Points de petite hauteur, entre algèbre, arithmétique et géométrie

Sara Checcoli

Mémoire d'Habilitation à diriger des recherches

Présenté par
SARA CHECCOLI

POINTS DE PETITE HAUTEUR, ENTRE ALGÈBRE, ARITHMÉTIQUE ET GÉOMÉTRIE

---

soutenue le 17 mai 2023 devant le jury composé de :

Francesco AMOROSO	Université de Caen	Rapporteur
Yuri BILU	Université de Bordeaux	Rapporteur
Sinnou DAVID	Sorbonne Université	Examinateur
Philipp HABEGGER	Universität Basel	Rapporteur
Gaël RÉMOND	CNRS, Université Grenoble-Alpes	Examinateur
Tanguy RIVOAL	CNRS, Université Grenoble-Alpes	Examinateur
Lea TERRACINI	Università degli studi di Torino	Examinatrice

REMERCIEMENTS

Je tiens tout d'abord à remercier Francesco Amoroso, Yuri Bilu et Philipp Habegger d'avoir accepté d'être les rapporteurs de mon mémoire et d'être membres de mon jury d'habilitation. C'est un honneur que ces mathématiciens qui m'ont tant inspiré aient porté un tel intérêt à mes travaux. Je remercie Francesco pour son soutien et ses conseils qui ont été fondamentaux pour le début de ma carrière en France. Yuri est pour moi une personne de référence depuis mes études en Master Algant, et son encouragement constant et enthousiaste a été très important pour moi. Philipp est une figure très active dans notre communauté mathématique et je le remercie pour son investissement ainsi que pour m'avoir donné l'opportunité de participer au semestre *Diophantine geometry* au MSRI, qui a été très bénéfique pour mes recherches.

Je souhaite également remercier très chaleureusement tous les autres membres du jury. Merci à Sinnou David pour nos conversations mathématiques et son intérêt pour mon travail. Merci beaucoup à Lea Terracini, avec qui j'espère pouvoir partager son amour des mathématiques et son énergie pendant encore longtemps. Je remercie Gaël Rémond d'avoir accepté de faire partie de ce jury, c'est une chance de l'avoir comme collègue et de pouvoir échanger avec lui. Enfin, je remercie Tanguy Rivoal qui, depuis mon arrivée à Grenoble, a été un point de repère professionnel et un ami précieux. Je le remercie pour son soutien sans faille et sa présence lorsque j'en ai eu besoin.

Dans l'imaginaire collectif, le travail du mathématicien est considéré comme un travail solitaire et un peu asceptique des relations humaines. Cela ne reflète en rien mon point de vue ni mon expérience. Au cours de ces années, j'ai eu la chance de collaborer avec de nombreuses personnes, je les remercie toutes pour leur générosité et leur partage mathématique. Grâce à elles, j'ai appris beaucoup de choses et j'ai grandi professionnellement et humainement. Ce mémoire ne serait pas le même sans elles.

Je tiens aussi à remercier toutes les institutions où j'ai travaillé depuis la fin de ma thèse et en particulier l'Institut Fourier qui m'a accueillie pendant près de 10 ans. Je souhaite remercier mes collègues qui ont rendu cet endroit de travail si agréable, humain et bienveillant. Merci à eux et elles de partager avec moi des mathématiques, des repas, de la musique, des conversations serieuses et philosophiques sur la vie et de bonnes bières.

Je remercie aussi énormément toute l'équipe administrative de l'Institut Fourier pour leur aide, leur patience et leur efficacité. Sans elle, mon travail ne pourrait pas se faire dans de si bonnes conditions.

J'ai la chance d'avoir plusieurs familles dans le monde, celle de Bologne où je suis née, mes pinguines, celle de Grenoble avec Giorgio et mes galeux et celle de Barbières. Je les remercie toutes pour leur amour et leur soutien au quotidien. Merci à Gaël d'être rentré dans ma vie (elle est tellement plus cool depuis) et d'y apporter tellement de joie et de passion. Enfin merci à mon Artu, merci de m'épater tous les jours, et de m'aimer "come l'universo osservabile. E i buchi neri".

INTRODUCTION

Dans ce mémoire, je présente les recherches que j'ai menées au cours des dix dernières années, depuis ma thèse jusqu'à aujourd'hui, sur certains problèmes en géométrie diophantienne.

Cette dernière est définie classiquement comme l'étude des solutions, en entiers ou rationnels, des systèmes d'équations polynomiales en utilisant des techniques et des outils issus de la géométrie algébrique. Plus précisément, à chaque système on associe un objet géométrique, la variété donnée par le lieu de ses zéros; on veut alors comprendre comment l'ensemble des solutions du système varie en fonction des propriétés géométriques de la variété.

L'objectif ultime est de décrire le plus explicitement possible cet ensemble. On veut savoir d'abord s'il est vide ou pas, et, le cas écheant, s'il est fini ou pas. S'il est fini on cherche à déterminer explicitement tous ses éléments, s'il est infini on se demande si on peut donner une formule pour les décrire ou comment ils sont distribués sur la variété.

Un outil très puissant dans ce cadre est la théorie des hauteurs, initiée par Weil. La hauteur peut être définie de nombreuses façons différentes, selon le contexte, mais le dénominateur commun est qu'il s'agit d'une mesure de la complexité arithmétique d'un objet dotée d'une propriété de finitude, c'est-à-dire qu'il existe un nombre fini d'objets de hauteur bornée.

Ce mémoire décrit mes contributions sur diverses questions concernant, de près ou de loin et dans des cadres différents, l'étude des points de petite hauteur.

Cette ligne de recherche a probablement été inaugurée dans les années 1930 par les travaux sur la mesure de Mahler d'un polynôme, qui donne des informations sur comment ses racines se distribuent autour du cercle unité. La hauteur (logarithmique de Weil) d'un nombre algébrique α peut être définie alors comme le rapport entre le logarithme de la mesure de Mahler du polynôme minimale de α et le degré de α.

Cette hauteur satisfait le théorème de finitude Northcott, qui affirme que tout ensemble de nombres algébriques ayant degré et hauteur bornés est fini, et une conjecture célèbre et toujours ouverte, issue d'une question de Lehmer, prévoit que le produit entre la hauteur d'un nombre algébrique et son degré ne peut être arbitrairement petit, à moins qu'il ne soit nul.

Il est naturel de se demander s'il existe des ensembles de nombres algébriques pour lesquels on peut *faire mieux* que le théorème de Northcott et la conjecture de Lehmer, c'est-à-dire pour lesquels les énoncés ci-dessus sont valables sans conditions sur le degré. De tels ensembles sont précisément ceux qui satisfont les propriétés de Northcott (N) et de Bogomolov (B) introduites par Bombieri et Zannier.

Plus précisement, la propriété (N) caractérise les extensions des rationnels contenant un nombre fini d'éléments de hauteur bornée tandis que la propriété (B) est satisfaite par les extensions dans lesquelles la hauteur de chaque élément, lorsqu'elle est non nulle, est limitée inférieurement par une constante absolue positive. Les deux propriétés sont valables pour les corps de nombres et un problème intéressant, bien que généralement difficile, est de décider de leur validité pour une extension infinie donnée des rationnels.

Parmi leurs premiers résultats sur ce sujet, Bombieri et Zannier ont montré que, pour un corps de nombres algébriques, les propriétés (N) et (B) sont impliquées par certaines propriétés locales du corps. Cela a été une motivation à l'étude, indépendante, de certaines propriétés locales des extensions galoisiennes des corps de nombres.

Le Chapitre 1 de ce manuscrit présente mes recherches, commencées pendant la thèse, sur ce dernier sujet. Après avoir introduit le problème et les motivations, je décris les résultats que j'ai obtenus, seule ou en collaboration avec U. Zannier et P. Dèbes. En particulier, on donne une caractérisation des extensions galoisiennes d'un corps de nombres ayant leurs degrés locaux uniformément bornés, uniquement en terme de leur groupe de Galois. On montre ensuite que la limitation (non uniforme) des degrés locaux n'est pas équivalente à une condition sur le groupe de Galois de l'extension. On discute également de certaines questions analogues dans le cadre des corps de fonctions. Nos principaux résultats dans ce contexte sont des théorèmes de type Chebotarev pour des extensions galoisiennes de corps de fonctions, finies ou infinies, sur divers corps de base.

Dans le Chapitre 2 de ce mémoire, je décris les résultats que j'ai obtenus, en collaboration avec M. Widmer et A. Fehm, sur les propriétés (N) et (B). En particulier, on étudie de nouveaux exemples de corps de nombres algébriques satisfaisant ces propriétés et, aussi en lien avec les résultats du Chapitre 1, comment, pour les extensions galoisiennes infinies des corps de nombres, ces propriétés sont liées à la structure de leur groupe de Galois et à certaines propriétés locales.

L'étude des points de petite hauteur, et les notions qui s'y rapportent, ont évolué au fil des décennies, prenant progressivement un caractère beaucoup plus géométrique.

Par exemple, sur une variété abélienne G, nous pouvons considérer la hauteur de Néron-Tate d'un point : cela fournit encore une mesure de la complexité du point, les points les plus "simples" étant les points de torsion de G.

Dans ce contexte, on dispose de plusieurs résultats célèbres qui illustrent bien l'idée générale selon laquelle, pour une variété, la géométrie régit l'arithmétique. Par exemple, la conjecture de Manin-Mumford, demontrée par Raynaud, prédit que dans une sous-variété X de G les points "simples" sont en général "rares" (i.e. non-denses), à

moins que la variété n'ait une forme "simple" aussi. Plus généralement, la conjecture de Bogomolov, demontrée grâce aux travaux de Ullmo et Zhang, assure que les petits points sur X continuent d'être rares à moins que X n'ait une structure précise.

Ces résultats, et bien d'autres, sont aujourd'hui considérés comme des cas particuliers de conjectures plus générales de la théorie des *intersections improbables* (unlikely intersections), un terme forgé par Bombieri, Masser et Zannier.

La philosophie qui sous-tend cette terminologie est que deux variétés X et Y dans un espace G ont peu de chances de se croiser si $\dim X + \dim Y < \dim G$.

Plus précisément, le type de résultats que l'on souhaite prouver est que, si X est fixée et Y varie dans une famille dénombrable $\mathscr{F}$ de sous-variétés de G de dimension inférieure à $\dim G - \dim X$ et ayant une certaine propriété *spéciale*, alors $X \cap Y$ devrait être vide pour la plupart des $Y \in \mathscr{F}$, à moins que X soit également *spéciale* dans un certain sens.

Le Chapitre 3 porte sur mes recherches dans ce contexte quand G est une variété abélienne. Après une introduction sur l'état de l'art dans ce domaine très actif, je décris les résultats que j'ai obtenus en collaboration avec F. Veneziano et E. Viada, prouvant, notamment, des cas particuliers de certaines conjectures dues à Bombieri, Masser, Zannier et à Zilber et quelques cas de la conjecture explicite de Mordell sur la détermination des points rationnels d'une courbe de genre au moins 2.

Dans le Chapitre 4, je présente mes résultats en collaboration avec J. Roques sur l'arithmétique des fonctions de Mahler, qui sont des séries de puissances à coefficients algébriques satisfaisant un type particulier d'équation fonctionnelle. Nous montrons, dans certains cas, comment certaines propriétés arithmétiques de ces fonctions se reflètent sur l'équation fonctionnelle. Il s'agit d'un sujet qui reste un peu périphérique par rapport à mes principaux centres de recherche et sur lequel j'ai été moins active que sur d'autres, mais qui est au centre d'un nouveau projet de recherche.

Chaque chapitre, que j'ai essayé de rendre aussi indépendant que possible des autres, commence par une introduction sur le sujet traité qui comprend les définitions les plus importantes. Elle est suivie de sections décrivant mes travaux, regroupés par thèmes plus spécifiques, et d'une dernière section dans laquelle je présente quelques pistes de recherche, dont certaines peuvent convenir à un début de projet de thèse de doctorat.

Une bibliographie commune se trouve à la fin de ce manuscrit.

LISTE DES ARTICLES PRÉSENTÉS

Travaux de thèse :

[CZ11] «On fields of algebraic numbers with bounded local degrees»
(with U. ZANNIER) *Comptes Rendus Mathématique*, Volume 349, Issue 1, 11-14 (2011).

[Che13] «Fields of algebraic numbers with bounded local degrees and their properties»
Transactions of the American Mathematical Society, Vol. 365, no. 4, 2223-2240 (2013).

Travaux après thèse :

[CW13] «On the Northcott property and other properties related to polynomial mappings»
(with M. WIDMER), *Mathematical Proceedings of Cambridge Philosophical Society*, 155, 1-12 (2013).

[CVV12] «A sharp Bogomolov-type bound »
(with F. VENEZIANO AND E. VIADA), *New York Journal of Mathematics*, 18, 891-910 (2012).

[CVV14] «On torsion anomalous intersections »
(with F. VENEZIANO AND E. VIADA), *Rendiconti Lincei - Matematica e Applicazioni*, Vol. 25, Issue 1, 1-36 (2014).

[CV14] «On the Torsion Anomalous Conjecture in CM abelian varieties »
(with E. VIADA), *Pacific Journal of Mathematics*, 271-2, 321-354 (2014).

[CD16] «Tchebotarev theorems for function fields»
(with P. DÈBES) *Journal of Algebra*, Volume 446, 346-372 (2016).

[CVV17] «On the explicit torsion anomalous conjecture »
(with F. VENEZIANO AND E. VIADA), *Transactions of the American Mathematical Society*, Vol. 369, no. 9, 6465–6491 (2017).

[CR17] «On certain arithmetic properties of Mahler functions. »
(with J. ROQUES), *Israel Journal of Mathematics*, Volume 228, Issue 2, 801–833 (2018).

[CVV19] «The explicit Mordell Conjecture for families of curves »
(with F. VENEZIANO AND E. VIADA), *Forum of Mathematics, Sigma,* Vol. 7, e31 (2019). With an appendix by M. Stoll.

[Che19] «A note on Galois groups and local degrees»
Manuscripta Mathematica, 159 (1), 1-12 (2019).

[CF21] «On the Northcott property and local degrees»
(with A. FEHM), *Proceedings of the American Mathematical Society*, 149, 2403-2414 (2021).

[CF22] «Constructing totally p-adic numbers of small height»
(with A. FEHM), *International Journal of Number Theory*, Vol.18, No.3, 501-514 (2022).

Contents

CHAPTER 1

LOCAL PROPERTIES OF GALOIS EXTENSIONS

The research presented in this chapter, part of which was done in my PhD thesis, investigates the relations between certain properties of an infinite Galois extension of the rationals. After introducing the problem and the motivations, which come from some results concerning points of small height, I describe the contributions made by my coauthors and myself on the topic. In particular, we give a characterization of Galois extensions of the rationals enjoying some strong local property, i.e. having uniformly bounded local degrees, solely in terms of their Galois group. We then show that the (non uniform) boundedness of the local degrees alone is not equivalent to any group-theoretical condition. We also discuss some questions in the function field setting. Our main results in this context are Chebotarev type theorems for Galois function field extensions, finite or infinite, over various base fields. The chapter ends with the description of some research leads.

List of articles presented in this chapter

[CZ11] «On fields of algebraic numbers with bounded local degrees»
(with U. ZANNIER) *Comptes Rendus Mathématique*, Volume 349, Issue 1, 11-14 (2011).

[Che13] «Fields of algebraic numbers with bounded local degrees and their properties»
Transactions of the American Mathematical Society, Vol. 365, no. 4, 2223-2240 (2013).

[Che19] «A note on Galois groups and local degrees»
Manuscripta Mathematica, 159 (1), 1-12 (2019).

[CD16] «Tchebotarev theorems for function fields»
(with P. DÈBES) *Journal of Algebra*, Volume 446, 346-372 (2016).

1.1. Introduction

During my thesis and in the years that followed I studied the relations between some properties which can occur for an infinite Galois extension of the rationals. Throughout this chapter all the fields are considered embedded in a fixed algebraic closure of $\mathbb{Q}$, denoted $\overline{\mathbb{Q}}$.

A central feature we study is the boundedness of the local degrees of the extension, first considered by Bombieri and Zannier in [BZ01]

Definition. *We say that a (possibly infinite) Galois extension $L/\mathbb{Q}$ has* bounded local degrees at a prime p *if there exists a constant b_p such that L can be embedded in a finite extension of $\mathbb{Q}_p$ of degree at most b_p. Equivalently, if for every valuation v_p of L which extends the p-adic one, the completion of L with respect to v_p is a finite extension of $\mathbb{Q}_p$ of degree bounded by b_p. Moreover, we say that $L/\mathbb{Q}$ has* uniformly bounded local degrees *if for all p we have $b_p \leq b$, where b is a constant depending only on L.*

Clearly, if $L/\mathbb{Q}$ is finite it has local degrees uniformly bounded by $[L:\mathbb{Q}]$. A non-trivial example of extension with uniformly bounded local degrees, provided in [BZ01], is the field $K^{(d)}$, defined as the compositum of all extensions of degree at most d of a number field K. For $d \geq 2$, this is an infinite Galois extension of K. Here the uniform boundedness of the local degrees comes from the fact that, for every p, $K^{(d)}$ can be embedded in the compositum of all extensions of $\mathbb{Q}_p$ of degree at most $d[K:\mathbb{Q}]$ and the number of such fields is bounded independently of p (see [BZ01, Proposition 1]).

The results presented in this chapter stemmed from the seminal paper [BZ01] of Bombieri and Zannier, defining and studying certain properties concerning points of small (absolute logarithmic Weil) height in infinite extensions of $\mathbb{Q}$. Although these properties are discussed in detail in Chapter 2 of this manuscript, we briefly recall here some definition and results concerning them that motivate our work.

Following [BZ01], we say that an infinite algebraic extension $L/\mathbb{Q}$ has the *Northcott property (N)* if it contains finitely many elements of bounded height.

Clearly, by Northcott's theorem, the set of all algebraic numbers of degree bounded by some constant satisfies property (N) and one of the problems investigated in [BZ01] is whether this is still true for the smallest field containing such a set, i.e. for fields of the form $K^{(d)}$. Even though this question remains open, among other results, they prove that property (N) holds for the field $K^{(d)}_{ab}$, which is the maximal subextension of $K^{(d)}$ being abelian over K. In this proof a crucial role is played by the uniform boundedness of the local degrees of $K^{(d)}$.

This fact and the considerations made in [BZ01] lead to the following questions, which may be interesting in their own right:

(Q1) Is every infinite algebraic extension of a number field K with uniformly bounded local degrees contained in $K^{(d)}$ for some positive integer d?

(Q2) More generally, for a Galois extension of K are there properties which are equivalent to having uniformly bounded local degrees?

(Q3) An important ingredient in the proof of property (N) for $K_{ab}^{(d)}$ is the fact that all its finite subextensions can be generated by algebraic elements of degree bounded solely in terms of d and $[K:\mathbb{Q}]$. Does the same phenomenon occur for $K^{(d)}$?

1.2. Description of the results

I. Extensions with uniformly bounded local degrees (description of the articles [CZ11] and [Che13])

The results presented in this section were obtained during my PhD and constitute my PhD thesis.

In [CZ11], in collaboration with Umberto Zannier, and [Che13] we address all the above questions. We remark that, even though the main results in there are stated only for $K = \mathbb{Q}$, all the proofs can be adapted easily in the general case, as discussed below.

In [CZ11] we completely answer question (Q1). More precisely, as recalled in the previous section, it is easy to see that if L is a subfield of $\mathbb{Q}^{(d)}$, then L has uniformly bounded local degrees at all primes and we adress the question whether the converse holds true. Our main result is the following:

Theorem 1 ([CZ11, Proposition 2.1 & Theorem 1.1])**.** *Let $L/\mathbb{Q}$ be an abelian extension. Then L has uniformly bounded local degrees if and only if $L \subseteq \mathbb{Q}^{(d)}$ for some positive integer d. However, there exists infinitely many non-abelian Galois extensions of $\mathbb{Q}$ having uniformly bounded local degrees which are not contained in $\mathbb{Q}^{(d)}$ for any positive integer d.*

The proof of the first part of the theorem uses the remark (see [CZ11, Remark 2]) that if an infinite Galois extension of a number field K has uniformly bounded local degrees, then the group $\mathrm{Gal}(L/K)$ must have finite exponent, a fact that follows easily by Chebotarev's density theorem and the proof of [CZ11, Proposition 2.1] adapts straightforward to any abelian extension of a number field K.

To prove the second part, we construct our extensions as composita of families of finite Galois extensions as it follows. We fix two odd primes p and q, with $q \equiv 1 \mod p$. For every m, let $G_m = E_m \rtimes W_m$ where E_m is the extraspecial group of order p^{2m+1} and exponent p and W_m is a faithful and absolutely irreducible E_m-module of dimension p^m over $\mathbb{F}_q$, the semidirect product being taken via the natural action of E_m on its module (see [DH92, Ch.A, §20 and Ch.B, §9] for the definition of extraspecial groups and details). By Shafarevich's theorem (see for instance [NSW00, Chapter 9, §5 and §6]) every finite solvable group can be realised as Galois groups over $\mathbb{Q}$. Hence there exists a Galois extension $L_m/\mathbb{Q}$ having G_m as Galois group (and actually, by Galois theory, one can find infinitely many such realisations pairwise linearly disjoint over $\mathbb{Q}$).

The main feature of the groups G_m is they have W_m as a *big* minimal normal subgroup. This condition is used to ensure that the compositum L of the fields L_m is not contained in $\mathbb{Q}^{(d)}$ (see [CZ11, Propositions 3.1 and 3.2]). The family $(G_m)_m$ has also uniformly bounded exponents. This is necessary, in view of the above considerations,

and it is used to prove that the constructed field L has uniformly bounded local degrees at all primes except those which ramify wildly. A bound for the local degrees at such primes is obtained using another result of Shafarevich on the number of generators of p-extensions of p-adic fields (see [Sha56]). All these results are valid for extensions of number fields K and the proof adapts easily.

In [Che13] we consider the more general Question (Q2) about possible characterizations of Galois extensions with uniformly bounded local degrees. In particular we show that the finiteness of the exponent of the Galois group is not only a necessary, but also a sufficient condition for the uniform boundedness of the local degrees. We also consider Question (Q3), that we answer in the negative, showing that the structure of $\mathbb{Q}^{(d)}$ reveals some unexpected sides. Our main result is the following:

Theorem 2 ([Che13, Theorem 1])**.** *For an infinite Galois extension $L/\mathbb{Q}$ the following properties are equivalent:*

(1) L has uniformly bounded local degrees at every prime;
(2) L has uniformly bounded local degrees at almost every prime;
(3) $Gal(L/\mathbb{Q})$ has finite exponent.

Moreover, if $L/\mathbb{Q}$ is abelian, the following are also equivalent:

(a) L has uniformly bounded local degrees;
(b) L is contained in $\mathbb{Q}^{(d)}$ for some positive integer d;
(c) every number field contained in L can be generated by elements of uniformly bounded degree.

However, in general, we have that (c) implies (b) which implies (a) and none of the inverse implications holds.

The implication (1) $\Rightarrow$ (3) was already in [CZ11, Remark 2], as recalled above, but that proof actually gives the implication (2) $\Rightarrow$ (3), so the novelty here is (3) $\Rightarrow$ (1).

We sketch here the proof of this result. Suppose that $\mathrm{Gal}(L/\mathbb{Q})$ has exponent b. We remark that to prove (1) it is sufficient to show that, for every prime p, for any finite Galois extension $F/\mathbb{Q}$ contained in L and for any place v of F above p, the p-adic completion $F_v/\mathbb{Q}_p$ has degree bounded solely in terms of b. If p is uramified or just tamely ramified in F, then for all v, the Galois group of $F_v/\mathbb{Q}_p$ is either cyclic or meta-cyclic, so its order is bounded by b^2. If p wildly ramifies in F, the number of generators of the p-part of $\mathrm{Gal}(F_v/\mathbb{Q}_p)$ can be bounded solely in terms of b by a result of Shafarevich already mentioned (see [Sha56]). Then one uses Zelmanov's theorem on the Restricted Burnside Problem (see [Zel97]), which shows that (up to isomorphism) there are only finitely many finite groups having a bounded number of generators and bounded exponent.

The case of abelian extensions was already done in [CZ11]. Here, using local class field theory, we give explicit bounds for the local degrees in some special cases. The non-equivalence of properties (a), (b) and (c), also partly already contained in [CZ11], is based on the same group-theoretical construction with extraspecial groups. Moreover we provide explicit realisations of such groups, using some elementary techniques in inverse Galois theory.

As remarked before, the same strategy adapts to show that Theorem 2 holds more generally when $\mathbb{Q}$ is replaced by a number field K.

II. Extensions with non-uniformly bounded local degrees (description of the article [Che19])

In [BZ01], the authors consider also another property concerning points of small height in infinite extensions, namely the so called Bogomolov property (B): we say that a Galois extension $L/\mathbb{Q}$ has *property (B)* if the height of every element in L is either zero or lower bounded by an absolute positive contant (depending only on L). In particular they prove that such property holds for infinite Galois extensions of $\mathbb{Q}$ having bounded local degrees at at least one prime (see [BZ01, Theorem 2]).

In [ADZ14, Theorem 1.5] Amoroso , David and Zannier prove that property (B) holds more generally for any Galois extension L/K of a number field K such that the subextension fixed by the center of $\mathrm{Gal}(L/K)$ has bounded local degrees at some prime. They also define property (B) for groups (see [ADZ14, Definition 5.5]): a profinite group G has *property (B)* if, for any number field K and for every Galois extension L/K having G as Galois group, the field L has property (B).

With this terminology, the results in [Che13] and [ADZ14] imply that property (B) holds for any group G such that the quotient of G over its center has finite exponent. Indeed, for any realisation of G, the subfield fixed by the center of G will have uniformly bounded local degrees. All known examples of groups with (B) satisfy this property, which is of course stronger than the (non-uniform) boundedness of the local degrees needed in [ADZ14, Theorem 1.5].

Therefore one might ask the following:

(Q4) Is it possible to give a characterization in terms of the Galois groups of Galois extensions of number fields having (possibly non-uniformly) bounded local degrees at some prime?

A positive answer to this question would provide a bigger family of groups with property (B).

In [Che19] we answer Question (Q4) in the negative, showing the following:

Theorem 3 ([Che19, Theorem 1])**.** *Let $\mathscr{S}$ be a set of rational primes. Let K be a number field and let $\mu(K)$ be the group of its roots of unity. Let $G = \prod_{m\geq 1} G_m$ be a direct product of an infinite family of finite groups $(G_m)_m$ with unbounded exponents and suppose that, for every m, the group G_m is one of the following types:*

(1) an abelian group of odd order;
(2) a solvable group of order prime to $|\mu(K)|$;
(3) an iterated semidirect products of abelian groups of order not divisible by the primes in $\mathscr{S}$.

Then G has a realisation over K with bounded local degrees at all primes in $\mathscr{S}$. If moreover the groups G_m's have coprime orders, then G admits also a realisation over K with unbounded local degrees at all primes in $\mathscr{S}$.

The proof of this result is based on the existence of solutions to certain *Grunwald problems*. The Grunwald problem, a strong variant of the inverse Galois problem, asks

the following: given a finite group G, a number field K, a finite set $\mathcal{T}$ of finite places of K and, for every $v \in \mathcal{T}$, a local Galois extension L_v/K_v of Galois group G_v embeddable in G, is there a finite Galois extension L/K of group G having completions isomorphic to L_v at the primes above v, for all $v \in \mathcal{T}$? When the answer is affirmative, we call L a *solution of the Grunwald problem for* $(G, \mathcal{T}, \{G_v\}_{v\in\mathcal{T}})$.

The Grunwald problem is shown to have a positive answer for any choice of possible local extensions, for instance, when G is an abelian group of odd order by the Grunwald-Wang theorem (see[Gru33], [Wan50]), when G is a solvable group of order prime to the order of the group of roots of unity in K (by Neukirch [Neu79]) and when G is an iterated product of abelian groups and the primes below all the places in $\mathcal{T}$ do not divide the order of G (by Demarche, Lucchini Arteche and Neftin [DLAN17]).

A central step in the proof of Theorem 3 is [Che19, Theorem 2] where we prove that a direct product of finite groups G_m can be realised in two ways (with bounded or unbounded local degrees at any fixed set of primes) whenever every *cyclic* Grunwald problem for G_m (i.e. where the local extensions are chosen to be cyclic) has *enough* solutions (i.e. for any given number field, there is at least one solution which is linearly disjoint from it). Theorem 3 then follows from the above mentioned results. Conjecturally (see [Col03, Section 2] and also [DLAN17, Section 2.5]) for every group G, there is a set of *bad* places (containing, for instance, those above primes dividing the order of G) such that if $\mathcal{T}$ is disjoint from this set, then any Grunwald problem for $(G, \mathcal{T})$ has a positive answer. So Theorem 3 should be true for any direct product of finite groups of unbounded exponents, provided that $\mathcal{S}$ does not contain bad primes.

Notice that in the statement of Theorem 3 the set $\mathcal{S}$ is not required to be finite. This implies that there is no group-theoretical condition on $\mathrm{Gal}(L/K)$ which is equivalent to the (non-uniform) boundedness of the local degrees of L/K even at *all* primes, underlying the fact that the uniform boundedness of the local degrees is a very strong condition. Even though without implications on Property (B), it is of some interest to ask to which extent the boundedness of the local degrees at all primes of an extension rigidifies the structure of its Galois group. We show (see [Che19, Remark 4]) that the Galois group of such extensions cannot be torsion free.

While the proof of Theorem 3 does not produce explicit constructions, some more explicit realisations with opposite local behaviour are provided in [Che19, Section3] for direct products of certain families of abelian groups. In [Che19, Proposition 2] we also show that the existence of realisations with bounded local degrees at some prime also occurs for other classes of profinite groups than direct products (namely, iterated semidirect products by finite nilpotent groups, see [Che19, Remark 7] for an explicit example). The proof relies on the existence of solutions to certain embedding problems with nilpotent kernel (see [NSW00, Theorems 9.5.10 and 9.5.11(i)]). This, however, produces extensions with a quite special local structure and this approach seems to be difficult to exploit for more general families of profinite groups.

III. Chebotarev theorems for function fields (description of the article [CD16])

In [CD16], in collaboration with Pierre Dèbes, we consider a function field variant of some of the results obtained in [CZ11], namely that for an infinite Galois extension of a number field K, the uniform boundedness of the local degrees implies the finiteness of the exponent of the Galois group of the extension.

A central ingredient in the proof was the existence part of Chebotarev density theorem for number fields: more precisely, we used the fact that, given a finite Galois extension of number fields F/K of group G, for every $\sigma \in G$ there exists a place v of K and a cyclic unramified local extension F_v/K_v whose Galois group is generated by a conjugate of σ. In [CD16] we introduce a sort of function field analog of this result, namely the *Chebotarev existence property* (see [CD16, Definition 2.5]). Before recalling its definition and describing our results we need to introduce some notation.

Let k be a field, X a smooth projective and geometrically integral k-variety, $k(X)$ its function field and $F/k(X)$ a finite Galois extension of group G. We mostly consider extensions such that F/k is *regular* i.e. such that $F \cap \overline{k} = k$. For every overfield $k \subset K$ and each point $t_0 \in X(K)$ not in the branch locus of the extension $F/k(X)$, the specialization of $F/k(X)$ at t_0 is a Galois extension of K whose Galois group identifies to some subgroup of G (well-defined up to conjugation in G). We say that $F/k(X)$ has the *Chebotarev existence property* if for every $\sigma \in G$, there exists a finite place v of k (possibly trivial), a finite extension K/k_v and a point $t_0 \in X(K)$ such that the specialization $(FK)_{t_0}/K$ is cyclic, unramified and its Galois group is conjugate to the subgroup generated by σ in G.

This definition is clearly modeled upon the situation for extensions of global fields. By the existence part of the Chebotarev density theorem for global fields, every finite regular Galois extension of global fields has the Chebotarev existence property: the case of number fields corresponds to the case where X is a point, while for global fields of positive characteristic, one takes X equal to the projective line (and v the trivial absolute value over the constant field).

A first result of [CD16] (see [CD16, Theorem 3.2 and Corollary 3.7]) provides a wider range of examples where the property holds. As a special case we have the following:

Theorem 4 ([CD16, Theorem 1.1])**.** *Let G be a finite group and let k be either a number field, or a finite field, or a PAC field with cyclic extensions of any degree, or a rational function field $\kappa(x)$ with κ a finite field of order prime to $|G|$. Then any finite Galois extension $F/k(T)$ with F/k regular has the Chebotarev existence property.*

Recall that a field k is *PAC (Pseudo Algebraically Closed)* if every absolutely irreducible variety defined over k has a k-rational point. As discussed in [CD16, §3.1.2], an example of a PAC field satisfying the condition in Theorem 4 is, for instance, $k = \mathbb{Q}^{tr}(i)$, where $\mathbb{Q}^{tr}$ is the field of totally real numbers (i.e. the field obtained by adjoining to $\mathbb{Q}$ all algebraic numbers having all real conjugates).

The main ingredients in our proofs are results by Dèbes and Ghazi [DG12] on a specialization property mixing Hilbert and Grunwald type results, concerning whether a given local Galois extension E/K comes from a specialization of a Galois extension $F/k(X)$.

The definition of the Chebotarev existence property extends to infinite extensions in the following way: an infinite Galois extension $F/k(X)$ has the *Chebotarev existence property* if it is the union of an increasing sequence of finite Galois extensions $F_n/k(X)$ all having the Chebotarev existence property. We remark that if k is finite or PAC, Theorem 4 is valid also for infinite Galois extensions (see [CD16, Remark 3.4]).

We also compare our property to the classical Hilbert specialization property. Recall that a finite Galois extension $F/k(T)$ of group G has the *Hilbert specialization property* if the Galois group of the specialization at t_0 equals G for infinitely many $t_0 \in \mathbb{P}^1(k)$.

Even if it only preserves the local structures, the Chebotarev property still encapsulates a good part of the Hilbert property, which is somehow squeezed between two variants of the Chebotarev property, as shown in [CD16, Proposition 4.6]). In addition, it allows more general base fields and base varieties and it is also defined for infinite extensions.

Recall that a field k is *Hilbertian* if the Hilbert specialization property holds for every finite Galois extension $F/k(T)$. We also say that k is *RG-Hilbertian*, when the Hilbert specialization property occurs for all finite Galois extension $F/k(T)$ with F/k regular. In analogy, we say that a field k is *Chebotarev* if the Chebotarev existence property holds for every finite Galois extension $F/k(T)$ with F/k regular.

If k is a PAC field a classical result (see [FV92, Theorem A]) shows that k is Hilbertian if and only if its absolute Galois group G_k is ω-free i.e. each finite embedding problem for G_k is solvable (see [FJ04, §27.1]), while k is RG-Hilbertian if and only if every finite group occurs as a quotient of G_k (see [FJ04, Theorem B]). In analogy to these results we prove that the property of being Chebotarev can also be read on G_k:

Corollary 5 ([CD16, Proposition 4.4])**.** *Let k be a PAC field with absolute Galois group G_k. Then k is Tchebotarev if and only if every cyclic group is a quotient of some open subgroup of G_k.*

If k is not PAC, the situation is more complex and it is discussed in [CD16, §4.2].

Finally, we investigate the motivating problem for our work i.e. the local-global results for infinite extensions implied by the Chebotarev existence property and we give a function field analog of [CZ11, Remark 2 and Proposition 2.1]. Let again $F/k(X)$ be a Galois extension of Galois group G. By *local specialization degrees* we mean the degrees of the cyclic unramified local specializations of $F/k(X)$.

Theorem 6 ([CD16, Theorem 1.3])**.** *Let $F/k(X)$ be a (possible infinite) Galois extension with the Chebotarev existence property. Then, if the local specialization degrees of $F/k(X)$ are uniformly bounded, the exponent of $G = \mathrm{Gal}(F/k(X))$ is finite. The converse holds too under some standard assumptions on k.*

Moreover, if G is abelian, the uniform boundedness of the local specialization degrees of $F/k(X)$ also implies that there exists an integer $d \geq 1$ such that F is in the compositum of all finite extensions of $k(X)$ of degree at most d.

As discussed in Section 1.2, in the number field case it is proved in [CZ11] that the hypothesis on G being abelian cannot be removed, providing counter-examples. We show that the same conclusion holds in the function field context in the situation where $\dim(X) > 0$ by providing counter-examples based on several group-theoretical constructions.

We finally want to mention that the exact analogue of [Che13, Theorem 1] for infinite Galois extensions of global function fields of positive characteristic p has been studied in [Bau16]. The author shows, in particular, that if the exponent of the Galois group is finite and not divisible by p, then the local degrees are uniformly bounded.

1.3. Some perspectives

(i) More on the structure of $\mathbb{Q}^{(d)}$.

As discussed in Section 1.1, an open and interesting question is whether property (N) holds for all fields of the form $K^{(d)}$ or, more generally, for Galois extensions with uniformly bounded local degrees. A better understanding of such fields is surely an important step towards this problem.

As explained in §1.2, one of the results proved in [CZ11] can be stated by saying that the set of Galois extensions of $\mathbb{Q}$ contained in $\mathbb{Q}^{(d)}$ for some d is strictly contained in the set of Galois extensions of $\mathbb{Q}$ with Galois group of bounded exponent. A natural question would be to understand if there exists a group-theoretical characterization of this proper subset (or of its complement). More precisely, let G be a pro-finite group with bounded exponent. Is there a group-theoretical condition on G equivalent to the fact that every infinite Galois extension of $\mathbb{Q}$ of group G is contained in $\mathbb{Q}^{(d)}$ for some d?

To start with: In [CZ11, Proposition 3.1] the following sufficient condition for not being a subfield of $\mathbb{Q}^{(d)}$ is given: let $(G_m)_m$ be an infinite family of finite groups and suppose that there exists an increasing sequence of integers $(c_m)_m$ such that whenever G_m is isomorphic to a quotient of a subgroup of a direct product of finite groups, then at least one of the factors in the direct product has order bigger than c_m. For each m, let $K_m/\mathbb{Q}$ be a Galois extension of group G_m. Then the compositum of the fields K_m is not contained in $\mathbb{Q}^{(d)}$ for any d.

A first more precise task would be to understand whether this condition is also necessary and whether there are examples of families of groups satisfying this property, other than those constructed using extraspecial groups and their modules as in [CZ11].

(ii) Even more on the structure of $\mathbb{Q}^{(3)}$.

A partial, though important result, would be the proof (or disproof) of property (N) for the simplest infinite non-abelian extension of $\mathbb{Q}$ of such type, namely the field $\mathbb{Q}^{(3)}$, the compositum of all quadratic and cubic extensions of $\mathbb{Q}$.

One feature of $\mathbb{Q}^{(3)}$, studied for instance in [GG14, Corollary 1.2], is the fact the its finite Galois subextensions are generated by elements of uniformly bounded degree (notice that this is not true anymore for $\mathbb{Q}^{(d)}$ with $d \geq 4$).

To start with: One can prove that if $L/\mathbb{Q}$ is finite, Galois and $L \subseteq \mathbb{Q}^{(3)}$, then $\mathrm{Gal}(L/\mathbb{Q})$ is isomorphic to a direct product of finite groups $H_1 \times \ldots \times H_s$ in which every direct factor H_i is either an elementary abelian 2-group, or an elementary abelian 3-group or a generalized dihedral group of the form $(\mathbb{Z}/3\mathbb{Z})^a \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$ with $\mathbb{Z}/2\mathbb{Z}$ acting on $(\mathbb{Z}/3\mathbb{Z})^a$ in the usual way. Exploiting this structure and extracting informations about the ramification in finite subextensions of $\mathbb{Q}^{(3)}$, could be a first step towards a proof of property (N) for such field.

(iii) Another local property linked to property (N).

As it will be discussed in detail in §2.2.II, property (N) is linked to some purely local properties of a field. In particular, as remarked in [BZ01, Remark after Theorem 2] for a (possibly infinite) Galois extension $L/\mathbb{Q}$ with bounded local degrees at a set of rational primes S (possibly infinite) a special role is played by the quantity

$$\beta(L) = \frac{1}{2} \sum_{p \in S} \frac{\log p}{e_p(p^{f_p} + 1)}$$

where e_p and f_p denote, respectively, the ramification index and the inertial degree of L at p. If $\beta(L)$ is divergent the field L has property (N).

In [BZ01], the authors notice that $\beta(L)$ always diverges when $L/\mathbb{Q}$ is finite and in [CF21] we show the first examples of infinite extensions where this phenomenon also happens. Moreover, our examples are not included in all previously known examples of fields with property (N). Thus the divergence of $\beta(L)$ can be considered as a *new* criterion to detect property (N) for a field and this motivates a better understanding of this quantity attached to a field.

To start with: As shown in [DZ07, Theorem 2.1], property (N) is preserved under finite extensions of fields. A first question to tackle, as also suggested in see [CF21, Remark 2.8], is whether the same happens for the divergence of $\beta(L)$. More precisely, if $L/\mathbb{Q}$ is a Galois extension such that $\beta(L) = \infty$ and if L'/L is finite with $L'/\mathbb{Q}$ Galois, is it true that $\beta(L') = \infty$?

CHAPTER 2

SMALL HEIGHT IN BIG FIELDS: AROUND THE PROPERTIES (N) AND (B)

In this chapter I present the research I have done on certain properties, introduced in [BZ01] by Bombieri and Zannier, on points of small height in infinite algebraic extensions of the rationals. The first is the Northcott property (N) which characterizes those extensions containing finitely many elements of bounded height. The second one, the Bogomolov property (B), is held by extensions in which the height of every element, when non-zero, is lower bounded by a positive absolute constant. Both properties hold for number fields and an interesting though generally hard problem is to decide their validity for a given infinite extension of the rationals. After recalling some basic definitions and discussing the state of the art, I describe the results obtained by my co-authors and myself on the subject. In particular, we study new examples of fields satisfying these properties and how, for infinite Galois extensions of number fields, they relate to the structure of the Galois group and to certain local properties. The chapter ends with the description of some research leads.

List of articles presented in this chapter

[CW13] «On the Northcott property and other properties related to polynomial mappings» (with M. WIDMER), *Mathematical Proceedings of Cambridge Philosophical Society*, 155, 1-12 (2013).

[CF21] «On the Northcott property and local degrees» (with A. FEHM), *Proceedings of the American Mathematical Society*, 149, 2403-2414 (2021).

[CF22] «Constructing totally p-adic numbers of small height» (with A. FEHM), *International Journal of Number Theory*, Vol.18, No.3, 501-514 (2022).

2.1. Introduction

This chapter is about the study of certain properties on the absence of points of small height in infinite extensions of the rationals, namely the properties of Northcott and Bogomolov, introduced by Bombieri and Zannier in [BZ01]. This topic, which initially partially motivated my PhD thesis and on which I have worked with several co-authors in the past years, is currently a central subject in my research.

Let me start with a few brief reminders of the key definitions. Here and throughout the chapter, we will denote by $\overline{\mathbb{Q}}$ a fixed algebraic closure of $\mathbb{Q}$.

Definition. *Let $\alpha \in \overline{\mathbb{Q}}$ and let $p(x) = a(x-\alpha_1)\cdots(x-\alpha_d) \in \mathbb{Z}[x]$ be its minimal polynomial. The* absolute logarithmic Weil height *(or, for short, the* height*) of α is the number*

$$h(\alpha) = \frac{1}{d}\log\left(|a|\prod_{i=1}^{d}\max(1,|\alpha_i|)\right).$$

As can easily be seen from the definition, h is a non-negative function and, by a classical theorem of Kronecker, it takes value zero precisely at zero and at the roots of unity. While this result classifies points of minimal height, many interesting questions remain open concerning points of non-zero small height.

A first important result in this setting is Northcott's theorem, which states that any set of algebraic numbers having bounded degree and bounded height is finite (and, in principle, can be explicitly described). A second inescapable statement is that of Lehmer's conjecture, asserting that if an algebraic number has *small* non-zero height, then it must have *big* degree over $\mathbb{Q}$. More precisely, it states that there is a constant $c > 0$ such that, for any $\alpha \in \overline{\mathbb{Q}}$, the product $h(\alpha)[\mathbb{Q}(\alpha):\mathbb{Q}]$ is either zero or bigger than c. Lehmer's conjecture has been proved to be true for several classes of algebraic numbers, but stands open in general. The best unconditional result is due to Dobrowolski [Dob79], which proves the conjectural bound up to a logarithmic factor.

One can now ask whether there are sets of algebraic numbers for which one can *do better* than Northcott's theorem and Lehmer's conjecture i.e. for which the above statements hold without conditions on the degree. Such sets are precisely those satisfying the properties of Northcott and Bogomolov introduced by Bombieri and Zannier [BZ01], whose definition in recalled here:

Definition (Bombieri, Zannier, [BZ01])**.** *A set of algebraic numbers L has the* Northcott property (N) *if it contains finitely many elements of bounded height, while it has the* Bogomolov property (B) *if there exists some constant $C > 0$ such that $h(\alpha) > C$ for all $\alpha \in L$ which are neither zero nor roots of unity.*

In this chapter we will be mainly interested in the case where L is a subfield of $\overline{\mathbb{Q}}$.

It is easy to see that property (N) implies property (B), while the proof that the converse is false is non trivial: the simplest counterexample is the field $\mathbb{Q}^{ab}$, the maximal abelian extension of $\mathbb{Q}$, which was proved to have property (B) by Amoroso and Dvornicich [AD00] and which clearly fails to have property (N) due to the presence of infinitely many roots of unity in the field.

By Northcott's theorem, both properties hold for number fields and, more in general, for sets of algebraic numbers with bounded degree. On the other side none of the properties hold for $\overline{\mathbb{Q}}$, as for instance $h(\sqrt[n]{2}) = (\log 2)/n$ tends to 0 as n increases.

An interesting, but generally hard, task is to study what happens between number fields and $\overline{\mathbb{Q}}$ i.e. given an infinite algebraic extension of $\mathbb{Q}$, decide whether it satisfies property (N) or (B). In recent decades there has been a lot of activity around this problem and I now briefly summarise the main known results on it.

Concerning property (B), we now know several examples of fields that satisfy it, but most of them fall into essentially two classes.

The first class is that of fields obtained by *adding torsion* to some base field. This class, as shown by the result of [AD00] evoked earlier, contains the field $\mathbb{Q}^{ab}$, the maximal abelian extension of $\mathbb{Q}$, which can be seen as the field obtained by adding to $\mathbb{Q}$ all the torsion points of the torus $\mathbb{G}_m$, i.e., all the roots of unity. This result has been generalised later by Amoroso and Zannier in [AZ00] and [AZ10] to the field K^{ab}, the maximal abelian extension of a number field K. Later Habegger [Hab13] proved an elliptic analogue of Amoroso and Dvornicich result, namely that property (B) holds for the field $\mathbb{Q}(E_{tor})$ obtained by adding to $\mathbb{Q}$ all coordinates of the torsion points of an elliptic curve E defined over $\mathbb{Q}$.

The second class is that of fields satisfying some *local conditions*. It contains, in view of a result of Schinzel [Sch73], the field $\mathbb{Q}^{tr}$ of totally real numbers i.e., the field obtained adjoining to $\mathbb{Q}$ all algebraic numbers having all real conjugates. The p-adic analogue of this result was later proved by Bombieri and Zannier [BZ01], who showed more generally that property (B) is satisfied by any Galois extension $L/\mathbb{Q}$ having *bounded local degrees at some prime p* i.e. embeddable in a finite extension of $\mathbb{Q}_p$. In particular, it holds for the field of totally p-adic numbers $\mathbb{Q}^{tp}$, which is the compositum of all finite Galois extensions of $\mathbb{Q}$ which are totally split at all primes above p. Another example of a Galois extension with bounded local degree, as exhibited in [BZ01], is given by $K^{(d)}$, the compositum of all extensions of a number field K of degree at most d.

Finally, in [ADZ14] Amoroso , David and Zannier have generalized both the above results, proving that property (B) holds for any Galois extension L/K of a number field K such that the subextension of L fixed by the center of $\mathrm{Gal}(L/K)$ has bounded local degrees at some prime. In particular, by [Che13], if the quotient of $\mathrm{Gal}(L/K)$ by its center has bounded exponent, then L has property (B). This gives a group theoretical criterion to detect if property (B) holds for a Galois extension.

As for property (N), results continue to be relatively rare and there are essentially two examples of fields which have been proved to satisfy it. The first, proved in [BZ01], is the field $K_{ab}^{(d)}$ which is the maximal abelian extension of a number field K which is contained in $K^{(d)}$. We remark that, using [CZ11], this result is equivalent to the following assertion: every Galois extension of a number field whose Galois group is abelian and of bounded exponent has property (N). This gives a group theoretical criterion to detect property (N).

As already discussed in Chapter 1, we also remark that the validity of property (N)

for $K^{(d)}$ and more generally for fields with uniformly bounded local degrees remains an open problem.

The second construction was given by Widmer [Wid11] and consists of fields obtained as unions of towers of number fields having discriminants that grow *fast* (the precise statement can be found in [Wid11, Theorem 3] and it is discussed in §2.2.II).

The following questions arise quite naturally and motivate the research described in the next sections:

(Q1) Given an infinite Galois extension $L/\mathbb{Q}$, is the structure of $\mathrm{Gal}(L/\mathbb{Q})$ related to the validity of property (B) or (N) for L? And if so, can we classify the groups for which it happens?

(Q2) Can we say more on how the local properties of a field determine property (N) and (B)?

(Q3) Are there new examples of fields with property (N) or (B)?

2.2. Description of the results

I. Properties (N) and (B) and Galois groups (description of the article [CW13])

In [CW13], in collaboration with Martin Widmer, we are mainly concerned with (Q1) and (Q3).

Concerning (Q1), as already noticed in §2.1, the results in [CZ11] and [Che13], combined with those in [ADZ14] and [BZ01], allow to detect, in some cases, property (B) and property (N) for a Galois extension by looking only at its Galois groups. More precisely, one can define property (B), as done in [ADZ14], and property (N) for groups: a profinite group G has *property (B)*, or *(N)* respectively, if, for any number field K and for every Galois extension L/K having G as Galois group, the field L has property (B) or (N), respectively.

With this terminology, the results in [Che13] and [ADZ14] imply that property (B) holds for any group G such that $G/Z(G)$ has finite exponent (here $Z(G)$ denotes the center of G), while those from [Che13] and [BZ01] show that property (N) holds for any abelian group of finite exponent (indeed any realisation of such group over a number field K must be contained in $K_{ab}^{(d)}$ for some d).

A very interesting result towards an answer to Question (Q1) would be to find new examples of groups with these properties. This currently seems to be very hard.

In [CW13] we consider another natural, though more modest, issue i.e. whether, given a profinite group G, there exists a dichotomy of the type: either G has property (B) (resp. (N)) or none of its realisations has property (B) (resp. (N)). We answer this question in the negative. More precisely, we prove the following:

Theorem 7 ([CW13, Theorem 4])**.** *Given any family of finite solvable groups $(G_m)_m$ there exists a family of number fields $(K_m)_m$ such that, for every $m \geq 1$, $K_m/\mathbb{Q}$ is Galois of group G_m, K_m is linearly disjoint over $\mathbb{Q}$ from the compositum of $K_1, \ldots, K_{m-1}$ and the compositum of all K_m's has property (N).*

To prove this result we use Shafarevich theorem [Sha56] to get *many* linealry disjoint realisations of a given finite solvable group G_m, Hermite's theorem combined with a classical result of Dedekind to ensure that at least one realisation $K_m/\mathbb{Q}$ of G_m has discriminant divisible by a *very big* prime and Widmer's criterion [Wid11, Theorem 3] to ensure that the compositum of the fields K_m's so constructed has property (N).

As a corollary, we can construct groups admitting two realisations over $\mathbb{Q}$, one with property (N) and one without property (N). As an example, for every odd prime p consider the finite solvable group $G_p = \mathrm{Gal}(\mathbb{Q}(\zeta_p, \sqrt[p]{2})/\mathbb{Q})$ and let G be the infinite direct product of the groups G_p. Then, by our theorem G occurs has the Galois group of a field with property (N) (and thus (B)), but also as the Galois group of the compositum of the fields $\mathbb{Q}(\zeta_p, \sqrt[p]{2})$, which clearly does not satisfy neither property (B) nor (N). We remark that, if one applies the theorem to the family of groups constructed in the proof of [CZ11, Theorem 1], one obtaines the first example of field with property (N) having uniformly bounded local degrees which is not contained in $\mathbb{Q}^{(d)}$.

As for (Q3), in [CW13, Theorem 3] we prove a sort of generalization of the results in [BZ01], by showing that the compositum $K^{(d)}$ of all extensions of K of degree at most d has property (B) not only when K is a number field, but more generally when $K/\mathbb{Q}$ is a Galois extension having finite exponent. We also show that, in this case, the maximal abelian extension of $\mathbb{Q}$ contained in $K^{(d)}$ has property (N). These results are proved by showing that, under the above assumptions, the extension $K^{(d)}/\mathbb{Q}$ is still Galois with Galois group of bounded exponent and thus, by [CZ11], it has uniformly bounded local degrees. The results then follow from [BZ01].

In [CW13, §6] we also discuss some problems related to properties introduced by Liardet and Narkiewicz to study polynomial mappings.

In [Nar62], Narkiewicz gave the following definition: a field of algebraic numbers K has *Property (P)* if only finite subsets of K can be fixed by some non-linear polynomial in $K[x]$. As property (N), property (P) holds for number fields, but not for algebraically closed fields and in [DZ08] Dvornicich and Zannier study the relation between the two properties. Amongst other results, they show that (N) implies (P) (see for instance [DZ08, Theorem 3.1]) and that, in contrast to property (N), property (P) is not preserved under taking finite extensions of fields (see [DZ08, Theorem 3.3]).

Narkiewicz (see for instance [Nar71, Problem 10.(i)]) conjectured that property (P) holds for $\mathbb{Q}^{(d)}$. For $d = 2$ this follows from [DZ08] combined with [BZ01], but the conjecture is open for $d > 2$. He also introduced several other properties including property (SP), an analogue in several variables of of property (P), property (R), a variant of property (P) for rational functions. Property $(\overline{P})$, a version of property (P) for invariants sets of elements of bounded degree, was also introduced by Liardet [Lia71]. In [Nar95], Narkiewicz suggested several open problems concerning the relation between all these

properties. Basing also on results from[DZ07, DZ08], we easily deduce answers to some of them and we study relations between all these properties and property (N).

II. Property (N) and local degrees (description of the article [CF21])

The article [CF21], in collaboration with Arno Fehm, deals with questions (Q2) and (Q3) and focuses in particular on the search of new examples of fields with property (N).

As discussed in §2.1, results on this property are quite rare and the only two criteria to detect such property for a field are the following:

(a) *Bombieri and Zannier's criterion* ([BZ01, Theorem 1]): if K is a number field, $d \geq 1$ is an integer and L is a subfield of $K_{ab}^{(d)}$, then L has property (N).

(b) *Widmer's criterion* ([Wid11, Theorem 3]): let $K_0 \subseteq K_1 \subseteq K_2 \subseteq \dots$ be an infinite tower of number fields and, for every $i \geq 1$, set

$$\delta_i = \inf_{K_{i-1} \subsetneq M \subseteq K_i} \left(\frac{|\Delta_M|^{\frac{1}{[M:K_{i-1}]}}}{|\Delta_{K_{i-1}}|} \right)^{\frac{1}{[M:K_0]}}$$

where for a number field F, Δ_F denotes its absolute discriminant. If $\delta_i \to \infty$ when i tends to infinity, then $L = \cup_{i \geq 0} K_i$ has property (N).

We remark that Widmer's criterion roughly says that if at each new step in the tower, the discriminants grow *enough* compared to the previous ones (in the above precise sense), then the union of the tower has property (N). Using this result, Widmer was able to give new examples of fields with property (N) (see for instance [Wid11, Theorem 4 & Corollary 2]).

It is quite natural to ask whether there are other criteria to detect property (N). It turns out that to obtain an answer to this question, it is convenient to look at a statement on property (B) shown in [BZ01]:

Theorem ([BZ01, Theorem 2])**.** *If $L/\mathbb{Q}$ is Galois and $S(L) \neq \emptyset$ is the set of primes at which L has bounded local degrees, then*

$$\liminf_{\alpha \in L} h(\alpha) \geq \beta(L) = \frac{1}{2} \sum_{p \in S(L)} \frac{\log p}{e_p(p^{f_p}+1)}$$

where e_p and f_p denote, respectively, the ramification index and the inertial degree of L at p.

In [BZ01, Remark, p.8], the authors notice that if $\beta(L) = \infty$ then L enjoys also property (N) (this is a simple consequence of Bolzano-Weierstrass theorem) and that $\beta(L) = \infty$ if L is a number field (this follows essentially by Chebotarev density theorem combined with the prime number theorem, as proved in [CF21, Proposition 2.1]).

They then ask whether the divergence of $\beta(L)$ can also occur for infinite extensions $L/\mathbb{Q}$, saying that they consider this event unlikely. One can further ask whether there

are infinite extensions $L/\mathbb{Q}$ for which $\beta(L)$ is divergent and that are not covered by the criteria of Bombieri-Zannier and Widmer i.e., whether the divergence of $\beta(L)$ is really a new criterion for property (N). In [CF21] we positively answer this last question, proving the following:

Theorem 8 ([CF21, Theorem 1.6])**.** *There exist an infinite Galois extension $L/\mathbb{Q}$ such that:*
(i) $\beta(L) = \infty$
(ii) $L \not\subset \mathbb{Q}_{ab}^{(d)}$ *for any* d*;*
(iii) L *does not satisfy Widmer's criterion.*

Although not explicitly stated, the proof of the theorem yields infinitely many linearly disjoint extensions of $\mathbb{Q}$ with the required properties. Here is briefly how it works: the field L is constructed as a compositum of infinitely many cyclic extensions $F_i/\mathbb{Q}$ having distinct prime degrees p_i. Thanks to the results in [CZ11], this condition alone ensures already that the field L, being an abelian extension of $\mathbb{Q}$ of unbounded exponent, is not contained in $\mathbb{Q}_{ab}^{(d)}$ for any d. Two constraints must be taken into account when constructing the F_i: on the one hand we want all primes up to a certain bound to split completely (this serves to make the sum $\beta(L)$ large) and on the other hand we want a good control on the absolute discriminant of F_i (to avoid that the sequence δ_i considered by Widmer is divergent). This is possible by constructing the F_i's inside composita of cyclotomic extensions of order certain primes congruent to 1 modulo p_i chosen appropriately via Walfisz's theorem (see [CF21, Lemma 3.1]).

We also show that, if one is only interested in the divergence of $\beta(L)$, there is some freedom in choosing the Galois group:

Theorem 9 ([CF21, Theorem 1.3])**.** *Given an infinite family of finite solvable groups $(G_m)_m$, there exists a Galois extension $L/\mathbb{Q}$ with* $\mathrm{Gal}(L/\mathbb{Q})$ *equal to the direct product of all the groups G_m's and such that $\beta(L) = \infty$.*

The proof of this result uses, among other ingredients, a refined version of Shafarevich theorem on the realisability of finite solvable groups. More precisely, in [CF21, Theorem 2.2 & Appendix A] we show that given G a finite solvable group and $\mathscr{S}$ a finite set of primes of a number field K, there exists a Galois extension of K with Galois group G in which all primes in $\mathscr{S}$ split totally. This theorem is applied to each of the groups G_m choosing the corresponding set of primes in a suitable way.

Another issue considered in [CF21] is about question (Q2). Recall that, as already remarked in §2.1, using [CZ11], Bombieri and Zannier's result on property (N) can be stated by saying that every abelian extension of a number field with uniformly bounded local degrees has property (N) and a difficult open problem is to decide whether the statement continues to be true without the condition on abelianity.

Then one could ask the simpler question of whether property (N) holds for all extensions with finite (but not necessarily uniformly bounded) local degrees. In [Feh18, Proposition 1.3] the author constructs extensions without property (N) and having local degree equal to one at infinitely many prime numbers (but also infinite local degree at infinitely many other prime numbers). In [CF21, Theorem 1.6] we prove the existence

of extensions with (non-uniformly) bounded local degree at all primes and which do not have property (N). This result is deduced from a theorem of Fili [Fil14, Theorem 1.2] on elements of small height in fields of totally p-adic numbers which is discussed in details in the next section.

III. Small totally p-adic numbers (description of the article [CF22])

In [CF22], in collaboration with Arno Fehm, we are mainly interested in (Q2). More precisely, we study elements of small height in fields satisfying some local properties.

As explained in §2.2.II, some of the results proved in [CF21] are based on a result of Fili [Fil14] on an upper bound for the height of totally p-adic numbers. As recalled above, for Galois extensions $L/\mathbb{Q}$ with bounded local degrees property (B) holds true and explicit lower bounds for the height have been given by Bombieri and Zannier [BZ01, Theorem 2]. In the special case where L is the intersection of a finite number of totally p-adic fields, they prove the following:

Theorem ([BZ01, Example 2 & special case of Theorem 2])**.**

$$\frac{1}{2}\sum_{i=1}^{n}\frac{\log(p_i)}{(p_i+1)} \leq \liminf_{\alpha\in\cap_{i=1}^{n}\mathbb{Q}^{tp_i}} h(\alpha) \leq \sum_{i=1}^{n}\frac{\log(p_i)}{(p_i-1)}.$$

As remarked by the authors, this shows that the lower bound in [BZ01, Theorem 2], at least in the totally p-adic case, is of the correct order of magnitude. Other proofs, refinements and generalizations were given in [Fil14, Pot15, FP15, FP19, PS19]. In particular in [Fil14] Fili generalises the result to extensions of number fields as it follows:

Theorem ([Fil14, Theorem 1.2])**.** *Let K be a number field and let $\mathfrak{p}_1,\dots,\mathfrak{p}_n$ be distinct prime ideals of the ring of integers $\mathcal{O}_K$ of K. For each i, let E_i be a finite Galois extension of the completion F_i of K at $\mathfrak{p}_i$. Denote by e_i and f_i the ramification index and the inertia degree of E_i/F_i and write $q_i=|\mathcal{O}_K/\mathfrak{p}_i|$. Then, if L is the maximal Galois extension of K contained in $\cap_{i=1}^{n}E_i$, one has:*

$$\liminf_{\alpha\in L} h(\alpha) \leq \frac{1}{[K:\mathbb{Q}]}\left(\sum_{i=1}^{n}\frac{\log(q_i)}{e_i(q_i^{f_i}-1)}\right).$$

Fili also conjectures that equality should hold, and this already taking the liminf only over algebraic integers (see [Fil14, Conjecture 1]). We remark that his proof uses capacity theory on analytic Berkovich spaces and does not provide explicit bounds on the degree and the height of a sequence of integral elements in the liminf.

In [CF22] we prove an effective version of Fili's result. More precisely:

Theorem 10 ([CF22, Theorem 1.3])**.** *Let K be a number field and let $\mathfrak{p}_1,\dots,\mathfrak{p}_n$ be distinct prime ideals of the ring of integers $\mathcal{O}_K$ of K. For each i, let E_i be a finite Galois extension of the completion F_i of K at $\mathfrak{p}_i$. Denote by e_i and f_i the ramification index and the inertia degree of E_i/F_i, write $q_i=|\mathcal{O}_K/\mathfrak{p}_i|$ and let L be the maximal Galois extension of K contained in $\cap_{i=1}^{n}E_i$.*

Set $C = \max\left\{[K:\mathbb{Q}], |\Delta_K|, \max_i(e_i f_i), \max_i q_i^{f_i}\right\}$ *where* Δ_K *is the absolute discriminant of* K*. Then for every* $0 < \epsilon < 1$ *and* $\rho \geq 3C^n$*, there exists* $\alpha \in \mathcal{O}_L$ *such that*

$$h(\alpha) \leq \frac{1}{[K:\mathbb{Q}]}\left(\sum_{i=1}^{n} \frac{\log(q_i)}{e_i(q_i^{f_i}-1)}\right) + 13nC^{2n+2}\frac{\log([K(\alpha):K])}{[K(\alpha):K]} + \begin{cases} 0, & n=1 \\ n\epsilon, & n>1 \end{cases}.$$

and

$$\rho \leq [K(\alpha):K] \leq \begin{cases} C\rho, & n=1 \\ \rho^{\frac{(4\log C)^{n+1}}{\log^n(1+\epsilon)}}, & n>1 \end{cases}.$$

Our effective proof is more elementary than Fili's one and it is inspired by Bombieri and Zannier's effective proof of [BZ01, Example 2]. We briefly sketch it here: given $\rho \geq 3C^n$ we construct a monic irreducible polynomial $g \in \mathcal{O}_K[X]$ such that:

(i) $\deg g$ is upper and lower bounded in terms of ρ as the degree of $[K(\alpha):K]$ in the statement;
(ii) the coefficients of g and all their conjugates have small enough absolute value;
(iii) g has all its roots in $\cap_{i=1}^{n} E_i$.

In Bombieri and Zannier's proof, (i) and (ii) were achieved by using the Chinese Remainder Theorem to deform the polynomial $\prod_{i=1}^{\rho}(X-i)$ into an irreducible polynomial of the same degree with coefficients small enough to give the desired bound for the height of the roots. Then a variant of Hensel's lemma was applied to show that the roots of the constructed polynomial are still in $\mathbb{Q}_{p_i}$ for each i.

In our generalisation, we start by constructing polynomials $\prod_{\alpha\in A_i}(X-\alpha)$, where $A_i \subseteq \mathcal{O}_{E_i}$ are certain special Galois invariant sets of representatives of residue rings of local fields. These are then merged into an irreducible polynomial g by applying the Chinese Remainder Theorem. The size of the sets A_i, and hence the degree of g, is carefully chosen to obtain (i) via Dirichlet's theorem on simultaneous approximation. To achieve (ii), we use a bound for the size of representatives in quotient rings of rings of integers. Property (iii) is then verified using a variant of Hensel's lemma. Finally, we use classical bounds for the height of a root of a polynomial defined over a number field in terms of its coefficients to show that g has a root α of height bounded from above as desired.

To the best of our knowledge, our theorem is the only result currently available that gives a bound on the height in terms of the degree of such a sequence of α, except for the case where $K = \mathbb{Q}$ and $E_i = \mathbb{Q}_{p_i}$ for all i, where such a bound can be deduced from [BZ01].

2.3. Some perspectives

(i) Bogomolov and Galois

This research goal is part of a project with Arno Fehm (University of Dresden). Our aim is to study lower bound for the height of the algebraic numbers in the following special set

$$\mathcal{G} = \{\alpha \in \overline{\mathbb{Q}} \mid \mathbb{Q}(\alpha)/\mathbb{Q} \text{ is Galois}\}.$$

Amoroso and David [AD99] proved that Lehmer's cojecture holds for elements in such set and, inspired by their result, Smyth in [APSV, problem 21, p.17], asked whether $\mathscr{G}$ actually satisfies property (B).

Later, Amoroso and Masser [AM16, Theorem 3.3] prove a very strong Lehmer type bound for $\mathscr{G}$: they show that given $\epsilon > 0$ there exists a constant $c(\epsilon) > 0$ such that $h(\alpha)[\mathbb{Q}(\alpha) : \mathbb{Q}]^{\epsilon} > c(\epsilon)$ for all $\alpha \in \mathscr{G}$ such that $h(\alpha) \neq 0$. This result clearly seems to suggest that Smyth's question has a positive answer.

Further evidence in this direction is provided by another result by Amoroso [Amo16b, Theorems 1.1 and 1.2]: motivated also by another question of Smyth in [APSV, p.17], he proves, in particular, that, for certain particular classes of algebraic numbers $\alpha_n \in \mathscr{G}$ with $\mathrm{Gal}(\mathbb{Q}(\alpha_n)/\mathbb{Q}) = S_n$ one has $h(\alpha_n) \geq c(n)$ for some explicit constant $c(n)$ which tends to infinity with n. Amoroso [Amo16b, Conjecture 1.3] conjectures also that this should happen for every generator of an S_n-extension. Let us also mention, in this context, the recent article [AD21, Theorem 1.1] where the authors show that the Galois group of a lacunary polynomial, under some natural assumptions, grows more than polynomially in the degree.

One of the difficulties in trying to provide a negative answer to Smyth's question is that there is essentially one known way to explicitly construct elements of small height, that is to take roots of 'sparse' polynomials (i.e. polynomials having few coefficients compared to the degree) and this does not give in general generators of Galois extensions. For instance, if α_n is a root of $x^n - 2$ or a root of $x^n - x - 1$ then, by using elementary properties of the Weil height, one can easily see that $h(\alpha_n)$ tends to zero as n grows. We remark however that the α_n's so constructed are such that $\mathbb{Q}(\alpha_n)/\mathbb{Q}$ is not Galois.

To start with: One of our first research objectives is to investigate other classes of generators of Galois extensions, in particular, to decide property (B) for the following set

$$\mathscr{G} \cap \mathbb{Q}(\zeta_n, b^{1/n} \mid n \geq 2)^*$$

for $b \in \mathbb{Q}^*$.

This set quite natural to investigate in this context. First, it is sufficiently interesting, since, as remarked before, the field $\mathbb{Q}(\zeta_n, b^{1/n} \mid n \geq 2)$ has not property (B). We also notice that, in this case, as remarked already in [Amo16b, p.3], we cannot expect an analogue of Amoroso's conjecture [Amo16b, Conjecture 1.3] to hold i.e. the height cannot increase with the size of the Galois group: for instance, one can easily show that $\alpha_n = \zeta_n + 2^{1/n}$ is in the set and it generates a Galois extension of degree $n\varphi(n)$, but $h(\alpha_n) \leq 2\log 2$.

However, a way deeper reason to expect property (B) for the above set comes from some conjecture suggested by G. Rémond [Rém17] to unify different versions (absolute and relative) of Lehmer's conjecture in tori and abelian varieties.

A very special case of [Rém17, Conjecture 3.1](see also conjecture [Amo16a, Conjecture 1.2]) says, roughly speaking, that all the small points in $\mathbb{Q}(\zeta_n, b^{1/n} \mid n \geq 2)^*$ are of the form $\zeta_n^i b^r$ for some $i \in \zeta$, $r \in \mathbb{Q}$. The validity of this special case of the conjecture would of course easily imply that the set we study has property (B).

In [Amo16a, Theorem 3.3] Amoroso was able to prove that the conjecture is true for the subfield $\mathbb{Q}(\zeta_{p^i}, b^{1/p^i} \mid i \geq 1)$ where $b \geq 2$ is an integer and p is an odd prime not dividing b and such that p^2 does not divide $b^{p-1}-1$, providing also a totally explicit lower bound for the height of non-small points.

Our first goal with A. Fehm would be to study Galois generators inside the field where we take as our n's all distinct primes (instead of powers of the same prime). To our knowledge, the only result in this context is proved by Plessis [Ple22, Theorem 1.5] who shows in particular, that for any prime p, there exists a constant $c > 0$ such that for any $a_1, b_1, a_2, b_2 \in \mathbb{Q}$, if $x = a_1 p^{b_1} + a_2 p^{b_2} \neq 0$, then either $h(x) \geq c$ or $x = \zeta p^r$ for some p-th root of unity ζ and $r \in \mathbb{Q}$. His approach uses equidistribution and the constant does not seem to be effective.

(ii) Bogomolov, Northcott and Galois.

As evoked in §2.2.I, it would be very interesting to better understand profinite groups with property (N) or (B). While a full classification of such groups seems to be way out of reach, a more attainable goal would be to study the following questions from [ADZ14]:

Question ([ADZ14, Problem 5.6])**.** *Let G be a profinite group with property (B).*
(i) Is it true that if H is a subgroup of G of finite index, then H satisfies (B)?
(ii) If K is a number field and L/K is a Galois extension with Galois group G, is it true that any finite extension of L satisfies (B)?

It is remarked in [ADZ14] that the validity of (i) implies the validity of (ii). Focusing on question (ii), we notice that it has a positive answer when considering property (N) instead of (B). This follows from the fact that property (N) is preserved for finite extensions, while this phenomenon does not occur for property (B). An example, given in [ADZ14, Theorem 5.3], is the field $\mathbb{Q}^{tr}$: it satisfies (B) by [Sch73], but its finite extension $\mathbb{Q}^{tr}(i)$ contains points of arbitrarily small non-zero height, as shown in [AN07, Theorem 1.3].

To start with: In a very recent joint project with L. Pottmeyer (University of Duisburg-Essen), partly motivated by the above questions, we investigate further the behaviour of property (B) under finite extensions.

We will first consider the easier question of whether there exist extensions $L/\mathbb{Q}$ which are *maximal with respect to (B)* i.e. which enjoy property (B) but always lose it under any finite extension. We do not expect such fields to exist. Indeed, as a first reason to be skeptical, first notice that property (B) is preserved under finite extensions for almost all known examples of fields satisfying it i.e. number fields, abelian extensions and extensions with bounded local degrees at some prime. As for $\mathbb{Q}^{tr}$, as shown in [Pot16, Theorem 1.1], a finite extension of it has property (B) if and only if it does not contain i. So, in some sense, $\mathbb{Q}^{tr}(i)$ is essentially the only case where things go wrong. As a second and more ambitious goal, we would like to understand whether actually $\mathbb{Q}^{tr}(i)/\mathbb{Q}^{tr}$ is the unique example of a finite extension of fields where property (B) is not preserved.

(iii) Northcott and Siegel.

In [GR17], Gaudron and Rémond introduce and study the notion of *Siegel fields*, which are subfields of $\overline{\mathbb{Q}}$ satisfying Siegel's lemma. More precisely, following [GR17, p.189], we say that a subfield $L \subseteq \overline{\mathbb{Q}}$ is a Siegel field if there exists a constant $c = c(L) > 0$ such that for all $a, b, c \in L$, not all zero, the equation $ax + by + cz = 0$ has a nontrivial solution with $x, y, z \in L$ and $H(x, y, z) \leq cH(a, b, c)^{1/2}$ (where $H(\cdot)$ denotes the non-logarithmic projective height).

Examples of Siegel fields are given by number fields (see [BV83] for a sharper result in this case) and also by $L = \overline{\mathbb{Q}}$ (see [RT99], [Zha95a]). In [GR17], the authors give new examples of Siegel fields and also examples of non-Siegel fields. In particular, they show that an infinite extension of $\mathbb{Q}$ with property (N) cannot be a Siegel field. This result stems from a very delicate study of successive minima, the so-called Zhang minima, in rigid adelic spaces. An open and difficult question is whether the converse is true or whether there are fields that are neither Siegel nor satisfying property (N).

To start with: Some first concrete examples to study to answer the previous question, are the fields $\mathbb{Q}^{ab}$ and $\mathbb{Q}^{tp}$, which are known to fail property (N). To the authors knowledge, as also underlined in [GR17, §5.6], for these fields the Siegel property has not been studied yet.

CHAPTER 3

ON SOME UNLIKELY INTERECTIONS IN ABELIAN VARIETIES

Unlikely intersections is a term coined by Bombieri, Masser and Zannier to describe a class of problems that can be seen as statements about the intersection of objects that should not intersect for dimensional reasons and that includes many famous conjectures. After an introduction on the state of the art in this very active area, I will describe the results obtained by my co-authors and myself on the subject, proving, in particular, certain cases of the so-called torsion anomalous conjecture and of the explicit Mordell conjecture. The chapter ends with the description of some research leads.

List of articles presented in this chapter

[CVV12] «A sharp Bogomolov-type bound »
(with F. VENEZIANO AND E. VIADA), *New York Journal of Mathematics*, 18, 891-910 (2012).

[CVV14] «On torsion anomalous intersections »
(with F. VENEZIANO AND E. VIADA), *Rendiconti Lincei - Matematica e Applicazioni*, Vol. 25, Issue 1, 1-36 (2014).

[CV14] «On the Torsion Anomalous Conjecture in CM abelian varieties »
(with E. VIADA), *Pacific Journal of Mathematics*, 271-2, 321-354 (2014).

[CVV17] «On the explicit torsion anomalous conjecture »
(with F. VENEZIANO AND E. VIADA), *Transactions of the American Mathematical Society*, Vol. 369, no. 9, 6465–6491 (2017).

[CVV19] «The explicit Mordell Conjecture for families of curves »
(with F. VENEZIANO AND E. VIADA), *Forum of Mathematics, Sigma,* Vol. 7, e31 (2019). With an appendix by M. Stoll.

3.1. Introduction

This chapter focuses on some problems on unlikely intersections in abelian varieties, a topic which has been central in my research in the first years after my PhD studies.

I do not presume in any way to give an exhaustive overview of the many results that have been proved on the subject, which is a very important and active area of research, nor an exhaustive list of the massive amount of corresponding literature. I refer the interested reader to Zannier's beautiful book [Zan12] for a detailed account on the topic and for more references.

Unlikely intersections is a term, introduced by Bombieri, Masser and Zannier (see for instance [BMZ07, BMZ08b]), that encompasses a wide class of problems in arithmetic geometry (and beyond). The philosophy underlying this terminology is that two varieties X and Y in a space G are unlikely to intersect if $\dim X + \dim Y < \dim G$.

More precisely, the kind of results one would like to prove is that, if X is fixed and Y varies in a denumerable family $\mathscr{F}$ of varieties of dimension less than $\dim G - \dim X$ and having some *special* property, then $X \cap Y$ is expected to be empty for most $Y \in \mathscr{F}$, unless X is also *special* in some sense.

Many famous conjectures and results can be interpreted as special cases of this general tenet. In this chapter we will focus on the case where G is an abelian variety, but most of the results we state have been proved also when $G = \mathbb{G}_m^n$ is a multiplicative torus or in more general settings. All varieties we consider are defined over $\overline{\mathbb{Q}}$, which, thanks to the recent work in [BD22], is the most interesting case in our setting. Also, for us varieties are always irreducible and subvarieties are always irreducible and closed in their ambient variety.

We recall that a proper subvariety of G is said to be a *translate*, a *torsion variety* respectively, if it is a finite union of translates of proper algebraic subgroups of G by points, by torsion points respectively. We say that X is *transverse*, *weak-transverse* respectively, in G if it not contained in any proper translate, torsion variety respectively.

With this terminology, the Manin-Mumford conjecture, proved in [Ray83], states that, if X is an algebraic subvariety of G and G_{tor} is the set of torsion points of G, then $X \cap G_{tor}$ is not Zariski-dense in X, unless X is itself a torsion variety. Or, equivalently, the Zariski-closure of $X \cap G_{tor}$ in X is a torsion subvariety of G.

If instead of G_{tor} one considers more generally a subgroup Γ of G of finite rank, the Mordell-Lang conjecture, proved in [Fal94], asserts that $X \cap \Gamma$ is not Zariski-dense in X, unless X is a translate. The special case when X is a non-singular curve defined over a number field k, G is its Jacobian and $\Gamma = G(k)$ are the k-rational points of G, is the famous Mordell conjecture, proved in [Fal83], stating that $X \cap \Gamma = X(k)$ is always finite when $\dim G \geq 2$.

All these conjectures can now be viewed as special cases of a series of conjectures formulated independently by Bombieri, Masser and Zannier in [BMZ07] (but already partially suggested in the founding work [BMZ99]) and Zilber [Zil02] in tori, and by Pink [Pin05] in the setting of mixed Shimura varieties. They imply in particular the following:

Conjecture 1. *Let X be an algebraic subvariety of a semi-abelian variety G and let $G^{[\dim X+1]}$ be the countable union of all algebraic subgroups of G having codimension at least* $\dim X+1$. *Then $X \cap G^{[\dim X+1]}$ is not Zariski-dense in X, unless X is not weak-transverse.*

While it is quite clear that this generalises the Manin-Mumford conjecture, an important aspect of Conjecture 1 is that it also generalises the Mordell-Lang conjecture: it is indeed equivalent to the assertion that, the intersection of X with the union of all algebraic subgroups of codimension at least $\dim X+1$, translated by points in a subgroup of G of finite rank, is non-dense in X, unless X is contained in a translate.

The case where X is a curve is of particular interest: when G is the multiplicative torus it was already treated, under the stronger assumption that X is not contained in any translate, in [BMZ99] and then fully proved in [Mau08] (and later reproved in [BHMZ10] with an alternative approach based on the work in [Hab09]). For G an abelian variety, it was established in [HP16]. In particular, they use a variation of the so called *Pila-Zannier method*, introduced for the first time by the two named authors to reprove the Manin-Mumford conjecture for abelian varieties, which is based on the combination of point counting results coming from the theory of o-minimality with other diophantine ingredients. We refer also to [Via03, RV03, Rém05, Rat08, Car09, Via08, Gal10, Via10] for some previous important partial results.

If $\dim X > 1$, then X can contain subvarieties of positive dimension accumulating points of the intersection $X \cap G^{[\dim X+1]}$ and this is where the notions of anomalous subvarieties come into play.

These objects have been introduced by Bombieri, Masser and Zannier in the toric case in [BMZ07]. In particular, following them, we say that a subvariety Y of X is *X-torsion anomalous* if it is an irreducible component of $X \cap H$, where $H \subset G$ is an irreducible torsion variety with $\operatorname{codim} H \geq \dim X - \dim Y + 1$. We also say that a torsion anomalous variety is *maximal* if it is not contained in a strictly larger torsion anomalous subvariety of X.

Clearly, one should first remove from X such subvarieties before trying to prove some finiteness statement in the context of Conjecture 1 and obviously it is enough to remove the maximal ones. We also remark that our definition is slightly different from the one in [BMZ07], where only varieties of strictly positive dimension are considered.

In [BMZ07], among many other results, the authors formulate two conjectures on the set X^{ta}, obtained by removing from X all the maximal torsion anomalous subvarieties: the Torsion Openness Conjecture states that X^{ta} is Zariski-open in X, while the Torsion Finiteness Conjectures predicts that $X^{ta} \cap G^{[\dim X+1]}$ is finite.

In [BMZ07], the authors notice, in particular, that these two conjectures together imply Conjecture 1. This last is actually a consequence of the following conjecture, formulated in [Zil02] for semi-abelian varieties:

Conjecture 2 (Torsion anomalous conjecture)**.** *Let X be a subvariety of an abelian variety G. Then, X contains finitely many maximal torsion anomalous varieties.*

The conjecture is trivial if $\operatorname{codim} X = 0$, while it follows from the Manin-Mumford conjecture if $\operatorname{codim} X = 1$ (as in this case the X-torsion anomalous varieties are precisely the torsion varieties contained in X). Also, X is itself X-torsion anomalous if it is contained in a torsion variety. So Conjecture 2 is interesting when X is weak-transverse of codimension at least 2.

When $\operatorname{codim} X = 2$ and $G = \mathbb{G}_m^n$ this follows from the work of Bombieri and Zannier [Zan00, Theorem 2] or from Bombieri, Masser and Zannier's article [BMZ07, Theorem 1.7]. When $\operatorname{codim} X = 2$ and G is an abelian variety, this has been proved in powers of elliptic curves with complex multiplication (for short, CM) in [CVV14] and in arbitrary products of elliptic curves with CM [CV14]. These articles will be discussed in details in §3.3. Recently, a proof has been given also in powers of elliptic curves without CM (see [HV19]) and in any abelian variety defined over an algebraically closed field of characteristic 0 in [BD22] as a consequence of the work in [HP16] (see [BD22, Corollary 1.6 and Theorem 7.1]). To the author's knowledge no other general results is known in higher codimension.

Returning to the general philosophy of unlikely intersections, other issues arise somewhat complementary in nature to those discussed so far. Take again a subvariety X of G and some special family of varieties $\mathscr{F}$ of dimension strictly less than $\dim G - \dim X$. Suppose that X is *not special*, so that $\cap_{Y \in \mathscr{F}} X \cap Y$ is *small*, as expected. How can one measure this smallness? Can one describe the set somehow explicitly?

Here we need to be precise about what *explicitly* means. We take, as an example, Mordell conjecture, discussed earlier, which will be important in the description of my work on this topic. As already mentioned, this predicts that a non-singular algebraic curve X of genus at least 2 defined over a number field k has only finitely many k-rational points.

This result was proved by Faltings in [Fal83] and since then other different proofs have been given in [Voj91], later simplified in [Fal91] and further in [Bom90], and very recently in [LV20]. Unfortunately, these proofs are not *effective*, in the sense that they do not give, even in principle, a bound for the height of the points in $X(k)$, which, by Northcott's theorem, would be enough to find them *explicitly*, i.e. to list them down.

Although no general effective method is known that works for every curve, some effective approaches do work under certain conditions, as we will discuss later (see §3.3.III for a detailed description).

For varieties of higher dimension, the same questions can be posed. For instance, in connection to Conjecture 2, given a subvariety X of an abelian variety G, can one give an explicit bound on the (suitably chosen) height and degree of the maximal torsion anomalous varieties it contains?

After some preliminaries in §3.2, in §3.3 I will describe some effective results I have obtained with my coauthors on unlikely intersections, including some applications to the effective Mordell-Lang and the explicit Mordell conjectures.

3.2. Some preliminaries

Before describing our results, so as not to burden the reading of the next section, it might be convenient to introduce here some notation and preliminaries. This dedicated section can be consulted by the reader, if needed, while reading the next parts. Headings are placed to make it easier to browse the section.

In §3.3 we describe some effective results we have obtained in the context of Conjecture 2, in which we provide explicit bounds on the height and the degree of the varieties involved. We want to specify here which heights and degrees we will use and recall some of the relevant properties they enjoy and which will be important to us.

(a) Heights and degrees. Let G be an abelian variety defined over $\overline{\mathbb{Q}}$. We fix a symmetric ample line bundle $\mathscr{L}$ on G to which we attach an embedding $i_{\mathscr{L}} : G \hookrightarrow \mathbb{P}^m$ (defined by the minimal power of $\mathscr{L}$ which is very ample). The degree and the height of a subvariety of G are those of its image via this embedding.

More precisely, given a subvariety of $X \subset \mathbb{P}^m$, its degree $\deg(X)$ is the maximal cardinality of a finite intersection between X and a linear subspace of dimension equal to $\operatorname{codim} X$.

The height of X can be either its *canonical* height $\hat{h}(X)$ or its *normalised* height $h(X)$, as defined and studied in [Phi91, Phi95]. In particular, for points, $\hat{h}$ reduces to the classical Néron-Tate height (see [Phi91, Proposion 9.(v)]) and h to a modified version of the Weil height (see [CVV17, §2.2]). For a general subvariety X, the difference $|h(X) - \hat{h}(X)|$ is bounded by a constant depending only on G and $\deg(X)$ (see [Phi95, Proposition 9.(iv)]). Both such heights satisfy a Northcott's theorem i.e. there are finitely many varieties of bounded degree and bounded height.

(b) The arithmetic Bézout theorem. The normalised height satisfies also other two important results. The first is an arithmetic Bézout theorem (see [BGS94, Theorem 5.4.4] and [Phi95, Theorem 3]) which gives a bound for the height of an intersection of two varieties in terms of their heights and degrees. More precisely, it ensures that given two closed and irreducible subvarieties $X, Y \subset \mathbb{P}_m$, the sum of the height of the irreducible components $Z_1, \dots, Z_n$ of $X \cap Y$ is bounded as

$$\sum_{i=1}^{n} h(Z_i) \leq \deg(X)h(Y) + \deg(Y)h(X) + c(m)\deg(X)\deg(Y)$$

where $c(m) > 0$ is an explicit constant.

(c) Zhang's inequality. The second is an inequality coming from the work of Zhang on the Bogomolov Conjecture, predicting that, if $X \subset G$ is a non-torsion subvariety, then there exists an $\epsilon > 0$ such that the set $\{P \in X \mid \hat{h}(P) \leq \theta\}$ is not Zariski dense in X. Equivalently, defining the *essential minimum* of X, $\hat{\mu}(X)$, as the infimum of the $\theta \in \mathbb{R}_{>0}$ such that the set $\{P \in X \mid \hat{h}(P) \leq \theta\}$ is Zariski-dense in X, the conjecture claims that $\hat{\mu}(X) > 0$ for non-torsion varieties. This is now a theorem thanks to the work in [Ull98] and [Zha98].

An important ingredient in the proofs of our results will be Zhang's inequality proved in [Zha95b, Theorem 1.10], from which one can deduce that

$$\hat{\mu}(X) \leq \frac{\hat{h}(X)}{\deg(X)} \leq (1+\dim X)\hat{\mu}(X)$$

and that the same statement holds with the canonical height replaced by the normalised ones, see [CVV17, Theorem 2.2].

(d) Galateau's result on Bogomolov's problem. When $X \subset G$ is not a torsion variety, the so-called Bogomolov's problem asks to find explicit lower bounds for its essential minimum in terms of geometrical invariants of X and G. This problem has been studied extensively (see for instance [DP98, DP02, DP07]).

If G has a positive density of ordinary primes (which should always be the case according to a conjecture of Serre) and X is transverse, Galateau [Gal10] proves a quasi-optimal lower bound, i.e. he shows that, for any $\epsilon > 0$ one has

$$\hat{\mu}(X) \geq \frac{c(G,\epsilon)}{deg(X)^{\frac{1}{\dim G - \dim X}+\epsilon}} \qquad (\clubsuit)$$

with $c(G,\epsilon) > 0$ is effective (and also depends on the line bundle $\mathscr{L}$ used to compute heights and degrees).

This theorem, together with the bounded height theorem of Habegger [Hab09], has been applied in [Via10] to prove Conejcture 1 for curves in abelian varieties with a positive density of ordinary primes. The case where X is not transverse is investigated in [CVV12] and applied in [CVV14]. Details on these articles are given in §3.3.

(e) Carrizosa's result on the relative Lehmer's problem. For points, the search for lower bounds for height in terms of the degree is a long-standing problem initiated by a question of Lehmer, now known as Lehmer's Conjecture.

This predicts the existence of a constant c such that, for any $\alpha \in \overline{\mathbb{Q}}$ which is not a root of unity, one has $h(\alpha) \geq c/[\mathbb{Q}(\alpha):\mathbb{Q}]$, where h is the absolute logarithmic Weil height. The conjecture is still open in general, though some results have been proved (see Chapter 2 of this manuscript for more details).

In particular, [AZ10] proved that it holds when α generates an abelian extension of a number field. More precisely they show that if k is a number field and $\alpha \in \overline{\mathbb{Q}}$ is not a root of unity, then

$$h(\alpha) \geq \frac{c(k)}{D}\left(\frac{\log\log 5D}{\log 2D}\right)^{13}$$

where $D = [k^{ab}(\alpha) : k^{ab}]$ and $c(k) > 0$.

An analogue of this results for points in an abelian variety G was given in [Rat04] when G is an elliptic curve with CM. Later Carrizosa in [Car09] generalised this result to any CM abelian variety, proving a lower bound for the height of a non-torsion point depending also on the minimal torsion variety containing the point. More precisely, she shows that if G is an abelian variety with CM defined over a number field k, k_{tor}

is the field of definition of all the torsion points of G, $P \in G$ is a non-torsion point and $H \subset G$ is a torsion variety of minimal dimension containing P, then for every $\epsilon > 0$ one has

$$\hat{h}(P) \geq c(G,\epsilon) \frac{\deg(H)^{\frac{1}{\dim H}-\epsilon}}{[k_{tor}(P) : k_{tor}]^{\frac{1}{\dim H}+\epsilon}}$$

where $c(G,\epsilon) > 0$. This result will be important in the proof of the main theorem of [CVV14], as explained in the next section.

3.3. Description of the results

I. Some effective cases of the torsion anomalous conjecture (description of the article [CVV12], [CVV14] and [CV14])

In [CVV14], in collaboration with Francesco Veneziano and Evelina Viada, we investigate Conjecture 2 when $G = E^N$ is the power of an elliptic curve E with CM defined over $\overline{\mathbb{Q}}$, claiming the finiteness of the maximal torsion anomalous varieties contained in any given subvariety $X \subseteq G$.

When talking about heights and degrees of varieties and for all other preliminary result, we refer to §3.2. We notice again that, unlike [BMZ07], our definition of torsion anomalous varieties includes points.

As already recalled, Conjecture 2 is only interesting when X is weak-transverse in G and $\operatorname{codim} X \geq 2$. Moreover, one may also assume that X is not a translate, as otherwise an easy argument shows that the set of X-torsion anomalous varieties is empty (see [CVV14, Proposition 3.7]).

In [CVV14] we study maximal torsion anomalous subvarieties according to their *relative codimension*, which is defined as it follows. If Y is X-torsion anomalous, then it is an irreducible component of $X \cap H$, where H is a torsion variety with $\operatorname{codim} X > \dim H - \dim Y$ and we can assume that H is *minimal for* Y i.e. it is a variety of minimal dimension satisfying these conditions. In this case, we call $\dim H - \dim Y$ the *relative codimension of* Y.

Notice that maximal torsion anomalous varieties of relative codimension one are in some sense the most anomalous, and the main result of [CVV14] proves their finiteness:

Theorem 11 ([CVV14, Theorem 1.4])**.** *Let $G = E^N$ be a power of an elliptic curve E with CM defined over $\overline{\mathbb{Q}}$. Let $X \subset G$ be a weak-transverse variety. Then there are finitely many maximal X-torsion anomalous varieties of relative codimension one. In addition, their degrees and normalised heights are upper bounded by effective constants whose dependence in the height and the degree of X is explicit.*

We refer to the statement of [CVV14, Theorem 1.4] for the exact shape of the constants alluded to in the theorem. We want to stress that one of the interesting aspects is that the dependence on X in the bounds we provide is completely explicit and all other constants depend only on G.

One of the corollaries of our theorem is that Conjecture 2 holds for varieties of codimension 2 in $G = E^N$, providing an analogue of [BMZ07, Theorem 1.7] (see also [CVV14, Corollaries 1.5 and 1.6]). In particular, this gives an effective proof of Conjecture 1 when X is a weak-transverse curve in $G = E^3$ when E is CM. We remark that, in this case, the finiteness of $X \cap G^{[2]}$ already stemmed from [RV03].

In [CVV14, §2], we also give another applications of our result in the context of the Mordell-Lang conjecture. In particular, in [CVV14, Corollary 2.1] we give an effective bound for the the height and the number of points in $X \cap \Gamma$, where X is a weak-transverse curve in E^N, $N > 2$ and $\Gamma \subseteq E^N(\overline{\mathbb{Q}})$ is a subgroup such that the $\mathrm{End}(E)$-module generated by the coordinates of its points has rank one.

This result follows from the fact that, if $P \in X \cap \Gamma$, then either P is torsion or it is contained in some intersection $X \cap H$, where H is a torsion variety of dimension 1. Thus P is torsion anomalous of relative codimension one, unless H is contained in X, a case which is discarded from the weak-transversality of X and the hypothesis $N > 2$, so that our main theorem can be applied. A bound on the cardinality of $X \cap \Gamma$ is then obtained using also Rémond's result [Rém00].

We now discuss the proof of our main result [CVV14, Theorem 1.4].

This is inspired by the first and pioneering approach to Conjecture 1 introduced in [BMZ99] when X is a curve in $G = \mathbb{G}_m^n$, which can be schematised by the following two-step argument. Let $G^{[2]}$ be the countable union of all algebraic subgroups of G of codimension at least 2. Then:

(i) one first shows that the height of all points in $X \cap G^{[2]}$ is bounded;
(ii) one then deduces from this a bound for the degree of such points, hence their finiteness by Northcott's theorem.

Using this strategy, in [BMZ99, Theorem 2] Conjecture 1 is proved under the stronger assumption that the curve X is transverse in $\mathbb{G}_m^n$.

While step (i) follows from [BMZ99] (see also [Mau08] and [Hab09]), for step (ii) one needs some geometry of numbers and good lower bounds for the height of the points of interest in terms of their degree. The latter are provided by a higher dimensional analogue of Dobrowolski's theorem on Lehmer's conjecture proved in [AD99]. We refer to [Zan12, p.26-28] for more details on the proof of [BMZ99, Theorem 2]. This proof was then adapted to the abelian case in [Via03].

Let's now come to sketch the proof of our main theorem. We denote by k the field of definition of E and by k_{tor} be the field of definition of all torsion points of E^N. We assume that Y is a torsion anomalous component of $X \cap H$ where H is a minimal torsion variety for Y and $1 = \dim H - \dim Y < \mathrm{codim} X$.

We first show that, using linear algebra and some geometry of numbers, we can construct an auxiliary torsion subvariety $H' \subset G$ with $\mathrm{codim} H' = \dim X - \dim Y$ and smaller degree $\deg(H') \ll_G (\deg(H))^{\frac{\dim X - \dim Y}{\mathrm{codim} H}}$ such that Y is still a (non-anomalous) component of the intersection $X \cap H'$. Here by $\ll_G$ we mean that the inequality holds up to a multiplicative constant depending on G. We refer to [CVV14, §4.2 and p.19] for more details on the construction of H'.

We then apply the arithmetic Bézout theorem [BGS94, Theorem 5.4.4] (see §3.2.(b)) to the intersection $X \cap H'$ to get

$$h(Y) \ll_G (h(V) + \deg(V))(\deg(H))^{\frac{\dim X - \dim Y}{\operatorname{codim} H}}.$$

We now want to get a lower bound for $h(Y)$ in terms of $\deg(H)$ good enough to be compared to the upper bound and eventually lead to a bound for $\deg(H)$ and thus, by the arithmetic Bézout theorem for $h(Y)$ and by the classical Bézout theorem for $\deg(Y)$. The proof now proceeds by separating three different cases.

If Y is a point, the lower bound for the height of Y follows from Carrizosa's result [Car09] (see §3.2.(e)). This case is treated in [CVV14, §6].

If Y is a translate of positive dimension we use a result by Philippon [CVV14, Lemma 7.2] which guarantees that $Y = H'' + p$ where H'' is a subgroup and $p \in G$ is a point such that $\hat{\mu}(H'' + p) = \hat{h}(P)$. We then combine Zhang's inequality [Zha95b, Theorem 1.10] (see §3.2.(c)) with Carrizosa's theorem [Car09] to get the sought for lower bound for $\hat{h}(Y)$ in terms of $\deg(H)$. This case is done in [CVV14, §7].

We notice that these are the only cases where the CM hypothesis on the elliptic curve E is needed, due to the use of [Car09].

Finally comes the case where Y is not a translate, proved in [CVV14, §5]. Here we use the following result, that we prove in [CVV12], in collaboration with Francesco Veneziano and Evelina Viada, which gives a lower bound for the essential minimum of a non trasverse variety in the spirit of the result of Galateau's bound (♣) from [Gal10] recalled in §3.2.(d):

Theorem 12 ([CVV12, Theorem 1.3])**.** *Let G be an abelian variety and assume that an effective Bogomolov bound* (♣) *holds for transverse subvarieties of G. Suppose that Y is a subvariety of G contained in a translate H, but not contained in any translate strictly contained in H. Then, for every $\epsilon > 0$*

$$\hat{\mu}(Y) \geq C'(G,\epsilon) \frac{\deg(H)^{\frac{1}{\dim H - \dim Y} - \epsilon}}{\deg(Y)^{\frac{1}{\dim H - \dim Y} + \epsilon}} \qquad (\diamondsuit)$$

where $C'(G,\epsilon) > 0$ is an effective constant (also depending on the line bundle $\mathscr{L}$ chosen to compute heights and degrees).

The novelty of this result consists in the dependence on the degree of H and is a new step in direction of a conjecture from [DP07].

The proof of [CVV12, Theorem 1.3] is essentially geometric and easily reduces to the case where H is an abelian subvariety (see [CVV12, p.908]). Here is a very short sketch of it. Let $\mathscr{L}$ be a fixed ample symmetric line bundle on G and let $\hat{\mu} = \hat{\mu}_{\mathscr{L}}$ be the corresponding essential minimum. In order to prove the result we need to compare the line bundle $\mathscr{L}$ on G with its restriction $\mathscr{L}|_H$ to H.

The idea is to identify H, via a suitable morphism ϕ, to a product $G' = G_1^{n_1} \times \cdot \times G_r^{n_r}$ where the G_i's are the simple factors of G. We then consider another bundle $\mathscr{M}$ on G'

given by the tensor product of the pullbacks of $\mathscr{L}$ via the projection morphisms from G onto $G_i^{n_i}$.

The main technical point in our proof is an equivalence of line bundles (see [CVV12, Theorem 3.4]) which shows that there is an isogeny $\Phi : G' \to G'$ such that $\mathscr{L}|_H$ can be described in terms of $\Phi^*\mathscr{M}$.

We then show that $\hat{\mu}$ well behaves under isogenies. More precisely, as $\Phi(Y)$ is transverse in G', we have that the bound (♣) holds for $\Phi(Y)$ with respect to $\mathscr{M}$ and we prove that this implies the validity of (♢) for $\Phi(Y)$ in G' with respect to the pullback $\Phi^*\mathscr{M}$ (see [CVV12, Theorem 2.5]). This result, together with our equivalence of line bundles and the comparisons of the degrees and essential minima of the objects involved (computed with respect to the different morphisms and line bundles), allow to conclude.

We remark that the hypothesis on G in Galateau's result (and so an effective Bogomolov bound (♣)) holds more generally when G is a product of elliptic curves or abelian surfaces (with or without CM) or any abelian variety with CM (see [Gal10, p.551] for more details).

In [CV14], in collaboration with Evelina Viada, we generalise our main result from [CVV14] to abelian varieties with CM under certain assumptions on the subvariety X. More precisely, we prove the following:

Theorem 13 ([CV14, Theorem 1.4])**.** *Let G be an abelian variety with CM defined over $\overline{\mathbb{Q}}$. Suppose that G is isogenous to a product of simple abelian varieties all having dimension at most g. Let X be a weak-transverse subvariety of G with* $\operatorname{codim} X > g$. *Then there are only finitely many maximal X-torsion anomalous subvarietiesof relative codimension 1. In addition, their degrees and normalised heights are upper bounded by effective constants whose dependence in the variety X is explicit.*

The proof follows the same lines as the one of [CVV14, Theorem 1.4]: here too, we deal separately with cases where the torsion anomalous variety is a point, a translate of positive dimension or a non-translate. The main ingredients are the same, but the geometrical part on the construction of the auxiliary subgroup is more delicate and it forces the condition on $\operatorname{codim} X$ in the statement. We also discuss some applications of our result to new cases of the effective Mordell-Lang conjecture (see [CV14, Theorem 1.5 and Corollary 1.6]).

II. Some explicit results for points and applications to the Mordell-Lang and the Mordell conjectures (description of the results in [CVV17] and [CVV19])

In [CVV17], in collaboration with Francesco Veneziano and Evelina Viada, we prove upper bounds for the height of torsion anomalous points of relative codimension one when $G = E^N$ is a power of an elliptic curve, with or without CM. The case when E has CM was already treated in [CVV14]. The main novelty of [CVV17] is to introduce a new method which is not sensitive to the CM hypothesis and which gives (as in [CVV14]) effective bounds in the CM case and completely explicit bounds in the non CM case.

Although restricting oneself to points may appear, at first sight, a too particular choice in the context of Conjecture 2, its importance stands out in applications to the Mordell-Lang and Mordell conjectures, as we will explain later.

In order to state our explicit results we need to fix some notation. We let E be an elliptic curve defined over $\overline{\mathbb{Q}}$. We fix (once and for all) a Weierstrass equation for E. This gives an embedding of E^N in $\mathbb{P}_2^N$, which, composed with the Segre-embedding, extends to an embedding of E^N in $\mathbb{P}_{3^N-1}$. When computing heights and degrees of points and subvarieties of E^N, these are considered as embedded in $\mathbb{P}_{3^N-1}$ via the previous map. In particular, we denote by $\hat{h}$ the associated Néron-Tate height on E^N, by h the normalised height (see §3.2.(a)) and by $h_{\mathscr{W}}(E)$ the height of the Weierstrass equation of E (as defined in [CVV17, §2.2]). We can now state our main result from [CVV17]:

Theorem 14 ([CVV17, Theorem 1.1])**.** *Let $X \subset E^N$ be an irreducible subvariety. Then the set of maximal X-torsion anomalous points of relative codimension one has Néron-Tate height bounded by an effective constant $C(X,E,N)$.*

In particular, if E has no CM, the constant is explicit and can be taken as:

$$C(X,E,N) = C_1(N)h(X)(\deg X)^{N-1} + C_2(E,N)(\deg X)^N + C_3(E,N)$$

where

$$C_1(N) = (N!)^N N^{3N-2}\left(3^{N^2+N+1}2^{2N^2+3N-1}(N+1)^{N+1}\Gamma\left(\frac{N+1}{2}\right)^2\Gamma\left(\frac{N+2}{2}\right)^2\pi^{2-N}\right)^{N-1}$$

$$C_2(E,N) = C_1(N)\left(\frac{3^N\log 2}{2} + 12N\log 2 + N\log 3 + 6Nh_{\mathscr{W}}(E)\right)$$

$$C_3(E,N) = \frac{7N^2}{6}\log 2 + \frac{N^2}{2}h_{\mathscr{W}}(E),$$

where Γ is the Euler Gamma function.

We remark that this result could not be obtained with the method used in [CVV14], because of the use of the Lehmer bound from [Car09] therein, which is not available in the non-CM case. In contrast, the new proof strategy we introduce in [CVV17] does not distinguish CM from non CM elliptic curves and it was also applied later in [Via18] to compute explicit constants in the CM case as well, where further technical complications arise due to the structure of the endomorphism ring of E. Also, the bounds we obtain do not depend on the field of definition of X, unlike other bounds in similar contexts. This is important for our applications.

Here is a sketch of our proof, which is based on an approximation process. Let $P \in X \cap H$ be a maximal torsion anomalous point of relative codimension one, with H a torsion variety (minimal for P) of dimension $\dim H = 1 < \operatorname{codim} X$.

We first build an auxiliary translate H' having small degree and height bounded in terms of $\hat{h}(P)$ and $\deg H'$ and such that P is still a component of the intersection $X \cap H'$. We can then bound $\hat{h}(P)$ using the arithmetic Bézout theorem in terms of the height and the degree of H'. Combining carefully these inequalities (and optimally choosing certain parameters involved in the construction) leads to the desired result.

The construction of the auxiliary subgroup (done in [CVV17, Propositions 3.1 and 3.2]) is the core of our strategy and it is inspired by the work in tori by Habegger [Hab08]. Its proof is based on sharp estimates for the heights and the degrees in E^N (see [CVV17, §2.2 and §6]) and some geometry of numbers (see [CVV17, §7.4]).

As a first corollary of our result (see [CVV17, Corollary 1.2]) we get the finiteness of the maximal torsion anomalous points of relative codimension one in E^N.

However, as already anticipated, the more interesting application of our result is the following explicit case of the Mordell-Lang conjecture:

Theorem 15 ([CVV17, Theorem 1.3])**.** *Let $X \subseteq E^N$ be a curve where E has no CM. Let $P \in X$ be a point whose coordinates generate a subgroup of rank either zero or one.*

If X is weak-transverse and $N \geq 3$ then

$$\hat{h}(P) \leq C_1(N)h(X)(\deg X)^{N-1} + C_2(E,N)(\deg X)^N + C_3(E,N),$$

where the constants are the same as in Theorem 14.

If X is transverse and $N = 2$ then

$$\hat{h}(P) \leq 10^{35}h(X)(\deg X)^2 + 10^{36}(h_{\mathscr{W}}(E)+1)(\deg X)^3 + 8(h_{\mathscr{W}}(E)+1).$$

We refer to the statement of [CVV17, Theorem 1.3] for more precise bounds. In particular, in both cases, if k is a field of definition for E and $E(k)$ has rank 1, then all points in $\mathscr{C}(k)$ have Néron-Tate height effectively bounded as above.

This allows to prove some effective case of the Mordell conjecture (i.e. to bound effectively the height of the rational points) for an infinite family of curves of increasing genus in E^2 where E is a suitably chosen and fixed elliptic curve (see [CVV17, Theorem 1.4]). However, the bounds we obtain are still too big to be implemented and find all the rational points on such curves i.e. to solve the explicit Mordell conjecture for them.

The search for a method to solve some cases of the explicit Mordell conjecture has been our main motivation in [CVV19].

Before describing our result, and in order to better put it in context and be able to appreciate its novelty, it is perhaps worth giving a brief overview of the main known methods for explicitly finding rational points on certain curves of genus at least 2.

Before we begin, we must warn that, as already mentioned in the Introduction, no general method is known to work for all curves. None of the known proofs of the Mordell conjecture (as in [Fal83], [Voj91], [Fal91], [Bom90] or very recently in [LV20]) are in fact effective. Nevertheless, these proofs generally provide an upper bound (effective since [Bom90] and explicit since [Rém00]) on the number of rational points of a curve, the so-called quantitative version of the Mordell conjecture. Here, raised by a question of Mazur, comes the problem of uniformity, i.e. how this bound depends on the parameters of the problem. Although this issue does not concern us closely, we would like to mention the very recent break-through in [DGH21, Küh21, GGK21].

Returning to the explicit Mordell conjecture, a first method, of p-adic nature, was introduced by Chabauty [Cha41] and later refined by Coleman [Col85]. The method

gives a bound on the number of rational points of a curve X when, for instance, the group of rational points of its Jacobian J_X has rank strictly less than the genus $g(X)$ of the curve.

The idea is the following: one fixes a prime p and considers the closure $\overline{J_X(\mathbb{Q})}$ of $J_X(\mathbb{Q})$ in $J_X(\mathbb{Q}_p)$. It is now sufficient to prove that the intersection $X(\mathbb{Q}_p) \cap \overline{J_X(\mathbb{Q})}$ is finite as it contains clearly $X(\mathbb{Q})$. As $\dim X(\mathbb{Q}_p) = 1$ as a submanifold of $J_X(\mathbb{Q}_p)$, if one supposes that $\dim \overline{J_X(\mathbb{Q})} < g(X)$, one expects, by reasoning on dimensions, that $X(\mathbb{Q}_p) \cap \overline{J_X(\mathbb{Q})}$ has dimension 0 and thus is finite (as a discrete subset of the compact space $J_X(\mathbb{Q}_p)$), which is what Chabauty proved. We also notice that, in general, $\dim \overline{J_X(\mathbb{Q})} \leq \mathrm{rank} J_X(\mathbb{Q})$, so the hypothesis $\mathrm{rank} J_X(\mathbb{Q}) < g(X)$ is enough to apply the theorem. This strategy was later refined by Coleman, using p-adic integration, to get an explicit exploitable bound on the size of the intersection.

This method gives often a sharp bound on the number of rational points and, when this happens, possibly in combination with ad hoc descent arguments, one can manage to find them explicitly. See for example [Fly97] for some explicit applications of the Chabauty–Coleman method, [Sik13] for investigations on possible extensions of the method, and [McCP12] for a general survey.

Later, Kim [Kim05, Kim09] proposed a method that allows to replace the restriction on the Jacobian of the curve with a condition on a larger object, the Selmer variety. This was further studied in [BD18, BDMTV19, BD21, BBBM21], where the authors were able to apply it to determine the set of rational points in a number of new cases.

A second method was developed by Dem'janenko [Dem68] and then generalised by Manin [Man69]. It applies to curves X defined over a number field k which admit *enough independent* morphisms $\phi_1, \ldots, \phi_N$ to an abelian variety A, where *enough* means that $N > \mathrm{rank} A(k)$ and *independent* means that no nontrivial integral linear combination of the ϕ_i's is constant. Under such hypothesis, one can effectively compute the finite set $X(k)$. However the method does not give an explicit upper bound for the height of the rational points, which makes it difficult to apply.

We refer to [Ser89, §5.2] for a description of the method and to [Kul99, KMS04, GK05] for some applications to curves admitting morphisms to certain special elliptic curves. We also mention that in [Via03] an effective method is given in a setting similar to that in which the Manin-Dem'janenko method is applicable.

We remark that in the special case where $A = E$ is an elliptic curve, the condition on the existence of N linearly independent morphisms from X to E is equivalent to the fact that the image of X in E^N under such morphisms is a transverse curve.

Our main result in [CVV19] is a good explicit upper bound for the height of the points in the intersection of a curve of genus at least 2 in E^N with the union of all algebraic subgroups of E^N of dimension one, where E is an elliptic curve without CM, proving explicitly a particular case of the Mordell-Lang conjecture in an elliptic setting.

As before, we suppose that an elliptic curve E is given by a fixed Weierstrass equation $y^2 = x^3 + Ax + B$ with $A, B \in \overline{\mathbb{Q}}$, providing an embedding of E^N into $\mathbb{P}_2^N$ and then, via the

Segre embedding, into $\mathbb{P}_{3^N-1}$. Heights and degrees are computed via such embedding (see §3.2). We denote, in particular, by h_W the Weil-height on $\overline{\mathbb{Q}}$ and by h_∞ a modified version of the Weil height, which takes into account only the contributions coming from the Archimedean places (see [CVV19, §2.1]). Here is the statement of our main theorem:

Theorem 16 ([CVV19, Theorem 1.2])**.** *Let E be an elliptic curve without CM given by the equation $y^2 = x^3 + Ax + B$ with $A, B \in \overline{\mathbb{Q}}$, let j_E be its j-invariant and Δ_E its discriminant.*

Let X be an irreducible curve of genus at least 2 embedded in E^N, $N \geq 2$. Suppose that $P \in X(\overline{\mathbb{Q}})$ is contained in a minimal algebraic subgroup of E^N of dimension one.

Then if $N = 2$ we have

$$\hat{h}(P) \leq 73 \cdot h_2(X) \deg X + 73\,(6 + c_1(E)/2)\,(\deg X)^2 + c_2(E)$$

while if $N \geq 3$ we have

$$\hat{h}(P) \leq 17 \cdot 3^N \cdot N! \cdot h_2(X)(\deg X)^2 + 2 \cdot 3^{2N} \cdot N! \cdot c_1(E)(\deg X)^3$$

where

$$c_1(E) = h_W(j) + 2h_W(\Delta) + 2h_\infty(j) + 4h_W(A) + 4h_W(B) + 30.$$
$$c_2(E) = h_W(\Delta) + h_\infty(j) + 2h_W(A) + 2h_W(B) + 8.$$

Our main theorem generalises and drastically improves a previous result obtained in [CVV17]: there we considered only weak-transverse curves and only torsion anomalous points. Moreover the bounds obtained in [CVV17] were much worse and not implementable in any concrete case.

To go beyond the more restrictive setting of [CVV17] we introduce new key elements in the proof. This change in approach leads to improvements of the bounds which are crucial for the applications we will discuss later.

We now give a sketch of the proof of [CVV19, Theorem 1.2]. If P is a point on X of rank zero, then it is a torsion point and the theorem is trivially true. So the interesting case are points of rank one.

We first use geometric construction which shows how to deduce the general case from the case $N = 2$ (see [CVV19, Theorem 4.3]). More precisely, we consider the projection $\pi : E^N \to E^2$ from E^N onto any two factors. If P is a point of rank one on $X \subset E^N$, we bound $\hat{h}(P)$ in terms of $\hat{h}(\pi(P))$ and the degree and the height of $\pi(X)$ in terms of those of X by using, amongst others, results by Masser and Wüstholz on isogenies of elliptic curves [MW90] and Zhang's inequality. This procedure, only briefly sketched here, is adapted to the different cases in which X is transverse or weak-transverse in E^N and allows us to reduce to the case of a curve X in E^2 of genus at least 2.

If $N = 2$, as in [CVV17], the core of the proof is construction of a suitable auxiliary subgroup of E^2 whose intersection with X still contains P as component. More precisely, we fix two parameters $k > 1$ and t big enough with respect to k and we construct an elliptic curve $\mathscr{E} \subset E^2$ such the translate $\mathscr{E} + P$ has degree at most t and height at most $18(k^2/t)\hat{h}(P) + 4tc_1(E)$. To this end we use, among other things, some classical results

of the geometry of numbers; as $N = 2$, we can do this in a much finer way than we did in [CVV17] and this is what prevents the bounds from growing too much.

We then notice that P is a component of the intersection $X \cap (\mathscr{E} + P)$, otherwise we would have $X = \mathscr{E} + P$, contradicting the fact that the genus of X is at least 2. Using the arithmetic Bézout theorem we can then bound the height of P in terms of the height and the degree of X and $\mathscr{E}$ and an optimal choice of the parameters k and t, together with accurate explicit comparisons described in [CVV19, §3] between the different height functions we use, lead to the conclusion.

A significant feature of our main theorem is that it can easily be applied to find all the rational points on certain explicit infinite families of curves of increasing genus. Just to give one example, we prove the following:

Theorem 17 ([CVV19, Theorem 1.5 & Appendix A.4])**.** *Let E be the elliptic curve given by the Weierstrass equation $y^2 = x^3 + x - 1$ and write $y_1^2 = x_1^3 + x_1 - 1$, $y_2^2 = x_2^3 + x_2 - 1$ for the equations of E^2 in $\mathbb{P}_2^2$ using affine coordinates $\big((x_1, y_1), (x_2, y_2)\big)$. Let O be the neutral element of E.*

Let $X_n \subset E^2$ be the projective closure of the curve defined via the additional equation $\Phi_n(x_1) = y_2$, where $\Phi_n(x)$ is the n-th cyclotomic polynomial. Then

$$
\begin{aligned}
&X_1(E_1)(\mathbb{Q}) = \{(O,O), \big((2,3),(1,1)\big), \big((2,-3),(1,1)\big)\} \\
&X_2(E_1)(\mathbb{Q}) = \{(O,O), \big((2,3),(2,3)\big), \big((2,-3),(2,3)\big)\} \\
&X_6(E_1)(\mathbb{Q}) = \{(O,O), \big((1,1),(1,1)\big), \big((1,-1),(1,1)\big), \big((2,3),(2,3)\big), \big((2,-3),(2,3)\big)\} \\
&X_n(E_1)(\mathbb{Q}) = \{(O,O)\} && \text{if } n > 2 \text{ and } n = p^m \text{ with } p \neq 3, 47, \\
&X_n(E_1)(\mathbb{Q}) = \{(O,O), \big((1,1),(2,3)\big), \big((1,-1),(2,3)\big)\} && \text{if } n = 3^m, \\
&X_n(E_1)(\mathbb{Q}) = \{(O,O), \big((1,1),(13,47)\big), \big((1,-1),(13,47)\big)\} && \text{if } n = 47^m, \\
&X_n(E_1)(\mathbb{Q}) = \{(O,O), \big((1,1),(1,1)\big), \big((1,-1),(1,1)\big)\} && \text{if } n \geq 7 \text{ is not a prime power.}
\end{aligned}
$$

The elliptic curve E in the theorem has no CM and is such that $E(\mathbb{Q})$ has rank 1. As already said, this is just an example of what we obtain and we refer to [CVV19, Theorem 1.5 and Appendix A] for many more examples.

For the curves we consider the bounds for the height of the rational points obtained applying our main theorem [CVV19, Theorem 1.2] are so good that we can carry out a fast computer search and determine all the rational points for all n up to a quite large bound. The computations have been executed with PARI/GP using an algorithm by K. Belabas based on a sieving method and described in [CVV19, §9]. In [CVV19, Appendix A] M. Stoll completes the study of the rational points by showing that, for n large enough, all rational points on the curves must be integral in E^2 and a quick computation with Magma is enough to find them. This is obtained by combining our upper bound for the height of the rational points with a lower bound obtained by studying the ℓ- adic behaviour of points on the curve close to the origin.

In [CVV19, Appendix A.1] M. Stoll makes a very nice and detailed comparison between our method and that of Manin-Dem'janenko, explaining concretely in which cases one method is more advantageous than the other.

We also remark that in [Via18] the author has established some generalizations of our results, for instance for elliptic curves with CM and higher Mordell-Weil rank. We finally mention the recent result in [VV21], where the authors generalise the method of [CVV19] to bound the height of points of rank at most $n-1$ on transverse curves embedded in E^n, where E is an elliptic curve defined over $\overline{\mathbb{Q}}$.

3.4. Some perspectives

(i) Lower bounds for the height in $\mathbb{G}_m^n$.

This research goal is part of a project with Francesco Amoroso, Gaël Rémond, Matteo Viale and Martin Weimann that started as part of an application for an IEA (International Emerging Actions) project of the CNRS.

As recalled in the Introduction, Conjecture 2 has been proved for varieties of codimension at most 2 in $\mathbb{G}_m^n$. Two proofs of this theorem are now known. The original one by Bombieri and Zannier, detailed in [Zan00], and one by Bombieri, Masser and Zannier in [BMZ07]. Moreover, as explained in §3.3, the elliptic analogue of this theorem has been proved using a new method in [CVV14]. The bounds that appear in the above cited proofs are not explicit, although they are effective.

An explicit version of such results for tori would provide, in particular, an explicit version of a result first conjectured by Schinzel [Sch65] which has notably applications to the factorization of lacunary polynomials and the search for their multiple roots (see for instance [FGS08, ALS15, ASZ17]).

The aim of this project is to develop the analogue for subvareties of $\mathbb{G}_m^n$ of the proof of [CVV14] by making the bounds explicit and in particular their dependence on n. This question has been explicitly asked several times, notably in [FGS08].

To start with: One of the points which has to be clarified and make explicit is a transfer theorem of Rémond [Rém17] which shows the equivalence between two versions of the generalized Lehmer conjecture of [AD03]. This is a key ingredient to ensure that our strategy produces explicit constants.

CHAPTER 4

ARITHMETIC PROPERTIES OF MAHLER FUNCTIONS

In this chapter, I present some results I have obtained on the arithmetic of Mahler functions, which are power series with algebraic coefficients satisfying a particular type of functional equation. After a brief introduction to the problem, I will describe the results I obtained in collaboration with my co-author in [CR17], showing, in particular, how certain arithmetic properties of Mahler functions mirror on the functional equation.

This is a topic that remains somewhat peripheral to my main research centres and on which I have been less active than others, but on which I have recently started a new project that I will describe at the end of the chapter.

List of articles presented in this chapter

[CR17] «On certain arithmetic properties of Mahler functions. »
(with J. ROQUES), *Israel Journal of Mathematics*, Volume 228, Issue 2, 801–833 (2018).

4.1. Introduction

A *Mahler function* is a power series $f(z) \in \overline{\mathbb{Q}}[[z]]$ satisfying an equation of the form

$$p_d(z) f(z^{\ell^d}) + p_{d-1}(z) f(z^{\ell^{d-1}}) + \ldots + p_0(z) f(z) = 0 \qquad (\star)$$

where $\ell \geq 2$ is an integer and $p_0(z), \ldots, p_d(z) \in \overline{\mathbb{Q}}[z]$ are not all zero. These functions have been extensively studied, starting with the seminal work of Mahler [Mah29, Mah30a, Mah30b], investigating the algebraic relations between their values at algebraic points.

The first example considered by Mahler was the function $f(z) = \sum_{n=0}^{\infty} z^{2^n}$: exploiting the fact that it satisfies the equation $f(z^2) - f(z) + z = 0$, Mahler was able to prove that $f(z)$, beside not being algebraic over $\overline{\mathbb{Q}}(z)$, even takes transcendental values at all non-zero algebraic points inside its domain of convergence, the unit disc. This new

approach in transcendence theory lead to a way more general method, later called *Mahler's method*, and was further explored and developed by many authors, such as Becker, Kubota, Loxton, van der Poorten, Masser, Nishioka, Töpfer, just to cite some. This introduction is not the appropriate place to say more about the vast literature on Mahler's method, of which I am by no means an expert. For a detailed account on the subject and a complete list of referencese I refer to Nishioka's book [Nis97] and to the recent very nice survey by Adamczewski [Ada19].

Other examples considered by Mahler already in [Mah29] include solutions of the following special Mahler equations

$$f(z) = p(z)f(z^\ell). \tag{$\star\star$}$$

For instance, if $p(x) = 1 - z$ the (unique, up to a multiplicative constant) solution of ($\star\star$) is $f(z) = \sum_{n=0}^{\infty}(-1)^{t_n}z^n$ where $(t_n)_n$ is the so called Thue-Morse sequence and t_n is the number of non-zero digits in the binary expansion of n. This is an example of an automatic sequence and it is precisely because of its connection to these objects that, in recent decades, Mahler's method took on renewed relevance and enhanced interest.

We briefly recall that, if $\mathscr{A}$ is a finite alphabet and $k \geq 2$ is an integer, a sequence $(f_n)_n \in \mathscr{A}^{\mathbb{N}}$ is called *k-automatic* if, for every n, f_n can be computed by a finite state machine (called *automaton*). This machine, takes in input the expansion of n in base k and, starting from an initial state, associates each digit it reads with a state transition. Each possible state comes with an associated output value and f_n equals the output attached to the last state reached after reading all the digits of n in base k. For more informations about the theory of automata, we refer to [AS03]. This notion was introduced by Cobham in [Cob68], who proved (see [Cob72]) that $(f_n)_n$ is k-automatic if and only if its *k-kernel* i.e. the set of the subsequences of the form $(f_{k^e n+a})_n$ with $e \geq 0$ and $0 \leq a < k^e$, is finite. The notion of k-automaticity was later generalised by Allouche and Shallit [AS92] to k-regularity: a sequence $(f_n)_n$ with values in a $\mathbb{Z}$-module R (possibly infinite) is k-regular if its k-kernel is contained in a finitely generated $\mathbb{Z}$-module. Thus, as shown in [AS03, Theorem 16.1.5], k-automatic sequences are precisely k-regular sequences taking finitely many values.

The link to Mahler functions comes from the fact that, as proved by Becker [Bec94], if $(f_n)_n$ is k-regular then its generating function $f(z) = \sum_{n=0}^{\infty} f_n z^n$ is a Mahler function (see [LP88] for the previously known special case of automatic sequences). The question arises naturally of whether it is possible to characterise Mahler functions coming from regular sequences. In this direction, Becker shows [Bec94, Theorem 2] that if $f(z)$ satisfies ($\star$) with $p_0(z) = 1$, then the coefficients of its series expansion form a k-regular sequence. He also conjectured [Bec94, p.279] that a weaker converse should hold and, more precisely, that if $f(z)$ is k-regular (i.e. it is the generating function of a k-regular sequence), then $f(z)/r(z)$ satisfies ($\star$) with $p_0(z) = 1$ for some k-regular rational function $r(z)$. A stronger form of this conjecture was recently proved in [BCCD19], where the authors show that one can even take $r(z) = z^m q(z)$ for some integer $m \geq 0$ and polynomial $q(z)$ with $q(0) = 1$ and such that $1/q(z)$ is k-regular. The following question arises then naturally:

(Q) Which properties of a Mahler function can be read on its functional equation? In particular, is it possible to detect on ($\star$) if its solutions are the generating function of some automatic sequence?

4.2. Description of the results

In [CR17], in collaboration with J. Roques, we are mainly interested in Mahler functions satisfying equation ($\star\star$) where $p(z) \in \mathbb{Z}[z]$ and $p(0) = 1$. Up to a multiplicative constant, ($\star\star$) has a unique solution given by the infinite product

$$f(z) = \prod_{i \geq 0} p(z^{\ell^i}).$$

As in question (Q), one of our aims is to study how the behaviour of $f(z)$ mirrors on the polynomial $p(z)$.

Duke and Nguyen [DN15] studied an aspect of this question in the case where ℓ is a prime and $p(z) = \Phi_m(z)$ is the m-th cyclotomic polynomial. They ask in particular under which conditions on $p(z)$ the solution $f(z)$ is a rational function.

One of the main results of [DN15] states that $f(z)$ is rational if and only if ℓ divides m, in which case $f(z) = 1/\Phi_d(z^{\ell^{r-1}})$ where $m = \ell^r d$, $r \geq 1$ and $\ell \nmid d$, and that $f(z)$ has the unit circle as a natural boundary otherwise (see [DN15, Theorem 1]).

The proof of their result partly bases on a modified version of Mahler's approach to the case $m = 1$, which consists in studying the behaviour of $f(z)$ as z approaches certain roots of unity. More precisely, they determine (see [DN15, Theorem 2]) the asymptotic behaviour of $f(z)$ as z tends radially to a root of unity of order prime to ℓ, by using the arithmetic properties of the Dirichlet series attached to $f(z)$. We mention that, in this setting, the asymptotic of the coefficients of $f(z)^{-1}$ was precisely described in [DF96] for any integer $\ell \geq 2$ prime to m.

As a first result, we obtain the following generalization of [DN15, Theorem 1].

Theorem 18 ([CR17, Theorem 1.1])**.** *Let $\ell \geq 2$ be an integer, $p(z) \in \mathbb{Z}[z]$ a polynomial with $p(0) = 1$ and let $f(z)$ be a solution of $f(z) = p(z) f(z^\ell)$.*

Suppose that $p(z)$ is monic and that there exists infinitely many integers m prime to ℓ such that $f(z)$ is bounded as z tends radially to any m-th primitive root of unity. Then $p(z)$ is the product of cyclotomic polynomials. Moreover, if ℓ is prime, the following conditions are equivalent:

(1) $p(z)$ is monic and, for almost all roots of unity ζ of order prime to ℓ, $f(z)$ is bounded as z tends to ζ radially;
(2) $p(z)$ is a product of cyclotomic polynomials of order divisible by ℓ;
(3) $f(z)$ is rational.

The proof relies on a simplified but more general version of [DN15, Theorem 2] (see [CR17, Proposition 2.1]) which describes the asymptotic behaviour of $f(z)$ as z approaches radially a root of unity ζ of order $\ell^n - 1$ and shows, in particular, that this depends on the value $\prod_{k=0}^{n-1} p(\zeta^{\ell^k})$. This description is then used to deduce some strong

bound for the absolute value of the norm of $p(z)$ evaluated at roots of unity, which implies that $p(z)$ is a product of cyclotomic polynomials. Our proof of [CR17, Proposition 2.1] is different in nature than the one of [DN15, Theorem 2]: we first consider a certain functional equation (a q-difference equation) satisfied by $f(\zeta e^t)$, where ζ is a root of unity of order prime to ℓ, then we construct another suitable solution to this equation and use it to study the behaviour of $f(\zeta e^t)$ as t tends to 0.

A second natural question we consider is how to characterize Mahler equations whose solutions are generating functions of automatic sequences, a problem which seems highly non trivial even for equation ($\star\star$). In this special case, we investigate whether it is possible to classify all polynomials $p(z)$ for which any solution $f(z) = \sum_{n=0}^{\infty} f_n z^n$ of ($\star\star$) is the generating function of an automatic sequence $(f_n)_n$. As remarked above, this is equivalent to asking that $(f_n)_n$ takes finitely many values.

It is easy to see that $(f_n)_n$ is automatic when $p(z)$ is a product of certain cyclotomic polynomials of order divisible by ℓ (see [CR17, Proposition 5.1]), and the question is whether there are other examples. The second result of the paper answers this question, for $p(z)$ monic, when either ℓ is big or $\deg p$ is small:

Theorem 19 ([CR17, Theorem 1.2])**.** *Let $\ell \geq 2$ be an integer and let $f(z) = \sum_{i=0}^{\infty} f_n z^n$ be a solution of $f(z) = p(z) f(z^\ell)$, with $p(z) \in \mathbb{Z}[z]$ monic such that $p(0) = 1$. Then:*

(1) If $\ell > \deg p$, $(f_n)_n$ is automatic if and only if the coefficients of $p(z)$ are in $\{0, \pm 1\}$.
(2) If $\deg p = \ell = 2$, $(f_n)_n$ is automatic if and only if $p(z) \in \{z^2 + 1, z^2 - z + 1\}$.
(3) If $\deg p = 3 \geq \ell$, $(f_n)_n$ is automatic if and only if $\ell = 2$ and $p(z) = z^3 + 1$ or $\ell = 3$ and $p(z) \in \{z^3 + 1, z^3 - z^2 + 1, z^3 - z + 1\}$.

Here are some ideas in the proof. It is easy to deduce from ($\star\star$) that the coefficients of $f(z)$ satisfy a divide-and-conquer type recurrence (see [Dum93] for more details). When $\ell > \deg p(x)$ the recurrence is particularly simple and is enough to prove the theorem. If $\ell \leq \deg p$, things gets more involved and the proof relies on the theory of Cartier operators (see [CR17, §5.3]).

A reason a parte to study Mahler functions with bounded coefficients is given in [CR17, §6] in relation to G-functions and E-functions, which are power series satisfying a homogeoneous linear differential equation and whose coeffcients fulfill special growth conditions.

As a consequence of a general index theorem for Mahler operators [CR17, Theorem 6.1], we prove in [CR17, Proposition 6.4]) that the coefficients of any Mahler function satisfy automatically certain conditions defining the G-functions and even some stronger properties (characteristic of globally bounded functions, see [CR17, Definition 6.3]).

We finally remark that similar problems have been recently considered by S. Li in his PhD thesis [Li20], where he shows, in particular, that given $\ell \geq 2$ and $d \geq 1$ there are finitely many polynomials $p(z) \in \mathbb{Q}[z]$ of degree d such that the solutions of ($\star\star$) are generating functions of some automatic sequence (see [Li20, Proposition 4.5]).

4.3. Some perspectives

(i) Mahler measure of automatic polynomials.

This research goal is part of a starting project with Tanguy Rivoal which aims to study the arithmetic properties of certain families of polynomials attached to automatic sequences.

To an automatic sequence $(f_n)_n$, we can attach a sequence of "automatic polynomials" $(p_m(x))_m$, where $p_m(x)$ is the polynomial having as coefficients the first m terms of the sequence. In this project, we are interested in understanding the growth of the Mahler measures of the sequences of such polynomials.

The only known results on this subject concern the polynomials associated with the Rudin-Shapiro sequence by Erdelyi ([Erd16, Erd20]) who, motivated by conjectures of Saffari and Montgomery, gives asymptotic formulas for the Mahler measure of these polynomials. He shows, in particular, that the sequence of these Mahler measures is unbounded and it is natural to ask whether the same phenomenon occur for any automatic sequence.

This question is also interesting because, as recalled before, the generating functions of automatic sequences are examples of Mahler functions. In the paper [ABS21], the authors study the growth of coefficients of Mahler functions. Their result implies that if the generating function of $(f_n)_n$ is a Mahler function, then the Mahler measures of the associated polynomials are, in general, unbounded, the only case left open being the one where the sequence is automatic.

In this framework, new results, even for a single new example of a family of automatic polynomials, would be very interesting and, apparently, highly non-trivial.

BIBLIOGRAPHY

[Ada19] B. Adamczewski, *Mahler's method*, Doc. Math. Extra Volume Mahler Selecta, 95–122 (2019).

[ABS21] B. Adamczewski, J. Bell and D. Smertnig. *A height gap theorem for coefficients of Mahler functions*. J. Eur. Math. Soc. to appear (2021).

[AS92] J.-P. Allouche and J. Shallit, *The ring of k-regular sequences*, Theoret. Comput. Sci. 98, 163–197 (1992).

[AS03] J.-P. Allouche and J. Shallit, *Automatic sequences. Theory, applications, generalizations*. Cambridge University Press, Cambridge, (2003).

[Amo16a] F. Amoroso, *On a conjecture of G. Rémond*. Ann. Scuola Norm. Sup. Pise Cl. Sci. (5) 15, 599-608 (2016).

[Amo16b] F. Amoroso, *Mahler measure on Galois extensions*. Bull. London Math. Soc., 48, 1008–1012 (2016).

[AD99] F. Amoroso and S. David, *Le problème de Lehmer en dimension supérieure*, J. Reine Angew. Math. 513, 145–179 (1999).

[AD03] F. Amoroso and S. David, *Minoration de la hauteur normalisée dans un tore*. J. Inst. Math. Jussieu 2, 335–381 (2003).

[AD21] F. Amoroso and S. David, *On the Galois group of lacunary polynomials*, Rivista di Matematica della Università di Parma, Istituto di Matematica, In press (2021).

[AD00] F. Amoroso and R. Dvornicich, *A lower bound for the height in abelian extensions*. Journal of Number Theory 80, 260–272 (2000).

[ADZ14] F. Amoroso, S. David and U. Zannier, *On fields with property (B)*. Proceedings of the AMS, vol. 142, Number 6, 1893–1910 (2014).

[ALS15] F. Amoroso, L. Leroux, and M. Sombra, *Overdetermined systems of sparse polynomial equations*. Found. Comput. Math. 15, 53-87 (2015).

[AM16] F. Amoroso and D. Masser, *Lower bounds for the height in Galois extensions*. Bull. London Math. Soc. 48, 1008–1012 (2016).

[AN07] F. Amoroso and F. Nuccio, *Algebraic Numbers of Small Weil's height in CM-fields: on a Theorem of Schinzel*. J. Number Theory 122, no. 1, 247–260 (2007).

[APSV] F. Amoroso, I. Pritsker, C. Smyth and J. Vaaler, *Appendix to Report on BIRS workshop 15w5054 on The Geometry, Algebra and Analysis of Algebraic Numbers: Problems proposed by participants*. Available at http://www.birs.ca/workshops/2015/15w5054/report15w5054.pdf

[AZ00] F. Amoroso and U. Zannier, *A relative Dobrowolski's lower bound over abelian extensions*. Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) 29, no. 3, 711–727 (2000).

[ASZ17] F. Amoroso, M. Sombra and U. Zannier, *Unlikely intersections and multiple roots of sparse polynomials*. Math. Zeitschrift 287, no 3-4, 1065-1081 (2017).

[AZ10] F. Amoroso and U. Zannier, *A uniform relative Dobrowolski's lower bound over abelian extensions*. Bull. London Math. Soc., 42, no. 3, 489–498 (2010).

[BBBM21] J. S. Balakrishnan, A. Besser, F. Bianchi and J. S. Müller, *Explicit quadratic Chabauty over number fields*. Israel Journal of Mathematics, 243 (1), 185–232 (2021).

[BD18] J. S. Balakrishnan and N. Dogra, *Quadratic Chabauty and rational points, I : P-adic heights*. Duke Mathematical Journal, 167 (11) (2018).

[BD21] J. S. Balakrishnan and N. Dogra, *Quadratic Chabauty and Rational Points II : Generalised Height Functions on Selmer Varieties*. International Mathematics Research Notices, 2021 (15), 11923–12008 (2021).

[BDMTV19] J. S. Balakrishnan, N. Dogra, J. S. Müller, J. Tuitman and J. Vonk, *Explicit Chabauty—Kim for the split Cartan modular curve of level 13*. Annals of Mathematics, 189 (3), 885–944 (2019).

[BD22] F. Barroero and G. Dill, *On the Zilber-Pink conjecture for complex abelian varieties*. Ann. Sci. Éc. Norm. Supér. (4) 55, no. 1, 261–284 (2022).

[Bau16] H. Bauchère. *Quelques remarques à propos d'un théorème de Checcoli*. J. Théor. Nombres Bordeaux 28, no. 3, 725–734 (2016).

[BCCD19] J. P. Bell, F. Chyzak M. Coons and P. Dumas, *Becker's conjecture on Mahler functions*, Trans. of the Amer. Math. Soc. 372, no. 5, 3405–3423 (2019).

[Bec94] P. G. Becker, *k-Regular power series and Mahler-type functional equations*, J. Number Theory 49, 269–286 (1994).

[Bom90] E. Bombieri. *The Mordell conjecture revisited*. Annali della Scuola Normale Superiore di Pisa-Classe di Scienze, 17(4):615–640 (1990).

[BHMZ10] E. Bombieri, P. Habegger, D. Masser, and U. Zannier, *A note on Maurin's theorem*. Atti Accad. Naz. Lincei Rend. Lincei Mat. Appl. 21, no. 3, 251–260 (2010).

[BV83] E. Bombieri and J. Vaaler, *On Siegel's lemma*. Inventiones Mathematicae. 73 (1): 11–32 (1983).

[BMZ99] E. Bombieri, D. Masser, and U. Zannier, *Intersecting a curve with algebraic subgroups of multiplicative groups*. Internat. Math. Res. Notices, no. 20, 1119–1140 (1999).

[BMZ07] E. Bombieri, D. Masser, and U. Zannier, *Anomalous subvarieties–structure theorems and applications*. Int. Math. Res. Not. IMRN. 19, 33 pages (2007).

[BMZ08a] E. Bombieri, D. Masser, and U. Zannier, *Intersecting a plane with algebraic subgroups of multiplicative groups*. Ann. Sc. Norm. Super. Pisa Cl. Sci. 7, no. 5, 51-80 (2008).

[BMZ08b] E. Bombieri, D. Masser, and U. Zannier, *On unlikely intersections of complex varieties with tori*. Acta Arith. 133, no. 4, 309-323 (2008).

[BZ01] E. Bombieri and U. Zannier, *A note on heights in certain infinite extensions of* $\mathbb{Q}$. Rend. Mat. Acc. Lincei, 12 , 5-14 (2001).

[BGS94] J-B. Bost, H. Gillet, and C. Soulé, *Heights of projective varieties and positive Green forms*. J. Amer. Math. Soc. **7**, no. 4, 903–1027 (1994).

[Car09] M. Carrizosa, *Petits points et multiplication complexe*. Int. Math. Res. Not. IMRN, no. 16, 3016–3097 (2009).

[Cha41] C. Chabauty, *Sur les points rationnels des courbes algébriques de genre supérieur à l'unité*. C. R. Acad. Sci. Paris, 212, 882–885 (1941).

[Che13] S. Checcoli, *Fields of algebraic numbers with bounded local degrees and their properties*. Transactions of the American Mathematical Society, 365, no. 4, 2223-2240 (2013) .

[Che19] S. Checcoli, *A note on Galois groups and local degrees*. Manuscripta Mathematica, 159 (1), 1-12 (2019).

[CD16] S. Checcoli and P. Dèbes, *Tchebotarev theorems for function fields*. J. Algebra, vol. 446, 346–372 (2016).

[CF21] S. Checcoli and A. Fehm, *On the Northcott property and local degrees*. Proc. Amer. Math. Soc. 149, 2403-2414 (2021).

[CF22] S. Checcoli and A. Fehm, *Constructing totally p-adic numbers of small height*. Int. Journ. Numb. Theory, Vol.18, No. 03, 501-514 (2022).

[CR17] S. Checcoli and J. Roques, *On certain arithmetic properties of Mahler functions*. Israel Journal of Mathematics, Volume 228, Issue 2, 801–833 (2018).

[CVV12] S. Checcoli, F. Veneziano and E. Viada, *A sharp Bogomolov-type bound*. New York Journal of Mathematics, 18 (2012) 891-910.

[CVV14] S. Checcoli, F. Veneziano and E. Viada, *On torsion anomalous intersections*. Rend. Lincei Mat. Appl., Volume 25, Issue 1, 1–36 (2014).

[CVV17] S. Checcoli, F. Veneziano and E. Viada, *On the explicit Torsion Anomalous Conjecture*. Trans. Amer. Math. Soc., Vol. 369, no. 9, 6465–6491 (2017).

[CVV19] S. Checcoli, F. Veneziano and E. Viada, *The explicit Mordell Conjecture for families of curves (with an appendix by M. Stoll)*. Forum of Mathematics, Sigma (2019), Vol. 7, e31, 62 pages.

[CV14] S. Checcoli and E. Viada,*On the Torsion Anomalous Conjecture in CM abelian varieties*. Pacific Journal of Math. 271-2 (2014), 321–345.

[CW13] S. Checcoli and M. Widmer, *On the Northcott property and other properties related to polynomial mappings*. Math. Proc. Camb. Phil. Soc., 155, 1–12 (2013).

[CZ11] S. Checcoli and U. Zannier, *On fields of algebraic numbers with bounded local degrees*. Comptes Rendus Mathématique, Volume 349, Issue 1, 11-14 (2011).

[Cob68] A. Cobham, *On the Hartmanis-Stearns problem for a class of tag machines*. Conference Record of 1968 Ninth Annual Symposium on Switching and Automata Theory, Schenectady, New York, 51–60 (1968).

[Cob72] A. Cobham, *Uniform tag sequences*. Math. Systems Theory 6, 164–192 (1972).

[Col85] R. F. Coleman, *Effective Chabauty*. Duke Mathematical Journal, 52 (3) (1985).

[Col03] J.-L. Colliot-Thélène, *Points rationnels sur les fibrations*. In Higher dimensional varieties and rational points (Budapest, 2001), Bolyai Soc. Math. Stud., vol. 12, Springer, 171–221 (2003).

[DP98] S. David and P. Philippon, *Minorations des hauteurs normalisées des sous-variétés de variétés abéliennes*. Number theory (Tiruchirapalli, 1996), Contemp. Math., vol. 210, Amer. Math. Soc., Providence, RI, 333–364 (1998).

[DP02] S. David and P. Philippon, *Minorations des hauteurs normalisées des sous-variétés de variétés abéliennes II*. Comment. Math. Helv. 77, no. 4, 639–700 (2002).

[DP07] S. David and P. Philippon, *Minorations des hauteurs normalisées des sous-variétés des puissances des courbes elliptiques*. Int. Math. res. pap. IMRP, no.3 (2007).

[DG12] P. Dèbes and N. Ghazi, *Galois covers and the Hilbert-Grunwald property*. Ann. Inst. Fourier 62, 989–1013 (2012).

[Del09] E. Delsinne, *Le problème de Lehmer relatif en dimension supérieure*. Ann. Sci. Éc. Norm. Supér. (4) 42, no. 6, 981–1028 (2009).

[DH92] K. Doerk and T. Hawkes, *Finite Solvable Groups*. De Gruyter, Berlin/New York (1992).

[DLAN17] C. Demarche, G. Lucchini Arteche and D. Neftin, *The Grunwald problem and approximation properties for homogeneous spaces*. Annales de l'institut Fourier, 67 no. 3, 1009–1033 (2017).

[Dem68] V. Dem'janenko, *Rational points of a class of algebraic curves*. Amer. Math. Soc. Transl., Vol. 66, pp. 246–272, Amer. Math. Soc., Providence (1968).

[DGH21] V. Dimitrov, Z. Gao and P. Habegger, *Uniformity in Mordell–Lang for curves*. Annals of Mathematics, 194(1):237–298 (2021).

[Dob79] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*. Acta Arith. 34, 391–401 (1979).

[Dum93] P. Dumas, *Récurrences mahlériennes, suites automatiques, études asymptotiques*. PhD Thesis, Université Bordeaux I (1993).

[DF96] P. Dumas and P. Flajolet, *Asymptotique des récurrences mahlériennes: le cas cyclotomique*. J. Théor. Nombres Bordeaux 8, no. 1, 1–30 (1996).

[DN15] W. Duke and H. Nguyen, *Infinite products of cyclotomic polynomials*. Bull. Aust. Math. Soc. 91, no. 3, 400–411 (2015).

[DZ07] R. Dvornicich and U. Zannier, *Cyclotomic Diophantine problems*. Duke Math. J. 139, no. 3, 527-554 (2007).

[DZ08] R. Dvornicich and U. Zannier, *On the properties of Northcott and Narkiewicz for fields of algebraic numbers*. Functiones et Approximatio 39, no. 1, 163-173 (2008).

[Erd16] T. Erdèlyi, *The Mahler measure of the Rudin-Shapiro polynomials*. Constr. Approx. 43, 357-369 (2016).

[Erd20] T. Erdèlyi, *The asymptotic value of the Mahler measure of the Rudin-Shapiro polynomials*. J. Anal. Math., 142, Issue: 2, 521-537 (2020).

[Fal83] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*. Inventiones Mathematicae (in German). 73 (3): 349–366 (1983).

[Fal91] G. Faltings, *Diophantine approximation on abelian varieties*. Ann. of Math. (2), 133(3), 549–576 (1991).

[Fal94] G. Faltings, *The general case of S. Lang's conjecture*. Barsotti Symposium in Algebraic Geometry (Abano Terme, 1991), Perspective in Math., vol. 15, Academic Press, San Diego, 175–182 (1994).

[Feh18] A. Fehm, *Three counterexamples concerning the Northcott property of fields*. Atti Accad. Naz. Lincei Rend. Lincei Mat. Appl., 29 (2) (2018).

[FGS08] M. Filaseta, A. Granville, and A. Schinzel, *Irreducibility and greatest common divisor algorithms for sparse polynomials*. Number theory and polynomials, London Math. Soc. Lecture Notes Ser., vol. 352, Cambridge Univ. Press, 155-176 (2008).

[Fil14] P. Fili, *On the heights of totally p-adic numbers*. J. Théor. Nombres Bordeaux 26(1): 103–109 (2014).

[FP15] P. Fili and C. Petsche, *Energy Integrals Over Local Fields and Global Height Bounds*. International Mathematics Research Notices 2015(5), 1278–1294 (2015).

[FP19] P. Fili and L. Pottmeyer, *Quantitative height bounds under splitting conditions*. Trans. Amer. Math. Soc. 372, 4605–4626 (2019).

[Fly97] E. V. Flynn, *A flexible method for applying Chabauty's theorem*. Compos. Math. 105(1) 1857, 79–94 (1997).

[FJ04] M. D. Fried and M. Jarden, *Field Arithmetic*. Second edition, Ergebnisse der Mathematik und ihrer Grenzgebiete, vol.11, Springer-Verlag, Berlin (2004).

[FV92] M. D. Fried and H. Völklein, *The embedding problem over a Hilbertian PAC-field*. Ann. of Math. (2) 135(3) 469–481 (1992).

[GG14] I. Gal and R. Grizzard, *On the compositum of all degree d extensions of a number field*. Journ. de Théorie des Nombres de Bordeaux 26, no. 3, 655-672 (2014).

[Gal10] A. Galateau, *Une minoration du minimum essentiel sur les variétés abéliennes*. Comment. Math. Helv. 85, no. 4, 775–812 (2010).

[GGK21] Z. Gao, T.Ge and L. Kühne, *The Uniform Mordell-Lang Conjecture*. arXiv:2105.15085 (2021).

[GR17] E. Gaudron and G. Rémond, *Corps de Siegel*. J. reine angew. Math. 726. 187–247 (2017).

[GK05] M. Girard and L. Kulesz, *Computation of sets of rational points of genus-3 curves via the Dem'janenko-Manin method*. LMS J. Comput. Math. 8, 267–300 (2005).

[Gru33] W. Grunwald, *Ein allgemeines Existenztheorem für algebraische Zahlkörper*. J. Reine Angew. Math. 169, 103–107 (1933).

[Hab08] P. Habegger, *Intersecting subvarieties of $\mathbb{G}_m^n$ with algebraic subgroups*. Math. Ann. 342, no. 2, 449–466 (2008).

[Hab09] P. Habegger, *Intersecting subvarieties of abelian varieties with algebraic subgroups of complementary dimension*. Invent. Math. 176, no. 2, 405–447 (2009).

[Hab13] P. Habegger, *Small Height and Infinite Non-Abelian Extensions*. Duke Math. J. 162 no. 11, 1895–2076 (2013).

[HP16] P. Habegger and J. Pila, *O-minimality and certain atypical intersections*. Ann. Sci. Ec. Norm. Supér. (4) 49, no. 4, 813–858 (2016).

[HV19] P. Hubschmid and E. Viada, *An addendum to the elliptic torsion anomalous conjecture in codimension 2*. Rend. Semin. Mat. Univ. Padova 141, 209–220 (2019).

[Kim05] M. Kim, *The motivic fundamental group of* $\mathbb{P}^1 \setminus \{0,1,\infty\}$ *and the theorem of Siegel*. Invent. Math. 161, no. 3, 629–656 (2005).

[Kim09] M. Kim, *The unipotent Albanese map and Selmer varieties for curves*. Publ. Res. Inst. Math. Sci. 45, no. 1, 89–133 (2009).

[Kul99] L. Kulesz, *Application de la méthode de Dem'janenko-Manin à certaines familles de courbes de genre 2 et 3*. J. Number Theory 76(1), 130–146 (1999).

[KMS04] L. Kulesz, G. Matera and E. Schost, *Uniform bounds on the number of rational points of a family of curves of genus 2*. J. Number Theory 108(2), 241–267 (2004).

[Küh21] L. Kühne, *Equidistribution in families of abelian varieties and uniformity*. arXiv: 2101.10272 (2021).

[Lau83] M. Laurent, *Equations diophantiennes exponentielles*, Invent. Math. 78, no. 2, 299–327 (1984).

[LV20] B. Lawrence and A. Venkatesh, *Diophantine problems and p-adic period mappings*. Inventiones mathematicae vol. 221, 893–999 (2020).

[Li20] S. Li, *Des résultats autour des suites automatiques*. PhD thesis. Sorbonne Université. hal Id: tel-02530147 (2020).

[Lia71] P. Liardet, *Sur les transformationes polynômiales et rationelles*. Sém. Th. Nombres Bordeaux 72, exp. 29 (1971).

[LP88] J. H. Loxton and A. J. van der Poorten, *Arithmetic properties of automata: regular sequences*. J. Reine Angew. Math. 392, 57–69 (1988).

[Mah29] K. Mahler, *Arithmetische Eigenschaften der Lösungen einer Klasse von Funktionalgleichungen*. Math. Ann. 101, 342–367 (1929).

[Mah30a] K. Mahler, *Arithmetische Eigenschaften einer Klasse transzendental-transzendente Funktionen*. Math. Z. 32, 545–585 (1930).

[Mah30b] K. Mahler, *Über das Verschwinden von Potenzreihen mehrerer Veränderlichen in speziellen Punktfolgen*. Math. Ann. 103, 573–587 (1930).

[Man69] Y. Manin, *The p-torsion of elliptic curves is uniformly bounded*. Izv. Akad. Nauk SSSR 33, 459-465 (1969).

[MW90] D.W. Masser and G.Wüstholz, *Estimating isogenies on elliptic curves*. Invent. Math. 100(1), 1–24 (1990).

[Mau08] G. Maurin, *Courbes algébriques et équations multiplicatives*. Math. Ann. 341, no. 4, 789–824 (2008).

[McCP12] W. McCallum and B. Poonen, *The method of Chabauty and Coleman*. Panoramas & Syntheses 36, 99–117 (2012).

[Nar62] W. Narkiewicz, *On polynomial transformations*. Acta Arith. 7, 241–249 (1962).

[Nar71] W. Narkiewicz, *Some unsolved problems*. Colloque de Théorie des Nombres (Univ. Bordeaux, Bordeaux, 1969), 159–164. Bull. Soc. Math. France, Mem. No. 25, Soc. Math. France (1971).

[Nar95] W. Narkiewicz, *Polynomial Mappings*. Lecture Notes in Mathematics 1600, Springer (1995).

[Nef12] D. Neftin, *Admissibility and field relations*. Israel Journal of Mathematics, 19, 559–584 (2012).

[Neu79] J. Neukirch, *On solvable number fields*. Invent. math. 53, 135–164 (1979).

[NSW00] J. Neukirch, A. Schmidt and K. Wingberg *Cohomology of number fields*. Springer, collection Grundlehren der mathematischen Wissenschaften (2000).

[Nis97] Ku. Nishioka, *Mahler functions and transcendence*. Lecture Notes in Math. 1631, Springer-Verlag, Berlin (1997).

[PS19] C. Petsche and E. Stacy, *A dynamical construction of small totally p-adic algebraic numbers*. J. Number Theory 202:27–36 (2019).

[Phi91] P. Philippon, *Sur des hauteurs alternatives. I*. Math. Ann. 289, no.2, 255–284 (1991).

[Phi95] P. Philippon, *Sur des hauteurs alternatives. III*. J. Math. Pures Appl.(9) 74, no.4, 345–365 (1995).

[Pin05] R. Pink, *A common generalization of the conjectures of André–Oort, Manin–Mumford, and Mordell–Lang*. Unpublished manuscript dated 17th April (2005).

[Ple22] A. Plessis, *A new way to tackle a conjecture of Rémond*. Preprint. https://arxiv.org/abs/2201.06226 (2022).

[Pot15] L. Pottmeyer, *Heights and totally p-adic numbers*. Acta Arith. 171(3):277–291 (2015).

[Pot16] L. Pottmeyer, *A note on extensions of $\mathbb{Q}^{tr}$*. Journ. de Théor. des Nombr. de Bordeaux, Tome 28, no. 3, pp. 735-742 (2016) .

[Ray83] M. Raynaud, *Courbes sur une variété abélienne et points de torsion*. Invent. Math. 71, no. 1, 207–233 (1983).

[Rat04] N. Ratazzi, *Théorème de Dobrowolski-Laurent pour les extensions abéliennes sur une courbe elliptique à multiplication complexe*. Int. Math. Res. Not., 58, 3121–3152 (2004).

[Rat08] N. Ratazzi, *Intersection de courbes et de sous-groupes et problèmes de minoration de dernière hauteur dans les variétés abéliennes C.M.* Ann. Inst. Fourier, 58, no. 5, 1575–1633 (2008).

[Rém00] G. Rémond, *Décompte dans une conjecture de Lang.* Invent. Math. 142, no. 3, 513–545 (2000).

[Rém05] G. Rémond, *Intersection de sous-groupes et de sous-variétés I.* Math. Ann. 333, 525–548 (2005).

[Rém17] G. Rémond, *Généralisations du problème de Lehmer et applications à la conjecture de Zilber-Pink.* Panoramas et Synthèses (volume États de la recherche) 52. 243–284 (2017).

[RV03] G. Rémond and E. Viada, *Problème de Mordell-Lang modulo certaines sous-variétés abéliennes.* Int. Math. Res. Not., no. 35, 1915–1931 (2003).

[RT99] D. Roy and J. Thunder, *An absolute Siegel's lemma.* J. reine angew. Math. 476 (1996), 1–26; Addendum and erratum, ibid. 508, 47–51 (1999).

[Sal82] D. Saltman, *Generic Galois extensions and problems in field theory.* Adv. in Math. 43, 250–283 (1982).

[Ser89] J.-P. Serre, *Lectures on the Mordell–Weil Theorem.* Aspects of Mathematics, E15 (Friedr. Vieweg & Sohn, Braunschweig), Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt (1989).

[Sch65] A. Schinzel, *On the reducibility of polynomials and in particular of trinomials*, Acta Arith. 11, 1-34 (1965).

[Sch73] A. Schinzel, *On the product of the conjugates outside the unit circle of an algebraic number.* Acta Arith., 24, 385–399. Addendum, ibidem, 26, 329–361 (1973).

[Sha56] I. R. Shafarevich, *On p-extensions.* AMS. Transl., Ser.2 4, 59-72 (1956).

[Sik13] S. Siksek, *Explicit Chabauty over number fields.* Algebra & Number Theory 7(4), 765–793 (2013).

[Smy81a] C. J. Smyth, *On the measure of totally real algebraic numbers. I.* J. Austral. Math. Soc., Ser. A, 30, 137–149 (1980-1).

[Smy81b] C. J. Smyth, *On the measure of totally real algebraic numbers. II.* Math. Comp., 37, 205–208 (1981).

[Ull98] E. Ullmo, *Positivité et discrétion des points algébriques des courbes.* Ann. of Math. 147, p. 167–179 (1998).

[VV21] F. Veneziano and E. Viada, *Explicit height bounds for K-rational points on transverse curves in powers of elliptic curves.* Pacific J. Math., 315(2): 477–503 (2021).

[Via03] E. Viada, *The intersection of a curve with algebraic subgroups in a product of elliptic curves*. Ann. Scuola Norm. Sup. Pisa Serie V. 2, 47–75 (2003).

[Via08] E. Viada, *The intersection of a curve with a union of translated codimension-two subgroups in a power of an elliptic curve*. Algebra Number Theory 2, no. 3, 249–298 (2008).

[Via09] E. Viada, *Nondense subsets of varieties in a power of an elliptic curve*. Int.Math. Res. Not. IMRN 7, 1213–1246 (2009).

[Via10] E. Viada, *Lower bounds for the normalized height and non-dense subsets of subvarieties of abelian varieties*. Int. J. Number Theory 6, no. 3, 471–499 (2010).

[Via18] E. Viada, *An explicit Manin–Dem'janenko theorem in elliptic curves*. Canad. J. Math. 70(5) 1905, 1173–1200 (2018).

[Voj91] P. Vojta, *Siegel's theorem in the compact case*. Annals of Mathematics. Second Series, 133 (3), 509–548 (1991).

[Wan50] S. Wang, *On Grunwald's theorem*. Ann. of Math. (2) 51, 471–484 (1950).

[Wid11] M. Widmer, *On certain infinite extensions of the rationals with Northcott property*. Monatsh. Math., 162, no. 3, 341-353 (2011).

[Zan00] U. Zannier, *Appendix to: 'Polynomials with special regard to reducibility' by Schinzel*. Encyclopedia Math. Appl., vol. 77, Cambridge Univ. Press (2000).

[Zan12] U. Zannier, *Some problems of unlikely intersections in arithmetic and geometry*. Annals of Mathematics Studies, vol. 181, Princeton University Press, Princeton, NJ (2012).

[Zha95a] S.-W. Zhang, *Positive line bundles on arithmetic varieties*. J. Amer. Math. Soc. 8, 187–221 (1995).

[Zha95b] S.-W. Zhang, *Small points and adelic metrics*. J. Algebraic Geom., 4(2):281–300 (1995).

[Zha98] S.-W. Zhang, *Equidistribution of small points on abelian varieties*. Ann. of Math. (2) 147, no. 1, 159–165 (1998).

[Zel97] E. I. Zelmanov, *On the Restricted Burnside Problem*. World Scientific Series in 20th Century Mathematics, Fields Medallists' Lectures Vol. 5, 623–632 (1997).

[Zil02] B. Zilber, *Exponential sums equations and the Schanuel conjecture*. J. London Math. Soc. (2), 65(1), 27–44 (2002).