On the degree of Kummer extensions for commutative algebraic groups

Perissinotto, F.

CHAPTER 1

Basic notions of Kummer theory

Let K be a field and fix an algebraic closure $\overline{K}$ of K. Fix a positive integer n coprime to the characteristic of K and let a be an element in $K^\times$. We denote by ζ_n a fixed root of unity of order n in $\overline{K}$ (in general the choice does not matter, but when we write ζ_n and ζ_{nt} we sometimes choose $\zeta_n = \zeta_{nt}^t$). If K contains the n-th roots of unity, then the extension $K(\sqrt[n]{a})/K$ obtained adjoining the n-th roots of a is clearly a Galois extension as $K(\sqrt[n]{a})$ is the splitting field of $x^n - a$ and is cyclic of order dividing n. Kummer theory states that, if $\zeta_n \in K$, every cyclic extension of K of order dividing n is the splitting field of $x^n - a$ for some element $a \in K^\times$.

More generally, the following holds (see [Lan02, Sec. VI.8]):

Theorem 1.0.1. *Let K be a field and n a positive integer coprime to $\mathrm{char}(K)$. Suppose that K contains the n-th roots of unity. Then for an extension L/K the following are equivalent:*

(i) L/K is abelian with exponent dividing n

(ii) $L = K(\sqrt[n]{G})$ for some subgroup $(K^\times)^n \subseteq G \subseteq K^\times$

Moreover, if L/K satisfies the equivalent conditions, the bilinear map

$$\begin{aligned} \mathrm{Gal}\left(L/K\right) \times G/(K^\times)^n &\to \mu_n \\ (\sigma, a) &\mapsto \frac{\sigma(\alpha)}{\alpha} \end{aligned} \tag{1.1}$$

is a perfect pairing, where α is any choice of n-th root of a. This pairing exhibits a Pontryagin duality between $\mathrm{Gal}(L/K)$ as profinite group and the group $G/(K^\times)^n$ endowed with the discrete topology.

We define any extension satisfying the equivalent conditions of Theorem 1.0.1 a *Kummer extension*.

Remark 1.0.2. If a Kummer extension L/K is finite, then the subgroup G of $K^\times$ such that $L = K(\sqrt[n]{G})$ is finitely generated. In this situation, the fact that (1.1) is a perfect pairing leads to the following group isomorphism:

$$\mathrm{Gal}\left(L/K\right) \cong {G(K^\times)^n}/{(K^\times)^n}$$

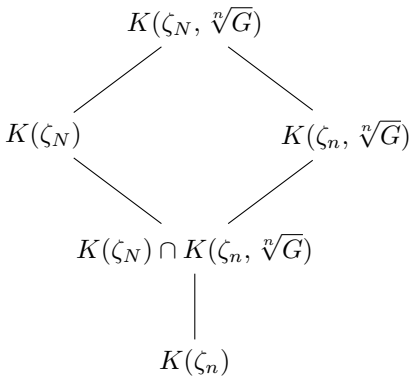
If K does not contain the n-th roots of unity, then the extension L/K where L is the splitting field of $x^n - a$ for some element $a \in K^\times$ is in general not an abelian extension. Indeed, $L = K(\zeta_n, \sqrt[n]{a})$ is abelian over $K(\zeta_n)$, but its Galois group is a subgroup of $\mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^\times$. In this situation, the following result by Schinzel characterises the abelian extensions:

Theorem 1.0.3 ([Sch77, Theorem 2])**.** *Let K be a field and n a positive integer coprime to $\mathrm{char}(K)$. Let $a \in K^\times$. The Galois group of the splitting field of $x^n - a$ is abelian if and only if there exists an element $b \in K^\times$ such that $a^w = b^n$ where w is the largest divisor of n such that K contains the w-th roots of unity.*

In general, for any field K, any pair of positive integers n, N with n dividing N and any finitely generated subgroup G of $K^\times$ we may want to study Kummer extensions of the form

$$K(\zeta_N, \sqrt[n]{G})/K(\zeta_N). \tag{1.2}$$

Notice first that, if the group G is generated by r elements, the Galois group of such Kummer extension is a subgroup of $(\mathbb{Z}/n\mathbb{Z})^r$ and hence its degree divides n^r. It is useful then to look at the following diagram of field extensions:



It follows that, given the prime decomposition $n = \prod \ell^m$, we have:

$$\begin{aligned} \mathrm{Gal}\left(\frac{K(\zeta_N, \sqrt[n]{G})}{K(\zeta_N)}\right) &\cong \mathrm{Gal}\left(\frac{K(\zeta_n, \sqrt[n]{G})}{K(\zeta_N) \cap K(\zeta_n, \sqrt[n]{G})}\right) \\ &\cong \prod_{\ell | n} \mathrm{Gal}\left(\frac{K(\zeta_{\ell^m}, \sqrt[\ell^m]{G})}{K(\zeta_N) \cap K(\zeta_{\ell^m}, \sqrt[\ell^m]{G})}\right) \end{aligned} \tag{1.3}$$

where the last isomorphism is simply the decomposition of the Galois group into its maximal ℓ-subgroups. If we want to only study the degree of the extension, it is useful to consider the integer

$$f_{N,n} := \frac{n^r}{[K(\zeta_N, \sqrt[n]{G}) : K(\zeta_N)]}$$

which we call the *failure of maximality* for the degree of the Kummer extension. Using the same decomposition of (1.3), we can write:

$$f_{N,n} = \prod_{\ell | n} f_{\ell^m, \ell^m} \cdot B(N, \ell^m) \tag{1.4}$$

where

$$B(N, \ell^m) = [K(\zeta_N) \cap K(\zeta_{\ell^m}, \sqrt[\ell^m]{G}) : K(\zeta_{\ell^m})].$$

We call the *ℓ-adic failure* the integer f_{ℓ^m, ℓ^m} and we call the *ℓ-adelic failure* the integer $B(N, \ell^m)$, which measures the so-called entanglement between the Kummer extension and the cyclotomic extension. Clearly, both f_{ℓ^m, ℓ^m} and $B(N, \ell^m)$ are powers of ℓ.

1.1 Kummer theory for number fields

Let now K be a number field. We fix here some notation that will be used throughout the thesis. We denote by μ_K the subgroup of $K^\times$ consisting of the roots of unity. For a positive integer n, we denote by μ_n the group of n-th roots of unity in $\overline{K}$. We also write $\mu_\infty = \cup_n \mu_n$ and, if ℓ is a prime number, $\mu_{\ell^\infty} = \cup_m \mu_{\ell^m}$. If N is a non-zero integer and ℓ is a prime number, then we write $v_\ell(N)$ for the ℓ-adic valuation. If $\alpha \in K^\times$ and $\wp$ is a prime of K (by which we mean a non-zero prime ideal of the ring of integers of K), then $v_\wp(\alpha)$ is the $\wp$-adic valuation of the fractional ideal generated by α.

In this section we describe the divisibility properties of elements in $K^\times$ and more in general of finitely generated subgroups of $K^\times$ in terms of the divisibility parameters. If G is a finitely generated subgroup of $K^\times$, knowledge of its divisibility parameters allows us to compute at once all the degrees of Kummer extensions $K(\zeta_N, \sqrt[n]{G})/K(\zeta_N)$ for all integers $n \mid N$ and the structure of their Galois groups (namely, the size of all cyclic components), see Theorem 1.1.10.

Let $a \in K^\times$. The natural notion of divisibility consists in checking whether a is a n-th power in K for some positive integer n but, for the purpose of Kummer theory, it is useful to consider divisibility up to roots of unity in K. Fix a prime ℓ. If a is such that ζa is not an ℓ-th power in K for any $\zeta \in \mu_K \cap \mu_{\ell^\infty}$, we say that a is *strongly ℓ-indivisible*.

Proposition 1.1.1 ([DP16, Proposition 9]). *Let $a \in K^\times$ be strongly ℓ-indivisible and suppose ℓ is odd or $\zeta_4 \in K$. For any non-negative integer m, the element a is strongly ℓ-indivisible in $K(\zeta_{\ell^m})$.*

Any element $a \in K^\times$ can be written as $a = \zeta_{\ell^h} b^{\ell^d}$ for some non-negative integers h and d, where ζ_{ℓ^h} is a root of unity of order ℓ^h and b is a strongly ℓ-indivisible element in $K^\times$. The integers d and h are called the *parameters for ℓ-divisibility* of the element a. Notice that h is uniquely determined if we impose the restriction that either $h = 0$ or $h > \max(0, v_\ell(\#\mu_K) - d)$.

Consider now finitely many elements $a_1, \cdots, a_r \in K^\times$. We say that $a_1, \cdots, a_r$ are *strongly ℓ-independent* if the element $a_1^{e_1} \cdots a_r^{e_r}$ is strongly ℓ-indivisible whenever $e_1, \cdots, e_r$ are integers not all divisible by ℓ. Let G be a finitely generated and torsion free subgroup of $K^\times$ of rank r. The following result lets us choose a basis of G through which we define the parameters for ℓ-divisibility for the group.

Theorem 1.1.2 ([DP16, Theorem 14]). *There is a basis $\{b_1, \cdots, b_r\}$ of G such that $b_i = B_i^{\ell^{d_i}} \zeta_i$ holds for some strongly ℓ-independent elements $B_1, \cdots, B_r$ of $K^\times$, for some non-negative integers $d_1, \cdots, d_r$ and for some roots of unity $\zeta_i \in \mu_K$ of order ℓ^{h_i}.*

For a basis of G as in Theorem 1.1.2, we say that the tuple of non-negative integers

$$(d_1, \cdots, d_r; h_1, \cdots, h_r)$$

represents the *parameters for ℓ-divisibility for the group G*. In particular, $d_1, \cdots, d_r$ are the d-parameters for ℓ-divisibility, and $h_1, \cdots, h_r$ are the h-parameters for ℓ-divisibility. The d-parameters are unique up to reordering, while the h-parameters are in general not unique, but can be made unique with additional restrictions (see [DP16, Appendix A.2]). Moreover, for almost all primes ℓ, all parameters of ℓ-divisibility for the group G can be taken to be 0, as consequence of the following result:

Theorem 1.1.3 ([PS19, Theorem 2.7]). *There exists a basis of G whose elements are strongly ℓ-independent for all but finitely many primes ℓ.*

The following results allows us to compute the degree and the structure of the Galois group $K(\zeta_{\ell^m}, \sqrt[\ell^m]{G})/K(\zeta_{\ell^m})$ (and hence the ℓ-adic failure f_{ℓ^m,ℓ^m}) for all positive integers m at once:

Theorem 1.1.4 ([DP16, Theorem 18]). *Suppose that ℓ is odd or $\zeta_4 \in K$. Let $t \geqslant 1$ be the largest integer such that $K(\zeta_\ell) = K(\zeta_{\ell^t})$. Let M, m be positive integers with $M \geqslant \max(t, m)$. Then we have*

$$v_\ell([K(\zeta_{\ell^M}, \sqrt[\ell^m]{G}) : K(\zeta_{\ell^M})]) = \max(0, \max_i(h_i - \delta_i + m - M)) + \delta_1 + \cdots + \delta_r$$

where $(d_1, \cdots, d_r; h_1, \cdots, h_r)$ are parameter for ℓ-divisibility of G in K and $\delta_i := \max(m - d_i, 0)$.

Theorem 1.1.5 ([ACP+25, Theorem 6 and Remark 12]). *Suppose that ℓ is odd or $\zeta_4 \in K$. Let $t \geqslant 1$ be the largest integer such that $K(\zeta_\ell) = K(\zeta_{\ell^t})$. Let M, m be positive integers with $M \geqslant \max(t, m)$. There exists an algorithm to compute the structure of the Galois group of the Kummer extension $K(\zeta_{\ell^M}, \sqrt[\ell^m]{G})/K(\zeta_{\ell^M})$. This structure only depends on the parameters for ℓ-divisibility of G over K, and the integers m and $\max(M, t)$. Moreover, we need to apply the algorithm above only finitely many times to compute the structure of the Galois group of $K(\zeta_{\ell^m}, \sqrt[\ell^m]{G})/K(\zeta_{\ell^m})$ at once for all $m \geqslant 1$.*

To extend Theorem 1.1.4 and Theorem 1.1.5 to the remaining case where $\ell = 2$ and $\zeta_4 \notin K$, we can investigate $K(\zeta_{2^M}, \sqrt[2^m]{G})/K(\zeta_{2^M})$ by replacing the field K by $K(\zeta_4)$. The only case left is when $M = m = 1$, for which we easily conclude thanks to the following lemma and the fact that $K(\sqrt{G})/K$ has exponent 2.

Lemma 1.1.6 ([DP16, Lemma 19]). *We have $[K(\sqrt{G}) : K] = e[K(\zeta_4, \sqrt{G}) : K(\zeta_4)]$ where $e = 2$ if G contains minus a square in $K^\times$ and $e = 1$ otherwise.*

Consider now, for a prime ℓ and positive integers m, N such that $\ell^m \mid N$, extensions of the form

$$(K(\zeta_{\ell^m}, \sqrt[\ell^m]{G}) \cap K(\zeta_N))/K(\zeta_{\ell^m}) \tag{1.5}$$

and their degree, which we called the ℓ-adic failure and we denoted by $B(N, \ell^m)$. This extension is a finite Kummer extension over $K(\zeta_{\ell^m})$, and therefore by Remark 1.0.2 there exists a subgroup H_{N,ℓ^m} of G such that:

$$K(\zeta_{\ell^m}, \sqrt[\ell^m]{G}) \cap K(\zeta_N) = K(\zeta_{\ell^m}, \sqrt[\ell^m]{H_{N,\ell^m}}). \tag{1.6}$$

Remark 1.1.7. By Theorem 1.0.3 we have

$$K(\zeta_{\ell^m}, \sqrt[\ell^m]{G}) \cap K(\zeta_N) = K(\zeta_{\ell^m})$$

for all primes ℓ such that $\ell \nmid \#\mu_K$, as the field $K(\zeta_{\ell^m}, \sqrt[\ell^m]{G}) \cap K(\zeta_N)$ is an abelian extension of K, obtained as the splitting field over K of a finite family of polynomials of the form $x^{\ell^m} - g$.

For the finitely many primes dividing $\#\mu_K$ we may use the following:

Theorem 1.1.8 ([PST21, Proposition 3.2 and Lemma 3.4]). *There exists a computable integer N_0 depending on ℓ, K and G such that, for every $m \geqslant t_0 := v_\ell(N_0)$ and $N \geqslant 1$ with $\ell^m \mid N$, we have*

$$K(\zeta_{\ell^m}, \sqrt[\ell^m]{G}) \cap K(\zeta_N) = (K(\zeta_{\ell^{t_0}}, \sqrt[\ell^{t_0}]{G}) \cap K(\zeta_{\gcd(N,N_0)}))(\zeta_{\ell^m})$$

and hence

$$B(N, \ell^m) = B(\gcd(N, N_0), \ell^{t_0}) \quad \textit{and} \quad H_{N,\ell^m} = H_{N_0,\ell^{t_0}}.$$

The following Proposition allows us to explicitly determine the groups H_{N,ℓ^m}:

Proposition 1.1.9. *Let $t = v_\ell(\#\mu_K)$, and let $\alpha \in K^\times$. For a prime ℓ, write $\alpha = \zeta_{\ell^h}\beta^{\ell^d}$, where $\beta \in K^\times$ is strongly ℓ-indivisible, d and h are the parameters for ℓ divisibility of α and either $h = 0$ or $t - d < h \leqslant t$. We define s to be the non-negative integer such that $\sqrt[\ell^s]{\beta} \in K(\mu_\infty)$ and $\sqrt[\ell^{s+1}]{\beta} \notin K(\mu_\infty)$. Then, for every positive integer m the following holds:*

$$K(\zeta_{\ell^m}, \sqrt[\ell^m]{\alpha}) \cap K(\mu_\infty) = \begin{cases} K(\zeta_{\ell^{m+h}}), & \text{if } 1 \leqslant m \leqslant d; \\ K(\zeta_{\ell^m}, \zeta_{\ell^{m+h}}\sqrt[\ell^{m-d}]{\beta}), & \text{if } d < m < d+s; \\ K(\zeta_{\ell^{h+d+s}}\sqrt[\ell^s]{\beta}), & \text{if } d+s \leqslant m < h+d+s; \\ K(\zeta_{\ell^m}, \sqrt[\ell^s]{\beta}), & \text{if } m \geqslant h+d+s. \end{cases}$$

Proof. If $m \leqslant d$, the statement is clear as $K(\sqrt[\ell^m]{\alpha}) = K(\zeta_{\ell^{m+h}})$. If $d < m < d+s$, then:

$$K(\zeta_{\ell^m}, \sqrt[\ell^m]{\alpha}) = K(\zeta_{\ell^m}, \zeta_{\ell^{m+h}}\sqrt[\ell^{m-d}]{\beta})$$

is contained in $K(\mu_\infty)$ as $m - d < s$. If $m \geqslant d+s$, then

$$K(\zeta_{\ell^m}, \sqrt[\ell^m]{\alpha}) = K\left(\zeta_{\ell^m}, \sqrt[\ell^{m-d-s}]{\zeta_{\ell^{h+d+s}}\sqrt[\ell^s]{\beta}}\right)$$

The element $\zeta_{\ell^{h+d+s}}\sqrt[\ell^s]{\beta}$ is contained in $K(\mu_\infty)$, but $\zeta_{\ell^{h+d+s+1}}\sqrt[\ell^{s+1}]{\beta}$ is not, as $\sqrt[\ell^{s+1}]{\beta} \notin K(\mu_\infty)$. This implies that $K(\zeta_{\ell^m}, \sqrt[\ell^m]{\alpha}) \cap K(\mu_\infty)$ is generated over $K(\zeta_m)$ by $\zeta_{\ell^{h+d+s}}\sqrt[\ell^s]{\beta}$.

□

Theorem 1.1.8 implies that, for the primes $\ell \mid \#\mu_K$, we are able compute the ℓ-adelic failure $B(N, \ell^m)$ and the structure of the Galois group of the extension 1.5 for all pairs (m, N) such that $\ell^m \mid N$ by computing them only for the finitely many pairs (m, N) with $m \leqslant t_0$ and $N \mid N_0$. To compute the group structure of the Galois group of the extension for a pair (m, N) we apply Theorem 1.1.5 with the group H_{N,ℓ^m} using the identity (1.6). We can therefore conclude:

Theorem 1.1.10. *Let K be a number field and let G be a finitely generated and torsion free subgroup of $K^\times$. Then the structure of the Galois group (and in particular of the degree) of the Kummer extension $K(\zeta_N, \sqrt[n]{G})/K(\zeta_N)$ can be computed for all positive integers n, N with $n \mid N$ at once.*

Proof. If G has rank r, Theorem 1.1.3 implies that $f_{\ell^m,\ell^m} = \ell^{mr}$ for almost all primes ℓ. The computation of the degree is then an easy consequence of formula (1.4), Theorem 1.1.4 and Theorem 1.1.8. The structure of the Galois group can be determined applying Theorem 1.1.5 to the extensions:

$$\frac{K(\zeta_{\ell^m}, \sqrt[\ell^m]{G})}{K(\zeta_{\ell^m}, \sqrt[\ell^m]{G}) \cap K(\zeta_N)} = \frac{K(\zeta_{\ell^m}, \sqrt[\ell^m]{G})}{K(\zeta_{\ell^m}, \sqrt[\ell^m]{H_{N,\ell^m}})}$$

using the parameters for ℓ-divisibility of G over the field $K(\zeta_{\ell^m}, \sqrt[\ell^m]{H_{N,\ell^m}})$. For almost all primes ℓ, Theorem 1.1.3 and [ACP+25, Remark 13] imply that such group is

isomorphic to $(\mathbb{Z}/\ell^m\mathbb{Z})^r$. Using Theorem 1.1.8 for the remaining primes, we may then reduce to finitely many computations. □

The computation of $f_{N,n}$ can be made very explicit when K is $\mathbb{Q}$ or a quadratic number field (see [PST20] and [HPST21]). More specifically, algorithms can be described to compute $f_{N,n}$ for all n, N with $n \mid N$ at once, where the output is an explicit formula with a finite case distinction. The algorithm for $K = \mathbb{Q}$ was implemented in SageMath (see [Tro19])

1.2 Kummer theory for algebraic groups

Let A be a connected commutative algebraic group over a number field K, and let $\alpha \in A(K)$. Fix an algebraic closure $\overline{K}$ of K. For a positive integer N we denote by $[N]$ the multiplication by N endomorphism of A and by $A[N]$ the subgroup of N-torsion points of $A(\overline{K})$, which is isomorphic to $(\mathbb{Z}/N\mathbb{Z})^b$, where b is the first Betti number of A. We denote by $K(A[N])$ the smallest extension of K on which the N-th torsion points are defined, and by $K(\frac{1}{N}\alpha)$ the smallest extension of K on which all points $\beta \in A(\overline{K})$ such that $N\beta = \alpha$ are defined. Clearly, $K(A[N]) \subseteq K(\frac{1}{N}\alpha)$. The analogue of Kummer extensions defined in the setting of fields at the beginning of this chapter are then field extensions of the form

$$K\left(\frac{1}{N}\alpha\right)/K(A[N]). \tag{1.7}$$

To study such extensions, we rely on Galois representations. We recall the construction of torsion and Kummer representations attached to A/K and α (see for example [LP21] and [LT22]).

For every integer N, we fix a basis $\{t_1^N, \cdots, t_b^N\}$ of $A[N]$ such that $Nt_i^M = t_i^{M/N}$ whenever $N \mid M$. Similarly, we fix a set of points $\{\beta^N\}_{N\in\mathbb{Z}_{>0}} \subseteq A(\overline{K})$ such that $\beta^1 = \alpha$ and $N\beta^M = \beta^{M/N}$ whenever $N \mid M$.

We denote by τ_N the *N-torsion representation*:

$$\tau_N : G_K \to \mathrm{Aut}(A[N])$$

given by the natural $\mathbb{Z}/N\mathbb{Z}$-linear Galois action of G_K on $A[N]$. Since we fixed a basis for $A[N]$, the Galois group of $K(A[N])/K$ can be identified with the image of τ_N, and hence with a subgroup of $\mathrm{GL}_b(\mathbb{Z}/N\mathbb{Z})$.

We denote by κ_N the *N-Kummer representation*:

$$\begin{aligned}\kappa_N : G_{K(A[N])} &\to A[N]\\ \sigma &\mapsto \sigma(\beta^N) - \beta^N.\end{aligned}$$

Notice that this definition does not depend on the choice of β^N, as σ is the identity on $K(A[N])$. Again, the Galois group of $K(\frac{1}{N}\alpha)/K(A[N])$ can be identified with the image of κ_N, and hence with a subgroup of $(\mathbb{Z}/N\mathbb{Z})^b$. It is then clear that the degree of the

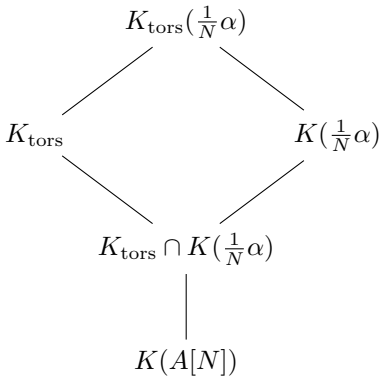
extension (1.7) is bounded by N^b, and hence we may define the *failure of maximality* for the degree of the extension as the integer

$$f_N := \frac{N^b}{\#\operatorname{Im}(\kappa_N)}.$$

We define the adelic Tate module of A, denoted by $T(A)$, as the projective limit over N of the groups $A[N]$, which is isomorphic to $\hat{\mathbb{Z}}^b$. We denote by K_{tors} the compositum of all $K(A[N])$ and by K_{kum} the compositum of all $K(\frac{1}{N}\alpha)$. By taking the inverse limit over N for τ_N and κ_N, we obtain the *adelic torsion representation* $\tau_\infty : G_K \to \operatorname{Aut}(T(A))$ and the *adelic Kummer representation* $\kappa_\infty : G_{K_{\mathrm{tors}}} \to T(A)$.

We can therefore identify the Galois group of the extension K_{tors}/K with $\operatorname{Im}(\tau_\infty)$ and hence with a subgroup of $\mathrm{GL}_b(\hat{\mathbb{Z}})$, and the Galois group of the extension $K_{\mathrm{kum}}/K_{\mathrm{tors}}$ with $\operatorname{Im}(\kappa_\infty)$ and hence with a subgroup of $\hat{\mathbb{Z}}^b$.

Remark 1.2.1 ([LT22, Remark 2.6])**.** The following diagram shows that the Galois group of $K_{\mathrm{tors}}(\frac{1}{N}\alpha)/K_{\mathrm{tors}}$ is isomorphic to the Galois group of $K(\frac{1}{N}\alpha)/K_{\mathrm{tors}} \cap K(\frac{1}{N}\alpha)$, and hence is a subgroup of $\operatorname{Im}(\kappa_N)$.



We have therefore that

$$f_N \Big| \frac{N^b}{\#\operatorname{Gal}\left(K_{\mathrm{tors}}(\frac{1}{N}\alpha)/K_{\mathrm{tors}}\right)}$$

and, if $\operatorname{Im}(\kappa_\infty)$ is an open subgroup of $T(A)$,

$$f_N \mid [T(A) : \operatorname{Im}(\kappa_\infty)]$$

Theorem 1.2.2 ([Ber88, Theorem 1])**.** *Let A be the product of an abelian variety by a torus. Assume that $\alpha \in A(K)$ is such that the set of its multiples $\mathbb{Z}\alpha$ is Zariski dense in A. Then $\operatorname{Im}(\kappa_\infty)$ is open in $T(A)$, and hence f_N is uniformly bounded in N.*

With the extra condition for the $\operatorname{End}_K(A)$-module of geometric torsion points $A(\overline{K})_{\mathrm{tors}}$ to be injective, the following theorem gives a criterion to decide whether $\operatorname{Im}(\kappa_\infty)$ is an open subgroup of $T(A)$, and if this is the case gives a bound for its index.

Theorem 1.2.3 ([Tro23a, Theorem 5.4])**.** *Let A be a connected commutative algebraic group over a number field K. Let $\alpha \in A(K)$ be such that $\mathbb{Z}\alpha$ is Zariski dense in A and let $\Gamma := \{\beta \in A(\overline{K}) \mid \exists n \in \mathbb{Z}_{\geqslant 1} : n\beta \in \langle\alpha\rangle\}$. Assume that $A(\overline{K})_{\mathrm{tors}}$ is an injective $\mathrm{End}_K(A)$-module. Suppose that there exist positive integers d, n, m such that:*

1. *$d(\Gamma \cap A(K)) \subseteq \langle\alpha\rangle + A(K)_{\mathrm{tors}}$;*
2. *$n \cdot H^1(\mathrm{Im}(\tau_\infty), A(\overline{K})_{\mathrm{tors}}) = 0$;*
3. *the subring of $\mathrm{End}(A(\overline{K})_{\mathrm{tors}})$ generated by $\mathrm{Im}(\tau_\infty)$ contains $m \cdot \mathrm{End}(A(\overline{K})_{\mathrm{tors}})$.*

Then $\mathrm{Im}(\kappa_\infty)$ contains $(dnm \cdot \hat{\mathbb{Z}})^b$.

Theorem 1.2.3 can be applied in the case A is an elliptic curve. In this case, explicit values of d, n, m can be found, and hence the bound is explicit:

Corollary 1.2.4 ([Tro23a, Theorem 5.11])**.** *Let A be an elliptic curve over a number field K and let $\alpha \in A(K)$ is given in terms of a basis of $A(K)/A(K)_{\mathrm{tors}}$. Then there exists an effectively computable positive constant c such that the index of $\mathrm{Im}(\kappa_\infty)$ in $T(A)$ divides c. In particular, f_N divides c for any integer N.*