On the degree of Kummer extensions for commutative algebraic groups

Perissinotto, F.

Introduction

Let K be a field for which we fix an algebraic closure $\overline{K}$ and let A be a commutative connected algebraic group over K. Let G be a finitely generated subgroup of $A(K)$. For a positive integer n, we may consider the n-torsion field $K(A[n])$ and the field $K(\frac{1}{n}G)$, which is the minimal field extension of K over which all elements $\beta \in A(\overline{K})$ such that $n\beta \in G$ are defined. The extension $K(\frac{1}{n}G)/K(A[n])$ is a Galois extension called *Kummer extension*, and the aim of this thesis is to study its degree for specific choices of K and A. The following cases will be considered: in Chapter 2, A is the multiplicative group and K is a multiquadratic or a quartic cyclic number field; in Chapter 3, A is any product of one-dimensional algebraic tori over a number field K; in Chapter 4, A is the multiplicative group and K is a finite extension of $\mathbb{Q}_p$ for a prime p; in Chapter 5, A is an abelian variety and K is a number field. Each of these four chapters is the content of a research paper, whose main results involve explicit computations or effective bounds for the degree of Kummer extensions.

If $A = \mathbb{G}_m$ is the multiplicative group, and if n is coprime to the characteristic of K, we are dealing with classical Kummer theory (see for example [Lan02, Sec.VI.8] and [Bir67]), which was first developed by Ernst Kummer in the 19th century in his celebrated work on Fermat's Last Theorem. If K is a field containing the n-th roots of unity for some positive integer n, the main result of Kummer theory (see Theorem 1.0.1) characterizes the abelian extensions of exponent dividing n. These extensions are called Kummer extensions and, if their degree is finite, they are of the form $K(\sqrt[n]{G})/K$ for some finitely generated subgroup G of $K^\times$.

Kummer extensions of number fields, and in particular their degree, have found important applications more recently in the study of certain density problems. Let K be a number field, let $\alpha \in K^\times$ and fix some prime number ℓ. Consider the set of primes $\wp$ of K for which the reduction of α modulo $\wp$ is well-defined and has multiplicative order coprime to ℓ (or more generally the order has a prescribed ℓ-valuation). This set admits natural density, and this density can be expressed in terms of the degrees of cyclotomic-Kummer extensions $K(\zeta_n, \sqrt[n]{\alpha})/K$, where n is some power of ℓ. This problem was first studied in the sixties by Hasse in [Has65, Has66] and recently explicit fomulas for

the density, also in the more general case of reductions of a subgroup G of $K^\times$, were given by Perucca, Debry and Sgobba in their papers [DP16] and [PS19]. This motivated Perucca to delve into the computation of degrees of Kummer extensions for number fields in a more general setting, namely for any extension $K(\zeta_N, \sqrt[n]{G})/K(\zeta_N)$ where n, N are positive integers such that $n \mid N$. Perucca, Sgobba, Tronto and Hörmann proved that these degrees can be explicitly computed at once for all n, N in [PST21], and developed algorithms in the case $K = \mathbb{Q}$ in [PST20] and in the case K is a quadratic number field in [HPST21], whose outputs are formulas for the degrees with a finite case distinctions. In Chapter 2 we extend this result to multiquadratic or quartic cyclic number fields, hence proving the following:

Theorem 1. *Let K be either a multiquadratic or a quartic cyclic number field. Let G be a finitely generated subgroup of $K^\times$. Then there exists an explicit finite procedure to compute at once the degrees*

$$[K(\zeta_N, \sqrt[n]{G}) : K(\zeta_N)]$$

for all positive integers n, N such that n divides N.

One of the latest results on Kummer extensions for number fields [ACP+25] went beyond the study of their degrees with the computation of the size of each cyclic component of the Galois group of $K(\zeta_N, \sqrt[n]{G})/K(\zeta_N)$ for all n, N with n dividing N. Motivated by the results on number field, we extended the problem of the computation of the degree of Kummer extensions also to other fields. If K is a finite field, then such computation is straightforward (see [PP24a]). If K is a p-adic field, namely a finite extension of $\mathbb{Q}_p$, formulas for the degrees can be given explicitly, using similar techniques as the ones used for number fields but with some substantial differences that come from structure of the multiplicative group of p-adic fields. This is the content of Chapter 4, where we prove the following:

Theorem 2. *Let p be a prime and let K be a finite extension of $\mathbb{Q}_p$. Let G be a finitely generated subgroup of $K^\times$ and let n, N be two positive integers such that $n \mid N$. Then there exists an explicit finite procedure to compute the degree $[K(\zeta_N, \sqrt[n]{G}) : K(\zeta_N)]$.*

Unlike number fields, if K is either a p-adic field or a finite field, it is not possible to compute at once all degrees for every n, N such that n divides N, unless we assume the knowledge of the multiplicative order of p in $(\mathbb{Z}/M\mathbb{Z})^\times$ for every integer M coprime to p. In this environment, it is also natural to compare local and global results. We compare Kummer extensions of number fields with the corresponding Kummer extensions of p-adic fields obtained by completion with respect to some non-zero prime ideal of their ring of integers in Chapter 4. We show that there is a positive density of primes of the number field such that the degree of the local Kummer extension is the same as the global one.

For any connected commutative algebraic group A over a number field K we may consider density problems akin to the ones for the multiplicative group. Namely, fix an element $\alpha \in A(K)$ and a prime ℓ. Consider the set of primes $\wp$ of K for which the

reduction of α modulo $\wp$ is well-defined and has order coprime to ℓ. We may investigate whether such set admits a natural density, and, if that is the case, we may want to compute such density. If b is the first Betti number of A, it can be shown that such density exists for every prime ℓ if the integer

$$f_N := \frac{N^b}{[K(\frac{1}{N}\alpha) : K(A[N])]},$$

which we call the *Kummer failure of maximality* for the degree of the Kummer extension, is bounded independently of N. If this condition is satisfied, Lombardo and Perucca [LP21] gave a non explicit formula for the density.

If $A = T$ is an algebraic torus, Bertrand [Ber88], following the work of Ribet [Rib79], proved that f_N is bounded independently of N. The density problem was studied by Perucca in the case T is one-dimensional, giving closed formulas for the density (see [Per17]). As for the multiplicative group, also in this case the density can be expressed in terms of degrees of Kummer extensions where N is a power of a prime ℓ, and Perucca provided explicit formulas for the degrees of such extensions. In Chapter 3 we take this a step further, proving the following two statements:

Theorem 3. *Let T be a finite product of one-dimensional tori defined over a number field K, and fix a finitely generated subgroup G of $T(K)$. If n, N are positive integers such that n divides N, then there is an explicit finite procedure to determine whether T is split over $K(T[N], \frac{1}{n}G)$ and to compute the degree of this field over K and over $K(T[N])$.*

Theorem 4. *Let T be a finite product of one-dimensional tori whose splitting field is a multiquadratic number field K, and fix a finitely generated subgroup G of $T(K)$. There exists an explicit finite procedure to compute at once the degree of $K(T[N], \frac{1}{n}G)/K(T[N])$, for all n, N positive integers such that n divides N.*

Let now A be an abelian variety over a number field K. As mentioned before, the primes $\wp$ of K for which the reductions of elements of $A(K)$ modulo $\wp$ have order coprime to a given prime ℓ admit a natural density if the failure of maximality f_N is uniformely bounded with respect to N. This problem (together with the one already mentioned for algebraic tori) was first studied by Ribet [Rib79], who proved the uniform boundedness of f_N as $N = \ell$ ranges over the prime numbers. He showed that the Kummer failure is trivial for all primes ℓ large enough, assuming a list of 'axioms' which were later proved by Faltings [Fal83] and Serre [Ser86]. The existence of a uniform bound for f_N as N ranges over all positive integers was proven by Bertrand [Ber88]. Hindry [Hin88] later gave a streamlined proof. In the case of elliptic curves, effective bounds for the Kummer failure are known. The work of Javan Peykar [Jav21] deals with CM elliptic curves, while the work of Tronto and Lombardo [LT22] handles the case of non-CM elliptic curves. In both cases, the effective bound is obtained by exploiting certain properties of the endomorphism ring. In his recent paper [Tro23a], Tronto refined these results, setting the foundations for possible similar results for other commutative connected algebraic groups. More precisely, he proves that, under certain conditions on the

endomorphism ring and the geometric torsion of the algebraic group (which are satisfied for elliptic curves), the Kummer failure can be bounded in terms of three independent parameters. In Chapter 5 we show that these three parameters exist for every abelian variety A over a number field and can be effectively bounded in terms of basic invariants of A/K, if A has complex multiplication over $\overline{K}$. We also show how to take care of the assumptions on the endomorphism ring and on the geometric torsion of the algebraic group of A. Ultimately, we are able to obtain bounds that only depend on the abelian variety A, on the field K, and on the divisibility of the point α (respectively, of the subgroup G of $A(K)$) for which we consider the Kummer extension.

One of the results of Chapter 5 is therefore the following:

Theorem 5. *Consider an abelian variety A defined over a number field K and with complex multiplication over $\overline{K}$. Let G be a finitely generated subgroup of $A(K)$. Suppose a set of generators of G is linearly independent over $\mathrm{End}_K(A)$ and is given in terms of a $\mathbb{Z}$-basis for $A(K)/A(K)_{\mathrm{tors}}$. There exists an effective upper bound for f_N, uniform in N and depending only on K, A and G.*

In his work on exponential Diophantine equations in the seventies, Schinzel investigated Galois groups of field extensions obtained by adjoining radicals. One of his results ([Sch77, Theorem 2], see Theorem 1.0.3), which is known as *Schinzel's theorem on radical extensions*, characterizes abelian radical extensions of a field and is an important asset in the study of Kummer extensions of fields. In Chapter 5 we look into possible analogues of Schinzel's theorem in the setting of abelian varieties. This problem lead us to the following, which generalizes a similar result for abelian varieties over $\overline{K}$ contained in a recent paper of Le Fourn, Lombardo and Zywina [LLZ23]:

Theorem 6. *Let A be an abelian variety over a number field K. The following are equivalent:*

(i) The extension $K(A[n])/K$ is abelian for every positive integer n.

(ii) The variety A is K-isogenous to a product of simple abelian varieties with CM over K.

Finally, Chapter 1 introduces Kummer theory, providing results ranging from standard theorems in the field to more advanced ones which are preparatory for the following chapters of this thesis. In particular, we will define for any field K and any prime ℓ the ℓ-adic and ℓ-adelic failures of maximality of the degree of a Kummer extension and, if K is a number field, we will define the parameters of ℓ-divisibility of a subgroup G of $K^\times$. These notions will be essential for Chapters 2, 3 and 4. Moreover, for any connected commutative algebraic group A over a number field K, we define the adelic torsion representation and the adelic Kummer representation, and we recall the theorem by Tronto which is the starting point of Chapter 5.