Copyright
by
Robert Vernon Lees Grizzard
2014

The Dissertation Committee for Robert Vernon Lees Grizzard
certifies that this is the approved version of the following dissertation:

Heights and Infinite Algebraic Extensions of the Rationals

Committee:

Jeffrey D. Vaaler, Supervisor

Daniel Allcock

Mirela Çiperiani

J. Felipe Voloch

Paul Fili

Heights and Infinite Algebraic Extensions of the Rationals

by

Robert Vernon Lees Grizzard, B.A. Math.

DISSERTATION

Presented to the Faculty of the Graduate School of

The University of Texas at Austin

in Partial Fulfillment

of the Requirements

for the Degree of

DOCTOR OF PHILOSOPHY

THE UNIVERSITY OF TEXAS AT AUSTIN

May 2014

Dedicated to my wife, Erica, and my son, Patrick.

Acknowledgments

I wish to deeply thank many people that helped make this dissertation possible. Firstly, I thank my advisor, Jeff Vaaler, as well as my fantastic collaborators Itamar Gal, Philipp Habegger, and Lukas Pottmeyer. I am also forever grateful to a huge list of talented mathematicians, including but not limited to Daniel Allcock, Jen Berg, Sara Checcoli, Mirela Çiperiani, Paul Fili, Joseph Gunther, David Helm, Adam Hughes, Keenan Kidwell, Gil Moss, Ekin Ozman, Fernando Rodríguez Villegas, and Felipe Voloch. I wish to thank my family and friends for their support, especially my wife, Erica, and my parents. Finally, I wish to thank Sandra Catlett, Dan Knopf, Nancy Lamm, and Lorenzo Sadun for their fantastic support in the non-mathematical aspects of graduate school.

Heights and Infinite Algebraic Extensions of the Rationals

Publication No. _____

Robert Vernon Lees Grizzard, Ph.D.
The University of Texas at Austin, 2014

Supervisor: Jeffrey D. Vaaler

This dissertation contains a number of results on properties of infinite algebraic extensions of the rational field, all of which have a view toward the study of heights in diophantine geometry. We investigate whether subextensions of extensions generated by roots of polynomials of a given degree are themselves generated by polynomials of small degree, a problem motivated by the study of heights. We discuss a relative version of the Bogomolov property (the absence of small points) for extensions of fields of algebraic numbers. We describe the relationship between the Bogomolov property and the structure of the multiplicative group. Finally, we describe some results on height lower bounds which can be interpreted as diophantine approximation results in the multiplicative group.

Table of Contents

Chapter 1

Introduction

The four parts of this dissertation contain results on what we will call "nice" extensions of fields of algebraic numbers. All such extensions will be assumed to lie in a fixed algebraic closure $\overline{\mathbb{Q}}$ of the rational field $\mathbb{Q}$ unless otherwise stated. By a nice extension, we mean one satisfying a property which is always satisfied by extensions of number fields, but may or may not be satisfied by extensions of possibly infinite algebraic extensions of $\mathbb{Q}$. Each of chapters 2-5 is self-contained. We refer the reader to the introductions in each chapter for precise statements of the main results.

Chapter 2 is joint work with Itamar Gal, and has been accepted for publication [22]. In this chapter we study the compositum $k^{[d]}$ of all degree d extensions of a number field k in a fixed algebraic closure. We show that k^d contains all subextensions of degree less than d if and only if $d \leq 4$. We prove that for $d > 2$ there is no bound $c = c(d)$ on the degree of elements required to generate finite subextensions of $k^{[d]}/k$. Restricting to Galois subextensions, we prove such a bound does not exist under certain conditions on divisors of d, but that one can take $c = d$ when d is prime. This question was inspired by work of Bombieri and Zannier on heights in similar extensions, and previously

considered by Checcoli.

Chapter 3, on relative Bogomolov extensions, was written solely by the author and has been submitted for publication separately. A subfield $K \subseteq \overline{\mathbb{Q}}$ has the Bogomolov property (property (B)) if there exists a positive ε such that no non-torsion point of $K^\times$ has absolute logarithmic height below ε. We define a relative extension L/K to be *Bogomolov* if this holds for points of $L^\times \setminus K^\times$. We construct various examples of extensions which are and are not Bogomolov. We prove a ramification criterion for this property, and use it to show that such extensions can always be constructed if some rational prime has bounded ramification index in K.

Chapter 4 discusses the relationship between property (B) and the structure of the multiplicative group, and also the analogous question for elliptic curves. It was observed by Vaaler that for a field K to satisfy property (B) implies that $K^\times/K^\times_{tors}$ is free abelian. Counterexamples to the converse of this statement, i.e. fields K where $K^\times/K^\times_{tors}$ is free abelian, yet K does not satisfy property (B), were constructed independently by the author and by Philipp Habegger and Lukas Pottmeyer. These examples, as well as an extensive investigation into the analogous question for elliptic curves, are the subject of a current joint work by the author, Habegger, and Pottmeyer, which will later be submitted for publication separately. Chapter 4 represents part of this paper.

Chapter 5 is part of a joint work in progress with Jeffrey Vaaler, which will later be submitted for publication separately. In this chapter we show

that, for a subfield K of $\overline{\mathbb{Q}}$, elements of $\overline{\mathbb{Q}}^\times/\overline{\mathbb{Q}}^\times_{tors}$ cannot be approximated by elements of the $\mathbb{Q}$-vector space spanned by $K^\times/\mathcal{K}^\times_{tors}$, in the metric induced by the height. These results can be thought of as diophantine approximation in the multiplicative group. Our results yield a generalization of Vaaler's aforementioned observation about property (B) and free abelian groups to relative Bogomolov extensions.

Chapter 2

The compositum of all degree d extensions of a number field (with Itamar Gal)

2.1 Introduction

Let k be a field. Throughout this paper, all extensions of k will be assumed to lie in a fixed algebraic closure $\overline{k}$. We are interested in fields obtained by adjoining to k all roots of irreducible polynomials of a given degree d. For any positive integer d we will write

$$k^{[d]} = k(\beta \mid [k(\beta) : k] = d), \text{ and}$$
$$k^{(d)} = k(\beta \mid [k(\beta) : k] \leq d) = k^{[2]}k^{[3]}k^{[4]} \cdots k^{[d]}.$$

We have $k^{[1]} = k^{(1)} = k$, and for all d it is clear that $k^{[d]}$ and $k^{(d)}$ are normal extensions of k. We are primarily interested in the case where k is a number field, in which case these are infinite Galois extensions. When $d > 2$ it is natural to ask what polynomials of degree less than d split in $k^{[d]}$. If $c < d$ and all irreducible polynomials of degree c split in $k^{[d]}$, then $k^{[c]} \subseteq k^{[d]}$. Notice that this occurs in particular when c divides d, since every degree c extension admits a degree d/c extension. If all polynomials of degree less than d split in $k^{[d]}$, then $k^{[d]} = k^{(d)}$. We will prove the following results along these lines.

Theorem 2.1.1. *If k is a number field* [†]*, then*

(a) $k^{[2]} \subseteq k^{[d]}$ *for all* $d \geq 2$,

(b) $k^{[3]} \subseteq k^{[4]}$, *and*

(c) for each $d \geq 5$, *there exists a prime* $p < d$ *such that* $k^{[p]} \not\subseteq k^{[d]}$.

The following corollary is immediate.

Corollary 2.1.2. *If k is a number field, then* $k^{[d]} = k^{(d)}$ *if and only if* $d < 5$.

We now introduce the notion of boundedness for an extension of fields. We will use this language to state our remaining results.

Definition 2.1.3. *We say an infinite extension M of k is* bounded over k *(or that M/k is* bounded*) if there exists a constant c such that all finite subextensions of M/k can be generated by elements of degree less than or equal to c. If there is no such c, we say that M/k is* unbounded.

If all finite Galois subextensions of M/k can be generated by elements of degree less than or equal to c, we say M/k is Galois bounded*; otherwise we say M/k is* Galois unbounded.

It was first shown by Checcoli that, for a number field k, the extension $k^{(d)}/k$ is not in general Galois bounded (see [12], Theorem 2, part ii). We will

[†]Many of our results contain the hypothesis that k is a number field or global function field. However, the astute reader will notice after reading the proofs that this hypothesis could be replaced with more technical restrictions on the field k – specifically, that certain embedding problems have solutions over k.

address the question of how boundedness and Galois boundedness depend on d for the fields $k^{(d)}$ and $k^{[d]}$. Further restricting attention to abelian Galois extensions greatly simplifies the discussion. It is easily seen that $k_{\mathrm{ab}}^{(d)}$ is bounded over k for all d, where the subscript denotes the maximal abelian subextension. This is contained in the proof of [14, Proposition 2.1] and can be seen in the statement of [12, Theorem 1.4]. It follows from the fact that a finite abelian group can be written as a product of cyclic groups, where the trivial subgroup is the intersection of subgroups of index not exceeding the greatest order of a cyclic factor.

In the case where k is a number field, Bombieri and Zannier ask in [10] whether, for any given constant T, only finitely many points in $k^{(d)}$ have absolute Weil height (see [9], p. 16 for a definition) at most T. Such a finiteness property is called the *Northcott property*. This problem has been further discussed in [47] and [13], but remains open. In Theorem 1 of [10] it is proved that this property is enjoyed by $k_{\mathrm{ab}}^{(d)}$, and the boundedness of $k_{\mathrm{ab}}^{(d)}/k$ plays a role in the proof. The authors of the present work are hopeful that understanding the boundedness properties in $k^{[d]}$ and $k^{(d)}$ will be useful in understanding such problems.

The following theorems summarize our results on boundedness and Galois boundedness.

Theorem 2.1.4. *If k is a number field, then $k^{[d]}$ is bounded over k if and only if $d \leq 2$.*

Theorem 2.1.5. *If k is any field and p is a prime number, then $k^{[p]}$ is Galois bounded over k. More precisely, all finite Galois subextensions of $k^{[p]}/k$ can be generated by elements of degree at most p over k.*

We will also establish the following partial converse to Theorem 2.1.5.

Theorem 2.1.6. *If k is a number field or global function field and $d > 2$, then $k^{[d]}/k$ is Galois unbounded in the following cases:*

(a) d is divisible by a square;

(b) d is divisible by two primes p and q such that $q \equiv 1 \pmod{p}$.

In particular, this includes the case where d is even and greater than 2.

In terms of the fields $k^{(d)}$, Theorems 2.1.4, 2.1.5, and 2.1.6 immediately imply the following.

Corollary 2.1.7. *Let k be a number field. Then*

(a) $k^{(2)}/k$ is bounded,

(b) $k^{(3)}/k$ is Galois bounded but not bounded, and

(c) $k^{(d)}/k$ is Galois unbounded for $d \geq 4$.

This paper is organized as follows. Sections 2 and 3 are devoted to preliminaries and background material on group theory and Galois theory. In Section 4 we prove Theorem 2.1.1; parts (a) and (b) appeal to existing results

on embedding problems, while part (c) follows by a purely group theoretic argument. We conclude Section 4 with an elementary construction which gives part (a) in the case where $k = \mathbb{Q}$. In Section 5 we prove Theorems 2.1.4 and 2.1.6 using explicit constructions. Finally, in Section 6 we prove Theorem 2.1.5 as an immediate corollary of a purely group theoretic statement (see Proposition 2.6.2).

Acknowledgments

The authors would like to thank Daniel Allcock, Sara Checcoli, Joseph Gunther, Andrea Lucchini, Jeffrey Vaaler, and anonymous referees for numerous useful communications. We would also like to express our appreciation to the `GAP` group. Although we did not use computer calculations directly for any of the results in this paper, we used the `GAP` software package extensively to improve our understanding of the group theoretic aspects of these problems.

2.2 Preliminaries on group theory

We recall some standard definitions. A *transitive group* of degree d will mean a finite permutation group acting faithfully and transitively on a set Ω of size d, such as the Galois group of an irreducible degree d polynomial acting on the roots. A transitive group is *primitive* if there is no nontrivial partition of Ω such that the group has an induced action on the blocks of the partition. Since all such blocks must be equal in size, any transitive group of prime degree must be primitive. For more background on transitive and

primitive groups, see [16] or [48].

Let us fix some notation for finite groups. We will denote by C_d, D_d, A_d, and S_d the cyclic, dihedral, alternating, and symmetric groups of degree d, respectively. Note that D_d has order $2d$. We denote the Klein 4-group by V.

A *subdirect product* G of some collection of groups $\{G_i\}_i$ is a subgroup of the direct product $\prod_i G_i$ with the property that the projection map from G to each factor G_i is surjective. We will sometimes write $G \leq_{sd} \prod_i G_i$ to abbreviate that G is such a group.

Let H_1, H_2 and Q be groups, and let $\alpha_1 : H_1 \to Q$ and $\alpha_2 : H_2 \to Q$ be surjective group homomorphisms. The *fibered product* of H_1 with H_2 over Q (with respect to the maps α_1 and α_2) is defined to be the subgroup $H_1 \times_Q H_2$ of the direct product $H_1 \times H_2$ given by

$$H_1 \times_Q H_2 = \{(h_1, h_2) \in H_1 \times H_2 \mid \alpha_1(h_1) = \alpha_2(h_2)\}.$$

Notice that we have

$$|H_1 \times_Q H_2| = \frac{|H_1| \cdot |H_2|}{|Q|}.$$

The following lemma can be found in different forms in many texts, and is variously attributed to Goursat or Goursat and Lambek. A short proof can be found in [11], p. 864.

Lemma 2.2.1 (Goursat's Lemma)**.** *Let H_1 and H_2 be groups. The set of*

subdirect products of $H_1 \times H_2$ is equal to the set of fibered products $H_1 \times_Q H_2$. In particular, every subdirect product of $H_1 \times H_2$ is of the form $H_1 \times_Q H_2$.

2.3 Galois theory and embedding problems

The following elementary proposition highlights the role of Galois theory in the proofs of our results.

Proposition 2.3.1. *Let k be a perfect field and let L/k be a finite Galois extension of fields. The following are equivalent:*

(a) L is generated by elements of degree d over k;

(b) in $\mathrm{Gal}(L/k)$ the trivial group is the intersection of subgroups of index d;

(c) $\mathrm{Gal}(L/k)$ is a subdirect product of transitive groups of degree d.

Proof. The equivalence (a) and (b) follows immediately from the Galois correspondence and the primitive element theorem. If (a) is satisfied, then L is a compositum of the splitting fields of some degree d polynomials. It follows from basic Galois theory that $\mathrm{Gal}(L/k)$ is a subdirect product of these Galois groups, which are transitive groups of degree d, so (c) is satisfied. Suppose (c) is satisfied, so we have $\mathrm{Gal}(L/k)$ acting on a disjoint union of sets of size d, transitively on each set. Then all point-stabilizers have index d, and the intersection of these subgroups is trivial, yielding (b). □

In order to establish Theorem 2.1.1, we must discuss the embedding problem in Galois theory. Let K/k be a Galois extension of fields, G a finite

group, and N a normal subgroup of G with a short exact sequence

$$1 \to N \to G \xrightarrow{\phi} \mathrm{Gal}(K/k) \to 1.$$

These data give us the *embedding problem* $(K/k, G, N)$. A *solution* to the embedding problem is an extension L/k with $L \supseteq K$ such that $\mathrm{Gal}(L/k) \cong G$ and the natural map $\mathrm{Gal}(L/k) \to \mathrm{Gal}(K/k)$ agrees with ϕ. Hence, a solution to the embedding problem is described by the following commutative diagram.

$$\begin{array}{ccccccccc} & & & & & & \mathrm{Gal}(L/k) & & \\ & & & & & & \downarrow \wr & \searrow & \\ 1 & \longrightarrow & N & \longrightarrow & G & \xrightarrow{\phi} & \mathrm{Gal}(K/k) & \longrightarrow & 1. \end{array}$$

For our purposes, all that is important is finding an extension L/k such that $L \supseteq K$ and $\mathrm{Gal}(L/k) \cong G$, and therefore we will not mention the map ϕ in what follows.

A celebrated result in this context is a theorem of Shafarevich, which states that if k any number field or global function field, any solvable group can be realized as the Galois group of some extension of k. Since products of solvable groups are solvable, this allows us to realize a solvable group as the Galois group of infinitely many extensions, whose pairwise intersections are k. A full proof of Shafarevich's Theorem, along with more background on embedding theory, can be found in [35].

The following proposition is a simple yet important observation which

is used implicitly throughout the proof of Theorem 2.1.1.

Proposition 2.3.2. *Let k be a field and let K/k be a finite extension. Then $K \subseteq k^{[d]}$ if and only if the following two conditions are met.*

(i) We can find a group H which is a subdirect product of transitive groups of degree d with some normal subgroup N such that there is a short exact sequence

$$1 \to N \to H \to \mathrm{Gal}(K/k) \to 1.$$

(ii) We can solve the corresponding embedding problem, i.e. find $L \supseteq K$ such that $\mathrm{Gal}(L/k) \cong H$.

Proof. If $K \subseteq k^{[d]}$, then K is contained in some finite Galois extension L/k generated by elements of degree d. By Proposition 2.3.1, we have that $\mathrm{Gal}(L/k)$ is a subdirect product of transitive groups of degree d, and (i) and (ii) are clearly satisfied via the short exact sequence

$$1 \to \mathrm{Gal}(L/K) \to \mathrm{Gal}(L/k) \to \mathrm{Gal}(K/k) \to 1.$$

Conversely, if (i) and (ii) are satisfied, then we have $K \subseteq L$ as in (ii), and $L \subseteq k^{[d]}$ by (i) and Proposition 2.3.1. □

2.4 Proof of Theorem 2.1.1

We implicitly apply Proposition 2.3.2 throughout. For integers $m < d$, we are interested in whether or not $k^{[m]} \subseteq k^{[d]}$. Let K be the splitting field of an irreducible polynomial of degree m in $k[x]$. In the case $m = 2$, we must have that $\mathrm{Gal}(K/k) \cong C_2$, and we use the following result due to O. Neumann (cf. [36], Theorem 2) in order to conclude that $K \subseteq k^{[d]}$.

Proposition 2.4.1. *Let K/k be a quadratic extension of number fields and let $d \geq 3$. Then there is a solution to the embedding problem $(K/k, S_d, A_d)$ arising from*

$$1 \to A_d \to S_d \to \mathrm{Gal}(K/k) \to 1.$$

In other words, every irreducible quadratic splits in the splitting field of some degree d polynomial (with symmetric Galois group).

This establishes part (a) of Theorem 2.1.1, that $k^{[2]} \subseteq k^{[d]}$ for all $d \geq 2$, and in particular it tells us that $k^{[3]} = k^{(3)}$. At the end of this section we give a short, elementary proof of part (a) of Theorem 1 in the case where $k = \mathbb{Q}$.

For part (b) of Theorem 1 it now suffices to consider the case $m = 3, d = 4$. We must have $\mathrm{Gal}(K/k) \cong S_3$ or C_3. The following is a special case of a classical result of Shafarevich that gives the solution to all embedding problems with nilpotent kernel (see [44], Claim 2.2.5).

Proposition 2.4.2. *Let k be a number field and let $f(x) \in k[x]$ be an irreducible cubic with splitting field K. Let V denote the Klein 4-group.*

(a) *If* $\mathrm{Gal}(K/k) \cong S_3$*, then there is a solution to the embedding problem* $(K/k, S_4, V)$ *arising from*

$$1 \to V \to S_4 \to \mathrm{Gal}(K/k) \to 1.$$

(b) *If* $\mathrm{Gal}(K/k) \cong C_3$*, then there is a solution to the embedding problem* $(K/k, A_4, V)$ *arising from*

$$1 \to V \to A_4 \to \mathrm{Gal}(K/k) \to 1.$$

In other words, every irreducible cubic splits in the splitting field of some quartic.

This proves that $k^{[3]} \subseteq k^{[4]}$, and combining with part (a) of Theorem 1 we now have that $k^{[4]} = k^{(4)}$.

To prove part (c) of Theorem 2.1.1 we consider the case $d \geq 5$. We will show that, for certain primes $p < d$, if $\mathrm{Gal}(K/k) \cong C_p$, then there is no possible subdirect product of transitive groups of degree d having $\mathrm{Gal}(K/k)$ as a quotient. That is, we cannot even find groups H and N satisfying a short exact sequence as in (2.3.2) above. We begin with a lemma.

Lemma 2.4.3. *For any integer* $d \geq 5$ *there exists a prime number* $p \in (\frac{d}{2}, d)$ *such that, if* G *is a transitive subgroup of* S_d *containing a* p*-cycle, then either* $G = S_d$ *or* $G = A_d$*.*

Proof. The transitive groups of degree d are well-known for small d – see for example [11] for the groups up to degree 11; GAP (see [29], [23]) has a library

of all of them for $d \leq 30$. It can be checked easily that we can use $p = 3$ when $d = 5$, and we can use $p = 5$ when $d = 6, 7$; in each of these cases, S_d and A_d are the only transitive subgroups with order divisible by p. Therefore all that remains is to prove our lemma in the case $d \geq 8$.

There exists at least one prime $p \in (\frac{d}{2}, d-2)$. This follows from Bertrand's Postulate, first proved by Chebyshev, which states that for $m > 3$ there exists a prime in the interval $(m, 2m-2)$ – see [27], p. 343, Theorem 418; cf. p. 373. Let p be such a prime, and suppose G is a transitive subgroup of S_d containing some p-cycle g. Without loss of generality, $g = (1\ 2\ 3\ \cdots\ p)$. Since G is transitive, for each $i \in \{p+1, \ldots, d\}$ there is some element $\sigma_i \in G$ such that $\sigma_i(1) = i$. If we let $g_i = \sigma_i g \sigma_i^{-1}$, then g_i will be a p-cycle in G whose support contains i. Since p is prime, each $\langle g_i \rangle$ acts primitively on its support, which is a set of size p. Since $p > \frac{d}{2}$, the pairwise intersections of the supports of the groups $\langle g_i \rangle$ are nontrivial. Therefore we can apply Proposition 8.5 from [48] inductively to see that the subgroup $H = \langle g, g_{p+1}, g_{p+2}, \ldots, g_d \rangle$ is a primitive subgroup of S_d. Since H contains a p-cycle and $p < d-2$, Theorem 13.9 from [48] tells us that either $H = S_d$ or $H = A_d$, and since $H \leq G$, our proof is complete. □

Part (c) will be an immediate corollary of the following proposition.

Proposition 2.4.4. *For any integer $d \geq 5$ there exists some prime $p < d$ such that, if $G \leq_{sd} G_1 \times \cdots \times G_n$ is a subdirect product of transitive groups of degree d, then G has no quotient that is cyclic of order p.*

Proof. Fix $d \geq 5$. By Lemma 2.4.3, there is a prime $p \in (\frac{d}{2}, d)$ such that the only transitive subgroups of S_d containing a p-cycle are S_d and A_d. We proceed by induction on n, noting that the case $n = 1$ follows immediately by our choice of p. In general, we will have that $G \leq_{sd} G_0 \times G_n$, where G_n is a transitive group of degree d and G_0 is a subdirect product of $n-1$ such groups. If N is any normal subgroup of G, we have that $N \leq_{sd} N_0 \times N_n$ for some normal subgroups $N_0 \trianglelefteq G_0$ and $N_n \trianglelefteq G_n$. By Goursat's Lemma, we may write G as a fibered product $G = G_0 \times_Q G_n$ for some group Q which is a quotient of both G_0 and G_n. Similarly, we have $N = N_0 \times_R N_n$ for some group R which is a quotient of both N_0 and N_n.

By the inductive hypothesis, neither G_0/N_0 nor G_n/N_n has order p. Suppose that $G/N \cong C_p$. Since G/N surjects onto both G_0/N_0 and G_n/N_n, the latter two groups must be trivial. Therefore, using (2.2), we have

$$p = \frac{|G|}{|N|} = \frac{|G_0| \cdot |G_n|/|Q|}{|N_0| \cdot |N_n|/|R|} = |G_0/N_0| \cdot |G_n/N_n| \cdot \frac{|R|}{|Q|} = \frac{|R|}{|Q|}.$$

This means that $|R|$ is divisible by p, and therefore $|G_n|$ and $|N_n|$ are both divisible by p as well. This means G_n must be isomorphic to either S_d or A_d. Hence the only possibilities for Q are S_d, A_d, C_2, or 1, and the only possibilities for R are S_d or A_d. None of these possibilities allows for the equality in (2.4). $\square$

This establishes part (c) of Theorem 2.1.1. Indeed, it shows that $k^{[p]} \subsetneq k^{[d]}$, for p and d as above, whenever k is any field that admits a degree cyclic

Galois extension of degree p.

In summary, if $d \leq 4$, an irreducible polynomial in $k[x]$ of degree less than d splits in the splitting field of a *single irreducible polynomial* of degree d. When $d > 4$, however, some irreducible polynomials of degree less than d do not split *in any compositum of such splitting fields*. We conclude this section by demonstrating that part (a) of Theorem 2.1.1 can be proved by a very elementary construction when $k = \mathbb{Q}$.

Elementary proof that $\mathbb{Q}^{[2]} \subseteq \mathbb{Q}^{[d]}$ *for all* $d \geq 2$. In general, $k^{[\ell]} \subseteq k^{[d]}$ if $\ell | d$. Hence it will suffice to show that $\sqrt{p} \in \mathbb{Q}^{[\ell]}$ for any prime $\ell \geq 3$, whenever p is a rational prime or $p = -1$. If p is any rational prime or equal to ± 1, define

$$f_p(x) = x^\ell - \ell(\ell p + 1)x + (\ell - 1)(\ell p + 1)$$

The discriminant Δ_p of this polynomial is given by the following (see for example [32]):

$$(-1)^{(\ell-1)(\ell-2)/2}\Delta_p = -(\ell - 1)^{\ell-1}\ell^{\ell+1}(\ell p + 1)^{\ell-1} \cdot p.$$

In particular, it follows that $\sqrt{p}$ will be in the splitting field of either $f_p(x)$ or $f_{-p}(x)$. We now show that $f_p(x)$ is irreducible. First notice that if $\ell \neq p$ then $f_p(x + 1)$ is Eisenstein at ℓ. Next we consider the case where $\ell = p$. To handle this case we use the following version of Dumas's Irreducibility Criterion. A proof can be found in [39, Section 2.2.1], where the langauge of Newton diagrams is used.

Proposition 2.4.5 (Dumas's Irreducibility Criterion)**.** *Let* $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n \in \mathbb{Z}[x]$. *Suppose there exists a prime* q *such that* $v_q(a_0) = 0$, $v_q(a_i)/i > v_q(a_n)/n$ *for* $i \in \{1, \ldots, n\}$ *and* $\gcd(v_q(a_n), n) = 1$. *Here* $v_q(\cdot)$ *denotes the greatest power of* q *dividing the argument. Then* $f(x)$ *is irreducible.*

Applying Dumas's criterion in the case $l = p$, we find that a sufficient condition for the irreducibility of f_p is the existence of a prime q and an integer m such that q^m exactly divides $p^2 + 1$, such that q is coprime to $p - 1$, and and such that m is coprime to p. Notice that

$$(p^2 + 1) - (p + 1)(p - 1) = 2.$$

Since 2 is an integer combination of $p^2 + 1$ and $p - 1$, it follows that $\gcd(p^2 + 1, p - 1)$ divides 2. Also notice that

$$p^2 + 1 = (p - 1)^2 + 2(p - 1) + 2 \equiv 2 \pmod 4.$$

Thus $p^2 + 1$ is not a power of 2, and we can take q to be any one of its odd prime factors. Now choose m such that q^m exactly divides $p^2 + 1$. Since $p^2 + 1 < q^p$ for $p, q \geq 3$, it follows that $1 < m < p$. Thus m is coprime to p, which completes the proof. □

2.5 Unboundedness: proofs of Theorems 2.1.4 and 2.1.6

In the spirit of Proposition 2.3.1, let G be a finite group and d a positive integer. Suppose that H is a subgroup of G that cannot be written as an intersection of subgroups of index less than or equal to d in G. If G is the

Galois group of a field extension L/k, this implies that the fixed field K of H is not generated over k by elements of degree less than or equal to d. In order to prove unboundedness results, we must exhibit groups with these properties which can be realized as Galois groups of subextensions of $k^{[d]}$. The example in the next lemma will be applied toward establishing Theorem 2.1.4.

Lemma 2.5.1. *Let p be an odd prime number, and let*

$$G = D_p^{n-1} \times C_p = \langle r_1, s_1, \ldots, r_{n-1}, s_{n-1}, r_n \rangle$$

be the direct product of $n-1$ copies of the dihedral group D_p and a cyclic group of order p, where for $i \in \{1, \ldots, n-1\}$ the i^{th} $D_p = \langle r_i, s_i \rangle$ is generated by the p-cycle r_i and the 2-cycle s_i, and $C_p = \langle r_n \rangle$. Let

$$H = \langle r_1 r_n, r_2 r_n, \ldots, r_{n-1} r_n \rangle \leq G.$$

If B is a subgroup of G with $H \lneq B \leq G$, then $r_n \in B$. In particular, the intersection of all such subgroups B strictly contains H.

Proof. Let $G_p = \langle r_1, \ldots, r_n \rangle$ be the unique Sylow p-subgroup of G, considered as an n-dimensional $\mathbb{F}_p$-vector space. Any Sylow 2-subgroup G_2 of G will be an $(n-1)$-dimensional $\mathbb{F}_2$-vector space which acts by conjugation on G_p, so that $G = G_p \rtimes G_2$.

Let $H \lneq B \leq G$. Note that H is a codimension 1 subspace of G_p, so if B contains any element of order p not in H, then B contains all of G_p. If

B contains any involution $\tau \in G$, notice that there will be some i such that τ acts non-trivially on the i^{th} copy of D_p, so that $\langle r_i r_n, \tau \rangle$ will contain r_n. Since every nontrivial element of G is either of order p, an involution, or of order $2p$ (a power of which is an involution), this completes our proof. □

Corollary 2.5.2. *Let k be a number field or a global function field, and let p be an odd prime number. Then $k^{[p]}/k$ is unbounded.*

Proof. Let G and H be as in Lemma 2.5.1. Since G is solvable we have an extension L/k with $\mathrm{Gal}(L/k) \cong G$. Let L^H be the fixed field in L of H, and notice that $L^H \subseteq k^{[p]}$. It is clear from our construction that $[L^H : k] = p \cdot 2^{n-1}$. The Galois correspondence tells us that every proper subextension of L^H/k corresponds to a subgroup B of G with $H \lneq B \leq G$. Furthermore, since the intersection of all such groups strictly contains H, the compositum of all proper subextensions of L^H/k is strictly a subfield of L^H. This shows that L^H is not generated by elements of degree less than $p \cdot 2^{n-1}$. □

Notice that the field extension L^H/k in the proof above is *not* Galois (H is not normal in G). As we will prove in the next section, this was necessarily so.

In order to prove our Galois unboundedness results, we must now introduce extraspecial p-groups. We write H_p for the finite Heisenberg group of order p^3, when p is a prime. This group is defined as the multiplicative group

of upper triangular matrices of the form

$$\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix},$$

with a, b, and c belonging to the finite field $\mathbb{F}_p$.

The group H_p plays an important role in our Galois unboundedness results. We review some of its properties. First, H_p has a natural action on the three-dimensional vector space $\mathbb{F}_p^3$. Analyzing this action, it is easy to see that when an element of H_p acts on a vector, the third coordinate is fixed, and H_p acts faithfully and transitively on a 2-dimensional affine subspace (the subspace with third coordinate equal to 1, say), which has p^2 elements. Thus we see that H_p is isomorphic to a transitive group of degree p^2.

The group H_p is an *extraspecial p-group*, meaning its center, commutator, and Frattini subgroups coincide and have order p. We can construct larger extraspecial p-groups as follows. Let n be a positive integer, and consider the normal subgroup $N_{p,n}$ of the direct product H_p^n given by

$$N_{p,n} = \{(z_1^{a_1}, \ldots, z_n^{a_n}) \mid \Sigma_{i=1}^n a_i \equiv 0 \pmod{p}\},$$

where z_i generates the center of the i^{th} copy of H_p. The quotient $H_p^n/N_{p,n}$ is an extraspecial p-group of order p^{2n+1} and exponent p (except when $p = 2$, when the exponent is 4), which we will denote by $E_{p,n}$. The basic properties of these groups are discussed in [17, Section A.20].

The following lemma can be found in [12] (cf. Proposition 2.4), where it is stated only for p odd. We briefly recall the proof below.

Lemma 2.5.3. *Let p be a prime number. The intersection of all subgroups of index less than p^n in $E_{p,n}$ contains the commutator subgroup. In particular, this intersection is nontrivial.*

Proof. Any subgroup H of $E_{p,n}$ of index less than p^n has order greater than p^{n+1} and is therefore non-abelian by [7, Theorem 4.7 (d)]. Since H contains a pair of non-commuting elements and the commutator subgroup $[E_{p,n}, E_{p,n}]$ is cyclic of order p, we have that H contains the commutator subgroup. □

Checcoli used this fact in [12] to show that, for a number field k, the extension $k^{(d)}/k$ is not in general Galois bounded. The idea of using extraspecial groups for this purpose is attributed to A. Lucchini. However, the author was not concerned with the question of which values of d suffered from this pathology, nor with the more general question of the boundedness of $k^{[d]}/k$. The use of extraspecial p-groups (which are certainly not the only groups with properties like the conclusion of Lemma 2.5.3, but are natural and easy to work with) remains our primary tool for proving that extensions are Galois unbounded. The following lemma simplifies our application of this principle.

Lemma 2.5.4. *Let d be a positive integer. Suppose there is a prime number p such that there is a solvable group G which is a subdirect product of transitive groups of degree d, and a quotient of G is isomorphic to H_p. Then $k^{[d]}/k$ is Galois unbounded for any number field or global function field k.*

Proof. By Shafarevich's Theorem, for any positive integer n we can realize G^n as the Galois group of some extension L/k, and we will have $L \subseteq k^{[d]}$. There

will be a Galois subextension K/k with Galois group H_p^n, and the subfield of K corresponding to the normal subgroup defined in (2.5) will have Galois group $E_{p,n}$, and will therefore not be generated by elements of degree less than p^n. □

The following lemma gives a construction of a permutation group that will allow us to apply Lemma 2.5.4 in our proof of part (b) of Theorem 2.1.6.

Lemma 2.5.5. *Let $d = pq$, where p and q are primes with $q \equiv 1 \pmod{p}$. Then there exists a transitive group of degree d which is isomorphic to $C_q^p \rtimes H_p$.*

Proof. Write $q = mp+1$. Consider p sets Ω_i of size q, written $\Omega_i = \{1_i, 2_i, \ldots, q_i\}$ for $i \in \mathbb{F}_p$. We write Ω for the disjoint union of the sets Ω_i. We will construct a group G of permutations of Ω, which acts imprimitively with respect to the partition into the sets Ω_i. Let σ be the permutation $(1\ 2\ \cdots\ q)$. The q-cycle σ is normalized by some $(q-1)$-cycle η in the symmetric group S_q and, since $q \equiv 1 \pmod{p}$, we have that η^m is a product of m disjoint p-cycles; we set $\tau = \eta^m$. The permutations σ and τ induce permutations on each set Ω_i, which we denote by σ_i and τ_i.

We define $\alpha = \tau_0\tau_1\cdots\tau_{p-1}$, $\beta = \tau_0^0\tau_1^1\cdots\tau_{p-1}^{p-1}$, and define γ to be the permutation on Ω sending j_i to j_{i+1}. Let $A = \langle\sigma_0, \sigma_1, \cdots, \sigma_{p-1}\rangle \cong C_q^p$, and $B = \langle\alpha, \beta, \gamma\rangle$. Notice that our construction ensures that A is normalized by

B. The interested reader will verify that $B \cong H_p$ via

$$\alpha \mapsto \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \beta \mapsto \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \gamma \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

The example below with $p = 3$, $q = 7$ makes the isomorphism more clear. The Heisenberg group B acts simultaneously on m "planes" of p^2 points, each plane consisting of points j_i with $i \in \mathbb{F}_p$ and j running over the indices in one of the disjoint p-cycles that make up τ.

We let

$$G = A \rtimes B$$

and notice that G acts transitively on Ω (indeed, $\langle \sigma_0, \gamma \rangle$ is already transitive on Ω). □

It would be quite tedious to write explicitly the generators of the group constructed in the proof of Lemma 2.5.5 for general p and q, but we will make this construction more clear by giving an example with $d = 21 = 3 \cdot 7$.

Example 2.5.6. We assume the notation of the preceding proof. The 7-cycle $\sigma = (1\ 2\ 3\ 4\ 5\ 6\ 7)$ is normalized by the 6-cycle $\eta = (2\ 6\ 5\ 7\ 3\ 4)$. Squaring this permutation yields a product of 3-cycles $\tau = (2\ 5\ 3)(6\ 7\ 4)$, which normalizes σ. As described above, we have

$$\Omega = \{ j_i \mid i \in \mathbb{F}_p, j \in \{1, \ldots, 7\} \}.$$

The permutations defined in the proof are given as follows:

$$\sigma_0 = \big(1_0\ 2_0\ 3_0\ 4_0\ 5_0\ 6_0\ 7_0\big),$$

$$\sigma_1 = \big(1_1\ 2_1\ 3_1\ 4_1\ 5_1\ 6_1\ 7_1\big),$$

$$\sigma_2 = \big(1_2\ 2_2\ 3_2\ 4_2\ 5_2\ 6_2\ 7_2\big),$$

$$\tau_0 = \big(2_0\ 5_0\ 3_0\big) \cdot \big(6_0\ 7_0\ 4_0\big),$$

$$\tau_1 = \big(2_1\ 5_1\ 3_1\big) \cdot \big(6_1\ 7_1\ 4_1\big),$$

$$\tau_2 = \big(2_2\ 5_2\ 3_2\big) \cdot \big(6_2\ 7_2\ 4_2\big),$$

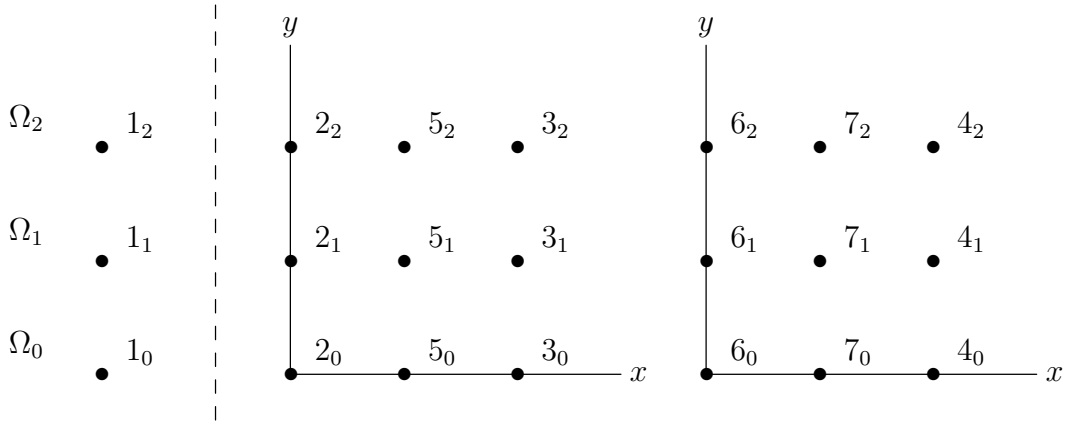
$$\alpha = \tau_0\tau_1\tau_2,$$

$$\beta = \tau_1\tau_2^2,$$

$$\gamma = \big(1_0\ 1_1\ 1_2\big) \cdot \big(2_0\ 2_1\ 2_2\big) \cdots \big(7_0\ 7_1\ 7_2\big), \quad \text{and}$$

$$G = \langle \sigma_0, \sigma_1, \sigma_2 \rangle \rtimes \langle \alpha, \beta, \gamma \rangle.$$

To verify that $\langle \alpha, \beta, \gamma \rangle \cong H_3$ as given by (2.5), we consider the following way of visualizing Ω.



Shown are two copies of the affine plane $z = 1$ inside of $\mathbb{F}_3^3 = \{(x, y, z) \mid x, y, z \in \mathbb{F}_3\}$. These eighteen points, together with the three points on the left, correspond to elements of Ω by the labelings. For example, the point $(2, 0, 1)$ in the plane on the left corresponds to $3_0 \in \Omega_0$. The blocks Ω_i are represented as the three horizontal rows in the diagram. The columns have been partitioned according to the cycle decomposition of permutations τ_i, so that α, β, and γ act via the matrices given in (2.5), simultaneously on each plane of nine points.

Proof of Theorem 2.1.6. Recall that if c divides d, then $k^{[c]} \subseteq k^{[d]}$. Since H_p is solvable and transitive of degree p^2, if follows immediately from Lemma 2.5.4 that $k^{[p^2]}$ is Galois unbounded over k for any prime p, yielding part (a). Checcoli showed how to realize these groups explicitly in [12]. Since the group constructed in Lemma 2.5.5 is solvable, we again apply Lemma 2.5.4 to see that $k^{[pq]}$ is Galois unbounded over k whenever p and q are primes with $q \equiv 1 \pmod{p}$. This gives part (b).

□

Proof of Theorem 2.1.4. We know that $k^{[2]} = k_{\mathrm{ab}}^{(2)}$, so $k^{[2]}/k$ is bounded. If $d > 2$, then d is divisible by c, where c is either 4 or an odd prime. We have $k^{[c]} \subseteq k^{[d]}$, and by Corollary 2.5.2 and part (a) of Theorem 2.1.6, $k^{[c]}$ is unbounded over k. □

We remark that our proofs actually demonstrate that $k^{[d]}/k$ is also unbounded in the case where k is a global function field and $d \geq 3$.

2.6 Galois boundedness in prime degree

In this section we prove Theorem 2.1.5. Clearly the general technique for showing boundedness is to find subgroups of small index inside of a Galois group G, whose intersection is a given subgroup H. If we want to show Galois boundedness, we take H to be normal. We will show that we can accomplish this task when G is a subdirect product of transitive groups of prime degree.

The following lemma characterizes the transitive groups of degree p.

Lemma 2.6.1. *If p is a prime number and G is a transitive group of degree p, then we have $G = T \rtimes B$, where T is simple and transitive, and B is a subgroup of C_{p-1}.*

This lemma can be proved by elementary means. It can also be seen quickly using the classification of finite simple groups: a theorem of Burnside (see [48], Theorem 11.7; cf. [16], Theorem 4.1B) implies that G is either a subgroup of $C_p \times C_{p-1}$ containing C_p, or an almost simple group, meaning that there is a simple group T such that $T \leq G \leq \mathrm{Aut}(T)$; in this case we also have that G is doubly transitive, meaning that G can send any two points to any other two points. That T is itself transitive of degree p follows from [48], Proposition 7.1, which states that every normal subgroup of a primitive permutation group is transitive. The Classification Theorem for Finite Simple Groups implies that there is a very small list of possibilities for T (see [20], Corollary 4.2), and the lemma can be easily checked in these cases.

We are now ready to establish a group theoretic result, of which Theorem 2.1.5 will be an immediate corollary.

Proposition 2.6.2. *Let p be a prime number and let G be a finite subdirect product of transitive groups of degree p. If N is a normal subgroup of G, then N is an intersection of subgroups of index at most p in G.*

Proof. Let $G \leq_{sd} G_1 \times \cdots \times G_n$, where G_i is a transitive group of degree p for $i \in \{1, \ldots, n\}$. If we consider each group G_i acting transitively on a set Ω_i of size p, we have G acting faithfully on the disjoint union of these sets, which we denote by Ω. Let π_i denote the projection onto G_i, and let T_i denote the (unique) minimal normal subgroup of G_i. As mentioned following Lemma 2.6.1, we know that each T_i is either isomorphic to C_p or to a simple non-abelian group. We write $K_i = G \cap G_i$, which is a normal subgroup of both G and G_i. We proceed by induction on n. The case $n = 1$ follows easily from Lemma 2.6.1, since if N is nontrivial we must have G/N abelian of order dividing $p-1$; if N is trivial, observe that the point-stabilizers in G have index p and trivial intersection.

For each i we have that G/K_i is a subdirect product of the groups $\{G_j\}_{j \neq i}$. Notice that we may apply the inductive hypothesis to write NK_i/K_i as an intersection of some subgroups $\{H_l/K_i\}_l$ of index at most p in G/K_i. Now the subgroups $\{H_l\}_l$ are of index at most p in G, and $NK_i = \cap_l H_l$. If K_i is trivial, then our proof is complete. Alternatively, if N acts trivially on Ω_i,

notice that

$$N = \big(\cap_{x \in \Omega_i} \mathrm{Stab}_G(x) \big) \cap NK_i = \big(\cap_{x \in \Omega_i} \mathrm{Stab}_G(x) \big) \cap \big(\cap_l H_l \big).$$

Since the stabilizers $\mathrm{Stab}_G(x)$ have index p in G, we have written N as an intersection of subgroups of index at most p in G. Thus we may assume that, for each i, the subgroup K_i is nontrivial, and N acts nontrivially on Ω_i. Moreover, since K_i is nontrivial and normalized by G_i, it follows that K_i contains the unique minimal normal subgroup T_i of G_i. In particular this means that $T_i \leq G$, and writing $T = \prod_i T_i$ we have that $T \leq G$. Furthermore, G/T is abelian of exponent dividing $p - 1$.

Since N acts nontrivially on each Ω_i, we know that $T_i \leq \pi_i(N)$. For each i such that T_i is non-abelian (recall that T_i is simple), we will have $T_i = [T_i, N] \leq N$. Write T_{ab} for the product of the T_i which are abelian (these are all isomorphic to C_p), and write T_{n} for the product of those which are non-abelian. We have $T_{\mathrm{n}} \leq N$, so

$$\frac{TN}{N} = \frac{T_{\mathrm{ab}} T_{\mathrm{n}} N}{N} = \frac{T_{\mathrm{ab}} N}{N} \cong \frac{T_{\mathrm{ab}}}{T_{\mathrm{ab}} \cap N}.$$

Therefore TN/N is an elementary abelian p-group. We also know that G/TN is abelian of exponent dividing $p - 1$, so the short exact sequence

$$1 \to TN/N \to G/N \to G/TN \to 1$$

splits by the Schur-Zassenhaus Theorem (Theorem 39 from Chapter 17 of [18]).

Let $V = TN/N$ and $B = G/TN$, so (2.6) gives us

$$G/N = V \rtimes B.$$

We want to show that there is a collection of subgroups of index at most p in G/N whose intersection is trivial. It is clear that we can find such subgroups whose intersection is V, since B is abelian of exponent dividing $p-1$. Therefore it suffices to find subgroups of G/N of index at most p whose intersection meets V trivially.

Considering the $\mathbb{F}_p$-vector space V as a B-module, Maschke's Theorem (Theorem 1 from Chapter 18 of [18]) tells us that V decomposes as a direct sum of irreducible B-modules. Since $x^{p-1} - 1$ splits over $\mathbb{F}_p$, it follows that these irreducible submodules are one dimensional. Now we have submodules V_i of index p (codimension-one submodules), which yield subgroups $V_i \rtimes B$ of index p in G/N, and the intersection of all of these meets V trivially. □

Proof of Theorem 2.1.5. Let k be any field, and let K/k be a finite Galois subextension of $k^{[p]}/k$, where p is prime. This implies that K is contained in a compositum L of the splitting fields of finitely many irreducible, separable polynomials of degree p over k. Let $G = \mathrm{Gal}(L/k)$ and $N = \mathrm{Gal}(L/K)$. Then G isomorphic to a subdirect product of transitive groups of degree p, and N is normal in G. Proposition 2.6.2 implies that N is an intersection of subgroups of index at most p in G. By the Galois correspondence, this means that K is the compositum of finitely many extensions of k of degree at most

p. Therefore, K/k is generated by elements of degree at most p. (In fact, it must be generated by elements whose degrees are either equal to p or divide $p-1$.) $\square$

Chapter 3

Relative Bogomolov extensions

3.1 Introduction

We work within a fixed algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ throughout this paper. We write h for the usual absolute logarithmic height on algebraic numbers. If K is a subfield of $\overline{\mathbb{Q}}$, then K satisfies the *Bogomolov property*, (B), if there exists some $\varepsilon > 0$ such that there is no element $\alpha \in K^\times$ such that $0 < h(\alpha) < \varepsilon$. This definition was first stated in [10]. Recall that $h(\alpha) = 0$ if and only if α is a root of unity [9, Theorem 1.5.9]. We introduce the following generalization of (B) to relative extensions.

Definition 3.1.1. Let $\mathbb{Q} \subseteq K \subseteq L \subseteq \overline{\mathbb{Q}}$ be fields. We say that L/K is *Bogomolov*, or that L/K satisfies the *relative Bogomolov property*, (RB), if there exists $\varepsilon > 0$ such that

$$\{\alpha \in L^\times \mid 0 < h(\alpha) < \varepsilon\} \subseteq K.$$

In other words, L/K satisfies (RB) if and only if there is no sequence $\{\alpha_n\} \subseteq L^\times \setminus K^\times$ with $0 < h(\alpha_n) \to 0$ as $n \to \infty$. The following facts are immediate from the definition.

Proposition 3.1.2. *Suppose $K \subseteq L \subseteq M$ are subfields of $\overline{\mathbb{Q}}$.*

(a) If K satisfies (B) (in particular if $K/\mathbb{Q}$ is finite), then L/K is Bogomolov if and only if L satisfies (B);

(b) M/K is Bogomolov if and only if M/L and L/K are both Bogomolov; and

(c) if $L \setminus K$ contains a root of unity and L/K is Bogomolov, then K satisfies (B).

Part (c) follows because multiplying an algebraic number by a root of unity does not affect the height. Therefore, if $K^\times$ contains a sequence with positive height tending to zero, then so does $L^\times \setminus K^\times$.

It has already been shown that finite extensions may not satisfy (RB), as demonstrated in [2, Example 5.3], where it is shown that $\mathbb{Q}^{tr}(i)/\mathbb{Q}^{tr}$ is not Bogomolov. Here $\mathbb{Q}^{tr}$ denotes the maximal totally real extension of $\mathbb{Q}$, which satisfies (B) [41]. Interestingly, Pottmeyer [38] has recently stated a bound that implies that every finite extension of $\mathbb{Q}^{tr}(i)$ (the so-called "maximal CM field") satisfies (RB), using an archimedean estimate of Garza [24].

One of the main parts of this paper is the construction of examples that show that there exist examples of extensions L/K which satisfy (RB) even though K does not satisfy (B). Example 3.4.2 is such an example where L/K is infinite – this construction uses our results from Section 3.3. Example 3.4.1 shows a finite extension L/K which does not satisfy (RB). This example is quite elementary and does not rely on other results in this paper.

It is natural to ask what conditions can be placed on a field K of algebraic numbers to ensure that there exists at least one relative Bogomolov extension L/K. To this end we prove the following, our main result.

Theorem 3.1.3. *Let $K/\mathbb{Q}$ be an algebraic extension. Assume there exists a (finite) rational prime ℓ and a number field $F \subseteq K$ such that no prime of $\mathcal{O}_F$ lying over ℓ is ramified in K/F – in particular this holds if $K/\mathbb{Q}$ is Galois and some prime ℓ has finite ramification index in K. Then there exist relative Bogomolov extensions L/K. These extensions can be constructed explicitly of the form $K(\sqrt[\ell]{\alpha})$ for appropriately chosen elements $\alpha \in K$.*

This theorem should be compared with [10, Theorem 2], which states that a Galois extension with bounded *local degrees* (ramification index times inertial degree) has the Bogomolov property.

We briefly describe what is known on fields with the Bogomolov property in order to put our results in context. Schinzel [41] showed in 1973 that there is a positive lower bound on the height of totally real numbers outside of $\{\pm 1\}$, establishing (B) for the maximal totally real field $\mathbb{Q}^{tr}$. This can be described as an "archimedean" height estimate, and was generalized by Garza to a lower bound on the height of algebraic numbers with at least one real conjugate [24]. Another common approach that has been used (for example for the archimedean part of the argument in [26]) for archimedean estimates is equidistribution, starting with Bilu's Theorem [8], but these techniques will not be used in the current paper in favor of the Schinzel-Garza inequality.

One non-archimedean strategy originates in Amoroso and Dvornicich's paper [3], where it is shown that (B) is enjoyed by the maximal abelian extension $\mathbb{Q}^{ab}$ of $\mathbb{Q}$, which was generalized to relative extensions and strengthened considerably in [4] and [5]. Their strategy involves estimating how close a certain automorphism in a Galois group is to the action of raising an element to a power, with respect to a place lying over some auxilliary prime. This strategy is quite powerful and is also used in [26], the elliptic curve analogue of [3][†] , and in [2], where it is summarized nicely by their Lemma 2.2. The main theorem (Theorem 1.2) of the latter paper generalizes both the results on abelian extensions and [10, Theorem 2], which states that (B) is satisfied by a field having bounded local degrees above some rational prime.

In our present efforts to prove that a relative extension L/K is Bogomolov when K may not satisfy (B), it is not clear that the Amoroso-Dvornicich technique can be used to produce any new results. Instead we appeal to more classical bounds in terms of ramification. Our main tool is the lower bound [45, Theorem 2], due to Silverman. This bound is written in notation more similar to ours in [47, Section 3], where the author uses it effectively to give examples of fields satisfying the closely related Northcott property, (N). This stronger property, first defined along with (B) in [10], is satisfied by a field K if for any T at most finitely points in K have height at most T. Silver-

[†]The theorem from [3] is a result about heights on $\mathbb{G}_m(\mathbb{Q}^{ab}) = \mathbb{G}_m(\mathbb{Q}(\mathbb{G}_{m,tors})$. Theorem 1 of [26] replaces the *inner* $\mathbb{G}_m$ with an elliptic curve. Another well-known analogue of [3] is the main result of [6], which is the analogous result for $A(\mathbb{Q}^{ab})$, where A is an abelian variety.

man's inequality generalizes to the relative case a type of bound going back to the theorem [31, Theorem 1] of Mahler, which is exactly the lower bound used in [10, Theorem 2], where as mentioned before the authors exploit the existence of a bound on local degrees above some finite rational prime. Our Theorem 3.1.3 has the related hypothesis of finite ramification above a prime – for this theorem we also require an archimedean estimate coming from the above stated theorem of Garza.

The rest of this paper is organized as follows. In Section 3.2 we introduce notation and prove a criterion, Theorem 3.2.4, for when we can use ramification information to conclude that a finite relative extension L/K is Bogomolov. In Section 3.3 we describe how to apply these techniques to bound below the heights of elements properly contained in an extension of the form $K(\sqrt[\ell]{\alpha})$, using Hecke's classical theory of ramification in Kummer extensions. We combine this with the archimedean Schinzel-Garza inequality to prove Theorem 3.1.3. Finally, in Section 3.4 we construct the aforementioned explicit examples. We use our ramification criterion to construct explicitly a field K such that for each $\alpha \in K^\times$ there is a Bogomolov extension of the form $K(\sqrt[\ell]{\alpha})$.

We conclude the introduction by mentioning a few questions for further investigation. As mentioned above, if $L \setminus K$ contains a root of unity ζ and K does not satisfy (B), then $L \setminus K$ contains elements of arbitrarly small positive height of the form $\zeta\alpha$, with $\alpha \in K$. If one could construct such an extension where the *only* elements of small height in $L \setminus K$ were obtained by multiplying elements of K by roots of unity, this would suggest a weaker version of (RB)

that could be explored. Pottmeyer has shown that all finite extensions of the maximal CM field are Bogomolov. In this same spirit, it would be interesting to exhibit fields $K \subsetneq \overline{\mathbb{Q}}$ admitting *no* Bogomolov extensions. One easy example of this can be found if K is the subfield of $\overline{\mathbb{Q}}$ fixed by complex conjugation, i.e. $\overline{\mathbb{Q}} \cap \mathbb{R}$ (if we first embed $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$), but one might expect this to happen for other fields K that are sufficiently "big," for example pseudo-algebraically closed (a "PAC field," a field K such that every geometrically irreducible variety over K has a K-rational point – see [21, Chapter 11] for more; see [2, Section 6] for speculations on PAC fields and property (B)). If this occurs for a field K satisfying (B), this field would be maximal with respect to the Bogomolov property.

Acknowledgments

The author wishes to thank Jeffrey Vaaler and Felipe Voloch for some useful discussions related to Corollary 3.3.3, and Lukas Pottmeyer for pointing out relevant properties of $\mathbb{Q}^{tr}(i)$.

3.2 Lower bounds and a ramification criterion for (RB)

First we establish some notation conventions. For a finite extension of number fields M/F, we write $D_{M/F}$ for the relative discriminant ideal, and $N_{M/F}$ for the relative ideal norm. For a tower of number fields $M'/M/F$ will

often use the well-known identity

$$D_{M'/F} = D_{M/F}^{[M':M]} \cdot N_{M/F}\left(D_{M'/M}\right) \text{ [34, Proposition 4.15].}$$

A prime $\mathfrak{p}$ of F will mean a prime ideal in the ring of integers $\mathcal{O}_F$, with corresponding non-archimedean valuation $v_\mathfrak{p}$. If π is a uniformizing parameter for the associated place v, and if $\mathfrak{p}$ divides the rational prime ℓ, we normalize the absolute value $|\cdot|_v$ so that $|\pi|_v^{[F:\mathbb{Q}]} = \ell^f$, where f is the associated residue class degree.

The absolute logarithmic height of an algebraic number α is given by

$$h(\alpha) = \sum_v \log^+ |\alpha|_v,$$

the sum being taken over the places of any number field containing α. We denote the multiplicative height $H(\alpha) = \exp h(\alpha)$. We will often use basic facts about the height such as [9, Lemma 1.5.18] and [9, Proposition 1.5.15] without specific reference.

Let F be a number field of degree d over $\mathbb{Q}$, and let K/F be an algebraic extension. We define

$$\rho(K/F) = \limsup \ \{\delta(M)/[M:F] \ \big| \ F \subseteq M \subseteq K, \ [M:F] < \infty\},$$

where $\delta(M)$ denotes the number of archimedean places of M. In this context the limit superior is taken over the directed set of finite subextensions of K/F. In other words, $\rho(K/F)$ is the least real number ρ such that for any finite extension M/F contained in K, there is a finite extension M'/M with $M' \subseteq K$

such that $\delta(M')/[M' : F] \leq \rho$. Note that $d/2 \leq \rho(K/F) \leq d$, and that $\rho(L/F) \leq \rho(K/F)$ for any tower $L/K/F$. Of course if K/F is finite, then $\rho(K/F) = \delta(K)/[K : F]$.

We will apply the following inequality of Silverman [45, Theorem 2], cf. [47, Section 3] to produce a ramification criterion for (RB).

Theorem 3.2.1 (Silverman)**.** *If γ generates a relative extension of number fields B/M, where $[B : M] = s$ and $[B : \mathbb{Q}] = d$, then*

$$H(\gamma) \geq s^{-\frac{\delta(M)}{2d(s-1)}} \cdot N_{M/\mathbb{Q}}\left(D_{B/M}\right)^{\frac{1}{2ds(s-1)}}.$$

This is a relative field discriminant version of a bound of Mahler [31, Theorem 10]. Widmer exploited the dependence only on relative ramification in this bound to produce a ramification criterion for the Northcott property [47]. The following proposition illustrates our use of Silverman's Inequality

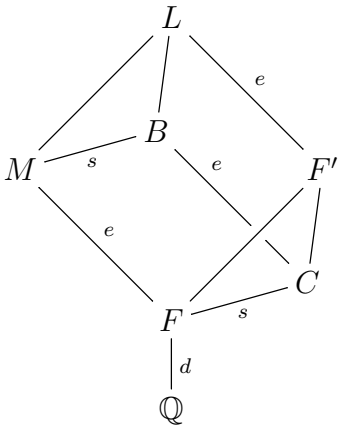
Proposition 3.2.2. *Let $M/F/\mathbb{Q}$ be a tower of finite extensions, and let $d = [F : \mathbb{Q}]$ and $e = [M : F]$. Assume α generates an extension F'/F and that F' and M are linearly disjoint over F. Let $L = M(\alpha)$. Suppose $\gamma \in L^\times \setminus M^\times$. Let $B = M(\gamma)$, $C = B \cap F'$, and $s = [B : M] = [C : F]$. We have*

$$H(\gamma) \geq s^{-\frac{\rho(M/F)}{2d(s-1)}} \cdot N_{F/\mathbb{Q}}\left(\frac{D_{C/F}^e}{\gcd\left(D_{C/F}^e, D_{M/F}^s\right)}\right)^{\frac{1}{2des(s-1)}}. \tag{3.2.1}$$

In particular, if no prime ramifying in F'/F is ramified in K/F, we have

$$H(\gamma) \geq s^{-\frac{\rho(M/F)}{2d(s-1)}} \cdot N_{F/\mathbb{Q}}\left(D_{C/F}\right)^{\frac{1}{2ds(s-1)}}. \tag{3.2.2}$$

Figure 3.2.3. *Diagram of the fields described in Proposition 3.2.2.*



Proof. We apply Silverman's Inequality to the extension B/M. Since M/F is finite, we have $\delta(M)/e = \rho(M/F)$, and thus we obtain

$$H(\gamma) \geq s^{-\frac{\rho(M/F)}{2d(s-1)}} \cdot N_{M/\mathbb{Q}}\left(D_{B/M}\right)^{\frac{1}{2des(s-1)}}. \tag{3.2.3}$$

Using basic properties of relative norms and discriminants, we have

$$N_{M/\mathbb{Q}}\left(D_{B/M}\right) = N_{F/\mathbb{Q}}\left(N_{M/F}\left(D_{B/M}\right)\right) = N_{F/\mathbb{Q}}\left(\frac{D_{B/F}}{D_{M/F}^{s}}\right).$$

Since $D_{B/F}$ is divisible by both $D_{C/F}^{e}$ and $D_{M/F}^{s}$, we now have

$$N_{M/\mathbb{Q}}\left(D_{B/M}\right) \geq N_{F/\mathbb{Q}}\left(\frac{\operatorname{lcm}\left(D_{C/F}^{e}, D_{M/F}^{s}\right)}{D_{M/F}^{s}}\right) = N_{F/\mathbb{Q}}\left(\frac{D_{C/F}^{e}}{\gcd\left(D_{C/F}^{e}, D_{M/F}^{s}\right)}\right).$$

Combining this inequality with (3.2.3) completes the proof of (3.2.1). Inequality (3.2.2) follows immediately. □

Now we move from the case of a finite extension M/F to that of a possibly infinite extension K/F, which leads to a criterion for a finite relative extension to satisfy (RB).

Theorem 3.2.4. *Let $K/\mathbb{Q}$ be an algebraic extension, and let $L = K(\alpha)/K$ be a finite extension. Let $f(x)$ denote the minimal polynomial of α over K. Let $L = K(\alpha)$ be a finite extension of K, and let F be a number field such that $F \subseteq K$ and $[F(\alpha) : F] = [L : K]$[‡]. Let $d = [F : \mathbb{Q}]$, $\rho = \rho(K/F)$, and $F' = F(\alpha)$. Assume that F' and K are linearly disjoint over F, and that no prime ramifying in F'/F is ramified in K/F. If $\gamma \in L^\times \setminus K^\times$, then*

$$H(\gamma) \geq \min\left\{ \left(N_{F/\mathbb{Q}}\left(D_{C/F}\right) \cdot s^{-\rho s} \right)^{\frac{1}{2ds(s-1)}} \;\middle|\; F \subsetneq C \subset F',\ s = s(C) = [C : F] \right\}. \tag{3.2.4}$$

In particular, if for each field C with $F \subsetneq C \subseteq F'$ we have

$$N_{F/\mathbb{Q}}\left(D_{C/F}\right) > s^{\rho s}, \tag{3.2.5}$$

where $s = [C : F]$ and $\rho = \rho(K/F)$, then L/K is Bogomolov.

Proof. Let M/F be a finite extension such that $M \subseteq K$ and $[M(\gamma) : M] = [K(\gamma) : K]$. For any field C with $F \subsetneq C \subseteq F'$, Proposition 3.2.2 gives us that

$$H(\gamma) \geq s^{-\frac{\rho(M/F)}{2d(s-1)}} \cdot N_{F/\mathbb{Q}}\left(D_{C/F}\right)^{\frac{1}{2ds(s-1)}},$$

and since $\rho(M/F) \leq \rho$, inequality (3.2.4) follows. Moreover, if inequality (3.2.5) is satisfied for all such fields C, then the lower bound in (3.2.4) is greater than one and depends only on K and L. □

[‡]This is satisfied, for example, if F contains the coefficients of $f(x)$

Remark 3.2.5. Notice that the lower bound in Theorem 3.2.4 depends on the choice a primitive element α – in fact α could be replaced by any collection of elements which generate the finite extension L/K.

3.3 Adjoining ℓ^{th} roots and the proof of Theorem 3.1.3

Extensions formed by adjoining an ℓ^{th} root of an element, where ℓ is a prime, are an easy source of examples in which we can successfully apply the bounds of the previous section. An extension of prime degree have no intermediate extensions, so application of Theorem 3.2.4 becomes much cleaner. Furthermore, the discriminants of such extensions when the base field contains a primitive ℓ^{th} root of unity (Kummer extensions) are completely understood thanks to classical work of Hecke (see [28, §39], cf. [15, Section 10.2.3]). We now illustrate how we can exploit this theory.

For the next lemma and its corollaries we use the following setup. Let $F/\mathbb{Q}$ be a finite extension of degree d, let $\alpha \in \mathcal{O}_F$, and let ℓ be a rational prime. Assume α is not an ℓ^{th} power in F, which by Capelli's Theorem [42, Theorem 19] implies that $x^\ell - \alpha$ is irreducible over F. Let $F' = F(\alpha^{1/\ell})$ for some choice of the root. Assume that $\ell\mathcal{O}_F$ and $\alpha\mathcal{O}_F$ are relatively prime ideals. In the following lemmas $\mathfrak{p}$ will always denote a prime of F lying over ℓ with residue class degree $f(\mathfrak{p}|\ell) = [\mathcal{O}_F/\mathfrak{p} : \mathbb{Z}/\ell\mathbb{Z}]$ and ramification index $e(\mathfrak{p}|\ell)$. For each $\mathfrak{p}|\ell$ define $a(\mathfrak{p})$ to be the greatest integer k such that the congruence

$$x^\ell - \alpha \equiv 0 \pmod{\mathfrak{p}^k} \tag{3.3.1}$$

has a solution in $\mathcal{O}_F$.

Lemma 3.3.1. *Let ρ be a real number with $\frac{1}{2} \leq \rho < 1$. If for each $\mathfrak{p}|\ell$ we have*

$$a(\mathfrak{p}) \leq 1 + \ell(1-\rho), \tag{3.3.2}$$

then we have

$$\ell^{\lceil \rho\ell \rceil}\mathcal{O}_F \mid D_{F'/F}, \tag{3.3.3}$$

where $\lceil x \rceil$ denotes the least integer greater than or equal to the real number x.

Proof of Lemma 3.3.1. Let $\mathfrak{p}$ be a prime of F lying over ℓ with ramification index $e = e(\mathfrak{p}|\ell)$ and residual degree $f = f(\mathfrak{p}|\ell)$. First, assume that F contains a primitive ℓ^{th} root of unity, and notice that this means that

$$\ell - 1 | e. \tag{3.3.4}$$

By [15, Theorem 10.2.9 (3)], (3.3.2) implies that $\mathfrak{p}$ is totally ramified in F'/F, and we have

$$v_{\mathfrak{p}}\left(D_{F'/F}\right) = (\ell-1)(\ell\frac{e}{\ell-1} + 1 - a(\mathfrak{p})). \tag{3.3.5}$$

Combining (3.3.2) with (3.3.4), we certainly have

$$a(\mathfrak{p}) \leq 1 + \frac{\ell e(1-\rho)}{\ell - 1},$$

and combining this with (3.3.5) yields

$$v_{\mathfrak{p}}\left(D_{F'/F}\right) \geq e \cdot \rho\ell.$$

This means that

$$D_{F'/F} \subseteq \prod_{\mathfrak{p}} \mathfrak{p}^{e(\mathfrak{p}|\ell)\cdot\lceil\rho\ell\rceil} = \ell^{\lceil\rho\ell\rceil}\mathcal{O}_F,$$

and we now have (3.3.3) in the case where F contains a primitive ℓ^{th} root of unity. In general, let $F'' = F(\zeta_\ell)$, where ζ_ℓ is a primitive ℓ^{th} root of unity. Let $n = [F'' : F]$. We have $n|\ell - 1$, and so $F'' \cap F' = F$ and $[F''F' : F'] = n$. We claim that

$$N_{F''/F}\left(D_{F''F'/F''}\right) \mid D^n_{F'/F}. \tag{3.3.6}$$

An easy way to see this is by considering relative different ideals as generated by the differents of elements, as in [34, Theorem 4.16]. Since F'/F and $F''F'/F''$ are generated by the same polynomial, it is clear that

$$\mathcal{D}_{F'/F}\mathcal{O}_{F''F'} \subseteq \mathcal{D}_{F''F'/F''}. \tag{3.3.7}$$

Taking the norm $N_{F''F'/F}$ of both sides of (3.3.7) yields (3.3.6). Our previous argument shows that $D_{F''F'/F''}$ is divisible by $\ell^{\lceil\rho\ell\rceil}\mathcal{O}_{F''}$, and so (3.3.6) gives us that $D^n_{F'/F}$ is divisible by $\ell^{\lceil\rho\ell\rceil\cdot n}\mathcal{O}_F$, and take n^{th} roots. □

To simplify application of this Lemma 3.3.1, we will prove the following two corollaries.

Corollary 3.3.2. *Suppose that for each $\mathfrak{p}|\ell$ we have*

$$v_{\mathfrak{p}}(\alpha^{\ell^f - 1} - 1) = 1, \tag{3.3.8}$$

where $f = f(\mathfrak{p}|\ell)$. Then each of the primes $\mathfrak{p}$ is totally ramified in F'/F, and

$$\ell^\ell\mathcal{O}_F \mid D_{F'/F}.$$

Proof. Since $(\mathcal{O}_F/\mathfrak{p})^\times$ has order $\ell^f - 1$, we have $\alpha^{\ell^f-1} - 1 \equiv 0 \pmod{\mathfrak{p}}$, so $x_1 = \alpha^{\ell^{f-1}}$ is a solution to (3.3.1) for $k = 1$. We have

$$v_\mathfrak{p}(x_1^\ell - \alpha) = v_\mathfrak{p}\left(\alpha^{\ell^f} - \alpha\right) = v_\mathfrak{p}\left(\alpha^{\ell^f-1} - 1\right).$$

Now, by [15, Proposition 10.2.13], there is no solution to (3.3.1) if $v_\mathfrak{p}\left(\alpha^{\ell^f-1} - 1\right) < k < \ell + 1$. If we assume (3.3.8) holds, this means that $a(\mathfrak{p}) = 1$ for all $\mathfrak{p}|\ell$, and the corollary follows directly from Lemma 3.3.1. □

Corollary 3.3.3. *Let ρ be a real number with $\frac{1}{2} \leq \rho < 1$. Assume that for each $\mathfrak{p}$ we have that $f(\mathfrak{p}|\ell) = 1$. There exists a constant c depending only on d and α such that if $\ell \geq c$, then*

$$\ell^{\lceil \rho\ell \rceil}\mathcal{O}_F \mid D_{F'/F}.$$

Proof. We now assume $f(\mathfrak{p}|\ell) = 1$ for all $\mathfrak{p}|\ell$. The corollary will be proved once we show that, for ℓ sufficiently large, the inequality (3.3.2) is satisfied. It is well known that, for an algebraic number β and a finite set of places S of a field containing β, we have

$$-h(\beta) \leq \sum_{v \in S} \log |\beta|_v \leq h(\beta) \text{ [9, (1.8, p. 20)]}. \tag{3.3.9}$$

We fix a prime $\mathfrak{p}|\ell$ and take the set S to consist of only that place v corresponding to $\mathfrak{p}$. We have $h(\alpha^{\ell-1} - 1) \leq \log 2 + (\ell - 1)h(\alpha)$, and so the left-hand inequality of (3.3.9) yields

$$-\log 2 - (\ell - 1)h(\alpha) \leq |\alpha^{\ell-1}|_v = -\frac{\log \ell}{d} \cdot v_\mathfrak{p}(\alpha^{\ell-1} - 1),$$

so that

$$v_{\mathfrak{p}}(\alpha^{\ell-1}-1) \leq \frac{d\log 2}{\log \ell} + \frac{(\ell-1)d\cdot h(\alpha)}{\log \ell} \leq 1+\ell(1-\rho)$$

if ℓ is sufficiently large in terms of d and α. As in the previous proof, the congruence (3.3.1) has no solution in F if $v_{\mathfrak{p}}\left(\alpha^{\ell-1}-1\right) < k < \ell+1$, and so we have $a(\mathfrak{p}) = v_{\mathfrak{p}}(\alpha^{\ell-1}-1)$, establishing the inequality (3.3.2) and completing the proof. □

Proof of Theorem 3.1.3. Let $K/\mathbb{Q}$ be an algebraic extension such that some rational prime ℓ has bounded ramification indices in K. Let F be a number field such that $F \subseteq K$ and no primes of F lying over ℓ are ramified in K/F, and set $d = [F : \mathbb{Q}]$. Let $\mathfrak{p}_1, \ldots \mathfrak{p}_n$ be the primes of F lying above ℓ. For $i = 1 \ldots n$, let β_i be a nontrivial element of $(\mathcal{O}_F/\mathfrak{p}_i^2)^\times$ such that $\beta^{\ell f} \equiv 1$. By the Chinese Remainder Theorem we can find an element $\alpha \in \mathcal{O}_F$ such $\alpha \equiv \beta_i \pmod{\mathfrak{p}_i}$ for each i. Therefore we have

$$v_{\mathfrak{p}_i}(\alpha^{\ell f-1}-1) = 1, \text{ for } i = 1 \ldots n.$$

Let $F' = F(\sqrt[\ell]{\alpha})$ for some choice of the root. Using Corollary 3.3.2 we now have

$$\ell^\ell \mid D_{F'/F},$$

and therefore

$$N_{F/\mathbb{Q}}\left(D_{F'/F}\right) \geq \ell^{\ell d}.$$

Let $L = K(\sqrt[\ell]{\alpha})$. We want to show that L/K is Bogomolov. If $\mathfrak{p}$ is a prime of F lying over ℓ, we know $\mathfrak{p}$ is unramified in K/F and totally ramified in F'/F, so we have that K and F' are linearly disjoint over F.

First suppose that $\rho(K/\mathbb{Q}) < 1$, so that $\rho := \rho(K/F) < d$. Our construction ensures now that

$$N_{F/\mathbb{Q}}\left(D_{F'/F}\right) \geq \ell^{d\ell} > \ell^{\rho\ell}, \tag{3.3.10}$$

and therefore L/K is Bogomolov by Theorem 3.2.4. (Note that there are no intermediate fields between F and F', since $[F' : F] = \ell$). More specifically, let $\gamma \in L \setminus K$, so that $\ell = [K(\gamma) : K]$. Then, combining (3.2.4) and (3.3.10) we have

$$\begin{aligned} H(\gamma) &\geq \left\{N_{F/\mathbb{Q}}\left(D_{F'/F}\right) \cdot \ell^{-\rho\cdot\ell}\right\}^{\frac{1}{2d\ell(\ell-1)}} \\ &\geq \left\{\ell^{d\ell} \cdot \ell^{-\rho\cdot\ell}\right\}^{\frac{1}{2d\ell(\ell-1)}} \geq \ell^{\frac{d-\rho}{2d(\ell-1)}} > 1, \end{aligned} \tag{3.3.11}$$

and in this case we are done using only our ramification criterion.

If $\rho = d$, we will have to use the following archimedean estimate of Garza.

Theorem 3.3.4 (Garza [24])**.** *Let K be a number field of degree d over $\mathbb{Q}$ with r real places and r' complex places. If $K = \mathbb{Q}(\gamma)$, then*

$$H(\gamma) \geq \left(2^{-d/r} + \sqrt{1 + 4^{-d/r}}\right)^{\frac{r}{2d}}. \tag{3.3.12}$$

Now we fix an arbitrary real number $\theta \in \left(\frac{2\ell-1}{2\ell}, 1\right)$. If $\rho(M/\mathbb{Q}) \leq \theta$, then as in (3.3.11) we have

$$H(\gamma) > \ell^{\frac{(1-\theta)}{2(\ell-1)}} > 1. \tag{3.3.13}$$

On the other hand, if $\rho(M/\mathbb{Q}) > \theta$, let r and s denote the number of real and complex archimedean places of M, respectively. Notice that $M(\gamma) = M(\sqrt[\ell]{\alpha})$ has r real places and $\frac{r(\ell-1)}{2} + s\ell$ complex places. This means that

$$\begin{aligned}\rho(\mathbb{Q}(\gamma)/\mathbb{Q}) \geq \rho(M(\gamma)/\mathbb{Q}) &= \frac{r + \frac{r(\ell-1)}{2} + s\ell}{\ell[M:\mathbb{Q}]} \\ &= \rho(M/\mathbb{Q}) - \frac{r_M}{[M:\mathbb{Q}]} \cdot \left(\frac{\ell-1}{2\ell}\right) > \theta - \frac{\ell-1}{2\ell}.\end{aligned}$$

If $\mathbb{Q}(\gamma)$ has r' real places and s' complex places, then we now have that

$$\frac{r'}{d'} = 2\rho(\mathbb{Q}(\gamma)/\mathbb{Q}) - 1 > 2\theta - 1 - \frac{\ell-1}{\ell} > 0$$

by our choice of $\theta > \frac{2\ell-1}{2\ell}$.

Now we may bound below the height of γ by an absolute constant using (3.3.12). Explicitly, writing $\phi = 2\theta - 1 - \frac{\ell-1}{\ell}$, we have

$$H(\gamma) \geq \left(2^{-\frac{1}{\phi}} + \sqrt{1 + 4^{-\frac{1}{\phi}}}\right)^{\frac{\phi}{2}} > 1. \tag{3.3.14}$$

Either (3.3.13) or (3.3.14) must hold. Taking the minimum of these bounds, we see that $H(\gamma)$ is bounded below by a constant greater than 1 which depends only on ℓ, and our proof is complete.

□

3.4 Examples

After establishing the following two examples, it is clear that, even if K does not satisfy (B), an extension L/K, may or may not satisfy (RB), whether L/K is finite or infinite.

Example 3.4.1 (L/K not Bogomolov)**.** Let b be a nonsquare rational number and let $K = \mathbb{Q}(b^{1/2}, b^{1/4}, b^{1/8}, \dots)$, for any choices of the roots. Notice that $b^{1/3} \notin K$, and let $L = K(b^{1/3})$. The extension L/K is not Bogomolov. To see this, consider the elements $b^{1/3}b^x \in L \setminus K$, where x is a rational number close to $-1/3$ with denominator a power of 2. Notice that $h(b^{1/3}b^x) = h(b^{x+\frac{1}{3}}) = (x + \frac{1}{3})h(b) \to 0$ as $x \to -1/3$. Many similar examples can be constructed easily, including of course infintie relative extensions.

Example 3.4.2 (L/K Bogomolov)**.** Let $K = \mathbb{Q}(3^{1/3}, 3^{1/9}, 3^{1/27}, \dots)$, and note that 3 is the only rational prime that ramifies in K. Let $3 < p_1 < p_2 < \cdots$ be an infinite sequence of primes congruent to 3 (mod 4). Set $K_0 = K$, and for each $n \geq 1$ set $K_n = K_{n-1}(\sqrt{p_n})$. For a given $n \geq 1$, we wish to apply Proposition 3.2.2 to estimate the height of an element $\gamma \in K_n^\times \setminus K_{n-1}$. To match the notation of Proposition 3.2.2 we set $F = \mathbb{Q}$ and choose $M \subseteq K_{n-1}$ to be a number field containing $\sqrt{p_1}, \sqrt{p_2}, \dots, \sqrt{p_{n-1}}$, and the coefficients for the minimal polynomial of γ over K_n. We use $C = F' = \mathbb{Q}(\sqrt{p_n})$. Note that in this case $N_{F/\mathbb{Q}}\left(D_{C/F}\right)$, is simply the discriminant of the quadratic field, which in this case is p_n. We have the trivial estimate $\rho(M/F) \leq d$, so applying (3.2.2), we have

$$H(\gamma) \geq 2^{-\frac{1}{2}} \cdot p_n^{\frac{1}{4}} = \left(\frac{p_n}{4}\right)^{\frac{1}{4}} \geq \left(\frac{p_1}{4}\right)^{\frac{1}{4}}.$$

Letting $L = \cup_n K_n$, we now have that L/K is an infinite Bogomolov extension, and in fact L can be constructed so that the lower bound on the height of an element of $L^\times \setminus K^\times$ is arbitrarily large.

If the roots $3^{1/3^i}$ are chosen in a compatible way (e.g. if we fix an embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ and impose that the roots are all real), then K has the property that all of its proper subfields are finite extensions of $\mathbb{Q}$. (The interested reader will verify that the only subfields of $\mathbb{Q}(3^{1/3^n})$ are $\mathbb{Q}(3^{1/3^i})$, $0 \leq i \leq n$.) Therefore, not only does K fail to satisfy (B), but it is not a Bogomolov extension of any subfield.

Example 3.4.3. We now construct a Galois extension $K/\mathbb{Q}$ which does not satisfy (B), but with the property that for every element $\alpha \in K^\times$, there is an integer n such that $K(\sqrt[n]{\alpha})/K$ is Bogomolov. As mentioned before, the maximal CM field $\mathbb{Q}^{tr}(i)$ also enjoys this property – in fact, all finite extensions of this field are Bogomolov. Our example is of a different sort, as it is generated by polynomials with no real roots, which prevents us from using archimedean estimates. It will suffice to consider α an algebraic integer, as any extension $K(\sqrt[n]{\alpha})$ could have been generated in this way by clearing denominators.

Set $K_0 = \mathbb{Q}$, $b_1 = 12$, and let K_n be generated over K_{n-1} by adjoining all of the roots of

$$f_n(x) = x^{b_n} + x + 1,$$

where b_n is a multiple of 12 chosen so that the discriminant of f_n is not divisible by any of the rational primes which are ramified in K_{n-1}. This is easily accomplished, since the discriminant of f_n is of the form $-\left(b_n^{b_n} + (b_n - 1)^{(b_n-1)}\right)$ (see [32] for example – we have used that $4|b_n$), which will not be divisible by any prime dividing b_n. By the Chebotarev Density Theorem, any number field

has infinitely many rational primes that are totally split in it. Therefore we can also choose a new prime ℓ_n at each step such that ℓ_n splits completely in K_{n-1} (and hence in K_m for all $m < n$), and also choose b_n to be divisible by $\ell_1\ell_2\cdots\ell_n$. In this way, we obtain an infinite set of primes $S = \{\ell_1, \ell_2, \dots\}$, none of which is ramified in any of the fields K_n. Furthermore, for any n we have that S contains arbitrarily large primes that split completely in K_n. Let $K = \cup_{n=1}^{\infty} K_n$. By making each b_n divisible by 3, we ensure that $f_n(x)$ is irreducible over $\mathbb{Q}$ with symmetric Galois group [37, Theorem 1], [43, Theorem 1]. By making each b_n even, we ensure that each polynomial $f_n(x)$ has no real roots, so we have $\rho(K/\mathbb{Q}) = \frac{1}{2}$. Using basic facts about the height, we see that if α_n is a root of $f_n(x)$, we have

$$b_n \cdot h(\alpha_n) = h(\alpha_n^{b_n}) = h(\alpha_n + 1) \leq \log 2 + h(\alpha_n) + h(1) = \log 2 + h(\alpha_n),$$

which yields

$$0 < h(\alpha_n) \leq \frac{\log 2}{b_n - 1},$$

which shows that K does not satisfy (B).

By construction the integers b_n are all at least 6, so the Galois group (over $\mathbb{Q}$) of each polynomial f_n is a symmetric group of degree at least 6. The splitting field of each f_n over $\mathbb{Q}$ is a simple A_n extension of a quadratic extension of $\mathbb{Q}$, and $K \cap \mathbb{Q}^{(2)}$ is the compositum of all these quadratic fields. Notice that any finite Galois subextension of $K/\left(K \cap \mathbb{Q}^{(2)}\right)$ has Galois group a product of simple alternating groups. To see this, note that the only proper,

nontrivial normal subgroups of a product of $G_1 \times G_2$ of simple nonabelian groups G_1 and G_2 are the "obvious" ones, $G_1 \times 1$ and $1 \times G_2$. We also see now that $K/\left(K \cap \mathbb{Q}^{(2)}\right)$ has no nontrivial solvable subextension.

We now fix an arbitrary $\alpha \in K^\times$, and we want to show that there is some integer n such that $K(\sqrt[n]{\alpha})/K$ is Bogomolov. For an odd prime $\ell \in S$, let β_ℓ denote some root of $x^\ell - \alpha$. We assume without loss of generality that α is not an ℓ^{th} power in K, or else we could replace α by an ℓ^{th} root until this hypothesis is satisfied, since there is no solvable subextension of $K/\left(K \cap \mathbb{Q}^{(2)}\right)$. This implies that $x^\ell - \alpha$ is irreducible over K, as its Galois group over $\left(K \cap \mathbb{Q}^{(2)}\right)(\alpha)$ is solvable of odd prime degree. For any m such that $\alpha \in K_m$, the only rational primes possibly ramifying in $K_m(\beta_\ell)$ will be those lying below prime divisors of $\alpha \mathcal{O}_{K_m}$, those ramified in K_m, and ℓ. Since ℓ does not ramify in any field K_n, we can choose $m = m(\alpha)$ large enough that $\alpha \in K_m$, and such that no primes ramifying in $K_m(\beta_\ell)$ divide the discriminant of f_n for any $n > m$, for any $\ell \in S$. As described above, we know that $K_m(\beta_\ell)$ and K are linearly disjoint over K_m. Let $d = [K_m : \mathbb{Q}]$.

Now by Corollary 3.3.3 we can fix an $\ell \in S$ such that ℓ splits completely in K_m and is large enough so that

$$\ell^{\lceil \rho \ell \rceil} \mathcal{O}_{K_m} \mid D_{K_m(\beta)/K_m},$$

where $\beta = \beta_\ell$, and $\rho = \frac{3}{4}$, say. Since none of the primes ramifying in $K_m(\beta)/K_m$ are ramified in K/K_m, and we have

$$N_{/\mathbb{Q}}\left(D_{K_m(\beta)/K_m)}\right) > \ell^{\ell d/2} = \ell^{\ell \rho (K/F)},$$

Theorem 3.2.4 shows that $K(\beta)/K$ is Bogomolov.

Chapter 4

Small points and free abelian groups (with Philipp Habegger and Lukas Pottmeyer)

4.1 Introduction

Let $\mathcal{G}$ denote either an algebraic torus (product of finitely many multiplicative groups) or an abelian variety defined over a number field K. Let $\overline{\mathbb{Q}}$ denote a fixed algebraic closure of $\mathbb{Q}$ containing K. If $\mathcal{G}$ is an abelian variety, by the canonical height on $\mathcal{G}$ we understand the Néron Tate height $\hat{h} : \mathcal{G}(\overline{\mathbb{Q}}) \to [0, \infty)$. If $\mathcal{G} = \mathbb{G}_m^r$ is a torus, we understand the sum of the absolute logarithmic Weil heights on the coordinates as the canonical height on $\mathcal{G}$. In both cases the height is well-defined modulo torsion, and induces a norm on the $\mathbb{Q}$-vector space $\mathcal{G}(\overline{\mathbb{Q}})/\mathcal{G}(\overline{\mathbb{Q}})_{tors}$ (in the case of the Néron-Tate height $\hat{h}$ on an abelian variety, the norm is given by $\sqrt{\hat{h}}$.) For the definitions and basic properties of these heights, see [9].

After [10], we say that a subfield $F \subseteq \overline{\mathbb{Q}}$ has the *Bogomolov property*, or *Property (B)* with respect to $\mathcal{G}$ if the canonical heights of non-torsion points of $\mathcal{G}(F)$ are bounded away from zero (recall that torsion points are exactly the points of height zero). This is equivalent to saying that the norm induced by the height is induces the discrete topology on $\mathcal{G}(F)/\mathcal{G}(F)_{tors}$. It was shown

by Lawrence [30] and Zorzitto [49] that a countable abelian group which is discrete under the topology induced by a norm is free abelian. (All groups considered here are countable, but the countability condition was later removed by Steprāns [46].) This immediately implies the following.

Proposition 4.1.1. *If F is a subfield of $\overline{\mathbb{Q}}$ that satisfies property (B) with respect to $\mathcal{G}$, then $\mathcal{G}(F)/\mathcal{G}(F)_{tors}$ is free abelian.*

In this chapter we will discuss the failure of the converse of this statement when $\mathcal{G}$ is a torus. We will prove the converse does not hold by explicitly constructing counterexample fields F. This amounts to showing

1. that $F^\times/F^\times_{tors}$ is free abelian, and
2. that $F^\times$ contains non-torsion points of arbitrarily small height.

In [25] we will also describe such examples for elliptic curves, and give more examples in the torus case as well.

4.2 Free Abelian Criteria

In this section we will develop two simple criteria for $\mathcal{G}(F)/\mathcal{G}(F)_{tors}$ to be free abelian. As the arguments are very general, we will not restrict ourselves to the $\mathbb{G}_m$ case here. Recall that a subgroup H of an abelian group G is called *pure* if G/H is torsion-free. The following version of Pontryagin's famous result on free abelian groups is proved (in stronger form) in [19, chapter IV, Theorem 2.3].

Theorem 4.2.1 (Pontryagin's Criterion)**.** *Let G be a countable abelian group. The following are equivalent:*

1. *G is free abelian;*
2. *G is torsion-free and every finite subset of G is contained in a finitely generated pure subgroup of G;*
3. *every finite subset of G is contained in a pure free abelian subgroup of G;*
4. *every finite rank subgroup of G is free abelian.*

Proposition 4.2.2 (Criterion A)**.** *Let $\mathcal{G}$ be an algebraic torus or elliptic curve defined over a number field K, and let F be a subfield of $\overline{\mathbb{Q}}$ which is a Galois extension of K. If $\mathcal{G}(F)_{\text{tors}}$ is finite, then $\mathcal{G}(F)/\mathcal{G}(F)_{\text{tors}}$ is free abelian.*

Proof. Set $c := |\mathcal{G}(F)_{\text{tors}}|$. We first prove the following inequality. For all $P \in \mathcal{G}(F)$ and all $k \in \mathbb{N}$ we have

$$[K(P) : K([k]P)] \leq c \tag{4.2.1}$$

All conjugates $\sigma(P)$ of P over $K([k]P)$ satisfy the equation $[k]\sigma(P) = [k]P$. Hence they are of the form $P+Q_\sigma$, where Q_σ is a k-torsion point of $\mathcal{G}$. As F was chosen to be Galois over K, all these Q_σ are contained in F. By assumption there are at most c of those and hence we have $[K(P) : K([k]P)] \leq c$.

To prove the proposition it suffices, by Pontryagin's Theorem 4.2.1, to prove that every finite rank subgroup G of $\mathcal{G}(F)/\mathcal{G}(F)_{\text{tors}}$ is free abelian. Let G

be such a subgroup and let $\overline{P_1}, \ldots, \overline{P_n}$ be a maximal set of linearly independent elements in G. Here $\overline{P_i}$ is the residue class of the element $P_i \in \mathcal{G}(F)$. Let $\overline{Q} \in G$ be arbitrary. Then there exist $(k_1, \ldots, k_n) \in \mathbb{Z}^n$ and $k \in \mathbb{Z}$ with $k \neq 0$ such that $[k_1]P_1 + \cdots + [k_n]P_n = [k]Q$. Every Galois conjugate of $[k]Q$ is of the form $\sigma([k_1]P_1) + \cdots + \sigma([k_n]P_n)$, $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$. Using (4.2.1) we find

$$[K(Q) : K] \leq c \prod_{i=1}^{n} [K(P_i) : K] =: C \quad .$$

This means that every element in G has a representative in $\mathcal{G}(F)$ with its degree bounded by the constant C. Northcott's theorem implies that the canonical height $\widehat{h}_{\mathcal{G}}$ is discrete on G. Hence, $\widehat{h}_{\mathcal{G}}$ (if $\mathcal{G}$ is a torus) or $\sqrt{\widehat{h}_{\mathcal{G}}}$ (if $\mathcal{G}$ is an elliptic curve) is a discrete norm on the abelian group G. By the theorem of Lawrence, Steprans, Zorzitto mentioned in the introduction we know that G is free abelian. This proves the proposition. □

Proposition 4.2.3 (Criterion B)**.** *Let $\mathcal{G}$ be an abelian variety or algebraic torus defined over some subfield F_0 of $\overline{\mathbb{Q}}$, and let F be a field with $F_0 \subseteq F \subseteq \overline{\mathbb{Q}}$. If for every finite extension M/F_0 with $M \subseteq F$, we have that $\mathcal{G}(M)/\mathcal{G}(M)_{\mathrm{tors}}$ is free abelian, and the torsion subgroup of $\mathcal{G}(F)/\mathcal{G}(M)$ has finite exponent, then $\mathcal{G}(F)/\mathcal{G}(F)_{\mathrm{tors}}$ is free abelian.*

Proof. This was proven by May ([33], Lemma 1) in the torus case. However, his proof applies one to one if $\mathcal{G}$ is an abelian variety. □

4.3 Example for $\mathbb{G}_m$

We will now construct examples of fields F which do not satisfy property (B), yet where $F^\times/F^\times_{tors}$ is free abelian.

There are many ways of seeing the following using height theory, but it was originally proved in [40].

Lemma 4.3.1. *Let d be any positive integer and $\mathbb{Q}^{(d)}$ the compositum of all number fields K, with $[K:\mathbb{Q}] \leq d$. Then $\mathbb{Q}^{(d)}$ contains only finitely many roots of unity.*

Theorem 4.3.2. *Let F be a finite extension of $\mathbb{Q}^{sym}$, then $F^\times/F^\times_{tors}$ is free abelian.*

Proof. As F is a finite extension of $\mathbb{Q}^{sym}$, there is an integer $d \geq 24$ such that $F \subseteq \mathbb{Q}^{sym}\mathbb{Q}^{(d)}$. We will prove that $(\mathbb{Q}^{sym}\mathbb{Q}^{(d)})^\times$ is free modulo torsion, which implies our stated result.

The extension $(\mathbb{Q}^{sym}\mathbb{Q}^{(d)})/\mathbb{Q}$ is Galois. By Proposition 4.2.2 it suffices to prove that there are only finitely many roots of unity in $\mathbb{Q}^{sym}\mathbb{Q}^{(d)}$. Let $\zeta \in \mathbb{Q}^{sym}\mathbb{Q}^{(d)}$ be a root of unity. Then there are finitely many fields $K_{n_1}, \ldots, K_{n_r}$ such that K_{n_i} is a finite Galois extension of $\mathbb{Q}$ with Galois group isomorphic to S_{n_i} for all $i \in \{1, \ldots, r\}$, and such that

$$\zeta \in K_{n_1} \cdots K_{n_r}\mathbb{Q}^{(d)}.$$

Of course we can assume that the fields $\mathbb{Q}^{(d)}, K_{n_1}\mathbb{Q}^{(d)}, \ldots, K_{n_r}\mathbb{Q}^{(d)}$ are pairwise distinct. Since d was chosen to be at least $24 = |S_4|$ we conclude $n_i \geq 5$ for all

$i \in \{1, \ldots, r\}$. The field $\mathbb{Q}^{(d)} \cap K_{n_i}$ is a Galois extension of $\mathbb{Q}$. Hence, the Galois group $\mathrm{Gal}(K_{n_i}\mathbb{Q}^{(d)}/\mathbb{Q}^{(d)})$ is isomorphic to a normal subgroup of $\mathrm{Gal}(K_{n_i}/\mathbb{Q}) \cong S_{n_i}$ for all $i \in \{1, \ldots, r\}$. By the assumption above $\mathbb{Q}^{(d)} \cap K_n \neq K_n$. Moreover $\mathbb{Q}^{(d)} \cap K_n \neq \mathbb{Q}$ because K_n contains a quadratic subfield. Therefore,

$$\mathrm{Gal}(K_{n_i}\mathbb{Q}^{(d)}/\mathbb{Q}^{(d)}) \cong A_{n_i} \text{ for all } i \in \{1, \ldots, r\}$$

The fields $K_{n_1}\mathbb{Q}^{(d)}, \ldots, K_{n_r}\mathbb{Q}^{(d)}$ are linear disjoint over $\mathbb{Q}^{(d)}$, as they are pairwise distinct and there Galois groups are simple. We can conclude

$$\mathrm{Gal}(K_{n_1} \cdots K_{n_r}\mathbb{Q}^{(d)}/\mathbb{Q}^{(d)}) \cong \prod_{i=1}^{r} A_{n_i}.$$

The extension $\mathbb{Q}^{(d)}(\zeta)/\mathbb{Q}^{(d)}$ is abelian and we have $\mathbb{Q}^{(d)}(\zeta) \subseteq K_{n_1} \cdots K_{n_r}\mathbb{Q}^{(d)}$. Thus, there is a normal subgroup $H \subseteq \prod_{i=1}^{r} A_{n_i}$ such that

$$\mathrm{Gal}(K_{n_1} \cdots K_{n_r}\mathbb{Q}^{(d)}/\mathbb{Q}^{(d)})/H \cong (\prod_{i=1}^{r} A_{n_i})/H \cong \mathrm{Gal}(\mathbb{Q}^{(d)}(\zeta)/\mathbb{Q}^{(d)}) \qquad (4.3.1)$$

is abelian. However, the only normal subgroups of $\prod_{i=1}^{r} A_{n_i}$ are of the form $\prod_{j \in J} A_{n_j}$ for some subset $J \subset \{1, \ldots, r\}$. Hence, the quotient on the left hand side of (4.3.1) is abelian, if and only if it is trivial. This implies, that ζ is an element of $\mathbb{Q}^{(d)}$. As ζ was an arbitrary root of unity in $\mathbb{Q}^{sym}\mathbb{Q}^{(d)}$, we find that the set of roots of unity in $\mathbb{Q}^{sym}\mathbb{Q}^{(d)}$ is equal to the set of roots of unity in $\mathbb{Q}^{(d)}$. This set is finite by Lemma 4.3.1. This was left to prove. □

Now consider the polynomials $f_n(x) = x^n - x - 1$. Corollary 3 of [37] tells us that the Galois group of the splitting field of $f_n(x)$ over $\mathbb{Q}$ is isomorphic

to the full symmetric group S_n. Let α be a root of $f_n(x)$, so $\alpha^n = \alpha + 1$. Using basic facts about the height, we see that

$$n \cdot h(\alpha) = h(\alpha^n) = h(\alpha + 1) \leq \log 2 + h(\alpha) + h(1) = \log 2 + h(\alpha),$$

which yields

$$0 < h(\alpha) \leq \frac{\log 2}{n-1}.$$

Now we see that any finite extension of $(\mathbb{Q}^{sym})^\times / (\mathbb{Q}^{sym})^\times_{tors}$ is free abelian, yet $\mathbb{Q}^{sym}$ contains points of arbitrarily small positive height.

Chapter 5

Multiplicative Diophantine approximation (With Jeffrey D. Vaaler)

5.1 Introduction

The main result of this section is the following result, which can be interpreted as a theorem on diophantine approximation in the multiplicative group, using the metric $(\alpha_1, \alpha_2) \mapsto h(\alpha_1 \alpha_2^{-1})$.

Theorem 5.1.1. *Let K be a subfield of $\overline{\mathbb{Q}}$, and let α an element of $\overline{\mathbb{Q}}^\times$. If there is no integer n such that $\alpha^n \in K$, then we have*

$$\inf\left\{h(\beta^\lambda \alpha^{-1}) \;\middle|\; \beta \in K, \lambda \in \mathbb{Q}\right\} \geq \max\left\{h(\alpha/\sigma\alpha) \;\middle|\; \sigma \in G_K\right\} > 0.$$

Note that the quantity on the left-hand side of the above inequality is well-defined independent of the choice of root β^λ.

Recall from Section 4.1 that a theorem of Lawrence and Zorzitto implies that a (torsion-free) abelian group which is made discrete by a norm must be free abelian. This means that if K is a subfield of $\overline{\mathbb{Q}}$ with the Bogomolov property (no small points), then $K^\times / K^\times_{tors}$ is free abelian. Now we achieve a version of this for relative Bogomolov extensions which are also Galois. Recall

from Section 3.1 that L/K is Bogomolov if there exists $\varepsilon > 0$ such that all points of L of height less than ε lie in K.

Corollary 5.1.2. *Let $K \subseteq L \subseteq \overline{\mathbb{Q}}$. If L/K is Galois and Bogomolov, then ${}^{(L^\times/K^\times)}\big/_{(L^\times/K^\times)_{tors}}$ is free abelian.*

Proof of Corollary. Let E_K denote the set of those algebraic numbers β such that $\beta^n \in K$ for some integer n (the "division closure" of $K^\times$). As the height defines a norm on $\overline{\mathbb{Q}}^\times/\overline{\mathbb{Q}}^\times_{tors}$, we may define a quotient norm on ${}^{(L^\times/K^\times)}\big/_{(L^\times/K^\times)_{tors}}$ by

$$\|\overline{\alpha}\| = \inf\left\{h(\alpha\beta^{-1}) \;\middle|\; \beta \in E_K\right\}.$$

By (5.1.1) we know that, for any α in $L^\times$ which is not in E_K, we have

$$\|\overline{\alpha}\| \geq \max\left\{h(\alpha/\sigma\alpha) \;\middle|\; \sigma \in G_K\right\}.$$

Since L/K is Galois and Bogomolov, the elements $\sigma\alpha/\alpha$ all lie in L, and thus their heights are bounded away from zero, meaning the norm we have defined is discrete. □

Ignoring the middle part of the inequality (5.1.1) yields a weaker statement which can be rephrased as follows.

Theorem 5.1.3. *Let K be an algebraic extension of $\mathbb{Q}$, and let α an element of $\overline{\mathbb{Q}}^\times$. Assume that for every $\varepsilon > 0$, there exists an integer $m \neq 0$, and a*

point β in $K^\times$, such that

$$h\big(\alpha^m\beta^{-1}\big) < \varepsilon|m|.$$

Then there exist an integer $n \neq 0$ such that α^n belongs to $K^\times$.

In Section 5.3 we will generalize this result to the completion $\mathcal{X}$ of $\mathcal{G} := \overline{\mathbb{Q}}^\times/\overline{\mathbb{Q}}^\times_{tors}$ with respect to the metric induced by the height, a Banach spaced which is described in [1]. For any subfield $K \subseteq \overline{\mathbb{Q}}$, let $\mathcal{F}_K$ be the image of $K^\times/K^\times_{tors}$ in $\mathcal{X}$, let $\mathcal{F}$ be the image of $\mathcal{G}$, let $\mathcal{E}_K$ denote the $\mathbb{Q}$-span of $\mathcal{F}_K$, and let $\mathcal{X}_K$ denote the closure of $\mathcal{E}_K$ in $\mathcal{X}$. We will prove the following.

Theorem 5.1.4. *For any subfield $K \subseteq \overline{\mathbb{Q}}$, we have $\mathcal{X}_K \cap \mathcal{F} = \mathcal{E}_K$.*

5.2 Inequalities for heights

In this section we give a proof of Theorem 5.1.1 by comparing the size of two distinct functions defined on the multiplicative group $\overline{\mathbb{Q}}^\times$ of nonzero algebraic numbers.

Lemma 5.2.1. *Let K be an algebraic extension of $\mathbb{Q}$, and let α a point in $\overline{\mathbb{Q}}^\times$. Write*

$$\alpha = \alpha_1, \alpha_2, \ldots, \alpha_M,$$

for the distinct conjugates of α over K. Then the following are equivalent.

(i) There exists an integer $n \neq 0$ such that α^n belongs to K.

(ii) For each $m = 1, 2, \ldots, M$, there exists ρ_m in $\overline{\mathbb{Q}}^\times_{tors}$ such that $\alpha_m = \rho_m\alpha$.

Proof. Assume that (i) holds. By replacing α with α^{-1} if necessary, we may assume that n is a positive integer. Write $\beta = \alpha^n$, so that α is a root of the monic polynomial $x^n - \beta$ in $K[x]$. The distinct roots of $x^n - \beta$ in $\overline{\mathbb{Q}}$ are

$$\{\alpha, \alpha\zeta_n, \alpha\zeta_n^2, \alpha\zeta_n^3, \ldots, \alpha\zeta_n^{n-1}\},$$

where ζ_n is a root of unity of order n. As the minimal polynomial for α over K divides $x^n - \beta$ in $K[x]$, all conjugates of α over K belong to the set (5.2). This clearly implies (ii).

Now suppose that (ii) holds. Then

$$\alpha_1\alpha_2\cdots\alpha_M = \alpha^M(\rho_1\rho_2\cdots\rho_M) = \alpha^M\zeta$$

belongs to K, where ζ is a root of unity. If ζ has order L, then

$$\alpha^{LM} = \left(\alpha^M\zeta\right)^L$$

belongs to K. Hence (i) holds with $n = LM$. □

Let $\mathrm{Aut}(\overline{\mathbb{Q}}/K)$ denote the group of automorphisms of $\overline{\mathbb{Q}}$ which fix each element of K. We define two functions

$$V_K : \overline{\mathbb{Q}}^\times \to [0,\infty), \quad \text{and} \quad W_K : \overline{\mathbb{Q}}^\times \to [0,\infty),$$

by

$$V_K(\alpha) = \inf\left\{|m|^{-1}h\left(\alpha^m\beta^{-1}\right) : m \neq 0 \text{ is an integer, and } \beta \in K^\times\right\},$$

and

$$W_K(\alpha) = \sup\left\{h\big(\alpha\tau(\alpha)^{-1}\big) : \tau \in \mathrm{Aut}(\overline{\mathbb{Q}}/K)\right\}.$$

As an algebraic number $\alpha \neq 0$ has finitely many distinct conjugates over K, it is clear that the supremum on the right of (5.2) is attained. Thus the supremum could be replaced by a maximum. Alternatively, write

$$\alpha = \alpha_1, \alpha_2, \ldots, \alpha_M,$$

for the distinct conjugates of α over K. Then we have

$$W_K(\alpha) = \max\left\{h\big(\alpha\alpha_m^{-1}\big) : m = 1, 2, \ldots, M\right\}.$$

Theorem 5.1.1 follows immediately from the following.

Lemma 5.2.2. *Let K be an algebraic extension of $\mathbb{Q}$, then for all α in $\overline{\mathbb{Q}}^{\times}$ we have*

$$\tfrac{1}{2}W_K(\alpha) \leq V_K(\alpha) \leq W_K(\alpha).$$

Proof. Let σ be an automorphism in $\mathrm{Aut}(\overline{\mathbb{Q}}/K)$ such that

$$W_K(\alpha) = h\big(\sigma(\alpha)\alpha^{-1}\big).$$

Let $m \neq 0$ be an integer and β an element of $K^\times$. Then we have

$$\begin{aligned} W_K(\alpha) &= |m|^{-1} h\big(\sigma\big(\alpha^m\big)\alpha^{-m}\big) \\ &= |m|^{-1} h\big(\sigma\big(\alpha^m\beta^{-1}\big)\beta\alpha^{-m}\big) \\ &\leq |m|^{-1} h\big(\sigma\big(\alpha^m\beta^{-1}\big)\big) + |m|^{-1} h\big(\beta\alpha^{-m}\big) \\ &= 2|m|^{-1} h\big(\alpha^m\beta^{-1}\big). \end{aligned}$$

We take the infimum on the right of (5.2) over all integers $m \neq 0$ and all β in $K^\times$, and obtain the inequality

$$\tfrac{1}{2} W_K(\alpha) \leq V_K(\alpha)$$

on the left of (5.2.2).

Next we suppose that (5.2) are the distinct conjugates of α over K. Then

$$\beta = \alpha_1\alpha_2\cdots\alpha_M$$

belongs to $K^\times$. It follows that

$$V_K(\alpha) \leq M^{-1} h\big(\alpha^M\beta^{-1}\big).$$

Then using (5.2) we find that

$$\begin{aligned} V_K(\alpha) &\leq M^{-1} h\big(\alpha^M\alpha_1^{-1}\alpha_2^{-1}\cdots\alpha_M^{-1}\big) \\ &\leq M^{-1} \sum_{m=1}^{M} h\big(\alpha\alpha_m^{-1}\big) \\ &\leq \max\big\{h\big(\alpha\alpha_m^{-1}\big) : m = 1, 2, \ldots, M\big\} \\ &= W_K(\alpha). \end{aligned}$$

This verifies the inequality on the right of (5.2.2). □

5.3 Generalizations to the Banach space $\mathcal{X}$

If α is point in $\overline{\mathbb{Q}}^\times$ and ρ is a point in $\overline{\mathbb{Q}}^\times_{tors}$, then it follows easily that

$$V_K(\rho\alpha) = V_K(\alpha) \quad \text{and} \quad W_K(\rho\alpha) = W_K(\alpha).$$

That is, both V_K and W_K are well defined on cosets of the quotient group

$$\mathcal{G} = \overline{\mathbb{Q}}^\times/(\overline{\mathbb{Q}}^\times_{tors}.$$

In this section we show that both of these functions are continuous on $\mathcal{G}$ with respect to the metric topology induced in $\mathcal{G}$ by the Weil height. Hence they have unique extensions to the completion $\mathcal{X}$. Because the image of $\mathcal{G}$ in $\mathcal{X}$ is dense in $\mathcal{X}$, the basic inequality (5.2.2) continues to hold at all points of the Banach space $\mathcal{X}$. This leads to a Galois correspondence between the closed subgroups $\mathrm{Aut}(\overline{\mathbb{Q}}/K) \subseteq \mathrm{Aut}(\overline{\mathbb{Q}}^\times/\mathbb{Q})$ and closed linear subspaces $\mathcal{X}_K \subseteq \mathcal{X}$. We now describe these results in more detail.

As in [1] we write

$$\mathcal{G} = \overline{\mathbb{Q}}^\times/(\overline{\mathbb{Q}}^\times_{tors},$$

so that $\mathcal{G}$ is a $\mathbb{Q}$-vector space (written multiplicatively). Also as in [1], we write

$$\mathcal{F} = \big\{ f_\alpha(y) : \alpha \in \mathcal{G} \big\}$$

for the image of $\mathcal{G}$ in the Banach space $\mathcal{X}$. Thus $\mathcal{F}$ is also a $\mathbb{Q}$-vector space but written additively, and $\mathcal{F}$ is a dense subset of $\mathcal{X}$. If $\mathbb{Q} \subseteq K \subseteq \overline{\mathbb{Q}}$ we write $\mathcal{G}_K$

for the image of $K^\times$ in $\mathcal{G}$, so that $\mathcal{G}_K$ is an abelian group and isomorphic to $K^\times/K^\times_{tors}$. Similarly we write

$$\mathcal{F}_K = \{f_\alpha(y) : \alpha \in \mathcal{G}_K\}$$

for the image of $\mathcal{G}_K$ in $\mathcal{F}$. Obviously $\mathcal{F}_K$ is also an abelian group, isomorphic to $K^\times/K^\times_{tors}$, but written additively. We use $\mathcal{F}_K$ to generate a linear subspace of the $\mathbb{Q}$-vector space $\mathcal{F}$, namely

$$\mathcal{E}_K = \operatorname{span}_{\mathbb{Q}} \mathcal{F}_K.$$

Each element of $\mathcal{E}_K$ is a finite linear combination

$$\sum_{n=1}^{N} q_n f_{\eta_n}(y),$$

where $q_1, q_2, \ldots, q_N$, are rational numbers, and $\eta_1, \eta_2, \ldots, \eta_N$, are elements of $\mathcal{G}_K$. If the positive integer m is the least common multiple of the denominators of $q_1, q_2, \ldots, q_N$, then it is clear that (5.3) can be written more simply as

$$m^{-1} f_\beta(y),$$

with β in $\mathcal{G}_K$. That is, (5.3) is a generic element in the $\mathbb{Q}$-vector space $\mathcal{E}_K$. Finally we define

$$\mathcal{X}_K = \operatorname{closure} \mathcal{E}_K,$$

so that $\mathcal{X}_K \subseteq \mathcal{X}$ is a closed linear subspace. Then the statement of Theorem 5.1.3 has the following alternative formulation.

Theorem 5.3.1. *Let K be an algebraic extension of $\mathbb{Q}$, and let f_α be an element of $\mathcal{F}$. Assume that for every $\varepsilon > 0$, there exists an integer $m \neq 0$, and a point f_β in $\mathcal{F}_K$, such that*

$$\left\| f_\alpha(y) - m^{-1} f_\beta(y) \right\|_1 < \varepsilon.$$

Then f_α belongs to $\mathcal{E}_K$.

The hypothesis (5.3.1) asserts that f_α is a limit point of $\mathcal{E}_K$ in $\mathcal{X}$, and therefore f_α belongs to $\mathcal{X}_K$. Thus we obtain Theorem 5.1.4: For any subfield $K \subseteq \overline{\mathbb{Q}}$, we have

$$\mathcal{F} \cap \mathcal{X}_K = \mathcal{E}_K.$$

Next we consider extensions of the maps V_K and W_K to the Banach space $\mathcal{X}$. We define

$$V_K : \mathcal{X} \to [0, \infty)$$

by

$$2V_K(F) = \inf \left\{ \|F - \boldsymbol{\xi}\|_1 : \boldsymbol{\xi} \in \mathcal{X}_K \right\}.$$

Then $F \mapsto 2V_K(F)$ is the usual quotient norm on $\mathcal{X}/\mathcal{X}_K$ induced by the norm $\| \ \|_1$ on $\mathcal{X}$. In particular $F \mapsto 2V_K$ is continuous on $\mathcal{X}$, and is constant on each coset in $\mathcal{X}/\mathcal{X}_K$. Because $\mathcal{E}_K$ is dense in $\mathcal{X}_K$, we also have

$$2V_K(F) = \inf \left\{ \|F - m^{-1} f_\beta\|_1 : m^{-1} f_\beta \text{ belongs to } \ \mathcal{E}_K \right\}.$$

Thus $F \mapsto V_K(F)$ is an extension of the map (5.2).

For each automorphism τ in $\mathrm{Aut}(\overline{\mathbb{Q}}/\mathbb{Q})$ we define a map

$$\Phi_\tau : L^1(Y, \mathcal{B}, \lambda) \to L^1(Y, \mathcal{B}, \lambda)$$

by

$$\Phi_\tau(F)(y) = F(\tau^{-1}y).$$

Then it is obvious that Φ_τ is a linear map. And it follows from Theorem 4 of [1] that

$$\int_Y \big|\Phi_\tau(F)(y)\big| \, \mathrm{d}\lambda(y) = \int_Y |F(y)| \, \mathrm{d}\lambda(y)$$

for each function F in $L^1(Y, \mathcal{B}, \lambda)$. Thus Φ_τ is an isometry of $L^1(Y, \mathcal{B}, \lambda)$ onto itself. Again from Theorem 4 of [1], we find that

$$\int_Y \Phi_\tau(F)(y) \, \mathrm{d}\lambda(y) = \int_Y F(y) \, \mathrm{d}\lambda(y),$$

and this shows that Φ_τ is also an isometry of $\mathcal{X}$ onto $\mathcal{X}$. For a function $F(y)$ in $\mathcal{X}$ we have

$$\Phi_\sigma\big(\Phi_\tau(F)\big)(y) = \Phi_{\sigma\tau}(F)(y).$$

Therefore the map $\tau \mapsto \Phi_\tau$ is a homomorphism from the group $\mathrm{Aut}(\overline{\mathbb{Q}}/\mathbb{Q})$ into the group $\mathcal{I}(\mathcal{X})$ of all isometries of $\mathcal{X}$ onto itself.

If $f_\alpha(y) = \log \|\alpha\|_y$ belongs to the $\mathbb{Q}$-vector subspace $\mathcal{F} \subseteq \mathcal{X}$, then it follows from (5.3) that

$$\Phi_\tau\big(f_\alpha\big)(y) = f_\alpha\big(\tau^{-1}y\big) = \log \|\tau\alpha\|_y,$$

and therefore the group of isometries

$$\left\{\Phi_\tau : \tau \in \mathrm{Aut}(\overline{\mathbb{Q}}/\mathbb{Q})\right\}$$

acts on the $\mathbb{Q}$-vector space $\mathcal{F}$.

If F belongs to $\mathcal{X}$ then it can be shown that $\tau \mapsto \Phi_\tau(F)(y)$ is a continuous map from the compact group $\mathrm{Aut}(\overline{\mathbb{Q}}^\times/K)$ into the Banach space $\mathcal{X}$. In particular the image of this map,

$$\left\{\Phi_\tau(F)(y) : \tau \in \mathrm{Aut}(\overline{\mathbb{Q}}^\times/K)\right\}$$

is a compact subset of $\mathcal{X}$. Therefore the value of the function $W_K : \mathcal{X} \to [0, \infty)$ given by

$$2W_K(F) = \sup\left\{\|F - \Phi_\tau(F)\|_1 : \tau \in \mathrm{Aut}(\overline{\mathbb{Q}}^\times/K)\right\}$$

is finite, and is taken on at a point in the group $\mathrm{Aut}(\overline{\mathbb{Q}}^\times/K)$. We note the simple bound

$$2W_K(F) \leq \sup\left\{\|F\|_1 + \|\Phi_\tau(F)\|_1 : \tau \in \mathrm{Aut}(\overline{\mathbb{Q}}^\times/K)\right\} \leq 2\|F\|_1.$$

It is clear that W_K defined on $\mathcal{X}$ by (5.3), extends the function W_K defined by (5.2).

Lemma 5.3.2. *The map W_K defined by* (5.3) *satisfies the triangle inequality*

$$W_K(F_1 + F_2) \leq W_K(F_1) + W_K(F_2),$$

and the Lipschitz inequality

$$\big|W_K(F_1) - W_K(F_2)\big| \le \|F_1 - F_2\|_1,$$

at all points F_1 and F_2 in $\mathcal{X}$.

Proof. Let σ be a point in $\mathrm{Aut}(\overline{\mathbb{Q}}^\times/K)$ such that

$$2W_K(F_1 + F_2) = \|(F_1 + F_2) - \Phi_\sigma(F_1 + F_2)\|_1.$$

Then we have

$$\begin{aligned} 2W_K(F_1 + F_2) &\le \|F_1 - \Phi_\sigma(F_1)\|_1 + \|F_2 - \Phi_\sigma(F_2)\|_1 \\ &\le 2W_K(F_1) + 2W_K(F_2), \end{aligned}$$

which verifies (5.3.2).

Now using (5.3) and (5.3.2) we find that

$$\begin{aligned} W_K(F_1) - W_K(F_2) &= W_K\big((F_1 - F_2) + F_2\big) - W_K(F_2) \\ &\le W_K(F_1 - F_2) \\ &\le \|F_1 - F_2\|_1. \end{aligned}$$

In a similar manner we get

$$W_K(F_2) - W_K(F_1) \le \|F_1 - F_2\|_1,$$

and this proves (5.3.2). □

Corollary 5.3.3. *Let K be an algebraic extension of $\mathbb{Q}$. At each point F in $\mathcal{X}$ we have*

$$\tfrac{1}{2}W_K(F) \le V_K(F) \le W_K(F).$$

Proof. We have already observed that $F \mapsto V_K(F)$ is the quotient norm on $\mathcal{X}/\mathcal{X}_K$ and is therefore continuous. The Lipschitz inequality (5.3.2) shows that $F \mapsto W_K(F)$ is also continuous. The inequality (5.3.3) has been proved for functions f_α in $\mathcal{F}$. As $\mathcal{F}$ is dense in $\mathcal{X}$, the inequality (5.3.3) must also hold for all functions F in $\mathcal{X}$. □

Corollary 5.3.4. *Let K be an algebraic extension of $\mathbb{Q}$. Then we have*

$$\mathcal{X}_K = \big\{F \in \mathcal{X} : \Phi_\tau(F) = F \text{ for all automorphisms } \tau \in \mathrm{Aut}(\overline{\mathbb{Q}}/K)\big\}.$$

Proof. Clearly a function F in $\mathcal{X}$ satisfies the condition

$$\Phi_\tau(F) = F \text{ for all automorphisms } \tau \in \mathrm{Aut}(\overline{\mathbb{Q}}/K),$$

if and only if $W_K(F) = 0$. By Corollary 5.3.3, $W_K(F) = 0$ if and only if $V_K(F) = 0$. As V_K is the quotient norm on $\mathcal{X}/\mathcal{X}_K$, it is obvious that $V_K(F) = 0$ if and only if F belongs to $\mathcal{X}_K$. This proves the identity (5.3.4). □

In the present setting, the fundamental theorem of Galois theory asserts that there is a bijection between intermediate fields K such that $\mathbb{Q} \subseteq K \subseteq \overline{\mathbb{Q}}$, and closed subgroups of $\mathrm{Aut}(\overline{\mathbb{Q}}/\mathbb{Q})$, given by

$$K \longleftrightarrow \mathrm{Aut}(\overline{\mathbb{Q}}/K).$$

The identity (5.3.4) allows us to extend this to certain special closed linear subspaces of $\mathcal{X}$ by

$$K \longleftrightarrow \mathrm{Aut}(\overline{\mathbb{Q}}/K) \longleftrightarrow \mathcal{X}_K.$$

Bibliography

[1] Daniel Allcock and Jeffrey D. Vaaler. A Banach space determined by the Weil height. *Acta Arith.*, 136(3):279–298, 2009.

[2] Francesco Amoroso, Sinnou David, and Umberto Zannier. On fields with the property (B). *Proc. Amer. Math. Soc.*, (to appear in print).

[3] Francesco Amoroso and Roberto Dvornicich. A lower bound for the height in abelian extensions. *J. Number Theory*, 80(2):260–272, 2000.

[4] Francesco Amoroso and Umberto Zannier. A relative Dobrowolski lower bound over abelian extensions. *Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4)*, 29(3):711–727, 2000.

[5] Francesco Amoroso and Umberto Zannier. A uniform relative Dobrowolski's lower bound over abelian extensions. *Bull. Lond. Math. Soc.*, 42(3):489–498, 2010.

[6] Matthew H. Baker and Joseph H. Silverman. A lower bound for the canonical height on abelian varieties over abelian extensions. *Math. Res. Lett.*, 11(2-3):377–396, 2004.

[7] Yakov Berkovich. *Groups of prime power order. Vol. 1*, volume 46 of *de Gruyter Expositions in Mathematics*. Walter de Gruyter GmbH & Co. KG, Berlin, 2008. With a foreword by Zvonimir Janko.

[8] Yuri Bilu. Limit distribution of small points on algebraic tori. *Duke Math. J.*, 89(3):465–476, 1997.

[9] Enrico Bombieri and Walter Gubler. *Heights in Diophantine geometry*, volume 4 of *New Mathematical Monographs*. Cambridge University Press, Cambridge, 2006.

[10] Enrico Bombieri and Umberto Zannier. A note on heights in certain infinite extensions of $\mathbb{Q}$. *Atti Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. Rend. Lincei (9) Mat. Appl.*, 12:5–14 (2002), 2001.

[11] Gregory Butler and John McKay. The transitive groups of degree up to eleven. *Comm. Algebra*, 11(8):863–911, 1983.

[12] Sara Checcoli. Fields of algebraic numbers with bounded local degrees and their properties. *Trans. Amer. Math. Soc.*, 365(4):2223–2240, 2013.

[13] Sara Checcoli and Martin Widmer. On the northcott property and other properties related to polynomial mappings. *Math Proc. Cambridge Philos. Soc.*, (to appear in print), 2011.

[14] Sara Checcoli and Umberto Zannier. On fields of algebraic numbers with bounded local degrees. *C. R. Math. Acad. Sci. Paris*, 349(1-2):11–14, 2011.

[15] Henri Cohen. *Advanced topics in computational number theory*, volume 193 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[16] John D. Dixon and Brian Mortimer. *Permutation groups*, volume 163 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1996.

[17] Klaus Doerk and Trevor Hawkes. *Finite soluble groups*, volume 4 of *de Gruyter Expositions in Mathematics*. Walter de Gruyter & Co., Berlin, 1992.

[18] David S. Dummit and Richard M. Foote. *Abstract algebra*. John Wiley & Sons Inc., Hoboken, NJ, third edition, 2004.

[19] P. C. Eklof and A. H. Mekler. *Almost free modules*, volume 65 of *North-Holland Mathematical Library*. North-Holland Publishing Co., Amsterdam, revised edition, 2002. Set-theoretic methods.

[20] Walter Feit. Some consequences of the classification of finite simple groups. In *The Santa Cruz Conference on Finite Groups (Univ. California, Santa Cruz, Calif., 1979)*, volume 37 of *Proc. Sympos. Pure Math.*, pages 175–181. Amer. Math. Soc., Providence, R.I., 1980.

[21] Michael D. Fried and Moshe Jarden. *Field arithmetic*, volume 11 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]*. Springer-Verlag, Berlin, third edition, 2008. Revised by Jarden.

[22] Itamar Gal and Robert Grizzard. On the compositum of all degree d extensions of a number field – to appear in print. *J. Théor. Nombres*

Bordeaux.

[23] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.5.4*, 2012.

[24] John Garza. On the height of algebraic numbers with real conjugates. *Acta Arith.*, 128(4):385–389, 2007.

[25] Robert Grizzard, Philipp Habegger, and Lukas Pottmeyer. Small points and free abelian groups – work in preparation.

[26] P. Habegger. Small height and infinite nonabelian extensions. *Duke Math. J.*, 162(11):2027–2076, 2013.

[27] G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers*. The Clarendon Press Oxford University Press, New York, fifth edition, 1979.

[28] Erich Hecke. *Lectures on the theory of algebraic numbers*, volume 77 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1981. Translated from the German by George U. Brauer, Jay R. Goldman and R. Kotzen.

[29] Alexander Hulpke. *Transitive permutation groups - A GAP data library. www.gap-system.org/Datalib/trans.html*.

[30] J. Lawrence. Countable abelian groups with a discrete norm are free. *Proc. Amer. Math. Soc.*, 90(3):352–354, 1984.

[31] K. Mahler. An inequality for the discriminant of a polynomial. *Michigan Math. J.*, 11:257–262, 1964.

[32] David W. Masser. The discriminants of special equations. *Math. Gaz.*, 50(372):158–160, 1966.

[33] W. May. Multiplicative groups of fields. *Proc. Lond. Math. Soc., III. Ser.*, 24:295–306, 1972.

[34] Władysław Narkiewicz. *Elementary and analytic theory of algebraic numbers*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, third edition, 2004.

[35] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2008.

[36] Olaf Neumann. On the imbedding of quadratic extensions into Galois extensions with symmetric group. In *Proceedings of the conference on algebraic geometry (Berlin, 1985)*, volume 92 of *Teubner-Texte Math.*, pages 285–295, Leipzig, 1986. Teubner.

[37] Hiroyuki Osada. The Galois groups of the polynomials $X^n + aX^l + b$. *J. Number Theory*, 25(2):230–238, 1987.

[38] Lukas Pottmeyer. A note on finite extensions of $\mathbb{Q}^{tr}$ (unpublished preprint).

[39] Victor V. Prasolov. *Polynomials*, volume 11 of *Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin, 2004. Translated from the 2001 Russian second edition by Dimitry Leites.

[40] Eugene Schenkman. On the multiplicative group of a field. *Arch. Math. (Basel)*, 15:282–285, 1964.

[41] A. Schinzel. On the product of the conjugates outside the unit circle of an algebraic number. *Acta Arith.*, 24:385–399, 1973. Collection of articles dedicated to Carl Ludwig Siegel on the occasion of his seventy-fifth birthday. IV.

[42] Andrzej Schinzel. *Polynomials with special regard to reducibility*, volume 77 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 2000. With an appendix by Umberto Zannier.

[43] Ernst S. Selmer. On the irreducibility of certain trinomials. *Math. Scand.*, 4:287–302, 1956.

[44] Jean-Pierre Serre. *Topics in Galois theory*, volume 1 of *Research Notes in Mathematics*. Jones and Bartlett Publishers, Boston, MA, 1992. Lecture notes prepared by Henri Damon [Henri Darmon], With a foreword by Darmon and the author.

[45] Joseph H. Silverman. Lower bounds for height functions. *Duke Math. J.*, 51(2):395–403, 1984.

[46] J. Steprāns. A characterization of free abelian groups. *Proc. Amer. Math. Soc.*, 93(2):347–349, 1985.

[47] Martin Widmer. On certain infinite extensions of the rationals with Northcott property. *Monatsh. Math.*, 162(3):341–353, 2011.

[48] Helmut Wielandt. *Finite permutation groups*. Translated from the German by R. Bercov. Academic Press, New York, 1964.

[49] F. Zorzitto. Discretely normed abelian groups. *Aequationes Math.*, 29(2-3):172–174, 1985.