Kummer theory for commutative algebraic groups

Tronto, S.

Introduction

This thesis consists of four research articles that treat different aspects of *Kummer theory for commutative algebraic groups*, with particular emphasis on explicit and effective results. To understand the motivation behind the study of this topic and what we are trying to achieve, we have to take a step back and see which aspects of classical Kummer theory we are trying to generalize to algebraic groups.

Kummer theory

If n is a positive integer and K is a field of characteristic coprime to n we may consider, for any non-zero $\alpha \in K$, the *set* $\sqrt[n]{\alpha}$ of all elements β in a fixed algebraic closure $\overline{K}$ of K such that $\beta^n = \alpha$. In other words, $\sqrt[n]{\alpha}$ is the set of all n-th roots of α. Given any n-th root β_0 of α, all the others are of the form $\zeta\beta_0$ for some n-th root of unity $\zeta \in \overline{K}$, that is an element such that $\zeta^n = 1$. The field generated over K by all n-th roots of α is a Galois extension of K which contains the n-th *cyclotomic field*, that is the field generated over K by all n-th roots of unity. This remains true if we replace α by a finitely generated subgroup A of the multiplicative group $K^\times$, and we consider the set $\sqrt[n]{A} = \{\beta \in \overline{K} \mid \beta^n \in A\}$. Roughly speaking, classical Kummer theory is the study of this kind of field extensions.

The most classical result in Kummer theory is the classification of the abelian extensions of exponent dividing n of a field K which contains all n-th roots of unity and whose characteristic does not divide n. Indeed, a bijection between the set of such extensions, contained in a fixed algebraic closure $\overline{K}$, and the set of subgroups of $K^\times$ that contain $(K^\times)^n$ is obtained by mapping L to $K^\times \cap (L^\times)^n$, see for example [Lan02, Theorem VI.8.2].

Kummer theory has interesting applications in studying certain *density problems*: if α is a non-zero element of a number field K, then the density of primes $\mathfrak{p}$ of K such that the multiplicative order of α modulo $\mathfrak{p}$ is coprime to some fixed prime ℓ, or has a prescribed ℓ-adic valuation, can be expressed in terms of the degrees of the cyclotomic-Kummer extensions $K(\zeta_{\ell^n}, \sqrt[\ell^n]{\alpha})$ for all $n > 0$, where ζ_{ℓ^n}

is a root of unity of order ℓ^n. See [Per15] for the case we have just described and [DP16, PS19] for a generalization to finite rank sugroups of $K^\times$. These problems are closely related to Artin's primitive root conjecture, as explained for example in [Mor12].

Computing the degrees of infinitely many field extensions might seem an arduous task. However, the following is known (for a direct proof, see [PS19, Theorem 1.1]): if A is a subgroup of $K^\times$ of finite rank r, then there is a constant $C > 0$ such that for every positive integer n the ratio between n^r and the degree $[K(\sqrt[n]{A}) : K(\zeta_n)]$ divides C. This result can be made effective, see [PST20a, Theorem 1.2], and the results of [PST20b] provide, for the case $K = \mathbb{Q}$, an algorithm whose output is a finite formula for these degrees. This algorithm has been implemented in SageMath, see [Tro19].

Algebraic groups

So far we have only discussed Kummer theory in the classical sense, but these concepts can be generalized as follows. Let K be a field, say for simplicity of characteristic zero, fix an algebraic closure $\overline{K}$ of K and let G be a commutative algebraic group over K. If S is a subset of $G(\overline{K})$, the *field extension of K generated by S* is the subfield of $\overline{K}$ obtained by adjoining to K the coordinates of the points of S. More precisely, identifying every x in S with a morphism of schemes $\operatorname{spec} \overline{K} \to \operatorname{spec} K(x)$, we have a collection of morphisms $K(x) \to \overline{K}$ as x varies in S, and the compositum of the images of these morphisms is by definition $K(S)$.

Let now $A \subseteq G(K)$ be a finitely generated subgroup. For any positive integer n we may consider the subset $n^{-1}A = \{P \in G(\overline{K}) \mid nP \in A\}$. Extensions of K of the form $K(n^{-1}A)$ are the object of study of *Kummer theory for commutative algebraic groups*. As one can see by taking $G = \mathbb{G}_m$, the multiplicative group over K, this theory is a direct generalization of classical Kummer theory. Even in this generality, Kummer extensions have many of the interesting properties of their classical counterparts. For example $K(n^{-1}A)$ is a Galois extension of K that contains the *n-torsion field* of G, that is the field extension of K generated by all n-torsion points of $G(\overline{K})$, and it is Galois and abelian over this field. Torsion fields are the direct generalization of cyclotomic fields, and many results on Kummer extensions can be deduced from properties of these fields.

If K is a number field, the density problem mentioned above can be stated *mutatis mutandis* in this more general context, and it is still related to the degrees of Kummer extensions. See [Pin04] for a discussion in the case of abelian varieties and [Per08, Per11] for the product of an abelian variety and a torus. This motivates the study of the degrees of Kummer extensions in the general context. In his foundational paper [Rib79], Ribet proved the following result: if

G is the product of an abelian variety and a torus and $A \subseteq G(K)$ is a free $\mathbb{Z}$-module of rank r with a basis over $\mathbb{Z}$ of points linearly independent over $\mathrm{End}_K(G)$, there exists a positive integer C such that the ratio between n^{rs} and the degree $[K(n^{-1}A) : K(G[n])]$ divides C for every positive integer n. Here s is the unique positive integer such that $G(\overline{K})[n] \cong (\mathbb{Z}/n\mathbb{Z})^s$ for every $n > 1$. See also [Ber88, Théorème 5.2] and [Hin88, Lemme 14]. The papers collected in this thesis are devoted to making this result more effective, trying to express the constant C in terms of known quantities related to the torsion fields of G.

Effective results for elliptic curves

The first two papers, written in collaboration with Lombardo, focus on the case of elliptic curves. Assume that G is an elliptic curve over a number field K and fix an algebraic closure $\overline{K}$ of K. Fix moreover a point $\alpha \in G(K)$. In [JR10] Jones and Rouse proved that for every prime ℓ, under some assumption on α and with a small exception for the prime 2, the surjectivity of the ℓ-adic Galois representation associated with G implies the maximality of the Kummer extensions $K(n^{-1}\alpha)$ over $K(G[n])$ if n is a power of ℓ. See [JR10, Theorem 5.2] for the non-CM case and [JR10, Theorem 5.8] for the CM case. Two questions, suggested by Perucca, arose: If the Galois representation is not surjective, can we describe, or at least bound, the failure of maximality of the Kummer extensions in terms of the failure of maximality of the Galois representations? Can these results be generalized to the case where n is any positive integer?

The first paper presented here [Chapter 1] aims at answering these questions. The main theorem [Chapter 1, Theorem 1.1] provides a positive answer, but only under the assumption that $\mathrm{End}_K(G) = \mathbb{Z}$. This theorem is an effective version of the classical result by Ribet in the case of a group G generated by a single point α, and it shows that the constant C mentioned above can be taken to depend only on properties of the *ℓ-adic* representations, for all the different primes ℓ, and other effectively computable quantities associated with G. Examples that demonstrate the inapplicability of these methods to the CM case are provided in [Chapter 1, Section 6]. The second main theorem [Chapter 1, Theorem 1.2] shows that over the field $\mathbb{Q}$ there exists a uniform version of this result under the assumption that the point α is not divisible in $G(\mathbb{Q})/G(\mathbb{Q})_{\mathrm{tors}}$ – that is, that there is no $\beta \in G(\mathbb{Q})$ such that α equals $n\beta + \tau$ for some integer $n > 1$ and some $\tau \in G(\mathbb{Q})_{\mathrm{tors}}$.

The goal of the second paper with Lombardo [Chapter 2] is to make the aforementioned result [Chapter 1, Theorem 1.2] explicit by finding an actual numerical value for the constant C, see [Chapter 2, Theorem 6.5]. These results have been achieved by giving uniform bounds to other interesting quantities related to the Galois representations of G. A notable example of such a quantity are the ex-

ponents of the cohomology groups of $\mathrm{Gal}(\mathbb{Q}(G(\overline{\mathbb{Q}})_{\mathrm{tors}}) \mid \mathbb{Q})$ with coefficients in the torsion subgroups of G, regarded as Galois modules. Bounds for similar quantities have been found independently by Cerchia and Rouse [CR21].

A technical framework for general Kummer theory

Some of the explicit results mentioned above depend on properties of Galois representations that are known in an effective form only for elliptic curves, but the methods used to show that the degrees of Kummer extensions are related to these quantities do not. In the third article reported here [Chapter 3] this is made clear by conceptualizing the theoretical background in a framework that is applicable to any commutative algebraic group over K that satisfies $\mathrm{End}_K(G) = \mathbb{Z}$. The methods used in this work are inspired by results of Palenstijn [Pal04, Pal14] and by discussions with Lenstra and Stevenhagen. As an application, the results of [Chapter 1] and [Chapter 2] are extended to groups A of rank higher than 1.

So far we have not yet successfully tackled the case when the endomorphism ring of G is larger than $\mathbb{Z}$, and it seems that our methods need a substantial refinement to be applied in that case. In his thesis [JP21], Javan Peykar addresses this problem in the case of elliptic curves with complex multiplication by taking $A \subseteq G(K)$ to be an $\mathrm{End}_K(G)$-module, and considering the modules of "division points" by a *Steinitz ideal*. Even if with some technical limitation, this method is very successful.

Motivated by this approach, the last paper in this thesis [Chapter 4] is mostly devoted to the study of purely algebraic properties of division modules over general rings. The Steinitz ideals used by Javan Peykar are replaced by *ideal filters*, and a generalization of the classical notion of injectivity, which to the author's knowledge is new, is provided. A notion of (J, T)-*extension*, where J is a fixed ideal filter and T a suitable R-module, generalizes the modules of division points. The properties of these objects are then studied with a category-theoretical point of view before generalizing some results on their automorphism groups that have appeared in the less general settings of [Pal04], [Pal14] and [JP21].

This long digression in commutative algebra bears in the end its fruits: the theory so constructed, which generalizes that of [Chapter 3], is finally applied to unify and generalize the results of [Chapter 1] and [JP21], showing that the two apparently different approaches are actually just different realizations of a more general theory. The degree of generality used in this paper opens the door to applications to higher-dimensional abelian varieties and other classes of commutative algebraic groups.