KUMMER THEORY FOR ELLIPTIC CURVES

SEBASTIANO TRONTO

ABSTRACT. These are the notes for an expository talk on the results of [2] given at the Leiden algebra seminar.

1. INTRODUCTION

Fix a number field K and an algebraic closure $\overline{K}$ of K. Let E be an elliptic curve over K without CM over $\overline{K}$. For $M \in \mathbb{Z}_{\geqslant 1}$ we denote by

$$E[M] := \{P \in E(\overline{K}) \mid MP = 0\}$$

the group of M-torsion points and by

$$K_M := K(E[M])$$

the *M-th division field* of E, that is the field generated by the coordinates of the M-torsion points of E. Alternatively, one can consider the action of $\mathrm{Gal}(\overline{K} \mid K)$ on $E[M]$ and define K_M as the subfield of $\overline{K}$ fixed by the subgroup of $\mathrm{Gal}(\overline{K} \mid K)$ that acts trivially on $E[M]$. This shows that $K_M \mid K$ is Galois.

Let now $\alpha \in E(K)$ be a point of infinite order. For $N \in \mathbb{Z}_{\geqslant 1}$ We denote by

$$N^{-1}\alpha := \{\beta \in \overline{K} \mid N\beta = \alpha\}$$

the set of N-division points of α. Fixing $\beta \in N^{-1}\alpha$ gives a bijection

$$\begin{aligned} \varphi_\beta : N^{-1}\alpha &\longrightarrow E[N] \\ \beta' &\longmapsto \beta' - \beta \end{aligned}$$

Notice that $K(N^{-1}\alpha) \supseteq K(E[N])$. For $M, N \in \mathbb{Z}_{\geqslant 1}$ with $N \mid M$ we let

$$K_{M,N} := K(E[M], N^{-1}\alpha)$$

which is a Galois extension of K. We are interested in studying extensions of K of this form; for example, we want to compute their degree. Since the extensions of the form $K_M \mid K$ are largely studied in the literature, we focus on the "Kummer part" $K_{M,N}|K_M$.

Remark 1.1. In the above, one can replace E by any commutative algebraic group over K. For example if one takes $E = \mathbb{G}_m$, the extension $K_{M,N}$ becomes $K(\zeta_M, \sqrt[N]{\alpha})$, that is a classical Kummer extension. In this situation, the degree $[K_{M,N} : K_M]$ is close to N: in fact there is a constant $C = C(K, \alpha)$ such that $N/[K_{M,N} : K_M]$ divides C for any M and N.

Our goal is to give an explicit version of the following result:

Theorem 1.2 (See [3])**.** *There is a constant $C = C(E, K, \alpha)$ such that $N^2/[K_{M,N} : K_M]$ divides C for any pair of positive integers M, N with $N \mid M$.*

More precisely, we give an explicit value for C that only depends on the ℓ-adic torsion representations associated with E/K and on divisibility properties of the point α.

It is enough to consider the case $M = N$: in fact, assume that there is a constant $C \geqslant 1$ such that $M^2/[K_{M,M} : K_M]$ divides C for all positive integers M. Then for any $N \mid M$, since $[K_{M,M} : K_{M,N}]$ divides $(M/N)^2$, we have that

$$\frac{N^2}{[K_{M,N} : K_M]} = \frac{N^2[K_{M,M} : K_{M,N}]}{[K_{M,M} : K_M]} \quad \text{divides} \quad \frac{M^2}{[K_{M,M} : K_M]},$$

which in turn divides C.

2. Galois representations

2.1. **The torsion representation.** The Galois group $\mathrm{Gal}(\overline{K} \mid K)$ acts on $E(\overline{K})$. Since $E[N]$ is defined over K, the action restricts to $E[N]$. Moreover it respects the group structure of E, so we get a map $\rho_N : \mathrm{Gal}(\overline{K} \mid K) \to \mathrm{Aut}(E[N])$, which we call the $(\bmod N)-$*torsion representation* associated with E. Fixing a basis of $E[N]$ induces an isomorphism $\mathrm{Aut}(E[N]) \cong \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, and thus we identify this map with $\rho_N : \mathrm{Gal}(\overline{K} \mid K) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$.

Passing to the limit on the powers of a fixed prime ℓ we get an action on $T_\ell(E) = \varprojlim E[\ell^n] \cong \mathbb{Z}_\ell^2$, and thus a representation $\rho_{\ell^\infty} : \mathrm{Gal}(\overline{K} \mid K) \to \mathrm{GL}_2(\mathbb{Z}_\ell)$, called *$\ell$-adic torsion representation.* Taking the product over all primes we get a representation $\rho_\infty : \mathrm{Gal}(\overline{K} \mid K) \to \mathrm{GL}_2(\hat{\mathbb{Z}})$, called the *adelic torsion representation*.

We denote by H_z the image of ρ_z for $z \in \mathbb{N} \cup \{\ell^\infty \mid \ell \text{ prime}\} \cup \{\infty\}$.

Theorem 2.1 (Serre). *The image of ρ_∞ is open in $\mathrm{GL}_2(\hat{\mathbb{Z}})$. Equivalently, ρ_{ℓ^∞} is surjective for almost all primes ℓ and its image is open in $\mathrm{GL}_2(\mathbb{Z}_\ell)$ for all ℓ.*

Recall that a subgroup of $\mathrm{GL}_2(\hat{\mathbb{Z}})$ or $\mathrm{GL}_2(\mathbb{Z}_\ell)$ is open if and only if it is closed and of finite index. Since

$$\mathrm{GL}_2(\mathbb{Z}_\ell) \supseteq I + \ell M_2(\mathbb{Z}_\ell) \supseteq I + \ell^2 M_2(\mathbb{Z}_\ell) \supseteq \cdots \supseteq I + \ell^n M_2(\mathbb{Z}_\ell) \supseteq \cdots$$

is a fundamental system of neighborhoods of the indentity in $\mathrm{GL}_2(\mathbb{Z}_\ell)$, the image of ρ_{ℓ^∞} must contain $I + \ell^n M_2(\mathbb{Z}_\ell)$ for some n. We call a minimal such n a *parameter of maximal growth* for the ℓ-adic torsion representation, and we denote it by n_ℓ.

2.2. **The Kummer representation.** Consider the action of $\mathrm{Gal}(\overline{K} \mid K_N)$ on $N^{-1}\alpha$. Fixing an element $\beta \in N^{-1}\alpha$ we get a map

$$\begin{aligned} \kappa_N \ \mathrm{Gal}(\overline{K} \mid K_N) &\longrightarrow E[N] \\ \sigma &\longmapsto \sigma(\beta) - \beta \end{aligned}$$

This map does not depend on the choice of β: if fact each $\beta' \in N^{-1}\alpha$ is of the form $\beta' = \beta + T$ for some $T \in E[N]$, thus $\sigma(\beta') - \beta' = \sigma(\beta + T) - \beta - T = \sigma(\beta) + \sigma(T) - \beta - T = \sigma(\beta) - \beta$ since σ fixes $E[N]$.

Moreover, the kernel of κ_N is exactly $\mathrm{Gal}(\overline{K} \mid K_{N,N})$, so that we have an injective map $\mathrm{Gal}(K_{N,N} \mid K_N) \hookrightarrow E[N]$. This tells us in particular that $[K_{N,N} : K_N]$ divides N^2.

Moreover, from the fundamental Galois theory exact sequence

$$1 \to \mathrm{Gal}(K_{N,N} \mid K_N) \to \mathrm{Gal}(K_{N,N} \mid K) \to \mathrm{Gal}(K_{N,N} \mid K_N) \to 1$$

one sees that H_N acts on $V_N := \mathrm{Im}\,\kappa_N$ by conjugation. This action coincides with the natural action of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ on $(\mathbb{Z}/N\mathbb{Z})^2$.

3. The ℓ-adic and adelic failures

Elementary field theory gives

$$\begin{aligned} \frac{N^2}{[K_{N,N} : K_N]} &\overset{(*)}{=} \prod_{\substack{\ell \mid N \\ \ell \text{ prime}}} \frac{\ell^{2v_\ell(N)}}{[K_{N,\ell^{v_\ell(N)}} : K_N]} = \\ &= \prod_{\substack{\ell \mid N \\ \ell \text{ prime}}} \frac{\ell^{2v_\ell(N)}}{[K_{\ell^{v_\ell(N)},\ell^{v_\ell(N)}} : K_{\ell^{v_\ell(N)}}]} \cdot \frac{[K_{\ell^{v_\ell(N)},\ell^{v_\ell(N)}} : K_{\ell^{v_\ell(N)}}]}{[K_{N,\ell^{v_\ell(N)}} : K_N]} = \\ &= \prod_{\substack{\ell \mid N \\ \ell \text{ prime}}} \frac{\ell^{2v_\ell(N)}}{[K_{\ell^{v_\ell(N)},\ell^{v_\ell(N)}} : K_{\ell^{v_\ell(N)}}]} \cdot [K_{\ell^{v_\ell(N)},\ell^{v_\ell(N)}} \cap K_N : K_{\ell^{v_\ell(N)}}] \end{aligned}$$

where $(*)$ holds because the degree $[K_{N,\ell^{v_\ell(N)}} : K_N]$ is a power of ℓ, so the fields $K_{N,\ell^{v_\ell(N)}}$ are linearly disjoint over K_N, and clearly they generate all of $K_{N,N}$.

Definition 3.1. Let ℓ be a prime and N a positive integer. Let $n := v_\ell(N)$. We call

$$A_\ell(N) := \frac{\ell^{2n}}{[K_{\ell^n,\ell^n} : K_{\ell^n}]}$$

the *ℓ-adic failure* at N and

$$B_\ell(N) := \frac{[K_{\ell^n,\ell^n} : K_{\ell^n}]}{[K_{N,\ell^n} : K_N]} = [K_{\ell^n,\ell^n} \cap K_N : K_{\ell^n}]$$

the *adelic failure* at N (related to ℓ). Notice that both $A_\ell(N)$ and $B_\ell(N)$ are powers of ℓ.

Example 3.2. It is clear that the ℓ-adic failure $A_\ell(N)$ can be nontrivial, that is, different from 1. Suppose for example that $\alpha = \ell\beta$ for some $\beta \in E(K)$: then we have

$$K_{\ell^n,\ell^n} = K_{\ell^n}(\ell^{-n}\alpha) = K_{\ell^n}(\ell^{-n+1}\beta),$$

and the degree of this field over K_{ℓ^n} is at most $\ell^{2(n-1)}$, so $\ell^2 \mid A_\ell(N)$. In Example 4.4 we will show that the ℓ-adic failure can be non-trivial also when α is strongly ℓ-indivisible.

We have to show the following:

(1) For every ℓ there is an explicit $a_\ell \in \mathbb{N}$ such that $A_\ell(N)$ divides ℓ^{a_ℓ} for every N, and $a_\ell = 0$ for almost all ℓ.
(2) For every ℓ there is an explicit $b_\ell \in \mathbb{N}$ such that $B_\ell(N)$ divides ℓ^{b_ℓ} for every N, and $b_\ell = 0$ for almost all ℓ.

4. The ℓ-adic failure

In case ρ_{ℓ^∞} is surjective, the following result takes care of the ℓ-adic failure:

Theorem 4.1 (Jones-Rouse, [1, Theorem 5.2])**.** *Assume that ρ_{ℓ^∞} is surjective and that α is ℓ-indivisible in $E(K)$. If $\ell = 2$ assume moreover that $K_{2,2} \not\subseteq K_4$. Then $A_\ell(N) = 1$ for every N.*

When the ℓ-adic torsion representation is not surjective and the point α is not necessarily indivisible, it is still possible to bound the ℓ-adic failure by "how much" the hypotheses of the Theorem fail.

In particular, a bound on the divisibility of the point α in the tower of ℓ-power division field tells us that there exist some non-trivial elements in V_{ℓ^n} for n big enough.

Lemma 4.2. *If $\alpha \in E(K)$ is not ℓ^{d+1}-divisible over K_{ℓ^∞}, then V_{ℓ^∞} contains a vector of valuation at most d.*

Then, if H_{ℓ^n} is big enough, we can use the action of H_{ℓ^n} on V_{ℓ^n} to move this element around and make V_{ℓ^n} larger.

Lemma 4.3. *Suppose that V_{ℓ^∞} contains a vector of valuation at most d and that H_{ℓ^n} contains all matrices that are congruent to the identity modulo ℓ^n. Then V_{ℓ^∞} contains $\ell^{d+n}\mathbb{Z}_\ell^2$.*

Idea of proof. Assume that $v := \ell^d \mathbf{e}_1 \in V_{\ell^\infty}$. Then for any $g = I + \ell^n M \in H_{\ell^\infty}$ we have $V_{\ell^\infty} \ni gv - v = \ell^{n+d} M\mathbf{e}_1$. Letting M vary we get all of $\ell^{d+n}\mathbb{Z}_\ell^2$. □

In the proposition above we can take $n = n_\ell$, so it remains to bound the divisibility of α in K_{ℓ^n}. First of all, write $\alpha = \ell^{d(\alpha,K)}\beta + T$, where $\beta \in E(K)$ is indivisible in $E(K)/E(K)_{\mathrm{tors}}$ and $T \in E(K)$ has order a power of ℓ. We call $d(\alpha, K)$ the *ℓ-divisibility parameter* of α over K.

The point β may not be indivisible in $E(K_{\ell^n})/E(K_{\ell^n})_{\mathrm{tors}}$, so the ℓ-divisibility of α may increase.

Example 4.4. Consider the elliptic curve E over $\mathbb{Q}$ given by the equation

$$y^2 + y = x^3 - 216x - 1861$$

with Cremona label 17739g1. We have $E(\mathbb{Q}) \cong \mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$, with a generator of the free part given by $P = \left(\frac{23769}{400}, \frac{3529853}{8000}\right)$, which is indivisible in $E(\mathbb{Q})/E(\mathbb{Q})_{\mathrm{tors}}$.

The 3-torsion field of E is given by $\mathbb{Q}(z)$, where z is any root of $x^6 + 3$. Over this field the point

$$Q = \left(\frac{803}{400}z^4 - \frac{416}{400}z^2 + \frac{507}{400}, \frac{89133}{8000}z^4 - \frac{199071}{8000}z^2 - \frac{95323}{8000}\right) \in E(\mathbb{Q}(z))$$

is such that $3Q = P$.

From the study of the cohomology groups $H^1(H_{\ell^k}, E[\ell^n])$ it follows that this phenomenon is also bounded by n_ℓ.

Proposition 4.5. *If $\alpha = \ell^{d(\alpha,K)}\beta + T$ with β and T as above, then $d(\alpha, K_{\ell^\infty}) \leqslant d(\alpha, K) + n_\ell$.*

It follows that that we can take $a_\ell = 4n_\ell + 2d$ for all the finitely many primes such that the ℓ-adic torsion representation is not surjective or $d(\alpha, K) \neq 0$, and $a_\ell = 0$ for all other primes.

5. The adelic failure

Recall that the adelic failure is $B_\ell(N) = [K_{\ell^n,\ell^n} \cap K_N : K_{\ell^n}]$, where $\ell = v_\ell(N)$. Let $R = N/\ell^n$ and consider the following diagram:

$$
\begin{tikzcd}
 & K_{\ell^n R,\ell^n} \arrow[dl, dash] \arrow[dr, dash] & \\
K_{\ell^n,\ell^n} \arrow[dr, dash] \arrow[dd, dash] & & K_{\ell^n R} \arrow[dl, dash] \arrow[dd, dash] \\
 & L := K_{\ell^n,\ell^n} \cap K_{\ell^n R} \arrow[dl, dash] \arrow[dd, dash] & \\
K_{\ell^n} \arrow[ddr, dash] & & K_R \arrow[dl, dash] \arrow[ddl, dash] \\
 & F := K_{\ell^n,\ell^n} \cap K_R \arrow[d, dash] & \\
 & T := K_{\ell^n} \cap K_R \arrow[d, dash] & \\
 & K &
\end{tikzcd}
$$

It is clear that $B_\ell(N) = [F : T]$, so we want to bound this quantity.

The extension $F \mid T$ is abelian, and if $T = K$ one can - with a bit of work - conclude that $[F : K] \mid \ell^{2n_\ell}$. A result of Campagna and Stevenhagen tells us that there is a finite and explicit set of primes S, depending only on E and K, such that $T = K$ holds for every $\ell \notin S$.

For the finitely remaining primes, one sets $\tilde{K} = \prod_{p \in S} K_p$ and repeats the argument: now we do have $\tilde{K}_{\ell^n} \cap \tilde{K}_R = \tilde{K}$, and $[\tilde{F} : \tilde{T}]$ divides $[\tilde{K} : K] \cdot \ell^{2\tilde{n}_\ell}$, where $\tilde{n}_\ell$ is the usual parameter for $E/\tilde{K}$. It is not hard to see that $\tilde{n}_\ell \leqslant n_\ell + v_\ell([\tilde{K} : K])$.

If follows that one can take $b_\ell = 2n_\ell + 3v_\ell([\tilde{K} : K])$ for the finitely primes ℓ that DO NOT satisfy the following conditions:

- ρ_{ℓ^∞} is surjective;
- $\ell \in S$;
- α is ℓ-indivisible in $E(K)/E(K)_{\mathrm{tors}}$;

and $b_\ell = 0$ for all ℓ that satisfy all the conditions above.

References

[1] R. Jones, J. Rouse, *Galois Theory of Iterated Endomorphisms*.

[2] Lombardo, D. - Tronto, S., *Explicit Kummer Theory for Elliptic Curves*, preprint arXiv:1909.05376.

[3] Ribet, K., *Kummer theory on extensions of abelian varieties by tori*, Duke Math. J. **46** (1979), 745–761.