

Winter School

# Heights and Algebraic Numbers

March 02. - March 04.2011  
Eberhard-Karls-Universität Tübingen

Martin Widmer<sup>1</sup>

**Quantitative and Qualitative Aspects of  
Northcott's Theorem**

March 10, 2011

<sup>1</sup>Present address: Department of Mathematics, Graz University of Technology,  
E-mail address: [widmer@math.tugraz.at](mailto:widmer@math.tugraz.at)



# Contents

<b>1</b>	<b>Basics</b>	<b>5</b>
1.1	Basic concept . . . . .	5
1.2	Absolute values . . . . .	7
1.2.1	Absolute values on a number field . . . . .	8
1.3	The height on $\overline{\mathbb{Q}}$ . . . . .	9
1.3.1	Arithmetic dynamics . . . . .	14
1.4	The height on $\overline{\mathbb{Q}}^n$ . . . . .	15
<b>2</b>	<b>Counting</b>	<b>17</b>
2.1	Introduction . . . . .	17
2.2	Counting lattice points . . . . .	22
2.3	Proof sketch of Schanuel's Theorem . . . . .	24
2.3.1	The strategy . . . . .	24
2.3.2	More details . . . . .	25
2.4	Proof strategies for Theorem 2.4 and Theorem 2.5 . . . . .	27
2.4.1	Theorem 2.4 . . . . .	27
2.4.2	Theorem 2.5 . . . . .	28
2.5	Integral points . . . . .	29
2.6	Proof sketch Theorem 2.13 for $d = 1$ . . . . .	31
<b>3</b>	<b>Height bounds for primitive points</b>	<b>33</b>
3.1	Introduction . . . . .	33
3.2	Bounds for the torsion part of class groups . . . . .	34
3.3	More results . . . . .	35
3.4	Numerical data . . . . .	37
<b>4</b>	<b>The Northcott property</b>	<b>43</b>
4.1	Introduction . . . . .	43
4.2	Proof of Theorem 4.7 . . . . .	47

4.3 Proof of Theorem 4.5 . . . . . 48

# Chapter 1

## Basics

In this chapter we introduce heights, give some typical applications, and state some of their most basic properties. A standard reference for heights is [1]. Other books containing material about heights are [10] and [11].

### 1.1 Basic concept

The leading question of this section is “What is a height and what is it good for?”. Roughly speaking a height is a real valued function that measures the arithmetic complexity of an algebraically defined object. Our objects are the algebraic numbers  $\overline{\mathbb{Q}}$  or more generally points in  $\overline{\mathbb{Q}}^n$ .

$$H : \overline{\mathbb{Q}}^n \longrightarrow [1, \infty).$$

A height should satisfy some “**Guiding Principles**”:

1. Height measures the arithmetic complexity.
2. There are only finitely many points of uniformly bounded height and degree, i.e.,  $|\{\alpha \in \overline{\mathbb{Q}}^n; [\mathbb{Q}(\alpha) : \mathbb{Q}] \leq d, H(\alpha) \leq X\}| < \infty$  for all  $X$  and  $d$ .
3. Height translates geometric relations into arithmetic relations.
4. Height has good behavior under algebraic operations.

#### Typical Applications

- A:** To prove finiteness results: show that the set has uniformly bounded height and degree and use 2..

There are many examples following this simple strategy, especially in:

- Diophantine geometry (Siegel’s theorem, Mordell-Weil theorem, Faltings’ theorem,...),
- Diophantine approximation (subspace theorem)
- arithmetic dynamics (finiteness of preperiodic points).

We will see an explicit example later on in this chapter.

Typically it is easy to prove the boundedness of the degree but hard to prove the boundedness of the height. However, we shall also meet some example where the converse holds.

**B:** Suppose  $S \subset \overline{\mathbb{Q}}^n$  is an infinite set of uniformly bounded degree. We can study its density by estimating its counting function

$$N(S, X) = |\{\alpha \in S; H(\alpha) \leq X\}|.$$

Here are a few examples:

a)  $S = \mathbb{Q}$ :

$$N(S, X) = \frac{12}{\pi^2} X^2 + O(X \log X).$$

b)  $S = V(\mathbb{Q})$  for  $V: x - yz^r = 0$  ( $r > 1$  fixed).

$$N(S, X) = \frac{8\zeta(r) - 2\zeta(r+1)}{\zeta(2)\zeta(r+1)} X^2 + O(X \log X).$$

c)  $S = \{\alpha \in \overline{\mathbb{Q}}; [\mathbb{Q}(\alpha) : \mathbb{Q}] = 22\}$

$$N(S, X) = c_1 X^{506} + O(X^{484} \log X).$$

c)  $S = \{\alpha \in \overline{\mathbb{Q}}; [\mathbb{Q}(\alpha) : \mathbb{Q}] = 22, \mathbb{Q}(\alpha) \text{ contains a quadratic subfield}\}$

$$N(S, X) = c_2 X^{264} + O(X^{253} \log X).$$

We will construct a height satisfying the guiding principles. For this we need absolute values.

## 1.2 Absolute values

In this section we collect some basic facts about absolute values without proofs. Proofs can be found in most books about algebraic number theory such as [16], [12] or [8]. Some of the material stems from [21]. We start with the most basic definition.

**Definition .** *Let  $K$  be a field. An absolute value on  $K$  is a map  $a \rightarrow |a|$  from  $K$  to  $\mathbb{R}$  such that*

$$i) |a| \geq 0 \text{ and } |a| = 0 \iff a = 0.$$

$$ii) |ab| = |a||b|.$$

$$iii) |a + b| \leq |a| + |b|.$$

Examples:

- a)  $K$  arbitrary and  $|a| = 1$  for  $a \neq 0$  and  $|0| = 0$ . This is the trivial absolute value.
- b)  $K = \mathbb{Q}$  and  $|a| = |a|_\infty$  the usual absolute value on  $\mathbb{Q}$ .
- c)  $K = \mathbb{Q}$  and  $p$  a positive prime. Then any nonzero  $a$  can be factored as  $a = p^\alpha r/s$  with  $p \nmid rs$  and a unique  $\alpha$ . We put  $|a|_p = p^{-\alpha}$ . This is the  $p$ -adic absolute value.

**Remark .** *The  $p$ -adic absolute value satisfies the ultrametric triangle inequality, i.e.,  $|a + b|_p \leq \max\{|a|_p, |b|_p\}$ .*

**Definition .** *An absolute value on  $K$  that satisfies the ultrametric triangle inequality is called a **non-Archimedean** absolute value on  $K$ . An absolute value on  $K$  that does not satisfy the ultrametric triangle inequality is called an **Archimedean** absolute value on  $K$ .*

**Definition .** a) *An absolute value on  $K$  induces a metric on  $K$  by  $d(a, b) = |a - b|$ .*

b) *We say the two absolute values  $|\cdot|_1$  and  $|\cdot|_2$  on  $K$  are equivalent ( $|\cdot|_1 \sim |\cdot|_2$ ) if they induce the same topology on  $K$ .*

c) *The equivalence class of a nontrivial absolute value on  $K$  is called a place of  $K$ .*

d) *The set of places of  $K$  is denoted by  $M_K$ .*

**Lemma 1.1.** *Let  $|\cdot|_1$  and  $|\cdot|_2$  be absolute values on  $K$ . The following are equivalent:*

- i)  $|\cdot|_1 \sim |\cdot|_2$ .*
- ii)  $|\cdot|_1 = |\cdot|_2^\alpha$  for some fixed  $\alpha > 0$ .*

**Remark .** *For  $|\cdot|_1 \sim |\cdot|_2$  we have:  
 $|\cdot|_1$  non-Archimedean  $\iff |\cdot|_2$  non-Archimedean.*

### 1.2.1 Absolute values on a number field

Let  $K$  be a number field with  $r$  real embeddings  $\sigma_1, \dots, \sigma_r : K \rightarrow \mathbb{R}$  and  $s$  pairs of complex conjugate embeddings  $\sigma_{r+1}, \dots, \sigma_{r+2s} : K \rightarrow \mathbb{C}$ . We order them in such a way that  $\sigma_{r+s+i} = \overline{\sigma_{r+i}}$  ( $1 \leq i \leq s$ ). Put  $d = [K : \mathbb{Q}] = r + 2s$  and write  $\mathcal{O}_K$  for the ring of integers in  $K$ .

#### Archimedean absolute values:

Each embedding  $\sigma_v = \sigma_i$  ( $1 \leq i \leq r + s$ ) gives an Archimedean place  $v$ . We choose a representative as follows:

$$|a|_v = |\sigma_v(a)|.$$

Each Archimedean place on  $K$  arises in this way and they are pairwise distinct. Moreover, each of the above representatives extends the usual absolute value on  $\mathbb{Q}$ .

#### Non-Archimedean absolute values:

Each nonzero prime ideal  $\wp_v$  of  $\mathcal{O}_K$  gives a non-Archimedean place  $v$ . We choose a representative as follows:

$$|a|_v = N_{\wp_v}^{-\frac{\text{ord}_{\wp_v}(a)}{e_v f_v}} = p_v^{-\frac{\text{ord}_{\wp_v}(a)}{e_v}},$$

where  $N_{\wp_v} = |\mathcal{O}_K/\wp_v|$  is the norm,  $p_v = \wp_v \cap \mathbb{Q}$  is the corresponding prime in  $\mathbb{Q}$ ,  $e_v = e(\wp_v/p_v)$  is the ramification index,  $f_v = f(\wp_v/p_v)$  is the residue degree, and  $\text{ord}_{\wp_v}(a)$  is the exponent of  $\wp_v$  in the prime factorisation of the principal ideal  $(a)$  (of course we can assume  $a \neq 0$ ).

Each non-Archimedean place on  $K$  arises in this way and they are pairwise distinct. Moreover, each of the above representatives extends the  $p_v$ -adic absolute value on  $\mathbb{Q}$ .

For each  $v \in M_K$  we put

$K_v =$  the completion of  $K$  at  $|\cdot|_v$ ,

$\mathbb{Q}_v =$  the completion of  $\mathbb{Q}$  at the restriction  $|\cdot|_{v|\mathbb{Q}}$  to  $\mathbb{Q}$ .

Then  $K_v/\mathbb{Q}_v$  is a finite extension and we call the degree of this extension the local degree at  $v$ ,

$$d_v = [K_v : \mathbb{Q}_v].$$

**Proposition 1.2.** *Suppose  $K$  and  $L$  are number fields. Then*

i)  $a \in K^* \implies |a|_v = 1$  for all but finitely many  $v \in M_K$ .

ii) **Product formula:**  $\prod_{v \in M_K} |a|_v^{d_v} = 1$  for all  $a \in K^*$ .

iii) If  $K \subset L$  and  $w \in M_L$ , then there exists a unique  $v \in M_K$  such that  $|\cdot|_{w|_K} = |\cdot|_v$ . Moreover,  $d_v \mid d_w$ , and we write  $w \mid v$ .

vi) If  $K \subset L$  and  $v \in M_K$  then there exist only finitely many  $w \in M_L$  with  $w \mid v$ , and we have  $\sum_{\substack{w \in M_L \\ w \mid v}} d_w = d_v [L : K]$ .

v) If  $v \in M_K$  and  $v \nmid \infty$  then  $d_v = e_v f_v$ .

### 1.3 The height on $\overline{\mathbb{Q}}$

Let  $K$  be a number field,  $d = [K : \mathbb{Q}]$ .

Relative height on  $K$ :

$$H_K : K \rightarrow [1, \infty)$$

$$H_K(\alpha) = \prod_{v \in M_K} \max\{1, |\alpha|_v\}^{d_v}.$$

Here are two examples:

a)  $K = \mathbb{Q}$ ,  $\alpha = p/q$  with coprime integers  $p, q$  and  $q \neq 0$ . Then

$$\begin{aligned} H_{\mathbb{Q}}(p/q) &= \prod_{v \in M_{\mathbb{Q}}} \max\{1, |p/q|_v\}^{d_v} = \prod_{v \in M_{\mathbb{Q}}} |q|_v^{d_v} \max\{1, |p/q|_v\}^{d_v} \\ &= \prod_{v \in M_{\mathbb{Q}}} \max\{|q|_v, |p|_v\}^{d_v} = \max\{|q|_{\infty}, |p|_{\infty}\}. \end{aligned}$$

- b)  $K = \mathbb{Q}(\sqrt{2})$ ,  $\alpha = \frac{1+\sqrt{2}}{3+\sqrt{2}}$ . Now  $N((1+\sqrt{2})) = 1$ , and so  $1+\sqrt{2}$  is a unit. And  $N((3+\sqrt{2})) = 7$ , and so  $(3+\sqrt{2})$  is a prime ideal of degree 1. Moreover, we have  $|\alpha|_v < 1$  for both Archimedean absolute values. Hence  $H_K(\alpha) = 7$ .

**Lemma 1.3.** *Suppose  $L/K$  is a finite extension of number fields and  $d = [K : \mathbb{Q}]$ ,  $D = [L : \mathbb{Q}]$ . Then*

$$H_K(\alpha)^{1/d} = H_L(\alpha)^{1/D} \text{ for all } \alpha \in K.$$

*Proof.* Using Proposition 1.2 we have

$$\begin{aligned} H_L(\alpha)^{1/D} &= \prod_{w \in M_L} \max\{1, |\alpha|_w\}^{d_w/D} = \prod_{v \in M_K} \prod_{\substack{w \in M_L \\ w|v}} \max\{1, |\alpha|_w\}^{d_w/D} \\ &= \prod_{v \in M_K} \prod_{\substack{w \in M_L \\ w|v}} \max\{1, |\alpha|_v\}^{d_w/D} = \prod_{v \in M_K} \max\{1, |\alpha|_v\}^{\sum_{w|v} d_w/D}. \end{aligned}$$

Moreover,  $\sum_{\substack{w \in M_L \\ w|v}} d_w = d_v[L : K] = d_v D/d$ . This completes the proof.  $\square$

Lemma 1.3 shows how we can define a height on  $\overline{\mathbb{Q}}$ .

**Definition** (Absolute non-logarithmic Weil height).

$$\begin{aligned} H : \overline{\mathbb{Q}} &\rightarrow [1, \infty) \\ H(\alpha) &= \prod_{v \in M_K} \max\{1, |\alpha|_v\}^{d_v/d}, \end{aligned}$$

where  $K$  is any number field containing  $\alpha$  and  $d = [K : \mathbb{Q}]$ .

The next lemma shows that the height behaves well under algebraic operations (i)–(iii)) and translates geometric relations into arithmetic relations (iv)).

**Lemma 1.4.**

- i)  $H(\alpha) = H(\sigma(\alpha))$  for all  $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ .
- ii)  $H(\alpha\beta) \leq H(\alpha)H(\beta)$ , and  $H(\alpha_1 + \cdots + \alpha_r) \leq rH(\alpha_1) \cdots H(\alpha_r)$ .
- iii)  $H(\alpha^n) = H(\alpha)^{|n|}$  for all  $n \in \mathbb{Z}$ .
- iv) Suppose  $f \in \overline{\mathbb{Q}}[x]$ ,  $f \neq 0$ ,  $\deg f = e$ . Then there exist  $c_f, C_f > 0$  such that
 
$$c_f H(\alpha)^e \leq H(f(\alpha)) \leq C_f H(\alpha)^e \quad \forall \alpha \in \overline{\mathbb{Q}}.$$

*Proof.* i), ii), iii) and the second inequality of iv) are easy. Let us prove the first inequality in iv). Put  $f_1 = f_1(x_1, x_2) = x_2^e$ , and  $f_2 = f_2(x_1, x_2) = x_2^e f(x_1/x_2)$ . So  $f_1, f_2$  are homogeneous polynomials of degree  $e$  without common zeros except  $(x_1, x_2) = (0, 0)$ . So the variety  $V(J)$  defined by the ideal  $J = (f_1, f_2)$  of  $\overline{\mathbb{Q}}[x_1, x_2]$  consists of the point  $(0, 0)$ , in particular  $x_1$  and  $x_2$  are contained in the vanishing ideal  $I(V(J))$ . By the Hilbert Nullstellensatz the latter is the radical of  $J$ , thus there exist positive integers  $r_i$  such that  $x_i^{r_i} \in J$ . After replacing  $r_i$  by  $r_1 r_2$  we may take a common  $r$ . Hence there exist polynomials  $g_{ij} \in \overline{\mathbb{Q}}[x_1, x_2]$  such that  $x_i^r = g_{i1} f_1 + g_{i2} f_2$ . As  $f_1, f_2$  are homogeneous of degree  $e$  we can replace  $g_{ij}$  by its homogeneous part of degree  $r - e$  and the equality remains valid. Next choose a number field  $K$  such that  $\alpha, f_1, f_2, g_{ij} \in K[x_1, x_2]$  and put  $d = [K : \mathbb{Q}]$ . For  $v \in M_K$  we set  $\epsilon_v(l) = l$  if  $v \mid \infty$  and  $\epsilon_v(l) = 1$  if  $v \nmid \infty$ . Suppose  $x_1, x_2$  are also in  $K$ . Then

$$|x_i^r|_v = \left| \sum_j g_{ij} f_j \right|_v \leq \epsilon_v(2) \max_j \{|g_{ij} f_j|_v\} \leq \epsilon_v(2) \max_j \{|g_{ij}|_v\} \max_j \{|f_j|_v\}.$$

Let  $\xi_0, \dots, \xi_{r-e}$  be the coefficients of  $g_{ij}$  and let  $c_{ij,v} = \max\{|\xi_0|_v, \dots, |\xi_{r-e}|_v\}$ . Note that either  $g_{i1}$  or  $g_{i2}$  is nonzero, and thus  $\max_j \{c_{ij,v}\} > 0$ . Now

$$\max_j \{|g_{ij}|_v\} \leq \epsilon_v(r - e + 1) \max_j \{c_{ij,v}\} \max_j \{|x_1|_v, |x_2|_v\}^{r-e}.$$

We conclude

$$\max\{|x_1|_v, |x_2|_v\}^r \leq \epsilon_v(2) \epsilon_v(r - e + 1) \max_{i,j} \{c_{ij,v}\} \max_j \{|x_1|_v, |x_2|_v\}^{r-e} \max_j \{|f_j|_v\},$$

and therefore

$$\max\{|f_1|_v, |f_2|_v\} \geq \frac{\max\{|x_1|_v, |x_2|_v\}^e}{\epsilon_v(2) \epsilon_v(r - e + 1) \max_j \{c_{ij,v}\}}.$$

Next we take the product with multiplicities  $d_v$  over all  $v \in M_K$ . The claim then follows by choosing  $x_1 = \alpha$  and  $x_2 = 1$ .  $\square$

**Lemma 1.5.** *Suppose  $\alpha$  is in  $\overline{\mathbb{Q}}$  with minimal polynomial  $D_\alpha(x) = a_0(x - \alpha_1) \cdots (x - \alpha_d) = a_0 x^d + \cdots + a_d \in \mathbb{Z}[x]$  (so  $a_0 > 0$ , and  $\gcd(a_0, \dots, a_d) = 1$ ). Then*

$$H(\alpha) = \left( a_0 \prod_{i=1}^d \max\{1, |\alpha_i|\} \right)^{1/d}.$$

*Proof.* Put  $L = \mathbb{Q}(\alpha_1, \dots, \alpha_d)$  and  $D = [L : \mathbb{Q}]$ . Let  $\sigma_i : \mathbb{Q}(\alpha_j) \rightarrow \mathbb{C}$  ( $1 \leq i \leq d$ ) be the embeddings of  $\mathbb{Q}(\alpha_j)$  and for each  $i$  denote by  $\tau_{ik}$  ( $1 \leq k \leq D/d$ ) its  $D/d$  extensions to embeddings of  $L$ . Then

$$\begin{aligned} \prod_{i=1}^d \max\{1, |\alpha_i|\}^{D/d} &= \prod_{i=1}^d \max\{1, |\sigma_i(\alpha_j)|\}^{D/d} = \prod_{i=1}^d \prod_{k=1}^{D/d} \max\{1, |\tau_{ik}(\alpha_j)|\} \\ &= \prod_{\substack{w \in M_L \\ w \nmid \infty}} \max\{1, |\alpha_j|_w\}^{d_w}. \end{aligned}$$

Now for the non-Archimedean places we need Gauss' Lemma. Suppose  $w \in M_L$ ,  $w \nmid \infty$  and  $g = b_0x^m + \dots + b_m \in L[x]$ . Put  $|g|_w = \max\{|b_0|_w, \dots, |b_m|_w\}$ . If  $g, h \in L[x]$  then by Gauss' Lemma  $|gh|_w = |g|_w|h|_w$ . Suppose  $w \mid p$  then

$$1 = |D_\alpha|_p = |D_\alpha|_w = |a_0|_w \prod_{j=1}^d \max\{1, |\alpha_j|_w\},$$

and therefore

$$\prod_{j=1}^d \prod_{w \nmid \infty} \max\{1, |\alpha_j|_w\}^{d_w} = \prod_{w \nmid \infty} |a_0|_w^{-d_w} = \prod_{p \in M_{\mathbb{Q}}} |a_0|_p^{-\sum_{w \mid p} d_w} = \prod_{p \in M_{\mathbb{Q}}} p^{\text{ord}_p(a_0)D} = a_0^D.$$

Combining all, and using Lemma 1.4 i), we find

$$\begin{aligned} H(\alpha)^{dD} &= \prod_{j=1}^d H(\alpha_j)^D = \left( \prod_{j=1}^d \prod_{w \nmid \infty} \max\{1, |\alpha_j|_w\}^{d_w} \right) \left( \prod_{j=1}^d \prod_{w \nmid \infty} \max\{1, |\alpha_j|_w\}^{d_w} \right) \\ &= \left( \prod_{i=1}^d \max\{1, |\alpha_i|\} \right)^D a_0^D. \end{aligned}$$

□

**Remark .** For  $f = \xi_0(x - \alpha_1) \cdots (x - \alpha_d) \in \mathbb{C}[x]$  the Mahler measure of  $f$  is defined as

$$M(f) = |\xi_0| \prod_{i=1}^d \max\{1, |\alpha_i|\}.$$

Note that  $M(\cdot)$  is multiplicative, i.e.,  $M(fg) = M(f)M(g)$ .

**Lemma 1.6.** *Suppose  $f = \xi_0 x^d + \dots + \xi_d \in \mathbb{C}[x]$ . Put  $|f| = \max\{|\xi_0|, \dots, |\xi_d|\}$ . Then*

$$2^{-d}|f| \leq M(f) \leq 2^{2d+1}|f|.$$

*Proof.* We start with the first inequality.

$$|\xi_i| = |\xi_0 \sum_{\substack{I \subset \{1, \dots, d\} \\ |I|=i}} \prod_{j \in I} \alpha_j| \leq \sum_{\substack{I \subset \{1, \dots, d\} \\ |I|=i}} |\xi_0| \prod_{j \in I} |\alpha_j| \leq \binom{d}{i} M(f) \leq 2^d M(f).$$

For the second inequality we factor  $f = PQ$  with  $P = \prod_{|\alpha_i| \leq 1} (x - \alpha_i)$  and  $Q = \xi_0 \prod_{|\alpha_i| > 1} (x - \alpha_i)$ . Note that by the maximum principle we have  $\|\varphi\|_r := \sup_{|x| \leq r} |\varphi(x)| = \sup_{|x|=r} |\varphi(x)|$  for any entire function  $\varphi : \mathbb{C} \rightarrow \mathbb{C}$ .

For  $|x| = 1/2$  and  $|\alpha_i| > 1$  we have  $|x - \alpha_i| \geq |\alpha_i| - 1/2 > (1/2)|\alpha_i|$ . Therefore

$$\|Q\|_{1/2} \geq 2^{-\deg Q} M(Q) = 2^{-\deg Q} M(f) \geq 2^{-d} M(f).$$

Now for  $|x| = 2$  and  $|\alpha_i| \leq 1$  we have  $|x - \alpha_i| \geq |x| - |\alpha_i| \geq 1$ . Therefore  $\inf_{|x|=2} |P(x)| \geq 1$ , and hence

$$\|Q\|_{1/2} \leq \|Q\|_2 \leq \frac{\|f\|_2}{\inf_{|x|=2} |P(x)|} \leq \|f\|_2 \leq 2^d |\xi_0| + \dots + 2^0 |\xi_d| \leq 2^{d+1} |f|.$$

Combining both estimates proves the lemma.  $\square$

The following theorem, proved by Northcott in [18], establishes the “guiding principle 2.”

**Theorem 1.7** (Northcott’s Theorem (1-dim)). *Sets of uniformly bounded height and degree are finite, i.e.,  $N(\mathbb{Q}(1; d), X) := |\{\alpha \in \overline{\mathbb{Q}}; [\mathbb{Q}(\alpha) : \mathbb{Q}] \leq d, H(\alpha) \leq X\}| < \infty$  for all  $d$  and all  $X$ .*

*Proof.* Each  $\alpha$  counted in  $N(\mathbb{Q}(1; d), X)$  has a minimal polynomial  $D_\alpha = a_0 x^e + \dots + a_e \in \mathbb{Z}[x]$  of degree at most  $d$ . Now  $H(\alpha) = M(D_\alpha)^{1/e} \leq X$ , and thus  $|D_\alpha| \leq 2^e M(D_\alpha) \leq (2X)^e$ . Hence we have at most  $(2(2X)^e + 1)^{e+1} \leq (5X)^{e(e+1)}$  possibilities for the minimal polynomials of degree  $e$ , and each of these has at most  $e$  distinct roots. Thus  $N(\mathbb{Q}(1; d), X) \leq \sum_{e=1}^d e(5X)^{e(e+1)} \leq (8X)^{d(d+1)}$ .  $\square$

Next we prove a simple consequence of Northcott’s Theorem.

**Theorem 1.8** (Kronecker’s Theorem).  $H(\alpha) = 1 \iff \alpha = 0$  or  $\alpha$  is a root of unity.

*Proof.* “ $\Leftarrow$ ”: clear.

“ $\Rightarrow$ ”: Recall that  $H(\alpha^n) = H(\alpha)^n = 1$  for all (positive) integers  $n$ . Moreover,  $[\mathbb{Q}(\alpha^n) : \mathbb{Q}] \leq [\mathbb{Q}(\alpha) : \mathbb{Q}]$ . By Northcott’s Theorem we conclude that  $\{\alpha^n; n \in \mathbb{Z}_{>0}\}$  is a finite set. Now the claim follows by the pigeon-hole principle.  $\square$

Northcott’s Theorem is very important and has many Diophantine applications. Therefore it would be interesting to establish generalizations and variations of Northcott’s Theorem. To this end we introduce the so-called Northcott property, which has been around for some while but was formally defined rather recently in [2].

**Definition** (Bombieri-Zannier 2001). *A subset  $\mathcal{A}$  of  $\overline{\mathbb{Q}}$  has the **Northcott property** (short property (N)) if  $|\{\alpha \in \mathcal{A}; H(\alpha) \leq X\}| < \infty$  for all  $X$ .*

So Northcott’s Theorem simply states that sets of uniformly bounded degree have the Northcott property. Let us now give a concrete example of a finiteness result using heights. Indeed, this example was Northcott’s original motivation to prove his theorem.

### 1.3.1 Arithmetic dynamics

Let  $\varphi : S \rightarrow S$  be a self map. For each point  $\alpha$  in  $S$  one has an orbit

$$O_\varphi(\alpha) = \{\alpha, \varphi(\alpha), \varphi(\varphi(\alpha)), \dots\}.$$

**Definition .** *A point  $\alpha \in S$  is preperiodic under  $\varphi \iff |O_\varphi(\alpha)| < \infty$*

The following basic problem is widely open.

**Problem 1.1** (Northcott, Dvornicich-Zannier 2008). *Suppose  $L \subset \overline{\mathbb{Q}}$  is a field,  $f : L \rightarrow L$  with  $f \in L[x]$  and  $\deg f > 1$ . Can one decide whether the number of preperiodic points in  $L$  under  $f$  is finite or infinite?*

**Theorem 1.9** (Northcott 1949). *Suppose  $f : S \rightarrow S$  with  $f \in \overline{\mathbb{Q}}[x]$  and  $\deg f > 1$ . And suppose  $S$  has the Northcott property. Then the number of preperiodic points in  $S$  under  $f$  is finite.*

*Proof.* We know that  $H(f(\alpha)) \geq c_f H(\alpha)^{\deg f}$  with some positive constant  $c_f \leq 1$ . Suppose  $H(\alpha) > c_f^{-2} \geq 1$ . Then  $H(f(\alpha)) \geq c_f H(\alpha)^{\deg f} \geq H(\alpha)^{3/2}$ . Therefore, writing  $f^{(n)}$  for the  $n$ -th iterate of  $f$ ,  $H(f^{(n)}(\alpha)) \geq H(\alpha)^{(3/2)^n} \rightarrow \infty$ . Therefore we have  $H(\alpha) \leq c_f^{-2}$  for any preperiodic point  $\alpha$ . As  $S$  has the property (N) the result follows.  $\square$

As an immediate consequence one gets an affirmative answer on Problem 1.1 for number fields.

**Corollary 1.10** (Northcott 1949). *Suppose  $L$  is a number field and  $f \in L[x]$  with  $\deg f > 1$ . Then the number of preperiodic points in  $L$  under  $f$  is finite.*

The upper bound obtained by the proof here, depends on  $c_f$  and on the degree of  $L$ . As we see from the proof of Lemma 1.4, the constant  $c_f$  depends not only on the degree but also on the coefficients of  $f$ . However, Morton and Silverman conjectured that there is a uniform bound depending only on the degrees.

**Conjecture 1.1** (Uniform boundedness conjecture (Morton-Silverman 1994)). *Suppose  $L$  is a number field and  $f \in L[x]$  with  $\deg f > 1$ . Then the number of preperiodic points in  $L$  under  $f$  is bounded from above solely in terms of  $\deg f$  and  $[L : \mathbb{Q}]$ .*

## 1.4 The height on $\overline{\mathbb{Q}}^n$

Let  $K$  be a number field,  $d = [K : \mathbb{Q}]$ .

Relative height on  $K^n$ :

$$H_K : K^n \rightarrow [1, \infty)$$

$$H_K(\alpha) = \prod_{v \in M_K} \max\{1, |\alpha_1|_v, \dots, |\alpha_n|_v\}^{d_v}.$$

The proof of Lemma 1.3 shows that

$$H_K(\alpha)^{1/d} = H_L(\alpha)^{1/D} \text{ for all } \alpha \in K^n \subset L^n.$$

Thus we can extend the definition of the absolute non-logarithmic Weil height to higher dimensions.

**Definition** (Absolute non-logarithmic Weil height).

$$H : \overline{\mathbb{Q}}^n \rightarrow [1, \infty)$$

$$H(\boldsymbol{\alpha}) = \prod_{v \in M_K} \max\{1, |\alpha_1|_v, \dots, |\alpha_n|_v\}^{d_v/d},$$

where  $K$  is any number field containing  $\alpha_1, \dots, \alpha_n$  and  $d = [K : \mathbb{Q}]$ .

Here is an example:

$\boldsymbol{\alpha} = (a_1/a_0, \dots, a_n/a_0) \in \mathbb{Q}^n$  with  $\gcd(a_0, \dots, a_n) = 1$ . Then

$$H(\boldsymbol{\alpha}) = \max\{|a_0|_\infty, \dots, |a_n|_\infty\}.$$

Note that

$$H(\boldsymbol{\alpha}) \geq \max\{H(\alpha_1), \dots, H(\alpha_n)\}.$$

Therefore Northcott's Theorem remains valid for  $\overline{\mathbb{Q}}^n$ .

**Theorem 1.11** (Northcott's Theorem). *Sets of uniformly bounded height and degree are finite. More precisely,  $N(\mathbb{Q}(n; d), X) := |\{\boldsymbol{\alpha} \in \overline{\mathbb{Q}}^n; [\mathbb{Q}(\boldsymbol{\alpha}) : \mathbb{Q}] \leq d, H(\boldsymbol{\alpha}) \leq X\}| \leq N(\mathbb{Q}(1; d), X)^n \leq (8X)^{nd(d+1)}$  for all  $d$  and all  $X$ .*

# Chapter 2

# Counting

## 2.1 Introduction

Suppose  $S \subset \overline{\mathbb{Q}}^n$  has uniformly bounded degree. By Northcott's Theorem we can associate a counting function to  $S$

$$N(S, X) = \{\alpha \in S; H(\alpha) \leq X\}.$$

Let  $k$  be a number field and

$$m = [k : \mathbb{Q}].$$

In view of Northcott's Theorem a natural set to study is

$$k(n; d) = \{\alpha \in \overline{\mathbb{Q}}^n; [k(\alpha) : k] \leq d\}.$$

**Problem 2.1** (Lang ( $d = 1$ ), Schmidt ( $d > 1$ )). *Find an asymptotic estimate for  $N(k(n; d), X)$  as  $X \rightarrow \infty$ .*

The Problem 2.1 has been solved for various cases.

**Theorem 2.1** (classical).

$$N(\mathbb{Q}(n; 1), X) = \frac{2^n}{\zeta(n+1)} X^{n+1} + O_n(X^n \mathcal{L}),$$

where  $\mathcal{L} = \log X$  if  $n = 1$  and  $\mathcal{L} = 1$  otherwise.

*Proof.* Let  $\alpha = (a_1/a_0, \dots, a_n/a_0)$  with  $\gcd(a_0, \dots, a_n) = 1$ . Then the representative  $\mathbf{a} = (a_0, \dots, a_n)$  is unique up to sign, and  $H(\alpha) = \max\{|a_0|_\infty, \dots, |a_n|_\infty\}$ .

Therefore

$$\begin{aligned} N(\mathbb{Q}(n; 1), X) &= \frac{1}{2} |\{\mathbf{a} \in \mathbb{Z}^{n+1} \cap [-X, X]^{n+1}; \gcd(a_0, \dots, a_n) = 1, a_0 \neq 0\}| \\ &= \frac{1}{2} |\underbrace{\{\mathbf{a} \in \mathbb{Z}^{n+1} \cap [-X, X]^{n+1}; \gcd(a_0, \dots, a_n) = 1\}}_{f_1(X)}| + O_n(X^n). \end{aligned}$$

To get rid of the primality condition we use the Möbius inversion formula. Let  $\mu : \mathbb{Z}_{>0} \rightarrow \{0, \pm 1\}$  be the Möbius function. It is multiplicative and defined by

$$\mu(a) = \begin{cases} 1 & : a = 1 \\ -1 & : a = \text{prime} \\ 0 & : a \text{ not square free.} \end{cases}$$

By the Möbius inversion formula we have

$$|f_1(X)| = \sum_d \mu(d) \sum_{\substack{b \\ d|b}} |f_b(X)|. \quad (2.1.1)$$

Note that

$$\begin{aligned} \sum_{\substack{b \\ d|b}} |f_b(X)| &= |(d\mathbb{Z})^{n+1} \setminus \{\mathbf{0}\} \cap [-X, X]^{n+1}| \\ &= \left(2 \left\lfloor \frac{X}{d} \right\rfloor + 1\right)^{n+1} - 1 = \left(\frac{2X}{d}\right)^{n+1} + O_n\left(\frac{X^n}{d^n}\right). \end{aligned} \quad (2.1.2)$$

For  $n > 1$  we can conclude

$$|f_1(X)| = \sum_d \mu(d) \left(\frac{2X}{d}\right)^{n+1} + O_n\left(\sum_d \frac{X^n}{d^n}\right).$$

But for  $n = 1$  the sum in the above error term does not converge. However, the right-hand side of (2.1.2) is certainly zero whenever  $d > X$ , and so we can restrict the sum in (2.1.1) to  $d \leq X$ . This yields

$$\begin{aligned} |f_1(X)| &= \sum_{d \leq X} \mu(d) \left(\frac{2X}{d}\right)^2 + O\left(\sum_{d \leq X} \frac{X}{d}\right) \\ &= \sum_d \mu(d) \left(\frac{2X}{d}\right)^2 + O\left(\sum_{d > X} \frac{X^2}{d^2}\right) + O\left(\sum_{d \leq X} \frac{X}{d}\right). \end{aligned}$$

The result drops out after noting that  $\sum_d \mu(d)/d^{n+1} = 1/\zeta(n+1)$ .  $\square$

Lang's problem has been solved by Schanuel in 1979. But before we state his theorem we introduce the Schanuel constant

$$S_k(n) = \frac{h_k R_k}{w_k \zeta_k(n+1)} \left( \frac{2^{r_k} (2\pi)^{s_k}}{\sqrt{|\Delta_k|}} \right)^{n+1} (n+1)^{r_k+s_k-1}. \quad (2.1.3)$$

Here  $h_k$  is the class number,  $R_k$  the regulator,  $w_k$  the number of roots of unity in  $k$ ,  $\zeta_k$  the Dedekind zeta-function of  $k$ ,  $\Delta_k$  the discriminant,  $r_k$  is the number of real embeddings of  $k$  and  $s_k$  is the number of pairs of distinct complex conjugate embeddings of  $k$ .

**Theorem 2.2** (Schanuel).

$$N(k(n; 1), X) = S_k(n) X^{m(n+1)} + O_{k,n}(X^{m(n+1)-1} \mathcal{L}), \quad (2.1.4)$$

where  $\mathcal{L} = \log X$  if  $n = m = 1$  and  $\mathcal{L} = 1$  otherwise.

*Proof.* Schanuel's original work is [20]. We give a fairly detailed sketch of the proof in Section 2.3.  $\square$

So far we have considered only the case  $d = 1$ . The case  $d > 1$  is more difficult. However, we already know that

$$N(\mathbb{Q}(n; d), X) \leq (8X)^{nd(d+1)}.$$

How good is this upper bound? The following lemma shows that at least for  $n = 1$  we have the correct exponent on  $X$ .

**Lemma 2.3.** For  $X \geq X_0(d)$  we have

$$N(\mathbb{Q}(1; d), X) \geq 2^{-d^2-3d-6} X^{d(d+1)}.$$

*Proof.* By Lemma 1.5 and Lemma 1.6 it suffices to count irreducible polynomials  $D = a_0 x^d + \dots + a_d \in \mathbb{Z}[x]$  with  $a_0 > 0$  and  $|D| \leq 2^{-2d-1} X^d = Y$ . For the irreducibility (over  $\mathbb{Q}$ ) we use the Eisenstein criterion with  $p = 2$ . So

$$a_0 = 2n_0 + 1, a_1 = 2n_1, \dots, a_{d-1} = 2n_{d-1}, a_d = 2(2n_d + 1).$$

We need also  $\gcd(a_0, \dots, a_d) = 1$ , and for this it suffices to have

$$\gcd(a_{d-1}/2, a_d/2) = 1.$$

Just as in the proof of Theorem 2.1 we see that the number of pairs  $(b_1, b_2)$  with coprime coordinates of modulus at most  $Y/2$  is  $Y^2/(2\zeta(2)) + O(Y \log Y) \geq$

$(Y/2)^2$  for  $Y \geq Y_0$ . Note that  $a_d/2$  is odd. However, any of the coprime pairs  $(b_1, b_2)$  with  $b_2$  odd gives us a pair  $(a_{d-1}/2, a_d/2)$ , and so we have at least

$$2^{-3}Y^2$$

possibilities for the pairs  $(a_{d-1}, a_d)$ , provided  $Y \geq Y_0$ . For the remaining coefficients  $a_0, \dots, a_{d-2}$  we have in total

$$[Y/2](2[Y/2] + 1)^{d-2} \geq 2^{-2}Y^{d-1}$$

possibilities, provided  $Y \geq Y_1$ . Thus for  $2^{-2d-1}X^d = Y \geq \max\{Y_0, Y_1\}$  we have at least  $2^{-5}Y^{d+1} = 2^{-d^2-3d-6}X^{d(d+1)}$  possibilities for the minimal polynomials  $D$ , and this proves the lemma.  $\square$

**Remark .** *Combining Schanuel's Theorem with Lemma 2.3 gives*

$$N(\mathbb{Q}(n; d), X) \geq c_{n,d}X^{d \max\{d+1, n+1\}},$$

*provided  $X \geq X_0(n, d)$ . It is known that the exponent  $d \max\{d+1, n+1\}$  is best possible.*

**Question 2.1.** *Does*

$$\lim_{X \rightarrow \infty} \frac{N(\mathbb{Q}(n; d), X)}{X^{d \max\{d+1, n+1\}}}$$

*exist and if so: what is it?*

For  $d = 1$  this, and much more, has been answered by Masser and Vaaler in [13] and [14].

**Theorem 2.4** (Masser-Vaaler 2007).

$$N(k(1; d), X) = dV_{\mathbb{R}}(d)^{r_k} V_{\mathbb{C}}(d)^{s_k} S_k(d) X^{md(d+1)} + O_{k,d}(X^{md(d+1)-d} \log X),$$

where

$$V_{\mathbb{R}}(d) = (d+1)^l \prod_{i=1}^l \frac{(2i)^{d-2i}}{(2i+1)^{d+1-2i}}$$

with  $l = [(d-1)/2]$  and the empty product is interpreted as 1, and

$$V_{\mathbb{C}}(d) = \frac{(d+1)^{d+1}}{((d+1)!)^2}.$$

*Proof.* We will sketch the proof. For a detailed account see [14].  $\square$

In particular,

$$\lim_{X \rightarrow \infty} \frac{N(\mathbb{Q}(1; d), X)}{X^{d(d+1)}} = dV_{\mathbb{R}}(d)S_{\mathbb{Q}}(d).$$

The latter is probably always a transcendental number, certainly if  $d$  is odd. On the other hand Masser and Vaaler observed

$$\lim_{X \rightarrow \infty} \frac{N(k(1; d), X^{1/d})}{N(k(d; 1), X)} = dV_{\mathbb{R}}(d)^{r_k} V_{\mathbb{C}}(d)^{s_k} \in \mathbb{Q}.$$

Therefore they asked (see [14]) if this extends to some “reciprocity law”.

**Question 2.2** (Masser-Vaaler 2007).

$$\lim_{X \rightarrow \infty} \frac{N(k(n; d), X^{1/d})}{N(k(d; n), X^{1/n})} \in \mathbb{Q}?$$

**Theorem 2.5** (Schmidt, Gao, W.). *Suppose that either  $k = \mathbb{Q}$  and  $n > d$  or that  $n > 5d/2 + 5$ . Then*

$$N(k(n; d), X) = \sum_{\substack{L \\ [L:k]=d}} S_L(d) X^{md(n+1)} + O_{k,d,n}(X^{md(n+1)-1}).$$

*Proof.* The cases  $(m, d) = (1, 2)$  are due to Schmidt [23] (in fact Schmidt handled also the cases  $n = 1, 2$ ). The cases  $m = 1, n > d$  were done by Gao [9], and the remaining cases are due to Widmer [27].  $\square$

**Remark .** *The best general bounds are due to Schmidt ([22]):*

$$c(k, n, d) X^{md \max\{d+1, n+1\}} \leq N(k(d; n), X) \leq C(n, m, d) X^{md(n+d)}. \quad (2.1.5)$$

*The upper bound holds for all  $X$  and the lower bound for  $X \geq X_0(k, n, d)$ . So in general the correct order of magnitude is not known.*

Analogous results to Schanuel’s Theorem and Theorem 2.5 for points on linear varieties have been proven by Thunder [25], and Christensen, Gubler [3] for  $d = 1$ , and by Widmer [30] for  $d \geq 1$ .

## 2.2 Counting lattice points

By a lattice in  $\mathbb{R}^n$  we mean the  $\mathbb{Z}$ -span of  $n$  linearly independent vectors  $v_1, \dots, v_n$  in  $\mathbb{R}^n$ . The determinant of the lattice is then given by the modulus of the determinant of the matrix whose columns are  $v_1, \dots, v_n$ . For a vector  $\mathbf{x}$  in  $\mathbb{R}^n$  we write  $|\mathbf{x}|$  for the Euclidean length of  $\mathbf{x}$ . For a point  $P$  in  $\mathbb{R}^n$  and a real  $R > 0$  we write  $B_P(R)$  for the closed Euclidean ball with radius  $R$  centered at  $P$ . The successive minima  $\lambda_1, \dots, \lambda_n$  of a lattice  $\Lambda$  in  $\mathbb{R}^n$  are understood in Minkowski's sense with respect to the unit ball  $B_0(1)$ , i.e., for  $i = 1, \dots, n$

$$\lambda_i = \inf\{\lambda; B_0(\lambda) \cap \Lambda \text{ contains } i \text{ linearly independent vectors}\}.$$

For general sets  $S$  one cannot say anything useful about  $|S \cap \Lambda|$ . Therefore  $S$  has to satisfy some conditions, e.g., its boundary must be "nice". To render this precise we introduce the following notion.

**Definition .** We say that a set  $A$  is in  $Lip(n, M, L)$  if  $A$  is a subset of  $\mathbb{R}^n$ , and if there are  $M$  maps  $\phi_1, \dots, \phi_M : [0, 1]^{n-1} \rightarrow \mathbb{R}^n$  satisfying a Lipschitz condition

$$|\phi_i(\mathbf{x}) - \phi_i(\mathbf{y})| \leq L|\mathbf{x} - \mathbf{y}| \text{ for } \mathbf{x}, \mathbf{y} \in [0, 1]^{n-1}, i = 1, \dots, M, \quad (2.2.6)$$

such that  $A$  is covered by the images of the maps  $\phi_i$ .

Any convex set has Lipschitz parameterizable boundary.

**Proposition 2.6.** Suppose  $S \subset B_P(R) \subset \mathbb{R}^n$  and  $S$  is convex. Then  $\partial S$  is in  $Lip(n, 1, 8n^{5/2}R)$ .

*Proof.* See [32] Theorem 2.6. □

Immediately from the previous proposition we get the following corollary.

**Corollary 2.7.** Suppose  $S \subset B_P(R) \subset \mathbb{R}^n$  and  $\partial S \subset (\cup_{i=1}^M \partial K_i)$  for convex sets  $K_1, \dots, K_M$ . Then  $\partial S$  lies in  $Lip(n, M, 8n^{5/2}R)$ .

The following counting theorem is more precise than the standard results (such as Theorem 2 in [12] or Theorem 5.1 in [11]) available in the literature. Firstly because it involves the first  $n-1$  successive minima, and secondly it is not restricted to homogeneously expanding domains. A simpler result, also not restricted to homogeneously expanding domains, was given by Masser and Vaaler in [14].

**Theorem 2.8.** *Let  $\Lambda$  be a lattice in  $\mathbb{R}^n$  with successive minima  $\lambda_1, \dots, \lambda_n$ . Let  $S$  be a bounded set in  $\mathbb{R}^n$  such that the boundary  $\partial S$  of  $S$  is in  $Lip(n, M, L)$ . Then  $S$  is measurable and moreover,*

$$\left| |S \cap \Lambda| - \frac{\text{Vol}(S)}{\det \Lambda} \right| \leq c_2(n)M \max_{0 \leq i < n} \frac{L^i}{\lambda_1 \cdots \lambda_i}.$$

For  $i = 0$  the expression in the maximum is to be understood as 1. Furthermore, one can choose  $c_2(n) = n^{3n^2/2}$ .

*Proof.* See [31] Theorem 5.4. □

From this we easily deduce the following special case for homogeneously expanding domains. The special feature here is that we can get rid of the annoying 1 in the error term, provided  $0 \notin S$ .

**Corollary 2.9.** *Let  $\Lambda$  be a lattice in  $\mathbb{R}^n$  with successive minima  $\lambda_1, \dots, \lambda_n$ . Let  $S_0$  be a set in  $\mathbb{R}^n$ , and suppose  $0 \notin S_0 \subset B_0(R)$  and  $\partial S_0 \in Lip(n, M, L_0)$ . Then  $S_0$  is measurable and moreover, for any  $t > 0$*

$$\left| |tS_0 \cap \Lambda| - \frac{\text{Vol}(S_0)t^n}{\det \Lambda} \right| \leq 2n^{3n^2/2}M(R + L_0)^{n-1} \left( \frac{t}{\lambda_1} \right)^{n-1}.$$

*Proof.* We distinguish two cases:

i)  $\lambda_1 > tR$ :

As  $0 \notin tS_0 \subset B_0(tR)$  we conclude  $|tS_0 \cap \Lambda| = 0$ . On the other hand, using Minkowski's second Theorem,

$$\frac{\text{Vol}(S_0)t^n}{\det \Lambda} \leq \frac{(2Rt)^n}{\lambda_1 \cdots \lambda_n} \leq 2^n \left( \frac{Rt}{\lambda_1} \right)^{n-1}.$$

ii)  $\lambda_1 \leq tR$ :

Clearly  $\partial tS_0 \in Lip(n, M, tL_0)$ . We apply Theorem 2.8 to deduce

$$\left| |tS_0 \cap \Lambda| - \frac{\text{Vol}(S_0)t^n}{\det \Lambda} \right| \leq n^{3n^2/2}M \max_{0 \leq i < n} \frac{(tL_0)^i}{\lambda_1 \cdots \lambda_i} \leq n^{3n^2/2}M(R + L_0)^{n-1} \left( \frac{t}{\lambda_1} \right)^{n-1}.$$

□

## 2.3 Proof sketch of Schanuel's Theorem

### 2.3.1 The strategy

Each  $\alpha \in k^n$  has a representative  $\mathbf{a} = (a_0, \dots, a_n)$ , i.e.,

- i)  $\mathbf{a} \in \mathcal{O}_k \setminus \{0\} \times \mathcal{O}_k^n := \mathcal{O}_n$
- ii)  $\alpha = \left(\frac{a_1}{a_0}, \dots, \frac{a_n}{a_0}\right)$ .

On  $\mathcal{O}_n$  we write  $\mathbf{a} \sim \mathbf{b}$  if  $\mathbf{a}$  and  $\mathbf{b}$  represent the same  $\alpha$  (i.e.  $a_i/a_0 = b_i/b_0$ ). Put

$$\mathcal{O}_{\mathbf{a}} = a_0\mathcal{O}_k + \dots + a_n\mathcal{O}_k.$$

Note that

$$\mathbf{a} \sim \mathbf{b} \implies \mathcal{O}_{\mathbf{a}} \sim \mathcal{O}_{\mathbf{b}},$$

i.e., if  $\mathbf{a}$  and  $\mathbf{b}$  are equivalent then  $\mathcal{O}_{\mathbf{a}}$  and  $\mathcal{O}_{\mathbf{b}}$  lie in the same ideal class.

Fix a nonzero ideal  $\mathfrak{C}$  and put

- $g_{\mathfrak{C}} = \{\mathbf{a} \in \mathcal{O}_n; \mathcal{O}_{\mathbf{a}} = \mathfrak{C}\}$
- $B(T) = \{\mathbf{a} \in \mathcal{O}_n; \prod_{v \in M_k} \max\{|a_0|_v, \dots, |a_n|_v\}^{d_v} \leq T^m\}$ .

Now for  $\mathbf{a}$  and  $\mathbf{b}$  in  $g_{\mathfrak{C}}$  we have

$$\mathbf{a} \sim \mathbf{b} \implies \mathbf{a} = \eta\mathbf{b} \text{ for some } \eta \in \mathcal{O}_k^*.$$

Let  $F \subset \mathcal{O}_k^{n+1}$  be a fundamental domain for the action  $(\eta, \mathbf{a}) \longrightarrow (\eta\mathbf{a})$  of  $\mathcal{O}_k^*$  on  $\mathcal{O}_k^{n+1}$ . Put

- $B_F(T) = B(T) \cap F$ ,
- $f_{\mathfrak{C}}(T) = g_{\mathfrak{C}} \cap B_F(T)$ .

Put  $f_{\mathfrak{C}}(\infty) = \bigcup_{T \geq 1} f_{\mathfrak{C}}(T)$ . Note: each  $\alpha \in k^n$  has exactly one representative  $\mathbf{a}$  in  $\bigcup_{\mathfrak{C} \in \mathcal{R}} f_{\mathfrak{C}}(\infty)$ , where the union runs over a full system  $\mathcal{R}$  of inequivalent ideals. Moreover, if  $\mathbf{a}$  lies in  $f_{\mathfrak{C}}(\infty)$  and represents  $\alpha$  then

$$H(\alpha) = \prod_v \max\{|a_0|_v, \dots, |a_n|_v\}^{d_v/m} = N\mathfrak{C}^{-1/m} \prod_{v|\infty} \max\{|a_0|_v, \dots, |a_n|_v\}^{d_v/m}.$$

Thus

$$H(\alpha) \leq X \iff \mathbf{a} \in f_{\mathfrak{e}}(N\mathfrak{e}^{1/m}X). \quad (2.3.7)$$

Therefore we have

$$N(k(n; 1), X) = \sum_{\mathfrak{e} \in \mathcal{R}} |f_{\mathfrak{e}}(N\mathfrak{e}^{1/m}X)|,$$

Using the Möbius function on nonzero ideals in  $\mathcal{O}_k$  and the Möbius inversion formula we get

$$|f_{\mathfrak{e}}(N\mathfrak{e}^{1/m}X)| = \sum_{\substack{\mathfrak{D} \\ \mathfrak{e}|\mathfrak{D}}} \mu(\mathfrak{e}^{-1}\mathfrak{D}) \underbrace{\sum_{\substack{\mathfrak{a} \\ \mathfrak{D}|\mathfrak{a}}} |f_{\mathfrak{a}}(N\mathfrak{e}^{1/m}X)|}_{|\mathfrak{D}^{n+1} \cap B_F(N\mathfrak{e}^{1/m}X)|}.$$

### 2.3.2 More details

We view  $\mathfrak{D} \subset \mathcal{O}_k \subset k$  as subsets of  $\mathbb{R}^r \times \mathbb{C}^s = \mathbb{R}^m$  via the embeddings  $\sigma_1, \dots, \sigma_r : k \rightarrow \mathbb{R}$ , and  $\sigma_{r+1}, \dots, \sigma_{r+s} : k \rightarrow \mathbb{C}$ . Extending each of these componentwise we get an embedding

$$\begin{aligned} \sigma : k^{n+1} &\longrightarrow \mathbb{R}^{r(n+1)} \times \mathbb{C}^{s(n+1)} \\ \sigma(\alpha) &= (\sigma_1(\alpha), \dots, \sigma_{r+s}(\alpha)) \end{aligned}$$

Now  $\sigma\mathfrak{D}^{n+1}$  is a lattice in  $\mathbb{R}^{m(n+1)}$  with

$$\det \sigma\mathfrak{D}^{n+1} = \left(2^{-s} \sqrt{|\Delta_k|} N\mathfrak{D}\right)^{n+1}.$$

Next we define two maps:

$$\begin{aligned} p : k^* &\longrightarrow \mathbb{R}_{>0}^{r+s} & \ell : \mathbb{R}_{>0}^{r+s} &\longrightarrow \mathbb{R}^{r+s} \\ p(\alpha) &= (|\sigma_i(\alpha)|)_{i=1}^{r+s} & \ell((x_i)_{i=1}^{r+s}) &= (d_i \log x_i)_{i=1}^{r+s}, \end{aligned}$$

where  $d_i = 1$  if  $i \leq r$  and  $d_i = 2$  if  $i > r$ . Let  $\Sigma \subset \mathbb{R}^{r+s}$  be the subspace defined by  $x_1 + \dots + x_{r+s} = 0$ . Then  $\ell \circ p : \mathcal{O}_k^* \rightarrow \Sigma$  is a group homomorphism with kernel  $T_k = \{\text{roots of unity in } k\}$ , and image a lattice in  $\Sigma$ . Let  $F \subset \Sigma$  be a fundamental domain for the action of  $\ell \circ p(\mathcal{O}_k^*)$  on  $\Sigma$ , and define the vector sum

$$F(T) = F + \delta(-\infty, \log T],$$

where  $\delta = (d_i)_{i=1}^{r+s}$ . Next put  $E_n = (\mathbb{R}^* \times \mathbb{R}^n)^r \times (\mathbb{C}^* \times \mathbb{C}^n)^s$ , and write temporarily  $|\cdot|$  for the supremum norm on  $\mathbb{C}^{n+1}$ . We define

$$\begin{aligned} S_F(T) &= \{(\mathbf{z}_1, \dots, \mathbf{z}_{r+s}) \in E_n; \ell((|\mathbf{z}_i|)_{i=1}^{r+s}) \in F(T)\}, \\ &= \underbrace{S_F(\infty)}_{\text{"F"}} \cap \underbrace{\{(\mathbf{z}_1, \dots, \mathbf{z}_{r+s}) \in E_n; \prod_{i=1}^{r+s} |\mathbf{z}_i|^{d_i} \leq T^m\}}_{\text{"B(T)"}}. \end{aligned}$$

Note that

$$\ell((|T\mathbf{z}_i|)_{i=1}^{r+s}) = \delta \log T + \ell((|\mathbf{z}_i|)_{i=1}^{r+s}).$$

Hence

$$S_F(T) = TS_F(1).$$

Moreover,

$$\ell((|\sigma_i(\eta\mathbf{a})|)_{i=1}^{r+s}) = \ell \circ p(\eta) + \ell((|\sigma_i(\mathbf{a})|)_{i=1}^{r+s}).$$

Thus for each  $\mathbf{a} \in \mathcal{O}_k^{n+1} \setminus \{\mathbf{0}\}$  there exist exactly  $\omega_k = |T_k|$  units  $\eta$  such that  $\sigma(\eta\mathbf{a}) \in S_F(\infty)$ , and so

$$|f_{\mathfrak{C}}(T)| = \frac{1}{\omega_k} |S_F(T) \cap \sigma g_{\mathfrak{C}}| = \frac{1}{\omega_k} \sum_{\substack{\mathfrak{D} \\ \mathfrak{C}|\mathfrak{D}}} \mu(\mathfrak{C}^{-1}\mathfrak{D}) |\sigma \mathfrak{D}^{n+1} \cap S_F(T)|.$$

**Lemma 2.10.** *Let  $\mathfrak{D}$  be a nonzero ideal in  $\mathcal{O}_k$ . Then  $\lambda_1(\sigma \mathfrak{D}^{n+1}) \geq \sqrt{\frac{m}{2}} N \mathfrak{D}^{1/m}$ .*

*Proof.* Let  $\alpha$  be a nonzero element of  $\mathfrak{D}$ . It suffices to consider the Euclidean length of  $(\sigma_1\alpha, \dots, \sigma_{r+s}\alpha)$ . The latter is

$$\begin{aligned} \left( \sum_{i=1}^{r+s} |\sigma_i\alpha|^2 \right)^{1/2} &\geq \left( \frac{1}{2} \sum_{i=1}^{r+s} d_i |\sigma_i\alpha|^2 \right)^{1/2} \geq \sqrt{\frac{m}{2}} \left( \prod_{i=1}^{r+s} |\sigma_i\alpha|^{2d_i} \right)^{1/(2m)} \\ &= \sqrt{\frac{m}{2}} N((\alpha))^{1/m} \geq \sqrt{\frac{m}{2}} N \mathfrak{D}^{1/m}. \end{aligned}$$

□

**Lemma 2.11.** *There exist constants  $M = M(n, k)$ ,  $L = L(n, k, F)$ , and  $R = R(n, k, F)$  such that  $S_F(1) \subset B_0(R)$  and  $\partial S_F(1) \in \text{Lip}(m(n+1), M, L)$ .*

## 2.4. PROOF STRATEGIES FOR THEOREM 2.4 AND THEOREM 2.527

*Proof.* Not difficult but somewhat tedious.  $\square$

**Lemma 2.12.**

$$|\sigma\mathfrak{D}^{n+1} \cap S_F(T)| = \frac{\text{Vol } S_F(1)T^{m(n+1)}}{\left(2^{-s}\sqrt{|\Delta_k|}N\mathfrak{D}\right)^{n+1}} + O_{n,k,F}\left(\frac{T^{m(n+1)-1}}{N\mathfrak{D}^{n+1-1/m}}\right).$$

*Proof.* As  $0 \notin S_F(T)$  this follows immediately from Lemma 2.10, Lemma 2.11 and Corollary 2.9.  $\square$

Now

$$|f_{\mathfrak{C}}(T)| = \frac{1}{\omega_k} \sum_{\mathfrak{B}} \mu(\mathfrak{B}) |\sigma(\mathfrak{B}\mathfrak{C})^{n+1} \cap S_F(T)|,$$

and with Lemma 2.12 and  $T = XN\mathfrak{C}^{1/m}$  Schanuel's Theorem follows after summing over  $\mathcal{R}$ .

## 2.4 Proof strategies for Theorem 2.4 and Theorem 2.5

### 2.4.1 Theorem 2.4

The basic idea is to count monic minimal polynomials over  $k$ , and to adapt Schanuel's proof to carry this out. For simplicity we assume  $k = \mathbb{Q}$ .

It suffices to count numbers  $\alpha$  of degree  $d > 1$ . We count monic irreducible polynomials  $D = x^d + (a_1/a_0)x^{d-1} + \dots + (a_d/a_0) \in \mathbb{Q}[x]$  with  $\gcd(a_0, \dots, a_d) = 1$  and  $a_0 > 0$ . Suppose  $\alpha$  is a root of  $D$ . Then

$$\begin{aligned} H(\alpha)^d &= a_0 \prod_{i=1}^d \max\{1, |\alpha_i|\} \\ &= \left( \prod_p \max\left\{1, \left|\frac{a_1}{a_0}\right|_p, \dots, \left|\frac{a_d}{a_0}\right|_p\right\} \right) M\left(x^d + \frac{a_1}{a_0}x^{d-1} + \dots + \frac{a_d}{a_0}\right) \\ &:= H_M\left(\frac{a_1}{a_0}, \dots, \frac{a_d}{a_0}\right) \end{aligned}$$

Now  $H_M : \mathbb{Q}^d \rightarrow [1, \infty)$  can be seen as a height function, and at the same time as a function  $M_0$  on monic polynomials of degree at most  $d$

defined by  $H_M\left(\frac{a_1}{a_0}, \dots, \frac{a_d}{a_0}\right) = M_0\left(x^d + \frac{a_1}{a_0}x^{d-1} + \dots + \frac{a_d}{a_0}\right)$ . Note that  $M_0$  is multiplicative, i.e.,  $M_0(fg) = M_0(f)M_0(g)$ . Adapting Schanuel's proof to this modified height  $H_M$  we get for the number of monic polynomials  $f$  of degree at most  $d$  with  $M_0(f) \leq X^d$

$$S_d(X^d)^{d+1} + O(X^{d^2}). \quad (2.4.8)$$

This implies that the number of such polynomials of degree  $< d$  is at most  $C_1 X^{d(d-1)}$  for some constant  $C_1$ . And using (2.4.8) together with the multiplicativity of  $M_0$  we see that the number of reducible polynomials counted in (2.4.8) is at most  $C_2 X^{d^2} \log(X+2)$ . As each  $D$  has exactly  $d$  pairwise distinct roots of equal height we conclude

$$N(\mathbb{Q}(1; d), X) = dS_d X^{d(d+1)} + O(X^{d^2} \log X).$$

### 2.4.2 Theorem 2.5

The strategy here is to prove a version of Schanuel's Theorem restricted to primitive points  $\alpha$ , i.e., fix an extension  $L/k$  of degree  $d$ , and then count the points  $\alpha \in L^n$  with  $k(\alpha) = L$ . Then sum over all possible extensions  $L$ .

Put  $(L/k)^n = \{\alpha \in L^n; k(\alpha) = L\}$ . Then we have the disjoint union

$$k(n; d) = \bigcup_{\substack{L \\ [L:k]=d}} (L/k)^n,$$

and thus

$$N(k(n; d), X) = \sum_{\substack{L \\ [L:k]=d}} N((L/k)^n, X).$$

The main goal is to show

$$N((L/k)^n, X) = S_L(n)X^{md(n+1)} + O_{k,n,d}(c_L(n)X^{md(n+1)-1}),$$

so that for  $n$  large enough

$$\sum_{\substack{L \\ [L:k]=d}} S_L(n), \quad \sum_{\substack{L \\ [L:k]=d}} c_L(n)$$

converge. Of course the more difficult part is the convergence of the error terms.

**Remark .** *This is a simplification of the strategy. In fact the error term for each  $L$  splits up in a bunch of terms and each of those has to be summed over a different set of fields  $L$ . Moreover, naively following Schanuel's proof yields a value for  $c_L(n)$  of size about  $\exp(\sqrt{|\Delta_L|}md(n+1) - 1)$  which is extremely far away from what we need.*

## 2.5 Integral points

Let  $\mathbb{Z}_{\overline{\mathbb{Q}}}$  be the ring of algebraic integers and let  $k$  be a number field of degree  $m = [k : \mathbb{Q}]$ , and write  $\mathcal{O}_k$  for its ring of integers. In this section we are interested in problems analogous to those of Section 2.1 but this time for integral points. We define

$$\mathcal{O}_k(n; d) = \{\alpha \in \mathbb{Z}_{\overline{\mathbb{Q}}}^n; [k(\alpha) : k] \leq d\}.$$

**Problem 2.2.** *Find an asymptotic estimate for  $N(\mathcal{O}_k(n; d), X)$  as  $X \rightarrow \infty$ .*

For  $k = \mathbb{Q}$  and  $d = 1$  the problem is trivial. The following result has been stated without proof in [11] p.80.

**Theorem 2.13** (Lang).

$$N(\mathcal{O}_k(1; 1), X) = \gamma_k X^m \log X^{q_k} + O_k(X^m (\log X)^{q_k-1}),$$

where  $\gamma_k$  is a positive constant depending on  $k$ , and  $q_k$  is the rank of the unit group of  $\mathcal{O}_k$ .

**Question 2.3.** *Can one improve the error term? Can one find a second, third, ... order main term?*

Indeed, we can expand the counting function in  $q_k + 1$  main terms. For  $0 \leq i \leq q_k$  we set

$$C_i(k, n) = \frac{2^{r_k n} (2\pi)^{s_k n} n^i}{|\Delta_k|^{n/2} i!} \binom{q_k}{i},$$

We have

$$N(\mathcal{O}_k(n; 1), X) = \sum_{i=0}^{q_k} C_i(k, n) X^{mn} (\log X^m)^i + O_{m,n}(X^{mn-1} (\log X)^{q_k}). \quad (2.5.9)$$

The main term can be written in a simpler form using the  $q$ -th Laguerre polynomial  $L_q(t) = \sum_{i=0}^q (-1)^i \binom{q}{i} \frac{t^i}{i!}$ . With this notation we have

$$\sum_{i=0}^{q_k} C_i(k, n) X^{mn} (\log X^m)^i = \frac{2^{r_k n} (2\pi)^{s_k n} X^{mn}}{|\Delta_k|^{n/2}} L_{q_k}(-n \log X^m).$$

The latter is a very special case of the following result, proved in the upcoming article [33]. But first we need some more notation. Let  $\mathcal{C}_d(k)$  be the collection of all field extensions of  $k$  of degree  $d$ , i.e.,

$$\mathcal{C}_d(k) = \{L \subset \overline{\mathbb{Q}}; [L : k] = d\},$$

and set

$$t_d(k) = \sup\{q_L; L \in \mathcal{C}_d(k)\}.$$

For  $0 \leq i \leq t_d(k)$  we introduce the formal sum

$$D_i = D_i(k, n, d) = \sum_{\substack{L \in \mathcal{C}_d(k) \\ q_L \geq i}} C_i(L, n). \quad (2.5.10)$$

Next we put for  $d > 1$

$$2' = \max\left\{2 + \frac{4}{d-1} + \frac{1}{m(d-1)}, 7 - \frac{d}{2} + \frac{2}{md}\right\} \leq 7.$$

Now we can state the result.

**Theorem 2.14** (W. 2010). *Let  $k$  be a number field with  $m = [k : \mathbb{Q}]$ . Suppose that either  $d = 1$  or that  $n > d + 2'$ , and set  $t = t_d(k)$ . Then the sum in (2.5.10) converges and, as  $X \geq 1$  tends to infinity, one has*

$$N(\mathcal{O}_k(n; d), X) = \sum_{i=0}^t D_i X^{mdn} (\log X^{md})^i + O_{n,m,d}(X^{mdn-1} (\log X)^t).$$

*Proof.* We illustrate the proof of the much simpler special case  $d = 1$  for  $(r_k, s_k, n) = (2, 0, 1)$  on the blackboard. The complete proof is given in [33].  $\square$

## 2.6 Proof sketch Theorem 2.13 for $d = 1$

The restriction to  $d = 1$  is significant and simplifies the proof considerably. We also assume  $n = 1$ , this is not so serious but simplifies the notation.

Let  $\sigma_i : k \rightarrow \mathbb{C}$  ( $1 \leq i \leq m$ ) be the embeddings ordered as usual ( $\sigma_{r+j+s} = \overline{\sigma_{r+j}}$  for  $1 \leq j \leq s$ ). Now for  $\alpha$  in  $\mathcal{O}_k$  we have

$$H(\alpha) = \prod_{v \in M_k} \max\{1, |\alpha|_v\}^{d_v/m} = \prod_{v|\infty} \max\{1, |\alpha|_v\}^{d_v/m} = \prod_{i=1}^{r+s} \max\{1, |\sigma_i(\alpha)|\}^{d_i/m},$$

where  $d_i = 1$  if  $i \leq r$  and  $d_i = 2$  if  $i > r$ . As in the proof of Schanuel's Theorem we use the embedding

$$\begin{aligned} \sigma : k &\rightarrow \mathbb{R}^r \times \mathbb{C}^s, \\ \sigma(\alpha) &= (\sigma_1(\alpha), \dots, \sigma_{r+s}(\alpha)). \end{aligned}$$

Put

$$S(X) = \{\mathbf{z} \in \mathbb{R}^r \times \mathbb{C}^s; \prod_{i=1}^{r+s} \max\{1, |z_i|\} \leq X^m\}.$$

Thus

$$N(\mathcal{O}_k(1, 1), X) = N(\mathcal{O}_k, X) = |\sigma(\mathcal{O}_k) \cap S(X)|.$$

So we could try to apply Theorem 2.8. However, the problem is that  $S(X)$  is "long and thin" with "small" volume. If one parameterizes the boundary by a single map (i.e.,  $\partial S \in \text{Lip}(m, 1, L)$ ) then  $L$  has order at least  $X^m$  giving an error term of order  $X^{m(m-1)}$ . But the volume, and thus the main term, is only of order  $X^m(\log X)^{q_k}$ .

The first step to overcome these difficulties is to split up the set  $S(X)$  in several subsets. For  $I \subset \{1, \dots, r+s\}$  put

$$S_I(X) = \{\mathbf{z} \in S(X); |z_i| \geq 1 \quad \forall i \in I \\ |z_i| < 1 \quad \forall i \notin I\}.$$

**Definition .** Let  $\mathcal{T}$  be the group of  $\mathbb{R}$ -linear maps  $\phi : \mathbb{R}^r \times \mathbb{C}^s \rightarrow \mathbb{R}^r \times \mathbb{C}^s$  of the form  $\phi(\mathbf{z}) = (\xi_i z_i)_{i=1}^{r+s}$  with  $\xi_i > 0$  and  $\prod_{i=1}^{r+s} \xi_i^{d_i} = 1$ .

Theorem 2.14 for  $n = d = 1$  follows easily from the following proposition.

**Proposition 2.15.** *Suppose  $\emptyset \neq I \subset \{1, \dots, r + s\}$  and  $\Lambda$  is a lattice in  $\mathbb{R}^r \times \mathbb{C}^s$ . Suppose there exists  $\mu > 0$  such that  $\lambda_1(\phi(\Lambda)) \geq \mu$  for all  $\phi \in \mathcal{T}$ . Then for all  $X \geq 0$*

$$\left| |\Lambda \cap S_I(X)| - \frac{\text{Vol } S_I(X)}{\det \Lambda} \right| \leq C_m \left( \frac{X}{\mu} \right)^{m-1} (\log(X + 2))^{|I|-1}.$$

*Proof.* We will illustrate the proof in the simplest nontrivial case  $r = 2, s = 0$  on the blackboard.  $\square$

**Lemma 2.16.** *Let  $\mathfrak{D}$  be a nonzero ideal in  $\mathcal{O}_k$  and  $\phi \in \mathcal{T}$ . Then  $\lambda_1(\phi(\sigma\mathfrak{D})) \geq \sqrt{m/2} N\mathfrak{D}^{1/m}$ .*

*Proof.* This is proved exactly in the same way as Lemma 2.10.  $\square$

Next note that

$$N(\mathcal{O}_k, X) = |\sigma(\mathcal{O}_k) \cap S(X)| = \sum_I |\sigma(\mathcal{O}_k) \cap S_I(X)|,$$

where the sum runs over all subsets  $I$  of  $\{1, \dots, r + s\}$ . For  $I = \emptyset$  and  $X \geq 1$  we have  $|\sigma(\mathcal{O}_k) \cap S(X)| = 1$ , and if  $I \neq \emptyset$  then we can apply Proposition 2.15 with  $\Lambda = \sigma\mathcal{O}_k$  and  $\mu = \sqrt{m/2}$ .

## Chapter 3

# Height bounds for primitive points

### 3.1 Introduction

Let  $L/k$  be a finite extension of number fields,  $m = [k : \mathbb{Q}]$ ,  $d = [L : k]$ , and  $D = md = [L : \mathbb{Q}]$ . Let  $D_{L/k}$  be the relative discriminant of  $L/k$ . Moreover we introduce the following invariant of  $L/k$

$$\delta(L/k) = \inf\{H(\alpha); L = k(\alpha)\}.$$

**Problem 3.1.** *Find good lower and upper bounds for  $\delta(L/k)$  in terms of  $N_{k/\mathbb{Q}}(D_{L/k})$ ,  $d$ , and  $m$ .*

Silverman gave a nice lower bound.

**Theorem 3.1** (Silverman 1984). *Suppose  $d > 1$ . Then*

$$\delta(L/k) \geq d^{-\frac{1}{2(d-1)}} N_{k/\mathbb{Q}}(D_{L/k})^{\frac{1}{2md(d-1)}}, \quad (3.1.1)$$

where  $N_{k/\mathbb{Q}}$  is the norm from  $k$  to  $\mathbb{Q}$ .

*Proof.* The proof is not difficult and uses essentially only the triangle inequality and Hadamard's inequality. However, we omit the proof. It can be found (as a special case) in [24].  $\square$

Silverman's Theorem has many applications; it is used in the proof of Theorem 2.5, Theorem 2.14, and it will also play a crucial role in Chapter 4. We also briefly sketch an application to the torsion part of class groups,

discovered by Ellenberg and Venkatesh.

In view of the many applications it would be nice to improve upon the exponent  $1/2md(d-1)$  in Silverman's Theorem. Unfortunately this exponent is best possible, as the following example due to Masser and Ruppert shows: take  $L = k(\alpha)$  with  $\alpha = (p/q)^{1/d}$  and primes  $p, q$  satisfying  $0 < p < q < 2p$  and  $p, q \nmid \Delta_k$ . So  $D_\alpha = qx^d - p$  is irreducible over  $k$  and  $[k(\alpha) : k] = d$ . Now  $(pq)^{d-1} \mid \Delta_{\mathbb{Q}(\alpha)}$ , and  $\Delta_{\mathbb{Q}(\alpha)}^m \mid \Delta_L = \Delta_k^d N_{k/\mathbb{Q}}(D_{L/k})$ . Hence

$$H(\alpha) = q^{\frac{1}{d}} \leq (2pq)^{\frac{1}{2d}} \leq 2^{\frac{1}{2d}} |\Delta_L|^{\frac{1}{2md(d-1)}} = 2^{\frac{1}{2d}} |\Delta_k|^{\frac{1}{2m(d-1)}} N_{k/\mathbb{Q}}(D_{L/k})^{\frac{1}{2md(d-1)}}$$

By the prime number theorem (or Bertrand's postulate) we can take  $p$  arbitrarily large. And this shows the claim.

For  $k = \mathbb{Q}$  Silverman's Theorem gives

$$\delta(L/\mathbb{Q}) \geq D^{-\frac{1}{2(D-1)}} |\Delta_L|^{\frac{1}{2D(D-1)}}.$$

We just saw that the right hand-side is essentially sharp. Ruppert ([19] Question 1) asked whether it is always possible to find such a small generator.

**Question 3.1** (Ruppert 1998). *Is there a constant  $C_D$  such that for all number fields  $L$  of degree  $D$*

$$\delta(L/\mathbb{Q}) \leq C_D |\Delta_L|^{\frac{1}{2D(D-1)}}?$$

For  $D = 2$  Ruppert answered this question in the affirmative. The proof is not easy and depends on a deep result of Duke. Moreover, the constant  $C_D$  he obtained is ineffective.

## 3.2 Bounds for the torsion part of class groups

Let  $Cl_L$  be the class group of the number field  $L$  and for a positive integer  $l$  write  $Cl_L[l] = \{a \in Cl_L; a^l = 1\}$  for its  $l$ -torsion part.

**Conjecture 3.1** (Brumer, Duke, Silverman, Zhang,...). *Suppose  $l > 0$  is prime and  $\epsilon > 0$ . Then there exists a constant  $C(\epsilon, l, D)$  such that for all number fields  $L$  of degree  $D$*

$$|Cl_L[l]| \leq C(\epsilon, l, D) |\Delta_L|^\epsilon.$$

Note that the trivial bound, using ‘‘Siegel-Brauer’’, has the exponent  $1/2 + \epsilon$  on  $|\Delta_L|$ . In [7] Ellenberg and Venkatesh obtained the first general nontrivial result. They have shown (see also [5]) that, under GRH one has

$$|Cl_L[l]| \leq C(\epsilon, l, D) |\Delta_L|^{\frac{1}{2} + \epsilon} \delta(L/\mathbb{Q})^{-\frac{D}{l} + \epsilon}.$$

Applying Silverman’s Theorem yields a nontrivial bound.

**Theorem 3.2** (Ellenberg-Venkatesh 2008). *Suppose  $l > 0$  is prime and  $\epsilon > 0$ . Assume GRH holds. Then there exists a constant  $C(\epsilon, l, D)$  such that for all number fields  $L$  of degree  $D$*

$$|Cl_L[l]| \leq C(\epsilon, l, D) |\Delta_L|^{\frac{1}{2} - \frac{1}{2(D-1)l} + \epsilon}.$$

For  $(l, D) = (3, 2)$  the result is unconditional.

Here GRH is needed to guarantee the existence of many small splitting primes. For  $(l, D) = (3, 2)$  they used that either  $\mathbb{Q}(\sqrt{m})$  or  $\mathbb{Q}(\sqrt{-3m})$  has many small splitting primes so that the torsion bound can be deduced for at least one of these fields. Applying the Scholz’ reflection principle gives the conclusion for the other field, and thus the result is unconditional.

Motivated by this particular application, and inspired by a geometric result of Arbarello and Cornalba, Ellenberg implicitly addressed the following question (see [5] p.4).

**Question 3.2** (Ellenberg 2009). *Is there a constant  $C_D$  such that for a ‘‘typical’’ number field  $L$  of degree  $D$*

$$\delta(L/\mathbb{Q}) \geq C_D |\Delta_L|^{\frac{1}{4D}}?$$

### 3.3 More results

We put

$$\mathcal{C} = \mathcal{C}_D(\mathbb{Q}) = \{L \subset \overline{\mathbb{Q}} : [L : \mathbb{Q}] = D\}.$$

and for a subset  $S \subset \mathcal{C}$ , and  $\eta \geq 0$  we set

$$S_\eta = \{L \in S : \delta(L/\mathbb{Q}) \geq |\Delta_L|^\eta\}.$$

To render Question 3.2 precise we enumerate the fields. This is done, probably most naturally, by the discriminant or the modulus thereof

$$N_\Delta(S, T) = |\{L \in S : |\Delta_L| \leq T\}|.$$

**Proposition 3.3** (Vaaler-W. 2009). *Suppose  $2 \mid D$  or  $3 \mid D$ . Then*

$$\lim_{T \rightarrow \infty} \frac{N_{\Delta}(\mathcal{C}_{\eta}, T)}{N_{\Delta}(\mathcal{C}, T)} = 1,$$

*provided  $\eta < \frac{1}{D(D+1)}$ .*

*Moreover, suppose  $F$  is number field of degree  $D/2$  if  $D$  is even and of degree  $D/3$  otherwise. Put  $B = \{L \in \mathcal{C}; F \subset L\}$ . Then*

$$\lim_{T \rightarrow \infty} \frac{N_{\Delta}(B_{\eta}, T)}{N_{\Delta}(B, T)} = 1,$$

*provided  $\eta < \frac{1}{D(1+D/[F:\mathbb{Q}])}$ .*

*Proof.* For  $S \subset \mathcal{C}$  we set  $P_S = \{\alpha \in \overline{\mathbb{Q}}; \mathbb{Q}(\alpha) \in S\}$  and  $N_{\delta}(S, T) = |\{L \in S : \delta(L/\mathbb{Q}) \leq T\}|$ . Directly from the definitions we get

$$N_{\Delta}(S \setminus S_{\eta}, T) \leq N_{\delta}(S \setminus S_{\eta}, T^{\eta}) \leq N_{\delta}(S, T^{\eta}),$$

and

$$N_{\delta}(S, T^{\eta}) \leq N(P_S, T^{\eta}).$$

By Schmidt's bound (2.1.5)

$$N(P_S, T^{\eta}) \leq \begin{cases} C_D T^{\eta D(D+1)} & : S = \mathcal{C}, \\ C_D T^{\eta D(1 + \frac{D}{[F:\mathbb{Q}]})} & : S = B. \end{cases}$$

On the other hand, counting only quadratic (or cubic) extensions of  $F$  of bounded discriminant, we get

$$N_{\Delta}(\mathcal{C}, T) \geq N_{\Delta}(B, T) \geq c_F T,$$

provided  $T \geq T_0(F)$ . With  $S = \mathcal{C}$  or  $S = B$  and the hypothesis of the proposition we conclude

$$\lim_{T \rightarrow \infty} \frac{N_{\Delta}(S \setminus S_{\eta}, T)}{N_{\Delta}(S, T)} = 0.$$

□

**Remark .** *So if  $D$  is even than a “typical” degree  $D$  field  $L$  has  $\delta(L/\mathbb{Q}) \geq |\Delta_L|^{\eta}$  whenever  $\eta > \frac{1}{D(D+1)}$ .*

*If  $D$  is even than a “typical” degree  $D$  field  $L$  of  $B$  has  $\delta(L/\mathbb{Q}) \geq |\Delta_L|^{\eta}$  whenever  $\eta > \frac{1}{3D}$ .*

*Suppose  $D = ab$  is composite and  $F$  is a field of degree  $b$ . The best general lower bound  $N_{\Delta}(B, T) \geq c(F, a)T^{1/2+1/a^2}$  is due to Ellenberg and Venkatesh [6] and suffices to answer Question 3.1 in the negative if  $D$  is composite.*

Recall that for  $D = 2$  Ruppert has positively answered his Question 3.1. For  $D = 2$  one has  $1/(2D(D - 1)) = 1/(2D)$ , and so in general the best exponent might be  $1/(2D)$ . Indeed, Ruppert ([19] Question 2) also addressed the following question.

**Question 3.3** (Ruppert 1998). *Is there a constant  $C_D$  such that for all number fields  $L$  of degree  $D$*

$$\delta(L/\mathbb{Q}) \leq C_D |\Delta_L|^{\frac{1}{2D}}?$$

The answer to this question is probably yes.

**Proposition 3.4** (Vaaler-W. 2009). *Suppose  $L$  has a real embedding or assume GRH. Then*

$$\delta(L/\mathbb{Q}) \leq C_D |\Delta_L|^{\frac{1}{2D}},$$

with a constant  $C_D$  depending only on  $D$ .

*Proof.* If  $L$  has a real embedding then one can apply Minkowski's convex body theorem to get a Pisot number generator of small enough height. The general case follows the proof of Theorem 1.1 in [29]. For details see [26].  $\square$

### 3.4 Numerical data

Let us look at some numerical data. We consider the quantity<sup>1</sup>

$$\frac{\log \delta(L/\mathbb{Q})}{\log |\Delta_L|}$$

as  $L$  runs over all number fields of degree  $D$ . What are the cluster points of this sequence? We already know that  $1/(2D(D - 1))$  is the smallest cluster point. The data material of the following figures stems from John Voight's tables on his webpage (<http://www.cems.uvm.edu/~voight/nf-tables/index.html>)

---

<sup>1</sup>In fact we use rather the quantity  $\inf\{|D_\alpha|^{1/\deg D_\alpha}; L = \mathbb{Q}(\alpha)\}$  instead of  $\delta(L/\mathbb{Q})$  but that doesn't change the cluster points

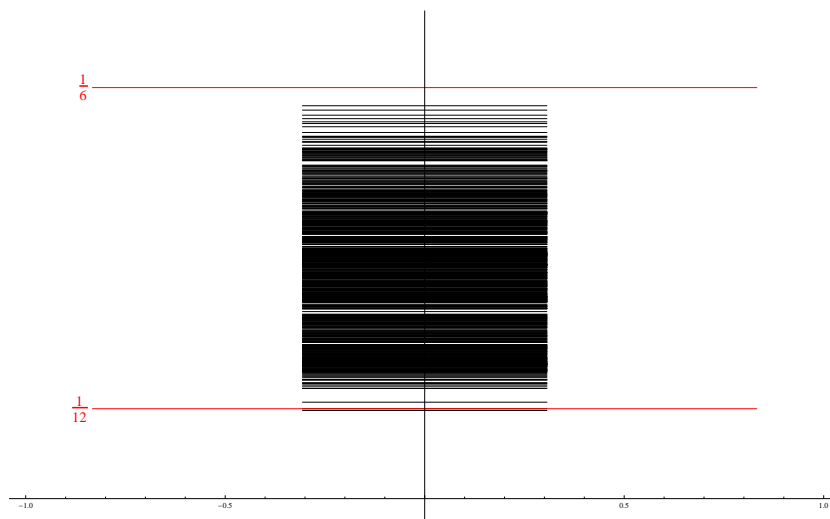


Figure 3.1: Totally real fields of degree  $D = 3$ , 630 fields,  $1/(2D(D-1)) = 1/(4D) = 1/12$ ,  $1/(2D) = 1/6$ .

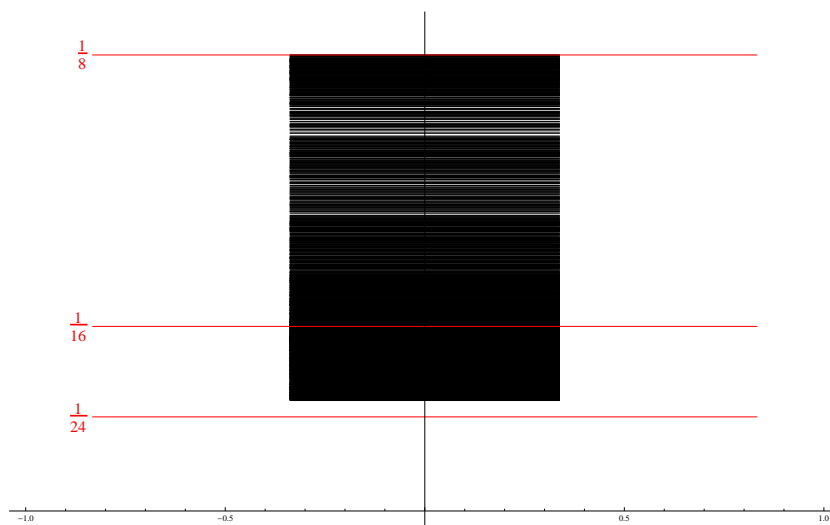
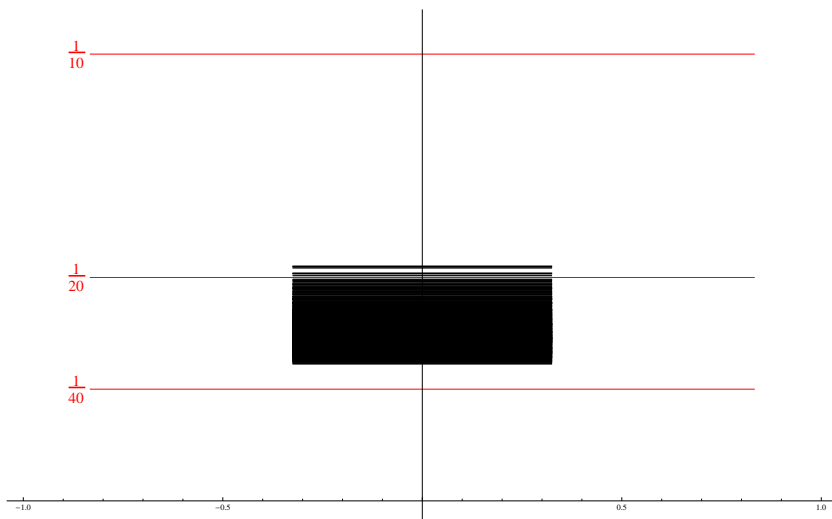
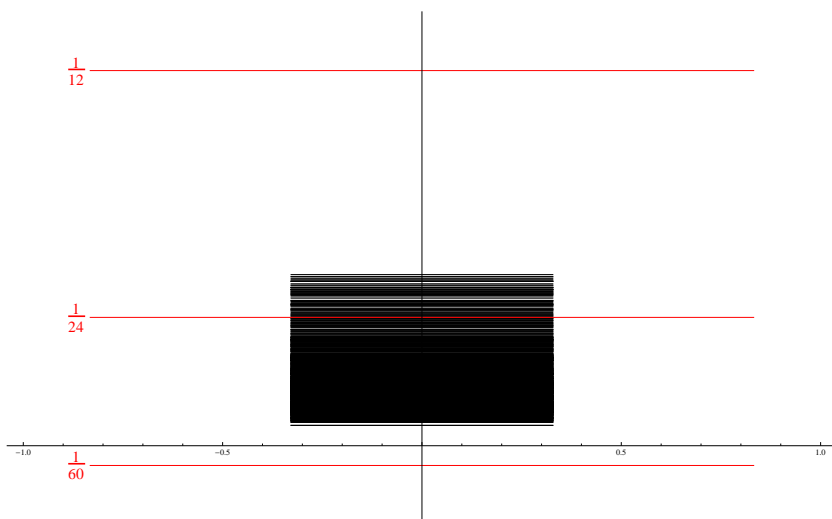


Figure 3.2: Totally real fields of degree  $D = 4$ , 1578 fields  $1/(2D(D-1)) = 1/24$ ,  $1/(4D) = 1/16$ ,  $1/(2D) = 1/8$

Figure 3.3: Totally real fields of degree  $D = 5$ , 674 fieldsFigure 3.4: Totally real fields of degree  $D = 6$ , 827 fields

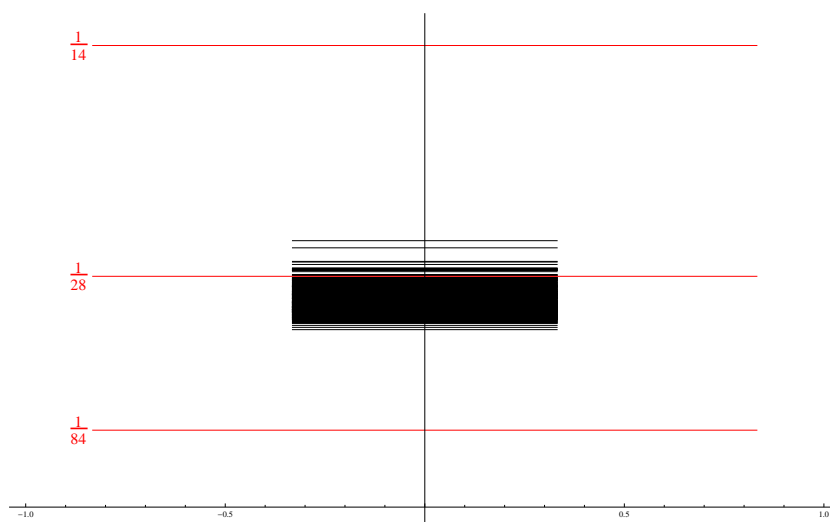


Figure 3.5: Totally real fields of degree  $D = 7$ , 301 fields

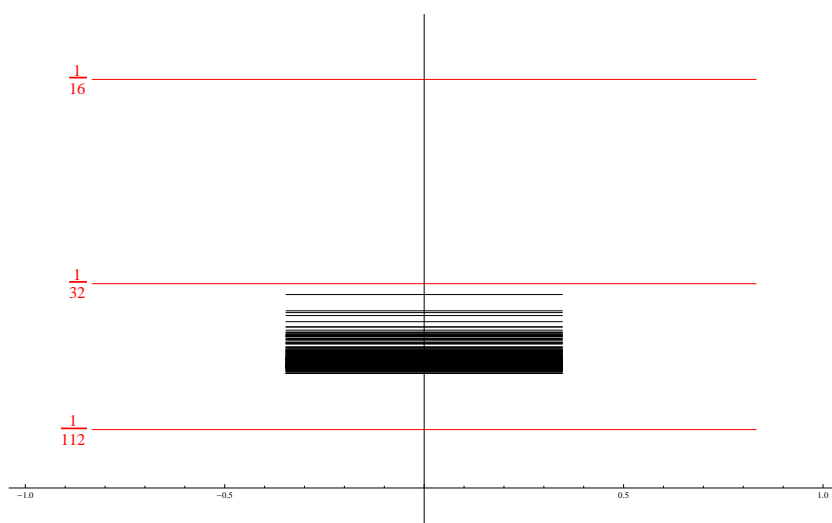


Figure 3.6: Totally real fields of degree  $D = 8$ , 164 fields

**Question 3.4.** *Are the cluster points dense in an interval, maybe even in  $[1/(2D(D-1)), 1/(2D)]$ ?*

*Is the smallest cluster point for totally real fields and  $D > 2$  larger than  $1/(2D(D-1))$ ?*



## Chapter 4

# The Northcott property

In this chapter we study extensions of Northcott's Theorem. Much of the presented material was taken verbatim from [28].

### 4.1 Introduction

Recall that a subset  $\mathcal{A}$  of  $\overline{\mathbb{Q}}$  has the Northcott property, short property (N), if for each positive real number  $X$  there are only finitely many elements  $\alpha$  in  $\mathcal{A}$  with  $H(\alpha) \leq X$ . We have already seen in Chapter 1 that Northcott's Theorem, and more generally the Northcott property, is very important and has many Diophantine applications. Bombieri, Zannier [2] and more explicitly Dvornicich and Zannier [4] proposed the following problem.

**Problem 4.1** (Bombieri-Zannier 2001, Dvornicich-Zannier, 2008). *Find other interesting sets than sets of uniformly bounded degree, e.g. infinite field extensions, with property (N).*

Indeed, a small variation of Northcott's argument shows, that Northcott's Theorem remains valid for any ground field with property (N). Hence any field of infinite degree with property (N) provides a generalization of Northcott's Theorem.

**Theorem 4.1** (Dvornicich-Zannier, 2008).  *$L$  has property (N)  $\implies$  sets of bounded degree over  $L$  have property (N). In particular, property (N) is preserved under finite extensions of fields.*

*Proof.* Let  $D_{\alpha,L}(x) = x^d + a_1x^{d-1} + \dots + a_d$  be the monic minimal polynomial of  $\alpha$  over  $L$ . The zeros of  $D_{\alpha,L}(x)$  have equal height thanks to Lemma 1.4

(i). Furthermore,

$$a_i = \text{symmetric function in the zeros of } D_{\alpha,L}(x).$$

Suppose  $H(\alpha) \leq X$  then by Lemma 1.4 (ii)

$$H(a_i) \leq 2^d X^{d^{2d}}.$$

Since the degree of the minimal polynomials is bounded we have only finitely many minimal polynomials  $D_{\alpha,L}$ , and thus only finitely many roots  $\alpha$ .  $\square$

Also a more concrete problem was addressed in [2] and [4]. Let  $k$  be a number field, and let  $k^{(d)}$  be the composite field of all extension of  $k$  of degree at most  $d$ .

**Question 4.1** (Bombieri-Zannier 2001). *Does  $k^{(d)}$  have property (N)?*

This question remains open but Bombieri and Zannier have shown the following result. Let  $k_{ab}^{(d)}$  be the maximal abelian subextension of  $k^{(d)}/k$ , i.e., the composite field of all abelian extensions  $F/k$  with  $F \subset k^{(d)}$ .

**Theorem 4.2** (Bombieri-Zannier 2001). *The field  $k_{ab}^{(d)}$  has property (N).*

*Proof.* This is proved in [2]. We show the proof on the blackboard.  $\square$

Clearly  $k_{ab}^{(2)} = k^{(2)}$  which answers Question 4.1 for  $d = 2$ .

**Corollary 4.3** (Bombieri-Zannier 2001).  *$k^{(2)}$  has property (N).*

Another consequence of Theorem 4.2 is the following result.

**Corollary 4.4** (Bombieri, Zannier). *The field  $\mathbb{Q}(1^{1/d}, 2^{1/d}, 3^{1/d}, 4^{1/d}, 5^{1/d}, \dots)$  has property (N).*

*Proof.* Take  $k = \mathbb{Q}(\zeta_d)$  with a primitive  $d$ -th root of unity. Then  $k(a^{1/d})/k$  is abelian of degree at most  $d$ . Thus  $\mathbb{Q}(1^{1/d}, 2^{1/d}, 3^{1/d}, 4^{1/d}, 5^{1/d}, \dots) \subset k_{ab}^{(d)}$ .  $\square$

So far we have seen only fields that can be generated (over  $\mathbb{Q}$ ) by algebraic numbers of uniformly bounded degree. Are there any other examples? Moreover, taking a finite extension of a field is a very special case of taking the compositum of two fields. In this direction one might ask: is property (N) preserved under composition of two fields? Both questions are answered by the following theorem.

**Theorem 4.5** (W. 2009). *Let  $k$  be a number field, let  $p_1 < p_2 < p_3 < \dots$  be a sequence of positive primes and let  $d_1, d_2, d_3, \dots$  be a sequence of positive integers. Then the field  $k(p_1^{1/d_1}, p_2^{1/d_2}, p_3^{1/d_3}, \dots)$  has the Northcott property if and only if  $|p_i^{1/d_i}| \rightarrow \infty$  as  $i$  tends to infinity. Here  $p_i^{1/d_i}$  is any  $d_i$ -th root of  $p_i$  and  $|\cdot|$  denotes the complex modulus.*

If the  $d_i$  are prime and not uniformly bounded then  $\mathbb{Q}(p_1^{1/d_1}, p_2^{1/d_2}, p_3^{1/d_3}, \dots)$  contains elements of arbitrarily large prime degree and thus it cannot be generated over  $\mathbb{Q}$  by algebraic numbers of bounded degree. The conclusion remains true if we drop the primality condition on  $d_i$ . This can be deduced from Proposition 1 in [2] which implies for any subfield  $L \subseteq \mathbb{Q}^{(d)}$  the local degrees  $[L_v : \mathbb{Q}_v]$  are bounded solely in terms of  $d$ . Now the local degrees of  $L = \mathbb{Q}(p_1^{1/d_1}, p_2^{1/d_2}, p_3^{1/d_3}, \dots)$  are not uniformly bounded and so  $L$  is not contained in  $\mathbb{Q}^{(d)}$  for any choice of  $d$ .

Moreover, Theorem 4.5 easily implies the following statement.

**Corollary 4.6** (W. 2009). *Property (N) is not generally preserved under taking the composite of two fields. More concretely: let  $p_i$  be the  $i + 1$ -th prime number and set  $d_i = \lfloor \sqrt{\log p_i} \rfloor$ . Let*

$$\begin{aligned} L_1 &= \mathbb{Q}(p_1^{1/d_1}, p_2^{1/d_2}, p_3^{1/d_3}, \dots), \\ L_2 &= \mathbb{Q}(p_1^{1/(d_1+1)}, p_2^{1/(d_2+1)}, p_3^{1/(d_3+1)}, \dots). \end{aligned}$$

*Then  $L_1$  and  $L_2$  both have property (N) but their composite field does not have property (N).*

Another example proving Corollary 4.6, again coming from Theorem 4.5, is as follows: consider the fields  $L_1 = \mathbb{Q}(p_1^{1/d_1}, p_2^{1/d_2}, p_3^{1/d_3}, \dots)$  and  $L_2 = \mathbb{Q}(\zeta_{d_1} p_1^{1/d_1}, \zeta_{d_2} p_2^{1/d_2}, \zeta_{d_3} p_3^{1/d_3}, \dots)$ , where  $d_i$  is as in Corollary 4.6 and  $\zeta_{d_i}$  are primitive  $d_i$ -th roots of unity. Then plainly  $L_1, L_2$  have the property (N) (by Theorem 4.5) but  $L_1 L_2$  does not because it contains infinitely many roots of unity.

Next we give a simple but rather general criterion for the property (N). Roughly speaking it states that the union of fields in a saturated (i.e. without intermediate fields) nested sequence of number fields with enough ramification at each step has property (N).

**Theorem 4.7** (W. 2009). *Let  $k$  be a number field, let  $k = K_0 \subsetneq K_1 \subsetneq K_2 \subsetneq \dots$  be a nested sequence of finite extensions and set  $L = \bigcup_i K_i$ . Suppose that*

$$\inf_{K_{i-1} \subsetneq M \subseteq K_i} \left( N_{K_{i-1}/\mathbb{Q}}(D_{M/K_{i-1}}) \right)^{\frac{1}{[M:K_0][M:K_{i-1}]}} \longrightarrow \infty \quad (4.1.1)$$

as  $i$  tends to infinity where the infimum is taken over all intermediate fields  $M$  strictly larger than  $K_{i-1}$ . Then the field  $L$  has the Northcott property.

If the nested sequence of number fields is saturated then (4.1.1) simplifies to

$$N_{K_{i-1}/\mathbb{Q}}(D_{K_i/K_{i-1}})^{\frac{1}{[K_i:K_0][K_i:K_{i-1}]}} \longrightarrow \infty. \quad (4.1.2)$$

As a simple application we get a very small step towards an affirmative answer on Question 4.1 for  $d = 3$ .

**Corollary 4.8** (W. 2009). *Let  $F_0$  be an arbitrary number field and let  $F_1, F_2, F_3, \dots$  be a sequence of field extensions of  $F_0$  with  $[F_i : F_0] \leq 3$  such that for each positive integer  $i$  there is a prime  $p_i$  with  $p_i \mid \Delta_{F_i}$  and  $p_i \nmid \Delta_{F_j}$  for  $0 \leq j < i$ . Then the compositum of  $F_0, F_1, F_2, F_3, \dots$  has the Northcott property.*

*Proof.* Write  $K_i$  for the compositum of  $F_0, \dots, F_i$ . For  $i > 0$  we have  $1 \leq [K_i : K_{i-1}] \leq 3$ , in particular  $K_i/K_{i-1}$  does not admit a proper intermediate field and so (4.1.1) simplifies to (4.1.2). By assumption there is a prime  $p_i$  which ramifies in  $F_i$  but not in  $F_j$  for  $0 \leq j < i$ . Thus

$$p_i^{[K_i:F_i]} \mid \Delta_{F_i}^{[K_i:F_i]} \mid \Delta_{K_i}.$$

On the other hand  $p_i$  does not ramify in  $F_0, \dots, F_{i-1}$  and so does not ramify in the compositum  $K_{i-1}$ , that is  $p_i \nmid \Delta_{K_{i-1}}$ . We conclude

$$p_i^{[K_i:F_i]} \mid N_{K_{i-1}/\mathbb{Q}}(D_{K_i/K_{i-1}})$$

and therefore

$$N_{K_{i-1}/\mathbb{Q}}(D_{K_i/K_{i-1}})^{\frac{1}{[K_i:K_0][K_i:K_{i-1}]}} \geq p_i^{\frac{[K_i:F_i]}{[K_i:K_0][K_i:K_{i-1}]}}. \quad (4.1.3)$$

Since  $[K_i : F_i] = [K_i : K_0]/[F_i : K_0]$  and  $[F_i : K_0] \leq 3$  and  $[K_i : K_{i-1}] \leq 3$  we see that the right hand-side of (4.1.3) is at least  $p_i^{1/9}$ . Now clearly  $p_i \longrightarrow \infty$  as  $i$  tends to infinity and so the statement follows from Theorem 4.7.  $\square$

## 4.2 Proof of Theorem 4.7

Let  $L$  be a field of algebraic numbers of infinite degree. Now we consider a nested sequence of fields

$$K_0 \subsetneq K_1 \subsetneq K_2 \subsetneq K_3 \subsetneq \dots$$

such that

- (i)  $K_0$  has the property (N),
- (ii)  $[K_i : K_{i-1}] < \infty$  for  $i > 0$ ,
- (iii)  $L = \bigcup_{i=0}^{\infty} K_i$ .

For a finite extension  $M/F$  of subfields of  $\overline{\mathbb{Q}}$  we define

$$\delta(M/F) = \inf\{H(\alpha); F(\alpha) = M\}.$$

Note that if  $M$  has the property (N) then the infimum is attained, i.e. there exists  $\alpha \in M$  with  $F(\alpha) = M$  and  $H(\alpha) = \delta(M/F)$ .

Since each  $K_i$  is a finite extension of  $K_0$  we deduce by (i) and Theorem 4.1 that each field  $K_i$  has property (N).

**Proposition 4.9.**  *$L$  has property (N) if and only if*

$$\inf_{K_{i-1} \subsetneq M \subseteq K_i} \delta(M/K_{i-1}) \longrightarrow \infty \quad \text{as } i \rightarrow \infty$$

where the infimum is taken over all intermediate fields  $M$  strictly larger than  $K_{i-1}$ .

*Proof.* For brevity let us write

$$A_i = \inf_{K_{i-1} \subsetneq M \subseteq K_i} \delta(M/K_{i-1}).$$

First we show that property (N) for the field  $L$  implies  $A_i \rightarrow \infty$ .

For each  $i > 0$  we can find  $\alpha_i \in K_i \setminus K_{i-1}$  with  $H(\alpha_i) = A_i$ , in particular the elements  $\alpha_i$  are pairwise distinct. Now suppose  $(A_i)_{i=1}^{\infty}$  has a bounded subsequence. Hence we get infinitely many elements  $\alpha_i \in L$  with uniformly bounded height and so  $L$  does not have property (N).

Next we prove that  $A_i \rightarrow \infty$  implies property (N) for the field  $L$ . Suppose  $L$  does not have property (N). Hence there exists an infinite sequence  $\alpha_1, \alpha_2, \alpha_3, \dots$  of pairwise distinct elements in  $L \setminus K_0$  with  $H(\alpha_j) \leq X$  for a certain fixed real number  $X$ . Let  $i = i(\alpha_j)$  be such that  $\alpha_j \in K_i \setminus K_{i-1}$ . Thus

$$K_{i-1} \subsetneq K_{i-1}(\alpha_j) \subseteq K_i$$

and hence

$$A_i \leq \delta(K_{i-1}(\alpha_j)/K_{i-1}) \leq H(\alpha_j) \leq X.$$

Since each field  $K_i$  has the property (N) we conclude  $i(\alpha_j) \rightarrow \infty$  as  $j \rightarrow \infty$ . Thus  $(A_i)_{i=1}^\infty$  has a bounded subsequence.  $\square$

Now we can easily complete the proof of Theorem 4.7. From Proposition 4.9 we know it suffices to show

$$\inf_{K_{i-1} \subsetneq M \subseteq K_i} \delta(M/K_{i-1}) \rightarrow \infty \quad \text{as } i \rightarrow \infty.$$

So let  $M$  be an intermediate field  $K_{i-1} \subsetneq M \subseteq K_i$  and set  $m = [M : K_{i-1}]$ . We apply Silverman's Theorem from Chapter 3 to get

$$\inf_{K_{i-1} \subsetneq M \subseteq K_i} \delta(M/K_{i-1}) \geq (1/2) \inf_{K_{i-1} \subsetneq M \subseteq K_i} (N_{K_{i-1}/\mathbb{Q}}(D_{M/K_{i-1}}))^{\frac{1}{2[K_{i-1}:\mathbb{Q}]m(m-1)}}. \quad (4.2.4)$$

Now using  $[K_{i-1} : \mathbb{Q}]m = [K_0 : \mathbb{Q}][M : K_0]$  and the hypothesis of the theorem we see that the right hand-side of (4.2.4) tends to infinity as  $i$  tends to infinity. This completes the proof of Theorem 4.7.

### 4.3 Proof of Theorem 4.5

Theorem 4.5 is a simple consequence of the following proposition.

**Proposition 4.10.** *Let  $K_0$  be a number field. For  $i = 1, 2, 3, \dots$  let  $\mathfrak{q}_i$  be a nonzero prime ideal in  $\mathcal{O}_{K_0}$ , and let  $D_i$  be a  $\mathfrak{q}_i$ -Eisenstein polynomial in  $\mathcal{O}_{K_0}[x]$ . Denote  $\deg D_i = d_i$ , and let  $\alpha_i$  be any root of  $D_i$ . Moreover, suppose that  $\mathfrak{q}_i$  is unramified in  $K_0(\alpha_j)$  for  $1 \leq j < i$ , and that  $N_{\mathfrak{q}_i} \alpha_i^{1/d_i} \rightarrow \infty$  as  $i$  tends to infinity. Then the field  $K_0(\alpha_1, \alpha_2, \alpha_3, \dots)$  has the Northcott property.*

*Proof.* Let us recall the following well-known fact (see for instance Theorem 24. (a) p.133 in [8]): Let  $F, K$  be number fields with  $F \subseteq K$ . Let  $\wp$  be a prime ideal in  $\mathcal{O}_F$ . The following are equivalent:

- (i)  $\wp$  ramifies totally in  $K$ .
- (ii)  $K = F(\alpha)$  for a root  $\alpha$  of a  $\wp$ -Eisenstein polynomial in  $\mathcal{O}_F[x]$ .

We can now prove Proposition 4.10. For  $i > 0$  let  $K_i = K_{i-1}(\alpha_i)$ . By assumption  $\mathfrak{q}_i$  is unramified in  $K_0(\alpha_j)$  for  $1 \leq j < i$  and thus also in  $K_{i-1}$  (see [15] Corollary 1.). Now clearly  $K_0 \subsetneq K_1 \subsetneq K_2 \subsetneq \dots$  and of course  $\bigcup_{i=0}^{\infty} K_i = K(\alpha_1, \alpha_2, \alpha_3, \dots)$ . We will apply Theorem 4.7 but first we have to make sure that condition (4.1.1) holds.

Now let  $i > 0$  and let  $M$  be an intermediate field with  $K_{i-1} \subsetneq M \subseteq K_i$ . Moreover set  $m = [M : K_{i-1}]$ . Let  $\wp$  be any prime ideal in  $\mathcal{O}_{K_{i-1}}$  above  $\mathfrak{q}_i$ . Since  $\mathfrak{q}_i$  is unramified in  $K_{i-1}$  we conclude that  $D_i$  is a  $\wp$ -Eisenstein polynomial in  $\mathcal{O}_{K_{i-1}}[x]$ . According to the Eisenstein criterion this implies that  $D_i$  is irreducible over  $K_{i-1}$  and since  $K_i = K_{i-1}(\alpha_i)$  we get  $[K_i : K_{i-1}] = d_i$ . Moreover we conclude that  $\wp$  ramifies totally in  $K_i/K_{i-1}$ . Let

$$\mathfrak{q}_i = \wp_1 \dots \wp_s$$

be the decomposition into prime ideals in  $\mathcal{O}_{K_{i-1}}$ . Since  $\wp_j$  ramifies totally in  $K_i/K_{i-1}$  it also ramifies totally in  $M/K_{i-1}$ . Hence

$$\wp_j = \mathfrak{B}_j^m$$

for  $1 \leq j \leq s$  and prime ideals  $\mathfrak{B}_j$  in  $\mathcal{O}_M$ . Let  $\mathfrak{D}_{M/K_{i-1}}$  be the different of  $M/K_{i-1}$  (for the definition see [17] p.195). Then we have  $\mathfrak{B}_j^{m-1} \mid \mathfrak{D}_{M/K_{i-1}}$  (see [17] (2.6) Theorem p.199) and therefore

$$(\mathfrak{B}_1 \dots \mathfrak{B}_s)^{m-1} \mid \mathfrak{D}_{M/K_{i-1}}.$$

The discriminant  $D_{M/K_{i-1}}$  is the norm of the different  $\mathfrak{D}_{M/K_{i-1}}$  from  $M$  to  $K_{i-1}$  (see [17] (2.9) Theorem p.201). Taking then norms from  $K_{i-1}$  to  $\mathbb{Q}$  we conclude

$$N_{K_{i-1}/\mathbb{Q}}(D_{M/K_{i-1}}) = N_{K_{i-1}/\mathbb{Q}}(N_{M/K_{i-1}}(\mathfrak{D}_{M/K_{i-1}})) = N_{M/\mathbb{Q}}(\mathfrak{D}_{M/K_{i-1}}).$$

Therefore

$$N_{M/\mathbb{Q}}((\mathfrak{B}_1 \dots \mathfrak{B}_s)^{m-1}) \mid N_{K_{i-1}/\mathbb{Q}}(D_{M/K_{i-1}}). \quad (4.3.5)$$

On the other hand we have

$$\begin{aligned} N_{M/\mathbb{Q}}((\mathfrak{B}_1 \dots \mathfrak{B}_s)^{m-1}) &= (N_{M/\mathbb{Q}}(\prod_{j=1}^s \mathfrak{B}_j^m))^{\frac{m-1}{m}} = (N_{M/\mathbb{Q}}(\prod_{j=1}^s \mathfrak{O}_j))^{\frac{m-1}{m}} \\ &= (N_{M/\mathbb{Q}}(\mathfrak{q}_i))^{\frac{m-1}{m}} = (N_{K_0/\mathbb{Q}}(\mathfrak{q}_i))^{[K_{i-1}:K_0](m-1)}. \end{aligned}$$

Combining the latter with (4.3.5) and not forgetting that  $1 < m = [M : K_{i-1}] \leq d_i$  we end up with

$$\begin{aligned} N_{K_{i-1}/\mathbb{Q}}(D_{M/K_{i-1}})^{\frac{1}{[M:K_0][M:K_{i-1}]}} &\geq (N_{K_0/\mathbb{Q}}(\mathfrak{q}_i))^{\frac{[K_{i-1}:K_0](m-1)}{[M:K_0]m}} = (N_{K_0/\mathbb{Q}}(\mathfrak{q}_i))^{\frac{(m-1)}{m^2}} \\ &\geq (N_{K_0/\mathbb{Q}}(\mathfrak{q}_i))^{\frac{1}{2m}} \geq (N_{K_0/\mathbb{Q}}(\mathfrak{q}_i))^{\frac{1}{2d_i}}. \end{aligned}$$

By hypothesis of the theorem  $(N_{K_0/\mathbb{Q}}(\mathfrak{q}_i))^{\frac{1}{d_i}}$  tends to infinity. Hence we can apply Theorem 4.7, and this completes the proof.  $\square$

Now we can prove Theorem 4.5.

Since  $H(p_i^{1/d_i}) = |p_i^{1/d_i}|$  we see that condition  $|p_i^{1/d_i}| \rightarrow \infty$  is necessary to obtain property (N). Now let us prove that this condition implies property (N). By Theorem 4.1 it suffices to show that  $\mathbb{Q}(p_i^{1/d_i}; i > i_0)$  has property (N) for some  $i_0$ . The hypothesis  $|p_i^{1/d_i}| \rightarrow \infty$  implies that there is an  $i_0$  such that  $p_i \nmid \Delta_{\mathbb{Q}(p_j^{1/d_j})}$  for all  $i \geq i_0$  and  $1 \leq j < i$ . Applying Proposition 4.10 with  $D_i = x^{d_i+i_0} - p_{i+i_0}$ ,  $\alpha_i = p_{i+i_0}^{1/d_{i+i_0}}$ , and  $K_0 = \mathbb{Q}$  completes the proof.

## Acknowledgements

I would like to thank Fabrizio Barroero, Christopher Frei, and Daniel Harrer for comments and corrections.

# Bibliography

- [1] E. Bombieri and W. Gubler, *Heights in Diophantine Geometry*, Cambridge University Press, 2006.
- [2] E. Bombieri and U. Zannier, *A Note on heights in certain infinite extensions of  $\mathbb{Q}$* , Rend. Mat. Acc. Lincei **12** (2001), 5–14.
- [3] C. Christensen and W. Gubler, *Der relative Satz von Schanuel*, Manuscripta Math. **126** (2008), 505–525.
- [4] R. Dvornicich and U. Zannier, *On the properties of Northcott and Narkiewicz for fields of algebraic numbers*, Functiones et Approximatio **39** (2008), 163–173.
- [5] J. Ellenberg, *Points of low height on  $\mathbb{P}^1$  over number fields and bounds for torsion in class groups*, to appear in Computational Arithmetic Geometry.
- [6] J. Ellenberg and A. Venkatesh, *The number of extensions of a number field with fixed degree and bounded discriminant*, Ann. of Math. **163** (2006), 723–741.
- [7] ———, *Reflection principles and bounds for class group torsion*, Int. Math. Res. Not. **no.1, Art. ID rnm002** (2007).
- [8] A. Fröhlich and M. J. Taylor, *Algebraic number theory*, Cambridge University Press, 1991.
- [9] X. Gao, *On Northcott's Theorem*, Ph.D. Thesis, University of Colorado (1995).
- [10] M. Hindry and J.H. Silverman, *Diophantine Geometry An Introduction*, Springer, 2000.
- [11] S. Lang, *Fundamentals of Diophantine Geometry*, Springer, 1983.

- [12] ———, *Algebraic Number Theory*, Springer, 1994.
- [13] D. W. Masser and J. D. Vaaler, *Counting algebraic numbers with large height I*, Diophantine Approximation - Festschrift für Wolfgang Schmidt (eds. H. P. Schlickewei, K. Schmidt, R. F. Tichy), Developments in Mathematics 16, Springer 2008, (pp.237–243).
- [14] ———, *Counting algebraic numbers with large height II*, Trans. Amer. Math. Soc. **359** (2007), 427–445.
- [15] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Springer, 1990.
- [16] J. Neukirch, *Algebraische Zahlentheorie*, Springer, 1992.
- [17] ———, *Algebraic Number Theory*, Springer, 1999.
- [18] D. G. Northcott, *An inequality in the theory of arithmetic on algebraic varieties*, Proc. Cambridge Phil. Soc. **45** (1949), 502–509 and 510–518.
- [19] W. Ruppert, *Small generators of number fields*, Manuscripta math. **96** (1998), 17–22.
- [20] S. H. Schanuel, *Heights in number fields*, Bull. Soc. Math. France **107** (1979), 433–449.
- [21] W. M. Schmidt, *Heights of algebraic points*, Number theory and its applications (C. Y. Yildirim and S. A. Stepanov, eds), Marcel Dekker, 1999, pp.185–225.
- [22] ———, *Northcott's Theorem on heights I. A general estimate*, Monatsh. Math. **115** (1993), 169–183.
- [23] ———, *Northcott's Theorem on heights II. The quadratic case*, Acta Arith. **70** (1995), 343–375.
- [24] J. Silverman, *Lower bounds for height functions*, Duke Math. J. **51** (1984), 395–403.
- [25] J. L. Thunder, *The number of solutions of bounded height to a system of linear equations*, J. Number Theory **43** (1993), 228–250.
- [26] J. D. Vaaler and M. Widmer, *On small generators of number fields*, in preparation (2009).

- [27] M. Widmer, *Counting points of fixed degree and bounded height*, Acta Arith. **140.2** (2009), 145–168.
- [28] ———, *On certain infinite extensions of the rationals with Northcott property*, to appear in Monatsh. Math. (2009).
- [29] ———, *Small generators of function fields*, to appear in J. Théor. Nombres Bordeaux (2009).
- [30] ———, *Counting points of fixed degree and bounded height on linear varieties*, J. Number Theory **130** (2010), 1763–1784.
- [31] ———, *Counting primitive points of bounded height*, Trans. Amer. Math. Soc. **362** (2010), 4793–4829.
- [32] ———, *Lipschitz class, narrow class, and counting lattice points*, accepted in Proc. Amer. Math. Soc. (2010), 13 pages.
- [33] ———, *The distribution of integral points in affine space*, preprint (2010), 32 pages.