) \longrightarrow 1$$

General framework - sketch of proof

- Focus on $K(\Gamma_A) = \bigcup_{n\geq 1} K(n^{-1}A)$

$$
\begin{tikzcd}
1 \arrow[r] & \mathrm{Gal}(K(\Gamma_A) \mid K(G_{\mathrm{tors}})) \arrow[r] & \mathrm{Gal}(K(\Gamma_A) \mid K) \arrow[r] & \mathrm{Gal}(K(G_{\mathrm{tors}}) \mid K) \arrow[r] \arrow[d, hook, "\rho"] & 1 \\
 & & & \mathrm{Aut}(G_{\mathrm{tors}}) &
\end{tikzcd}
$$

General framework - sketch of proof

- Focus on $K(\Gamma_A) = \bigcup_{n\geq 1} K(n^{-1}A)$

$$
\begin{tikzcd}
1 \arrow[r] & \mathrm{Gal}(K(\Gamma_A) \mid K(G_{\mathrm{tors}})) \arrow[r] \arrow[d, hook] & \mathrm{Gal}(K(\Gamma_A) \mid K) \arrow[r] \arrow[d, hook] & \mathrm{Gal}(K(G_{\mathrm{tors}}) \mid K) \arrow[r] \arrow[d, hook, "\rho"] & 1 \\
& \mathrm{Aut}_{A+G_{\mathrm{tors}}}(\Gamma_A) & \mathrm{Aut}_A(\Gamma_A) & \mathrm{Aut}(G_{\mathrm{tors}}) &
\end{tikzcd}
$$

General framework - sketch of proof

- Focus on $K(\Gamma_A) = \bigcup_{n\geq 1} K(n^{-1}A)$

$$
\begin{tikzcd}
1 \arrow[r] & \mathrm{Gal}(K(\Gamma_A) \mid K(G_{\mathrm{tors}})) \arrow[r] \arrow[d, hook] & \mathrm{Gal}(K(\Gamma_A) \mid K) \arrow[r] \arrow[d, hook] & \mathrm{Gal}(K(G_{\mathrm{tors}}) \mid K) \arrow[r] \arrow[d, hook, "\rho"] & 1 \\
& \mathrm{Aut}_{A+G_{\mathrm{tors}}}(\Gamma_A) & \mathrm{Aut}_A(\Gamma_A) & \mathrm{Aut}(G_{\mathrm{tors}}) &
\end{tikzcd}
$$

- Study the abelian groups $A \subseteq A + G_{\mathrm{tors}} \subseteq \Gamma_A$ and their relative automorphism groups.

Automorphism groups

- We have an exact sequence:

$$1 \to \mathrm{Aut}_{A+G_{\mathrm{tors}}}(\Gamma_A) \to \mathrm{Aut}_A(\Gamma_A) \to \mathrm{Aut}(G_{\mathrm{tors}}) \to 1$$

- There is a canonical isomorphism:

$$\begin{aligned} \mathrm{Aut}_{A+G_{\mathrm{tors}}}(\Gamma_A) &\xrightarrow{\sim} \mathrm{Hom}(\Gamma_A/(A+G_{\mathrm{tors}}), G_{\mathrm{tors}}) \\ \sigma &\mapsto (\varphi_\sigma : [b] \mapsto \sigma(b) - b) \end{aligned}$$

- In particular $\mathrm{Aut}_{A+G_{\mathrm{tors}}}(\Gamma_A)$ is abelian.

Structure of Γ_A

- Any isomorphism $A \xrightarrow{\sim} \mathbb{Z}^r$ can be extended (non-canonically) to

$$\Gamma_A \xrightarrow{\sim} \mathbb{Q}^r \oplus (\mathbb{Q}/\mathbb{Z})^s$$

- It follows that

$$\mathrm{Hom}(\Gamma_A/(A + G_{\mathrm{tors}}), G_{\mathrm{tors}}) \cong \mathrm{Hom}\left((\mathbb{Q}/\mathbb{Z})^r, (\mathbb{Q}/\mathbb{Z})^s\right) \cong \mathrm{Mat}_{s\times r}(\hat{\mathbb{Z}})$$

$$\mathrm{Aut}(G_{\mathrm{tors}}) \cong \mathrm{Aut}((\mathbb{Q}/\mathbb{Z})^s) \cong \mathrm{GL}_s(\hat{\mathbb{Z}})$$

Torsion-Kummer representation

Fixing an isomorphism $\Gamma_A \xrightarrow{\sim} \mathbb{Q}^r \oplus (\mathbb{Q}/\mathbb{Z})^s$ we have:

$$\begin{tikzcd}
1 \arrow[r] & \mathrm{Gal}(K(\Gamma_A) \mid K(G_{\mathrm{tors}})) \arrow[r] \arrow[d, hook, "\kappa"] & \mathrm{Gal}(K(\Gamma_A) \mid K) \arrow[r] \arrow[d, hook] & \mathrm{Gal}(K(G_{\mathrm{tors}}) \mid K) \arrow[r] \arrow[d, hook, "\rho"] & 1 \\
1 \arrow[r] & \mathrm{Mat}_{s\times r}(\hat{\mathbb{Z}}) \arrow[r] & \mathrm{Aut}_{\mathbb{Z}^r}(\mathbb{Q}^r \oplus (\mathbb{Q}/\mathbb{Z})^s) \arrow[r] & \mathrm{GL}_s(\hat{\mathbb{Z}}) \arrow[r] & 1
\end{tikzcd}$$

We want to bound the index of $V := Im(\kappa)$ in $\mathrm{Mat}_{s\times r}(\hat{\mathbb{Z}})$.

Main idea

Strategy:

- Prove that $S := \bigcap_{f \in V} \ker f$ is small.
- By Pontryagin duality V will be large.

Problem:

- We need V to be a $\mathrm{Mat}_{s\times s}(\hat{\mathbb{Z}})$-module...
- ...but it is only a $\hat{\mathbb{Z}}[H]$-module.

Solution:

- If $\hat{\mathbb{Z}}[H] \supseteq N \cdot \mathrm{Mat}_{s\times s}(\hat{\mathbb{Z}})$, then $N \cdot \mathrm{Mat}_{s\times s}(\hat{\mathbb{Z}}) \cdot V \subseteq V$.

Enter Cohomology

For simplicity identify $\mathrm{Hom}(\Gamma_A/(A+G_{\mathrm{tors}}), G_{\mathrm{tors}})$ with $\mathrm{Mat}_{s\times r}(\hat{\mathbb{Z}})$.

- Notice that $S = \bigcap_{f\in V} \ker f = \dfrac{\Gamma_A \cap G(K(G_{\mathrm{tors}}))}{A+G_{\mathrm{tors}}}$.
- Define

$$\begin{aligned} \varphi : S &\to H^1(\mathrm{Gal}(K(G_{\mathrm{tors}}) \mid K), G_{\mathrm{tors}}) \\ [b] &\mapsto (\varphi_b : \sigma \mapsto \sigma(b) - b) \end{aligned}$$

- We have $\ker\varphi \subseteq S[d_A]$.
- If $M \cdot H^1(\mathrm{Gal}(K(G_{\mathrm{tors}}) \mid K), G_{\mathrm{tors}})$, then $d_A M \cdot S = 0$.

End of the proof

- The $\mathrm{Mat}_{s\times s}(\hat{\mathbb{Z}})$-module W generated by V satisfies

$$d_A M \cdot \left(\bigcap_{f\in W} \ker f \right) = 0$$

- By Pontryagin duality $W \supseteq d_A M \cdot \mathrm{Mat}_{s\times r}(\hat{\mathbb{Z}})$.
- So $V \supseteq N \cdot W \supseteq d_A NM \cdot \mathrm{Mat}_{s\times r}(\hat{\mathbb{Z}})$.
- Then for every $n \geq 1$

$$\frac{n^{rs}}{[K(n^{-1}A) : K(G[n])]} \quad \text{divides} \quad (d_A NM)^{rs}$$

Final comments

- $\hat{\mathbb{Z}}[H]$ can be studied "prime by prime" (CRT).
- Same for the cohomology group (inflation-restriction sequence).
- The exponent of the cohomology group can be bounded by finding "small" central elements in H (Sah's lemma).

Thank you for your attention!