

Diophantine approximation by conjugate algebraic numbers

Guillaume Alain

Thesis submitted to the
Faculty of Graduate and Postdoctoral Studies
University of Ottawa
in partial fulfillment of the requirements for the
M.Sc. degree in the

Ottawa-Carleton Institute for Graduate Studies
and Research in Mathematics and Statistics

©2006 Guillaume Alain

CONTENTS

1. Introduction	1
2. Preliminaries and basic results of diophantine approximation	4
2.1. Height and Mahler measure	4
2.2. Vinogradov symbols	5
2.3. Resultant and discriminant	6
2.4. Continued fractions	7
2.5. Convex set and convex bodies	10
2.6. Successive minima of convex bodies	11
2.7. \mathbb{Q} -structures and bilinear forms	13
2.8. Duality for convex bodies and lattices	13
2.9. Duality of the minima	14
2.10. A particular application	14
3. Approximation of a real number using all conjugate roots of a polynomial	17
3.1. Introduction	17
3.2. Construction of polynomials	18
3.3. Proof of the theorems	20
3.4. Optimality of the exponents of approximation	22

3.5. A different approach to Proposition 3.1	24
4. Preliminaries and basic results on number fields	29
4.1. Number fields, ring of integers and discriminant	29
4.2. Fractional ideals, unique factorization and norms	30
4.3. Height of a subspace, orthogonal subspaces	31
5. Approximation over an imaginary quadratic field	33
5.1. Introduction	33
5.2. Some lemmas on vector spaces	35
5.3. Construction of the sequence of best approximations	38
5.4. Specific properties coming from the negation of Theorem 5.1	41
5.5. Relations between coordinates of the best approximations	42
5.6. A lemma on ideals	49
5.7. The sequence of best approximations	50
5.8. Specific properties of the sequence of best approximations	50
5.9. Optimality	53
6. Conclusion	54
References	56

Notation

$H(P)$	height of a polynomial $P \in \mathbb{C}[T]$	§2.1
$M(P)$	Mahler measure of a polynomial $P \in \mathbb{C}[T]$	§2.1
$H(\alpha)$	height of an algebraic number α	§2.1
$M(\alpha)$	Mahler measure of an algebraic number α	§2.1
$R[T]$	ring of polynomials in T with coefficients from the ring R	
$R[T]_{\leq n}$	polynomials of $R[T]$ with degree $\leq n$	
\mathbb{N}^*	the set of positive integers, excluding 0	
$\bar{\alpha}$	some conjugate of an algebraic number α	
$\lfloor x \rfloor$	the largest integer m with $m \leq x$	
$\lceil x \rceil$	the smallest integer M with $x \leq M$	
$\overline{\mathbb{Q}}$	the set of algebraic numbers of \mathbb{C} over \mathbb{Q}	
\gg, \ll	Vinogradov symbols	§2.2
$D(\alpha)$	discriminant of an algebraic number α	§2.3
$[a_0, \dots, a_n]$	finite continued fraction with partial quotients a_0, \dots, a_n	§2.4
$[a_0, a_1, \dots]$	infinite continued fraction with partial quotients a_0, a_1, \dots	§2.4
$V(H)$	co-volume of a lattice H	§2.5
$\mu(S)$	Lebesgue measure of an integrable set S	§2.5
$\lambda_i \mathcal{C}$	i -th minimum of a convex \mathcal{C}	§2.6
$\langle \mathbf{g}_1, \dots, \mathbf{g}_i \rangle_{\mathbb{R}}$	subspace of \mathbb{R}^n generated over \mathbb{R} by the vectors $\mathbf{g}_1, \dots, \mathbf{g}_i \in \mathbb{R}^n$	
$E(\mathbb{Q})$	a \mathbb{Q} -structure for a real vector space E	§2.7
$[\mathbf{x}]_{\mathcal{B}}$	coordinates of the vector \mathbf{x} in the basis \mathcal{B}	
A^T	transpose of a matrix A	
\mathcal{C}^*	dual of a convex body \mathcal{C}	§2.8
Λ^*	dual of a lattice Λ	§2.8
$\lambda_i(\mathcal{C}^*)$	i -th minimum of the dual of \mathcal{C}	
$P^{[k]}(x)$	$= \frac{1}{k!} P^{(k)}(x)$, the k -th divided derivative of $P \in \mathbb{C}[T]$	
$s\mathcal{C}$	dilatation of a convex body \mathcal{C} by a factor of $s > 0$	
\mathcal{O}_K	ring of integers of a number field K	§4.1
$Tr(x)$	trace of x	§4.1
$N(x)$	norm of x	§4.1
D_K	discriminant of a number field K	§4.1
\mathbb{I}_K	set of fractional ideals of \mathcal{O}_K	§4.2
$N(\mathfrak{a})$	norm of a fractional ideal \mathfrak{a}	§4.2
$\langle E \rangle_{\mathcal{O}_K}$	set of linear combinations over \mathcal{O}_K of elements of E	
$H(S)$	height of a subspace S of K^m	§4.3
S^\perp	orthogonal of S	§4.3
$f(x) = \mathcal{O}(g(x))$	standard ‘‘Big-Oh’’ notation	

Vectors are usually denoted in boldface font. When we refer to their individual coefficients, we use regular font with indices. For example, $\mathbf{x} = (x_0, \dots, x_n)$ and $\mathbf{x}_i = (x_{i,0}, \dots, x_{i,n})$.

Acknowledgements

Je remercie sincèrement mon superviseur Damien Roy pour ses conseils, son temps et son aide pour la rédaction de cette thèse et pour tout ce qui est venu avant.

Je suis redevable au CRSNG pour leur généreux financement et ainsi qu'à l'Université d'Ottawa pour ses différentes formes d'aide financière.

Je remercie mes parents de manière générale parce que si je prenais le temps de les remercier pour tout ce qu'ils ont fait pour moi je n'en finirais jamais.

Merci finalement à Zeus, qui, bien qu'habitué à recevoir des animaux en sacrifice, saura pourquoi je le remercie mais ne saura probablement que faire de remerciements dans une thèse de mathématiques.

Abstract

In 1969, Davenport and Schmidt provided upper bounds for the approximation of a real number by algebraic integers. Their novel approach was based on the geometry of numbers and involved the duality for convex bodies.

In the present thesis we study the approximation of a real number by conjugate algebraic numbers. We find inspiration in Davenport and Schmidt's method, but ultimately our approximations come from the theory of continued fractions. We get a general optimal result for which we offer two different proofs.

We then extend two of Davenport and Schmidt's important results to the context of an imaginary quadratic number field. Our method follows that of Michel Laurent who simplified Davenport and Schmidt's argument in 2003. One of their original results is optimal and so is our extension.

Résumé

En 1969, Davenport et Schmidt ont établi des estimations pour l'approximation d'un nombre réel par des entiers algébriques. Leur approche utilise de manière astucieuse la géométrie des nombres, en particulier la dualité des corps convexes.

Nous nous penchons premièrement sur l'approximation d'un nombre réel par des nombres algébriques conjugués. Notre approche est basée sur la méthode de Davenport et Schmidt, mais nous construisons nos approximation à l'aide de la théorie des fractions continues. Nous obtenons un résultat général qui est optimal et pour lequel nous fournissons deux preuves.

Nous adaptons ensuite deux résultats importants de Davenport et Schmidt à un corps quadratique imaginaire. Pour ce faire, nous suivons la simplification de Michel Laurent pour la méthode de Davenport et Schmidt. Un de leurs deux résultats est optimal et il en va de même pour notre adaptation.

1. Introduction

An outstanding problem in Diophantine approximation, motivated initially by Mahler's and Koksma's classification of numbers, is to provide sharp estimates for the approximation of a real number by algebraic numbers of bounded degree. Starting with the pioneer work [Wi] of E. Wirsing in 1961, this problem has been studied by many authors and extended in several directions. A good account of this can be found in Chapter 3 of [Bu].

For our purpose, let us simply mention that, in 1969, H. Davenport and W. M. Schmidt gave estimates for the approximation by algebraic integers [DS] and that, more recently, D. Roy and M. Waldschmidt looked at simultaneous approximations by several conjugate algebraic integers [RW]. While the latter work was limited to at most one quarter of the conjugates, we consider in the present thesis the problem of simultaneous approximation of a real number by all (resp. all but one) conjugates of an algebraic number (resp. algebraic integer).

Upon defining the *height* $H(P)$ of a polynomial $P \in \mathbb{R}[T]$ to be the largest absolute value of its coefficients, and the *height* $H(\alpha)$ of an algebraic number $\alpha \in \mathbb{C}$ to be the height of its irreducible polynomial in $\mathbb{Z}[T]$, our main result reads as follows.

Theorem A. *Let $\xi \in \mathbb{R} \setminus \mathbb{Q}$ and let $n \in \mathbb{N}^*$. There exist positive constants c_1, c_2 depending only on ξ and n with the following properties :*

(i) *There are infinitely many algebraic numbers α of degree n such that*

$$\max_{\bar{\alpha}} |\xi - \bar{\alpha}| \leq c_1 H(\alpha)^{-2/n}$$

where the maximum is taken over all conjugates $\bar{\alpha}$ of α .

(ii) *There are infinitely many algebraic integers α of degree $n + 1$ such that*

$$\max_{\bar{\alpha} \neq \alpha} |\xi - \bar{\alpha}| \leq c_2 H(\alpha)^{-2/n}$$

where the maximum is taken over all conjugates of $\bar{\alpha}$ of α with $\bar{\alpha} \neq \alpha$.

The statement of part (i) is optimal up to the value of c_1 for each $\xi \in \mathbb{R} \setminus \mathbb{Q}$, while the statement of part (ii) is optimal up to the value of c_2 at least for quadratic irrational values of ξ . This seems to be the first instance where an optimal exponent of approximation is known for all values of the degree n in this type of problem. The fact that we can control the

degree of the approximations originates from an observation of Y. Bugeaud and O. Teulié in [BT].

Definitions and preliminaries concerning the above result will be found in Chapter 2, while a complete proof along with other results will be given in Chapter 3. In pursuing such a result, we followed Davenport and Schmidt's method closely and came up with a longer proof than the one given in the first part of Chapter 3. We then found a way to avoid using the duality of convex bodies and to simplify our proof. The last part of Chapter 3 contains the alternative demonstration that we first had.

The second part of this thesis deals with the two following important results found in the original article [DS] by Davenport and Schmidt in 1969.

Theorem DS2a. *Let $n \geq 2$ be an integer and let $\xi \in \mathbb{R}$. Suppose that ξ is either transcendental over \mathbb{Q} or algebraic over \mathbb{Q} of degree $> n/2$. Let $\lambda = \lfloor n/2 \rfloor^{-1}$. Then there are arbitrarily large values of X such that the inequalities*

$$|x_0| \leq X \quad , \quad |x_0 \xi^k - x_k| \leq cX^{-\lambda} \quad (k = 1, \dots, n)$$

where c is a suitable positive number depending on n and ξ , have no nonzero solution $(x_0, \dots, x_n) \in \mathbb{Z}^{n+1}$.

Davenport and Schmidt provide sharper and optimal bounds in the case where $n = 2$.

Theorem DS1a. *Let $\xi \in \mathbb{R}$. Suppose that ξ is either transcendental over \mathbb{Q} or algebraic over \mathbb{Q} of degree ≥ 3 . Let $\lambda = (-1 + \sqrt{5})/2 \approx 0.618$. Then there are arbitrarily large values of X such that the inequalities*

$$|x_0| \leq X \quad , \quad |x_0 \xi - x_1| \leq cX^{-\lambda} \quad , \quad |x_0 \xi^2 - x_2| \leq cX^{-\lambda}$$

where c is a suitable positive number depending on ξ , have no nonzero solution $(x_0, x_1, x_2) \in \mathbb{Z}^3$.

Let K be a quadratic imaginary number field and let \mathcal{O}_K be its ring of integers over \mathbb{Z} . In Chapter 5, we extend the above two theorems by replacing in their statements \mathbb{R}, \mathbb{Q} and \mathbb{Z} by \mathbb{C}, K and \mathcal{O}_K respectively. This is motivated by the well-known analogy that exists between the ring \mathbb{Z} of integers of \mathbb{Q} and the ring \mathcal{O}_K of integers of an imaginary quadratic field.

Davenport and Schmidt's Theorem DS1a refines their Theorem DS2a for $n = 2$ under the condition that ξ is not algebraic of degree at most 2. The same applies also to our extensions

of their theorems. The optimality of Theorem DS1a was recently shown by Roy in [RoC] and applies also to our extension of this theorem.

Chapter 4 provides the necessary preliminaries about number fields, rings of integers, ideals and norms.

Finally, in Chapter 6 we discuss some questions that arise naturally from the material covered in this thesis.

2. Preliminaries and basic results of diophantine approximation

For any ring R , we let $R[T]$ denote the ring of polynomials in T over R . For any $n \in \mathbb{N}$, we denote by $R[T]_{\leq n}$ its additive subgroup formed by polynomials of degree $\leq n$.

2.1. Height and Mahler measure.

Let $P(T) = a_0 + a_1T + \cdots + a_nT^n \in \mathbb{C}[T]$ and let $\alpha_1, \dots, \alpha_n \in \mathbb{C}$ be the roots of P . We define the *height* of P as

$$H(P) = \max \{|a_0|, \dots, |a_n|\}$$

and the *Mahler measure* of P as

$$M(P) = |a_n| \prod_{i=1}^n \max \{1, |\alpha_i|\}.$$

Proposition 2.1. *The Mahler measure of P is also equal to*

$$M(P) = \exp \left(\int_0^1 \ln |P(e^{2\pi i\theta})| d\theta \right).$$

Note that this integral converges even if P has zeros on the unit circle. The equality of the two formulas for $M(P)$ follows from Jensen's formula (see [Wald] p.22).

Using either of the above definitions for the Mahler measure, we have that

$$M(PQ) = M(P)M(Q) \quad \text{for } P, Q \in \mathbb{C}[T].$$

Proposition 2.2. *The Mahler measure and the height of P are equivalent in the sense that*

$$\frac{M(P)}{n+1} \leq H(P) \leq 2^n M(P).$$

The first of the above inequalities follows easily from the representation of the Mahler measure given by Proposition 2.1. The second one follows from the other representation (as a product) upon noting that $H(P) \leq |a_n| (1 + |\alpha_1|) \cdots (1 + |\alpha_n|)$.

Using Proposition 2.1 and the definition of the height, it is easy to obtain :

Proposition 2.3.

$$H(P)H(Q) \leq 2^{\deg P + \deg Q} (\deg P + \deg Q + 1) H(PQ)$$

$$H(PQ) \leq \min\{\deg P + 1, \deg Q + 1\} H(P)H(Q)$$

Both notions of height and Mahler measure are extended to algebraic numbers $\alpha \in \overline{\mathbb{Q}}$ by defining $H(\alpha)$ and $M(\alpha)$ to be respectively the height and Mahler measure of the unique (up to sign) irreducible polynomial of α over \mathbb{Z} .

2.2. Vinogradov symbols.

In dealing with infinite sequences, some terms or constants of lesser importance are often omitted for the sake of clarity. Let us take for example the Proposition 2.3. If we consider polynomials of degree bounded by $n \in \mathbb{N}$ and we are not interested in the precise value of multiplicative constants depending only on n , then we may restate it as

Proposition 2.4. *There exists constants $c_2 > c_1 > 0$ depending only on n such that for all polynomials $P, Q \in \mathbb{R}[T]_{\leq n}$ we have*

$$c_1 H(P)H(Q) \leq H(PQ) \leq c_2 H(P)H(Q).$$

This way of hiding constants terms can be done efficiently in some situations, but in many others it can completely clutter the exposition.

The Vinogradov symbols \ll and \gg provide a clean way to hide details of no importance in a similar way that the “Big-Oh” notation simplifies the study of algorithmic complexity. For example, we can rewrite the conclusion of the above proposition as

$$H(P)H(Q) \ll_n H(PQ) \ll_n H(P)H(Q)$$

If it is clear from the context that constant factors involving only n are not important, we may use the \ll and \gg symbols without specifying what we are hiding. The expression “ $X \ll Y$ ” reads as “ X is smaller than some constant times Y ”. Both “ $X \ll Y$ ” and “ $X \gg Y$ ” statements can be combined into “ $X \gg\ll Y$ ”.

Throughout this document, the constants implied by the Vinogradov symbols will depend only on ξ and n , except in Chapter 5 where they will also involve a dependence on the quadratic imaginary field K chosen.

2.3. Resultant and discriminant.

A good introduction to resultants can be found in chapters 27-28 of [Wae] or in §10 of [Lang].

Let $f, g \in \mathbb{C}[X]$ be polynomials written as

$$\begin{aligned} f(X) &= v_0 X^n + \dots + v_n = v_0(X - t_1) \cdots (X - t_n), \\ g(X) &= w_0 X^m + \dots + v_m = w_0(X - u_1) \cdots (X - u_m), \end{aligned}$$

with $v_0 \neq 0 \neq w_0$. We define their *resultant* as the following $(m+n) \times (m+n)$ determinant

$$(1) \quad R(f, g) = \begin{vmatrix} v_0 & \cdots & v_n & & & \\ & \ddots & & \ddots & & \\ & & & v_0 & \cdots & v_n \\ w_0 & \cdots & w_m & & & \\ & \ddots & & \ddots & & \\ & & & w_0 & \cdots & w_m \end{vmatrix},$$

where the first m rows involve the coefficients v_0, \dots, v_n of $f(X)$, the last n rows involve the coefficients w_0, \dots, w_m of $g(X)$, and the unspecified entries are all zeros. With the above notation, we have the following :

Proposition 2.5.

$$R(f, g) = v_0^m w_0^n \prod_{i=1}^n \prod_{j=1}^m (t_i - u_j) = v_0^m \prod_{i=1}^n g(t_i) = (-1)^{mn} w_0^n \prod_{j=1}^m f(u_j).$$

Proposition 2.6.

$$R(f, g) = 0 \iff f \text{ and } g \text{ have a common root.}$$

We define the *discriminant* of f to be

$$D(f) = v_0^{2n-2} \prod_{i \neq j} (t_i - t_j) = v_0^{-1} R(f, f').$$

If $f, g \in \mathbb{Z}[X]$, their resultant is an integer since all entries of the matrix found in (1) are integers. Moreover, if $g = f'$, then v_0 divides all entries in the leftmost column of the matrix

in (1), thus v_0 divides $R(f, f')$ in \mathbb{Z} and so $D(f) \in \mathbb{Z}$. We have that $D(f) = 0 \iff f$ has double roots.

For an algebraic number $\alpha \in \mathbb{C}$, we let f be its minimal polynomial over \mathbb{Z} and we define the *discriminant* of α to be $D(\alpha) := D(f)$.

For the purposes of this thesis, we will simply require the following proposition about the discriminant.

Proposition 2.7. *For an algebraic number $\alpha \in \mathbb{C}$, let $f(X) = a(X - \alpha_1) \cdots (X - \alpha_n)$ be its minimal polynomial over \mathbb{Z} . Then we have that*

$$1 \leq |D(\alpha)| = |a|^{2n-2} \prod_{1 \leq i < j \leq n} |\alpha_i - \alpha_j|^2.$$

2.4. Continued fractions.

A good general reference for this section is chapter 7 of [NiZ].

Given $a_0 \in \mathbb{Z}$ and $a_1, a_2, \dots, a_n \in \mathbb{N}^*$, we define

$$[a_0, a_1, \dots, a_n] := a_0 + \frac{1}{a_1 + \frac{1}{\dots + \frac{1}{a_{n-1} + \frac{1}{a_n}}}}.$$

The above expression is called a *finite continued fraction*. The a_0, \dots, a_n terms are called the *partial quotients*. It is easy to collect terms in the numerator and denominator to write $[a_0, a_1, \dots, a_n] = p_n/q_n$ for some relatively prime $p_n, q_n \in \mathbb{Z}$ with $q_n \geq 1$. One can give a broader definition to finite continued fractions that allows partial quotients to be real numbers, but for our purposes we shall only consider the case where they are positive integers (except for $a_0 \in \mathbb{Z}$).

There is a way to use the Euclidean algorithm to write any rational number as a continued fraction of the form $[a_0, a_1, \dots, a_n]$ for some $n \in \mathbb{N}$. This expansion as a finite continued fraction would be unique if it were not for the fact that $[a_0, a_1, \dots, a_n] = [a_0, a_1, \dots, a_n - 1, 1]$ when $a_n \geq 2$. In §7.2 of [NiZ] we find the following :

Theorem 2.8. *If $[a_0, a_1, \dots, a_j] = [b_0, b_1, \dots, b_n]$ and if $a_j > 1$ and $b_n > 1$, then $j = n$ and $a_i = b_i$ for $i = 0, 1, \dots, n$.*

Example 2.9.

$$[1, 1, 1, 1] = 5/3 \quad , \quad 23/7 = [3, 3, 2] = [3, 3, 1, 1].$$

Given $a_0 \in \mathbb{Z}$ and an infinite sequence of positive integers $a_1, a_2, \dots \in \mathbb{N}^*$, let $p_n/q_n := [a_0, a_1, \dots, a_n]$ with relatively prime $p_n, q_n \in \mathbb{Z}$. We use the expression $[a_0, a_1, \dots]$ to denote

$$[a_0, a_1, \dots] := \lim_{n \rightarrow \infty} \frac{p_n}{q_n}.$$

The assumptions on the partial quotients ensure that the right hand side converges to some irrational real number ξ . An *infinite continued fraction* is such an expression

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \ddots}} = [a_0, a_1, \dots] = \lim_{n \rightarrow \infty} \frac{p_n}{q_n} = \xi.$$

Every $\xi \in \mathbb{R} \setminus \mathbb{Q}$ can be written in a unique way as a infinite continued fraction.

Example 2.10. If we look at the case where all the partial quotients are 1, we have

$$\begin{aligned} [1, 1] &= 1 + \frac{1}{1} = \frac{3}{2}, & [1, 1, 1] &= 1 + \frac{1}{1 + \frac{1}{1}} = \frac{5}{3}, \\ [1, 1, 1, 1] &= \frac{8}{5}, & [1, 1, 1, 1, 1] &= \frac{13}{8}. \end{aligned}$$

Let

$$\theta = \lim_{n \rightarrow \infty} \underbrace{[1, 1, \dots, 1]}_{n \text{ times}} = 1 + \frac{1}{1 + \ddots} = 1 + \frac{1}{\theta}.$$

We get that $\theta^2 = \theta + 1$ and $\theta \geq 1$, so $\theta = (1 + \sqrt{5})/2$.

The sequence of $p_1/q_1, p_2/q_2, \dots$ in this case is $\frac{3}{2}, \frac{5}{3}, \frac{8}{5}, \frac{13}{8}, \dots$ with the Fibonacci numbers in numerators and denominators. Thus when the partial quotients are all 1 the associated infinite continued fraction converges to the Golden Ratio.

The sequence of rational numbers $p_1/q_1, p_2/q_2, \dots$ coming from the continued fraction expansion of $\xi \in \mathbb{R}$ are referred to as the *convergents* of ξ . We henceforth always assume that the pairs $(p_i, q_i) \in \mathbb{Z}^2$ are relatively prime integers with $q_i \geq 1$. When $\xi \notin \mathbb{Q}$ there are infinitely many of them, they are uniquely determined and they satisfy the following equality.

Proposition 2.11. *For all $i \geq 1$, we have*

$$p_i q_{i-1} - p_{i-1} q_i = (-1)^{i-1}.$$

The main interest for the theory of continued fractions in this thesis lies in the following result.

Theorem 2.12. *Let $\xi \in \mathbb{R} \setminus \mathbb{Q}$ and let $\{p_n/q_n\}_{n \geq 0}$ denote the sequence of convergents of ξ . Then for each $n \geq 0$ we have that*

$$\left| \xi - \frac{p_n}{q_n} \right| < \frac{1}{q_n q_{n+1}}.$$

Moreover, if $a/b \in \mathbb{Q}$ satisfies $|b\xi - a| < |q_n \xi - p_n|$ for some $n \geq 0$, then we have $|b| \geq q_{n+1}$.

The last part of the theorem explains why the convergents $\{p_n/q_n\}$ are said to be the best rational approximations for ξ .

A number $\xi \in \mathbb{R} \setminus \mathbb{Q}$ is said to be *badly approximable* if one of the following equivalent conditions holds

- (1) the partial quotients a_0, a_1, \dots of ξ are bounded,
- (2) there exists constants $c_1, c_2 > 0$ such that the denominators of the convergents satisfy

$$c_1 q_n < q_{n+1} < c_2 q_n$$

for all $n \geq 1$,

- (3) there is a constant $\epsilon > 0$ such that for each $a/b \in \mathbb{Q}$ we have

$$\frac{\epsilon}{b^2} < \left| \xi - \frac{a}{b} \right|.$$

It follows from a theorem of Khintchine that the set of badly approximable numbers is of Lebesgue measure 0 (see Chapter 1 of [Bu]). A short argument shows that its cardinality is that of \mathbb{R} . The following general result of Liouville shows that all real quadratic numbers are badly approximable.

Theorem 2.13 (Liouville, 1844). *Suppose that $\alpha \in \mathbb{R}$ is an algebraic number of degree d . There is a constant $c(\alpha) > 0$ such that*

$$\left| \alpha - \frac{p}{q} \right| > \frac{c(\alpha)}{q^d}$$

for every rational p/q distinct from α .

It is an open problem to determine whether or not all algebraic numbers of degree ≥ 2 are badly approximable. However, we have the following result.

Theorem 2.14 (Roth, 1955). *Suppose that $\alpha \in \mathbb{R}$ is algebraic of degree $d \geq 2$. Then for each $\delta > 0$, the inequality*

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{q^{2+\delta}}$$

has only finitely many solutions in rationals p/q .

2.5. Convex set and convex bodies.

A *convex set* in Euclidean space \mathbb{R}^n is a subset \mathcal{C} of \mathbb{R}^n such that for any $x, y \in \mathcal{C}$ and any $t \in [0, 1]$ we have that

$$tx + (1 - t)y \in \mathcal{C}.$$

A *convex body* is a compact convex set which contains a neighborhood of 0 and which is symmetric with respect to 0 in the sense that $-x \in \mathcal{C}$ for each $x \in \mathcal{C}$. Note that the symmetry implies that 0 needs to be in the convex body and that $\mu(\mathcal{C}) > 0$ as it contains a neighborhood of 0.

A *lattice* of \mathbb{R}^n is a sub- \mathbb{Z} -module of \mathbb{R}^n generated over \mathbb{Z} by a basis of \mathbb{R}^n over \mathbb{R} . Lattices can equivalently be defined as discrete subgroups of \mathbb{R}^n of rank n .

If H is a lattice and $\{e_1, \dots, e_n\}$ is a basis of H over \mathbb{Z} , we define the *co-volume* or *determinant* of H as the volume of the parallelepiped supported by the vectors of that basis. It is denoted by $V(H)$ and we have that $V(H) = |\det(e_1, \dots, e_n)|$. It does not depend on the choice of basis for H . This explains why we can write $V(H)$ without any mention to a particular basis.

Theorem 2.15 (Minkowski's first convex body theorem, 1896). *Let H be a lattice of \mathbb{R}^n and let \mathcal{C} be a convex, integrable set, symmetric about 0. If one of the following properties holds*

- (i) $\mu(\mathcal{C}) > 2^n V(H)$,
- (ii) $\mu(\mathcal{C}) \geq 2^n V(H)$ and \mathcal{C} is compact

then $\mathcal{C} \cap H$ contains some nonzero point.

This theorem can be used in various situations to infer the existence of integer solutions to particular inequalities. For example, it gives an alternative proof to the following proposition for which the pigeon-hole principle is usually used.

Proposition 2.16. *For any $\xi \in \mathbb{R}^*$, there exists infinitely many pairs $(p, q) \in \mathbb{Z}^2$ with $q > 0$ such that*

$$(2) \quad |q\xi - p| \leq \frac{1}{q}$$

Proof. Consider the lattice \mathbb{Z}^2 . For $X > 1$ define the convex body

$$\mathcal{C}_X = \{(x, y) \in \mathbb{R}^2; |x| \leq X, |y| \leq X^{-1}\}.$$

Put $S = T^{-1}(\mathcal{C}_X)$ where $T : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ is the linear transformation whose matrix relative to the canonical basis is $\begin{bmatrix} 1 & 0 \\ -\xi & 1 \end{bmatrix}$. We have that S is also a convex body and that

$$S = \{(x, y) \in \mathbb{R}^2; |x| \leq X, |y - \xi x| \leq X^{-1}\}.$$

The volume of S is given by $\mu(S) = \det(T)^{-1} \mu(\mathcal{C}_X) = 1 \cdot 4 = 4$.

As $V(\mathbb{Z}^2) = 1$, we have that $\mu(S) \geq 4 V(\mathbb{Z}^2)$ and so S must contain some nonzero $(p, q) \in \mathbb{Z}^2$. We may assume that $q > 0$ because of the symmetry of S and thus the proposition is proven. \square

2.6. Successive minima of convex bodies.

Fix a lattice H and a convex body \mathcal{C} of \mathbb{R}^n . Note that the convexity of \mathcal{C} implies that for any two $a, b \in \mathbb{R}^+$, we have that $a\mathcal{C} \subseteq b\mathcal{C} \iff a \leq b$.

For all $\lambda \in \mathbb{R}$, we have that $\mu(\lambda\mathcal{C}) = |\lambda|^n \mu(\mathcal{C})$. Since $\mu(\mathcal{C}) > 0$ by the definition of a convex body, there exists $\lambda > 0$ such that $H \cap \lambda\mathcal{C}$ contains a basis of \mathbb{R}^n . In fact, any given point of H is contained in $\lambda\mathcal{C}$ for a sufficiently large value of λ .

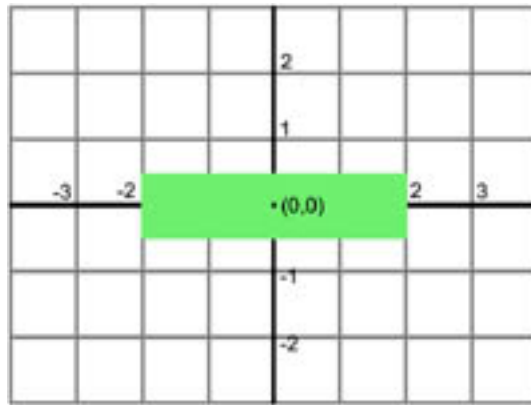
For $1 \leq i \leq n$, we define

$$\lambda_i := \inf_{\lambda > 0} \{ \lambda \ ; \ \lambda\mathcal{C} \text{ contains a set of } i \text{ linearly independent points of } H \}.$$

The compactness of \mathcal{C} implies that those infima are in fact minima. The real number λ_i is called the *i-th minimum of \mathcal{C} with respect to H* . The mention of the lattice H may be omitted when, for example, various convexes are studied and the lattice H is fixed. Since $\lambda_1 \leq \dots \leq \lambda_n$, they are often referred to as the *successive minima of \mathcal{C}* .

To each minimum λ_i can be associated (recursively) an element $\mathbf{g}_i \in \lambda_i\mathcal{C} \cap H$ not lying in the subspace $\langle \mathbf{g}_1, \dots, \mathbf{g}_{i-1} \rangle_{\mathbb{R}}$ of \mathbb{R}^n of dimension $i - 1$ generated by $\mathbf{g}_1, \dots, \mathbf{g}_{i-1}$. The selection of the \mathbf{g}_i 's is not unique. For all $0 < \lambda < \lambda_i$ we have that $\mathbf{g}_i \notin \lambda\mathcal{C}$ by construction.

Example 2.17. For the following convex body and the lattice \mathbb{Z}^2



we have that $\lambda_1 = 0.5$ and $\lambda_2 = 2$. We can choose $\mathbf{g}_1 = (1, 0)$ along with $\mathbf{g}_2 = (0, 1)$ or $\mathbf{g}_2 = (2, 1)$.

The following result generalizes Theorem 2.15. For more details see chapter 4 of [Sc].

Theorem 2.18 (Minkowski's second convex body theorem, 1907). *Let $n \in \mathbb{N}^*$ and let H be a lattice of \mathbb{R}^n . Let \mathcal{C} be a convex body in \mathbb{R}^n and let $\lambda_1, \dots, \lambda_n$ be its successive minima. Then*

$$\frac{2^n}{n!} V(H) \leq \lambda_1 \cdots \lambda_n \mu(\mathcal{C}) \leq 2^n V(H).$$

We say that Minkowski's second convex body theorem generalizes his first convex body theorem because if we assume that $\mu(\mathcal{C}) \geq 2^n V(H)$ and use the above theorem, we get that

$$\lambda_1^n \mu(\mathcal{C}) \leq \lambda_1 \cdots \lambda_n \mu(\mathcal{C}) \leq 2^n V(H) \leq \mu(\mathcal{C}).$$

It follows that $\lambda_1 \leq 1$ and thus \mathcal{C} contains a nonzero point of H as asserted by Theorem 2.15.

2.7. \mathbb{Q} -structures and bilinear forms.

Let E be a real vector space of finite dimension over \mathbb{R} . A \mathbb{Q} -structure is a \mathbb{Q} -subspace of E generated by some basis of E over \mathbb{R} . It is denoted by $E(\mathbb{Q})$ and it depends on the initial choice of basis.

Let E, F be vector spaces over \mathbb{R} of the same dimension $n < \infty$, with respective \mathbb{Q} -structures $E(\mathbb{Q})$ and $F(\mathbb{Q})$. We say that a bilinear form $g : E(\mathbb{Q}) \times F(\mathbb{Q}) \rightarrow \mathbb{Q}$ is *non-degenerate* if one of the following equivalent conditions holds :

1. The matrix $(g(x_i, y_j))$ of g is invertible for some choice of bases $\mathcal{B} = \{x_i\}$ of $E(\mathbb{Q})$ and $\mathcal{B}^* = \{y_j\}$ of $F(\mathbb{Q})$.
2. For each $x \in E(\mathbb{Q})$ with $x \neq 0$, there exists $y \in F(\mathbb{Q})$ such that $g(x, y) \neq 0$.
3. For each $y \in F(\mathbb{Q})$ with $y \neq 0$, there exists $x \in E(\mathbb{Q})$ such that $g(x, y) \neq 0$.

The equivalence of the conditions is established by considering the matrix representation of the bilinear form

$$g(x, y) = [x]_{\mathcal{B}}^T \left(g(x_i, y_j) \right) [y]_{\mathcal{B}^*}$$

For a non-degenerate \mathbb{Q} -bilinear form $g : E(\mathbb{Q}) \times F(\mathbb{Q}) \rightarrow \mathbb{Q}$, we can extend g by linearity into a \mathbb{R} -bilinear non-degenerate application

$$g : E \times F \rightarrow \mathbb{R}$$

also denoted g .

2.8. Duality for convex bodies and lattices.

Let the notation be as in previous section §2.7. Let $\mathcal{C} \subseteq E$ be a convex body. We define the *dual of \mathcal{C} in F* as

$$\mathcal{C}^* = \{y \in F; \quad \forall x \in \mathcal{C} \quad |g(x, y)| \leq 1\}$$

It is also a convex body.

Let $\Lambda \subseteq E(\mathbb{Q})$ be a lattice in E . We define the *dual lattice of Λ with respect to g* as

$$\Lambda^* = \{y \in F; \quad \forall x \in \Lambda \quad |g(x, y)| \in \mathbb{Z}\}$$

Note that $\Lambda^* \subseteq F(\mathbb{Q})$.

The lattice Λ can be written as $\Lambda = \mathbb{Z}x_1 \oplus \cdots \oplus \mathbb{Z}x_n$ for some $x_1, \dots, x_n \in E(\mathbb{Q})$. Moreover, there exists $y_1, \dots, y_n \in F(\mathbb{Q})$ such that $g(x_i, y_j) = \delta_{ij}$ and $\Lambda^* = \mathbb{Z}y_1 \oplus \cdots \oplus \mathbb{Z}y_n$.

We denote by $\lambda_i(\mathcal{C})$ the i -th minimum of \mathcal{C} with respect to Λ and by $\lambda_i(\mathcal{C}^*)$ the i -th minimum of \mathcal{C}^* with respect to Λ^* . When the \mathbb{Q} -structures and the bilinear form g are clear from the context, one often uses the notation $\lambda_i^*(\mathcal{C}) := \lambda_i(\mathcal{C}^*)$ without explicit references to Λ^* or \mathcal{C}^* .

2.9. Duality of the minima.

The next proposition due to Mahler (see [Sc]) relates the successive minima of \mathcal{C} with those of \mathcal{C}^* . It provides information about the integer points in \mathcal{C} from the study of its dual.

Proposition 2.19 (Mahler, 1939). *Let $n \in \mathbb{N}^*$, let Λ be a lattice of \mathbb{R}^n and let \mathcal{C} be a convex body of \mathbb{R}^n . Then we have*

$$\lambda_i(\mathcal{C})\lambda_{n-i+1}(\mathcal{C}^*) \gg \ll 1$$

where the constant implied by the Vinogradov symbol depends only on n .

Note that Theorem 2.18 implies that we have both

$$\lambda_1(\mathcal{C}) \cdots \lambda_n(\mathcal{C}) \gg \ll 1 \quad \text{and} \quad \lambda_1(\mathcal{C}^*) \cdots \lambda_n(\mathcal{C}^*) \gg \ll 1.$$

2.10. A particular application.

We now give a few interesting results for a particular situation that will be encountered in Chapter 3. The use of the following bilinear form g comes from [RW].

Fix $\xi \in \mathbb{R} \setminus \mathbb{Q}$ and $n \in \mathbb{N}^*$. We work in the vector space $\mathbb{R}[T]_{\leq n}$. All results concerning convexes can be translated to $\mathbb{R}[T]_{\leq n}$ if we simply identify \mathbb{R}^{n+1} with $\mathbb{R}[T]_{\leq n}$ in the usual way by associating the point (x_0, \dots, x_n) to the polynomial $x_n T^n + \dots + x_0$. We will use the \mathbb{Q} -structure $\mathbb{Q}[T]_{\leq n}$ and the lattice $\mathbb{Z}[T]_{\leq n}$ in $\mathbb{R}[T]_{\leq n}$. We define g to be the non-degenerate bilinear form $g : \mathbb{R}[T]_{\leq n} \times \mathbb{R}[T]_{\leq n} \rightarrow \mathbb{R}$ given by

$$g(P, Q) := \sum_{k=0}^n (-1)^k P^{(k)}(0) Q^{(n-k)}(0).$$

Let $G(T) = \sum_{k=0}^n (-1)^k P^{(k)}(T) Q^{(n-k)}(T)$. Since $G'(T) \equiv 0$, we have another way to evaluate g as

$$g(P, Q) = \sum_{k=0}^n (-1)^k P^{(k)}(\xi) Q^{(n-k)}(\xi).$$

In this context we have the following result :

Proposition 2.20. *Let $M_0, \dots, M_n \in \mathbb{R}_{>0}$. Define convex bodies of $\mathbb{R}[T]_{\leq n}$ by*

$$\begin{aligned} \mathcal{C} &= \{P \in \mathbb{R}[T]_{\leq n}; \quad |P^{(k)}(\xi)| \leq M_k\}, \\ \mathcal{D} &= \{Q \in \mathbb{R}[T]_{\leq n}; \quad |Q^{(k)}(\xi)| \leq M_{n-k}^{-1}\}, \end{aligned}$$

and denote by \mathcal{C}^* the dual of \mathcal{C} with respect to the bilinear form g defined above. Then we have

$$\frac{1}{n+1} \mathcal{D} \subseteq \mathcal{C}^* \subseteq \mathcal{D}.$$

Proof. For $P \in \mathcal{C}$, $Q \in \mathcal{D}$, the triangle inequality gives that $|g(P, Q)| \leq n+1$. This implies that $\frac{1}{n+1} \mathcal{D} \subseteq \mathcal{C}^*$.

For $k = 0, \dots, n$ we have that

$$\frac{M_k}{k!} (T - \xi)^k \in \mathcal{C}.$$

So for each $Q(T) \in \mathcal{C}^*$ and $k = 0, \dots, n$, we have that $|Q^{(n-k)}(\xi)| \leq M_k^{-1}$. Hence $\mathcal{C}^* \subseteq \mathcal{D}$. \square

It is difficult to work directly with the convex \mathcal{C}^* . Proposition 2.20 suggests that a better approach is to work with the successive minima of \mathcal{D} for which we have

$$\lambda_i(\mathcal{D}) \gg\ll \lambda_i(\mathcal{C}^*) \gg\ll \lambda_{n+2-i}(\mathcal{C}).$$

3. Approximation of a real number using all conjugate roots of a polynomial

3.1. Introduction.

The object of this chapter is to prove the following two theorems.

Theorem A. *Let $\xi \in \mathbb{R} \setminus \mathbb{Q}$ and let $n \in \mathbb{N}^*$. There exist positive constants c_1, c_2 depending only on ξ and n with the following properties.*

(i) *There are infinitely many algebraic numbers α of degree n such that*

$$\max_{\bar{\alpha}} |\xi - \bar{\alpha}| \leq c_1 H(\alpha)^{-2/n}$$

where the maximum is taken over all conjugates $\bar{\alpha}$ of α .

(ii) *There are infinitely many algebraic integers α of degree $n + 1$ such that*

$$\max_{\bar{\alpha} \neq \alpha} |\xi - \bar{\alpha}| \leq c_2 H(\alpha)^{-2/n}$$

where the maximum is taken over all conjugates of $\bar{\alpha}$ of α with $\bar{\alpha} \neq \alpha$.

Badly approximable real numbers are defined in §2.4 and for each such numbers, we have the following refinement of Theorem A.

Theorem B. *Let $\xi \in \mathbb{R} \setminus \mathbb{Q}$ be badly approximable and let $n \in \mathbb{N}^*$. Then there exist positive constants c_1, \dots, c_4 depending only on ξ and n with the following properties. For each real number $X \geq 1$, there is an algebraic number α of degree n satisfying (i) and $c_3 X \leq H(\alpha) \leq c_4 X$. There is also an algebraic integer α of degree $n + 1$ satisfying (ii) and $c_3 X \leq H(\alpha) \leq c_4 X$.*

We start by fixing a $\xi \in \mathbb{R} \setminus \mathbb{Q}$ and a positive integer $n \geq 1$. We construct a sequence of polynomials of $\mathbb{Z}[T]$ whose derivatives at ξ satisfy certain conditions (Proposition 3.1). Then we use them to produce a new sequence of irreducible polynomials satisfying specific inhomogeneous Diophantine properties (Proposition 3.2). With Proposition 3.3 we conclude that their roots satisfy Theorem A. Theorem B follows from an observation concerning badly approximable numbers.

We also prove that both results are optimal up to the value of the implied constants c_1, c_2 . Finally, in the last part of this chapter, we provide an alternate proof to a crucial intermediate result (Proposition 3.1) using an argument based on the duality for convex bodies.

3.2. Construction of polynomials.

Fix an irrational real number $\xi \in \mathbb{R} \setminus \mathbb{Q}$ and a positive integer $n \geq 1$. For each integer $q \geq 1$, we denote by \mathcal{C}_q the convex body of $\mathbb{R}[T]_{\leq n}$ which consists of all polynomials $P \in \mathbb{R}[T]_{\leq n}$ satisfying

$$|P^{[k]}(\xi)| \leq q^{2k-n} \quad (0 \leq k \leq n)$$

where $P^{[k]}(\xi) = P^{(k)}(\xi)/k!$ denotes the k -th divided derivative of P at ξ (the coefficient of $(T - \xi)^k$ in the Taylor expansion of P at ξ). We first prove :

Proposition 3.1. *Let q be the denominator of a convergent of ξ . Then the last minimum of \mathcal{C}_q with respect to the lattice $\mathbb{Z}[T]_{\leq n}$ is $\leq 2^n$, and its first minimum is $\geq \left(2^{n^2}(n+1)!\right)^{-1}$. Moreover, the convex body $2^n \mathcal{C}_q$ contains a basis of $\mathbb{Z}[T]_{\leq n}$ over \mathbb{Z} .*

Proof. Put $L_1 = qT - p$ where p/q denotes a convergent of ξ with denominator q . If $q > 1$, we also define $L_0 = q_0T - p_0$ where p_0/q_0 is the previous convergent of ξ (in reduced form). If $q = 1$, we simply take $L_0 = 1$. The theory of continued fractions tells us that these linear forms satisfy

$$(3) \quad |L_i(\xi)| \leq q^{-1} \quad \text{and} \quad |L'_i(\xi)| \leq q$$

for $i = 0, 1$, and moreover that their determinant (or Wronskian) is ± 1 (see Proposition 2.11). The latter fact means that $\{L_0, L_1\}$ spans $\mathbb{Z}[T]_{\leq 1}$ over \mathbb{Z} . Therefore the products $P_j = L_0^j L_1^{n-j}$ ($0 \leq j \leq n$) span $\mathbb{Z}[T]_{\leq n}$ over \mathbb{Z} and, since the rank of $\mathbb{Z}[T]_{\leq n}$ is $n+1$, they form in fact a basis of $\mathbb{Z}[T]_{\leq n}$ over \mathbb{Z} . Using (3), we also find that

$$|P_j^{[k]}(\xi)| \leq \binom{n}{k} q^{2k-n} \leq 2^n q^{2k-n} \quad (0 \leq j, k \leq n).$$

Thus $\{P_0, \dots, P_n\}$ is a basis of $\mathbb{Z}[T]_{\leq n}$ contained in $2^n \mathcal{C}_q$. This proves the last assertion of the proposition as well as the fact that the last minimum of \mathcal{C}_q is $\leq 2^n$.

Identify $\mathbb{R}[T]_{\leq n}$ with \mathbb{R}^{n+1} under the map which sends a polynomial $a_0 + a_1T + \dots + a_nT^n$ to the point (a_0, a_1, \dots, a_n) . Then the linear map $\theta : \mathbb{R}[T]_{\leq n} \rightarrow \mathbb{R}^{n+1}$ given by $\theta(P) =$

$(P(\xi), P^{[1]}(\xi), \dots, P^{[n]}(\xi))$ has determinant 1 and so \mathcal{C}_q has volume $\prod_{k=0}^n (2q^{2k-n}) = 2^{n+1}$. Since the lattice $\mathbb{Z}[T]_{\leq n}$ has co-volume 1 (it is identified with \mathbb{Z}^{n+1}), it follows from Minkowski's second convex body theorem that the successive minima $\lambda_1, \dots, \lambda_{n+1}$ of \mathcal{C}_q with respect to $\mathbb{Z}[T]_{\leq n}$ satisfy $((n+1)!)^{-1} \leq \lambda_1 \cdots \lambda_{n+1} \leq 1$. Since $\lambda_2 \leq \dots \leq \lambda_{n+1} \leq 2^n$, this implies that $\lambda_1 \geq \left(2^{n^2}(n+1)!\right)^{-1}$. \square

The construction of polynomials given by the next proposition uses only the last assertion of Proposition 3.1.

Proposition 3.2. *Let q be the denominator of a convergent of ξ . There exist an irreducible polynomial $P(T) \in \mathbb{Z}[T]$ of degree n and an irreducible monic polynomial $Q(T) \in \mathbb{Z}[T]$ of degree $n+1$ satisfying*

$$c_5 q^{2k-n} \leq |P^{[k]}(\xi)|, |Q^{[k]}(\xi)| \leq 3c_5 q^{2k-n} \quad (0 \leq k \leq n)$$

where $c_5 = (n+1)2^{n+1}$.

Proof. The last assertion of Proposition 3.1 tells us the existence of a basis $\{P_0, \dots, P_n\}$ of $\mathbb{Z}[T]_{\leq n}$ satisfying

$$(4) \quad |P_j^{[k]}(\xi)| \leq 2^n q^{2k-n} \quad (0 \leq j, k \leq n).$$

Since $\{P_0, \dots, P_n\}$ is a basis of $\mathbb{Z}[T]_{\leq n}$ over \mathbb{Z} , we can write $T^n + 2 = \sum_{j=0}^n b_j P_j(T)$ for some $b_0, \dots, b_n \in \mathbb{Z}$. Consider the polynomial

$$R(T) = 2c_5 \sum_{k=0}^n q^{2k-n} (T - \xi)^k$$

where $c_5 = (n+1)2^{n+1}$. Since $\{P_0, \dots, P_n\}$ is also a basis of $\mathbb{R}[T]_{\leq n}$ over \mathbb{R} , we can also write $R(T) = \sum_{j=0}^n \theta_j P_j(T)$ for some $\theta_0, \dots, \theta_n \in \mathbb{R}$. Choose integers a_0, \dots, a_n such that $a_j \equiv b_j \pmod{4}$ and $|a_j - \theta_j| \leq 2$ for $j = 0, \dots, n$, and define $P(T) = \sum_{j=0}^n a_j P_j(T)$.

By construction $P(T)$ belongs to $\mathbb{Z}[T]_{\leq n}$ and is congruent to $T^n + 2$ modulo 4. Thus it is a polynomial of degree n that is irreducible over \mathbb{Q} by virtue of Eisenstein's criterion (for the prime 2). Since $P(T) - R(T) = \sum_{j=0}^n (a_j - \theta_j) P_j(T)$, we deduce from (4) that

$$|P^{[k]}(\xi) - R^{[k]}(\xi)| \leq \sum_{j=0}^n |a_j - \theta_j| |P_j^{[k]}(\xi)| \leq c_5 q^{2k-n} \quad (0 \leq k \leq n).$$

Since $R^{[k]}(\xi) = 2c_5 q^{2k-n}$, it follows that $c_5 q^{2k-n} \leq |P^{[k]}(\xi)| \leq 3c_5 q^{2k-n}$ for $k = 0, \dots, n$, as required.

The construction of $Q(T)$ is similar. Write

$$T^{n+1} + 2 = T^{n+1} + \sum_{j=0}^n b'_j P_j(T) \quad \text{and} \quad (T - \xi)^{n+1} + R(T) = T^{n+1} + \sum_{j=0}^n \theta'_j P_j(T),$$

with $b'_0, \dots, b'_n \in \mathbb{Z}$ and $\theta'_0, \dots, \theta'_n \in \mathbb{R}$. Choose integers a'_0, \dots, a'_n such that $a'_j \equiv b'_j \pmod{4}$ and $|a'_j - \theta'_j| \leq 2$ for $j = 0, \dots, n$. Then the polynomial

$$Q(T) = T^{n+1} + \sum_{j=0}^n a'_j P_j(T) \in \mathbb{Z}[T]$$

is irreducible (by virtue of Eisenstein's criterion for 2), monic of degree $n + 1$, and it satisfies also $|Q^{[k]}(\xi) - R^{[k]}(\xi)| \leq c_5 q^{2k-n}$ for $k = 0, \dots, n$. \square

3.3. Proof of the theorems.

Theorems A and B will be proven by combining Proposition 3.2 with the following result.

Proposition 3.3. *Let $\xi \in \mathbb{R}$, let $n \in \mathbb{N}^*$, let $\delta > 0$ and let \mathcal{P} be a subset of $\mathbb{Z}[T]$. Suppose that the elements of \mathcal{P} are either polynomials of degree n or monic polynomials of degree $n + 1$. Then the following conditions are equivalent :*

- (i) *There exists a constant $c_6 > 0$ such that $|P^{[k]}(\xi)| \leq c_6 H(P)^{1-(n-k)\delta}$ for each $P \in \mathcal{P}$ and each $k = 0, 1, \dots, n$.*
- (ii) *There exists a constant $c_7 > 0$ such that $|\xi - \alpha| \leq c_7 H(P)^{-\delta}$ for each $P \in \mathcal{P}$ and for n of the roots α of P , counting multiplicity.*

Proof. Fix $P \in \mathcal{P}$ and write it in the form

$$P(T) = a_0(T - \alpha_1) \cdots (T - \alpha_m)$$

where $m = \deg P$ and $\alpha_1, \dots, \alpha_m$ are the roots of P ordered so that $|\xi - \alpha_1| \leq \dots \leq |\xi - \alpha_m|$. We put $\varepsilon = H(P)^{-\delta}$ and consider the polynomial

$$R(T) = P(\varepsilon T + \xi) = a_0 \varepsilon^m \prod_{k=1}^m (T + \varepsilon^{-1}(\xi - \alpha_k)).$$

The height of R is

$$H(R) = \max_{0 \leq k \leq m} |R^{[k]}(0)| = \max_{0 \leq k \leq m} |P^{[k]}(\xi)| \varepsilon^k,$$

and its Mahler measure is

$$M(R) = |a_0| \varepsilon^m \prod_{k=1}^m \max \{1, \varepsilon^{-1} |\xi - \alpha_k|\} = |a_0| \prod_{k=1}^m \max \{\varepsilon, |\xi - \alpha_k|\}.$$

For convenience, we also define

$$L = \begin{cases} |a_0| & \text{if } m = n \\ \max \{\varepsilon, |\xi - \alpha_m|\} & \text{if } m = n + 1 \end{cases}$$

so that the formula for $M(R)$ becomes

$$M(R) = L \prod_{k=1}^n \max \{\varepsilon, |\xi - \alpha_k|\}$$

(recall that $a_0 = 1$ when $m = n + 1$). Our argument below is based on the standard inequalities relating these notions of heights, namely

$$M(R) \leq (m + 1)H(R) \quad \text{and} \quad H(R) \leq 2^m M(R).$$

If condition (ii) holds, we find that $M(R) \leq \max\{1, c_7^n\} \varepsilon^n L$. We also have $L \ll H(P)$ since $|a_0| \leq H(P)$ and since $|\xi - \alpha| \ll \max\{1, |\alpha|\} \ll H(P)$ for any root α of P . Then, for each $k = 0, \dots, n$, we obtain

$$|P^{[k]}(\xi)| \ll \varepsilon^{-k} H(R) \ll \varepsilon^{-k} M(R) \ll \varepsilon^{n-k} H(P)$$

which shows that condition (i) holds.

Conversely, assume that condition (i) holds. In this case we find that $H(R) \leq c_6 \varepsilon^n H(P)$. We claim that $H(P) \ll L$. If we take this for granted, we deduce that

$$L \varepsilon^{n-1} |\xi - \alpha_n| \leq M(R) \ll H(R) \ll \varepsilon^n L$$

which implies that condition (ii) holds.

To prove the claim, we observe that

$$H(P) \gg \ll H(P(T + \xi)) = \max_{0 \leq k \leq m} |P^{[k]}(\xi)|.$$

By hypothesis, we have $|P^{[k]}(\xi)| \leq c_6 H(P)^{1-\delta}$ for $k = 0, \dots, n - 1$ and we also have $|P^{[m]}(\xi)| = 1$ if $m = n + 1$. Finally, we have $|P^{[n]}(\xi)| = |a_0|$ if $m = n$, and $|P^{[n]}(\xi)| = |\sum_{k=1}^m (\xi - \alpha_k)| \leq m |\xi - \alpha_m|$ if $m = n + 1$, showing that $|P^{[n]}(\xi)| \ll L$. All this implies that

$$H(P) \ll \max\{1, L\}.$$

If $L \geq 1$, we deduce that $H(P) \ll L$ as requested. If $L \leq 1$, then this gives $H(P) \ll 1$ and we find $L \geq \epsilon = H(P)^{-\delta} \gg 1$, thus $H(P) \ll L$ is again satisfied. \square

Proof of Theorems A and B. We simply prove Part (ii) of Theorems A and B since the proof of Part (i) is similar and slightly easier.

For each denominator q of a convergent of ξ , Proposition 3.2 shows the existence of an irreducible monic polynomial $Q \in \mathbb{Z}[T]$ of degree $n + 1$ satisfying $H(Q) \gg\ll q^n$ and

$$|Q^{[k]}(\xi)| \leq c_6 H(Q)^{(2k-n)/n} = c_6 H(Q)^{1-(n-k)(2/n)}, \quad (0 \leq k \leq n)$$

for some constant $c_6 = c_6(\xi, n)$. The family \mathcal{P} of these polynomials satisfies the condition (i) of Proposition 3.3 for the choice $\delta = 2/n$, and so it satisfies also the condition (ii) of the same proposition for the same value of δ and for some constant c_7 . For each $Q \in \mathcal{P}$, choose a root α of Q for which $|\xi - \alpha|$ is maximal. Since Q is irreducible, this root α is an algebraic integer of degree $n + 1$ and height $H(\alpha) = H(Q)$, whose conjugates $\bar{\alpha}$ over \mathbb{Q} are the $n + 1$ distinct roots of Q . Therefore, we get $\max_{\bar{\alpha} \neq \alpha} |\xi - \bar{\alpha}| \leq c_7 H(\alpha)^{-2/n}$. This proves Part (ii) of Theorem A since we find infinitely many such numbers α by varying Q . \square

If ξ is badly approximable, the ratios of the denominators of consecutive convergents of ξ are bounded. Thus, for each $X \geq 1$, there exists such a denominator q with $q \gg\ll X^{1/n}$, and so there exists $Q \in \mathcal{P}$ with $H(Q) \gg\ll X$. Consequently, the root α of Q that we chose above satisfies $H(\alpha) \gg\ll X$ and this proves Part (ii) of Theorem B.

3.4. Optimality of the exponents of approximation.

Let $\xi \in \mathbb{R} \setminus \mathbb{Q}$ and let $n \in \mathbb{N}^*$. If $n = 1$, the result is optimal for any badly approximable ξ (see §2.4).

If $n \geq 2$, we have that for any algebraic number α of degree n with conjugates $\alpha_1, \dots, \alpha_n$, the discriminant $D(\alpha)$ of α satisfies

$$|D(\alpha)| \leq H(\alpha)^{2(n-1)} \prod_{1 \leq j < k \leq n} |\alpha_j - \alpha_k|^2 \leq H(\alpha)^{2(n-1)} \left(2 \max_{1 \leq i \leq n} |\xi - \alpha_i| \right)^{n(n-1)},$$

upon noting that, for any j, k , we have that $|\alpha_j - \alpha_k| \leq |\alpha_j - \xi| + |\alpha_k - \xi| \leq 2 \max |\alpha_i - \xi|$.

The discriminant $D(\alpha)$ is a non-zero integer, its absolute value is ≥ 1 (see Proposition 2.7), and thus we deduce that

$$\max_{1 \leq i \leq n} |\xi - \alpha_i| \geq \frac{1}{2} H(\alpha)^{-2/n}$$

(compare with §5 of [Wi]). This implies that part (i) of Theorem A is optimal up to the value of the implied constant.

Similarly, the result in part (ii) of Theorem A is optimal up to the value of the implied constant when ξ is a quadratic irrational number. To prove this, suppose that an algebraic integer α of degree $n+1$ has conjugates $\alpha_1, \dots, \alpha_{n+1}$ distinct from ξ with the first n satisfying

$$(5) \quad \max_{1 \leq i \leq n} |\xi - \alpha_i| \leq 1$$

Let $Q(T) \in \mathbb{Z}[T]$ be the irreducible polynomial of ξ over \mathbb{Z} . Since α is an algebraic integer, the product $Q(\alpha_1) \cdots Q(\alpha_{n+1})$ is an ordinary integer (see Proposition 2.5) and since it is non-zero (because ξ is not a conjugate of α), we deduce that

$$1 \leq \prod_{i=1}^{n+1} |Q(\alpha_i)|.$$

For each $i = 1, \dots, n$, we have $|Q(\alpha_i)| \ll |\xi - \alpha_i|$ since ξ is a root of Q and $|\alpha_i| \ll 1$ because of (5). We also have $|Q(\alpha_{n+1})| \ll \max\{1, |\alpha_{n+1}|\}^2$ since Q has degree 2. This gives

$$1 \ll H(\alpha)^2 \prod_{i=1}^n |\xi - \alpha_i|$$

and consequently $\max_{1 \leq i \leq n} |\xi - \alpha_i| \gg H(\alpha)^{-2/n}$.

Remark. The case where $\xi \in \mathbb{Q}$ is not interesting as it leads to much weaker estimates. In this case, one finds that, for each algebraic number α of degree n with $\alpha \neq \xi$, one has $\max_{\bar{\alpha}} |\xi - \bar{\alpha}| \gg H(\alpha)^{-1/n}$, and that, for each algebraic integer α of degree $n+1$ with $\alpha \neq \xi$, one has $\max_{\bar{\alpha} \neq \alpha} |\xi - \bar{\alpha}| \gg H(\alpha)^{-1/n}$.

3.5. A different approach to Proposition 3.1.

In the proof of Proposition 3.1 we constructed explicitly a basis of solutions by using the consecutive convergents of ξ . We will now show a very similar result using an argument involving duality of convex bodies. To this end, we first prove several technical lemmas. Recall for any ring R , we denote by $R[T]_{\leq n}$ the set of polynomials of $R[T]$ of degree $\leq n$.

Lemma 3.4. *Let $\xi \in \mathbb{R}$ and $n \in \mathbb{N}^*$. Suppose that a polynomial $Q \in \mathbb{R}[T]_{\leq n}$ factors as a product $Q(T) = L(T)^r M(T)$ for some linear form $L(T) \in \mathbb{R}[T]_{\leq 1}$, some integer $r \in \{0, \dots, n\}$ and some $M(T) \in \mathbb{R}[T]_{\leq n-r}$. Write $|L'(\xi)| = |L'(0)| = X$ for convenience and suppose that for some $0 < c < 1$ we have that*

$$|L(\xi)| \leq X^{-1} \quad \text{and} \quad |Q^{(k)}(\xi)| \leq cX^{2k-n} \quad \text{for all } k = 0, \dots, n.$$

Then we have that

$$(6) \quad |M^{(t)}(\xi)| \ll cX^{2t-(n-r)} \quad \text{for all } t = 0, \dots, n-r$$

where the symbol \ll involves a constant depending only on n .

Proof. We prove (6) by descending induction on t , starting with $t = n-r$. Here, the constants implied in the Vinogradov symbols depend only on n . Looking at $Q^{(n)}(\xi)$, we find

$$\begin{aligned} |L'(\xi)|^r |M^{(n-r)}(\xi)| &\ll |Q^{(n)}(\xi)| \ll cX^n \\ \Rightarrow |M^{(n-r)}(\xi)| &\ll cX^{n-r}. \end{aligned}$$

Now assume that (6) holds for each $t \in \{N+1, \dots, n-r\}$ where N is some integer with $0 \leq N \leq n-r$. We find

$$Q^{(r+N)}(\xi) = \left(\sum_{s=0}^{r-1} a_s L(\xi)^{r-s} L'(\xi)^s M^{(r+N-s)}(\xi) \right) + a_r L'(\xi)^r M^{(N)}(\xi)$$

for some positive integers a_0, \dots, a_r depending only on r, n and N . For all terms in the sum, we use the upper bound (6) provided by the induction hypothesis and the fact that $M^{(t)}(\xi) = 0$ when $t > n-r$ since $\deg(M) \leq n-r$. For $s = 0, \dots, r-1$ this gives

$$\begin{aligned} |L(\xi)^{r-s} L'(\xi)^s M^{(r+N-s)}(\xi)| &\ll X^{-(r-s)} X^s cX^{2(r+N-s)-n+r} \\ &\ll cX^{2(r+N)-n} \end{aligned}$$

As $|Q^{(r+N)}(\xi)| \leq cX^{2(r+N)-n}$ by hypothesis, we deduce that

$$\begin{aligned} |L'(\xi)^r M^{(N)}(\xi)| &\ll cX^{2(r+N)-n} \\ \Rightarrow |M^{(N)}(\xi)| &\ll cX^{2N-n+r} \end{aligned}$$

which completes the induction step. \square

Corollary 3.5. *Let $\xi \in \mathbb{R}, n \in \mathbb{N}^*$ and $L(T) = qT - p \in \mathbb{Z}[T]$ be such that $|L(\xi)| < q^{-1}$ and $\gcd(p, q) = 1$. There exists a constant $c = c(n) > 0$ with the following property. Any polynomial $Q(T) \in \mathbb{Z}[T]_{\leq n}$ which satisfies*

$$(7) \quad |Q^{(k)}(\xi)| \leq cq^{2k-n} \quad \forall k = 0, \dots, n$$

has the form $Q(T) = a_0 L(T)^n$ for some $a_0 \in \mathbb{Z}$.

Proof. Suppose that a polynomial $Q(T) \in \mathbb{Z}[T]_{\leq n}$ satisfies (7) for some constant c with $0 < c < 1$. Let $r \geq 0$ be the largest integer such that L^r divides Q in $\mathbb{Q}[T]$. Write $Q = L^r M$, and put $X = |q|$. By Gauss' lemma we have that $M(T) \in \mathbb{Z}[T]$ since $\gcd(p, q) = 1$. If $r = n$ we are done, so assume that $r < n$. We have that $M(p/q) \neq 0$ by the maximality of r .

By the previous Lemma 3.4, we have that $|M^{(t)}(\xi)| \leq c_1 c X^{2t-(n-r)}$ for each $t = 0, \dots, n-r$ and some constant $c_1 = c_1(n) > 0$. Since $q^{n-r} M(p/q) \in \mathbb{Z} \setminus \{0\}$, we have

$$\begin{aligned} 1 \leq |q^{n-r} M(p/q)| &= \left| q^{n-r} \left(\sum_{t=0}^{n-r} \frac{M^{(t)}(\xi)}{t!} \left(\frac{p}{q} - \xi \right)^t \right) \right| \\ &= \left| \sum_{t=0}^{n-r} \frac{M^{(t)}(\xi)}{t!} q^{n-r-t} (p - q\xi)^t \right| \\ &= \left| \sum_{t=0}^{n-r} \frac{(-1)^t}{t!} M^{(t)}(\xi) L'(\xi)^{n-r-t} L(\xi)^t \right| \\ &\leq c_1 c \sum_{t=0}^{n-r} X^{2t-(n-r)} X^{n-r-t} X^{-t} \leq (n+1)c_1 c. \end{aligned}$$

This is impossible if $c < ((n+1)c_1)^{-1}$. \square

Proposition 3.6. *Let $\xi \in \mathbb{R}, n \in \mathbb{N}^*$. For $c > 0$ sufficiently small, there are arbitrarily large values of $X \in \mathbb{R}^+$ such that*

$$(8) \quad |Q^{(k)}(\xi)| \leq cX^{2k-n} \quad (k = 0, \dots, n)$$

has no nonzero solution $Q(T) \in \mathbb{Z}[T]_{\leq n}$.

Proof. Suppose that this proposition does not hold. Then for all $c > 0$ there exists X_0 such that for all $X \geq X_0$ we have a nonzero $Q(T) \in \mathbb{Z}[T]_{\leq n}$ satisfying (8). Choose c to be the minimum between $\frac{1}{2}$ and the constant $c(n) > 0$ provided by Corollary 3.5. We proceed to the construction of a sequence of best approximations. Our construction here is inspired by

Davenport and Schmidt's method in [DS]. Their method shall be followed more closely in §5.3. Refer to that section for more information.

Define

$$E(X) = \left\{ Q \in \mathbb{Z}[T]_{\leq n} \setminus \{0\} \mid |Q^{(k)}(\xi)| \leq cX^{2k-n} \quad (k = 0, \dots, n) \right\}$$

and for $Q \in E(X)$, define

$$W(Q) = \sup_{X \in \mathbb{R}^+} \{X \mid Q \in E(X)\}.$$

For any X we have that $E(X)$ is finite. Since $E(X) \subseteq \mathbb{Z}[T]_{\leq n}$ and since $\xi \notin \mathbb{Q}$, we have that $W(Q) < \infty$ for each $Q \in E(X)$. Therefore the large inequality in the definition of $E(X)$ ensures that the supremum in the definition of $W(Q)$ is achieved, so $Q \in E(W(Q))$.

For the given choice of X_0 mentioned above, choose $Q_0 \in E(X_0)$ to be such that

$$W(Q_0) = \max_{Q \in E(X_0)} W(Q).$$

The choice of Q_0 is not unique, but it is of no consequence. We say that Q_0 is the *best approximation* available at X_0 .

Let $X_1 > X_0$ be the smallest positive real number such that there exists $Q \in E(X_1)$ with $W(Q) > W(Q_0)$. Choose $Q_1 \in E(X_1)$ to be such that

$$W(Q_1) = \max_{Q \in E(X_1)} W(Q).$$

Repeat the process to have $X_2 > X_1$ and some Q_2 defined in an analogous way. Continuing indefinitely, we get a sequence $\{(X_i, Q_i)\}_{i \geq 0}$ such that

- (i) $X_0 < X_1 < \dots$
- (ii) $W(Q_0) < W(Q_1) < \dots$
- (iii) If $X_i \leq X < X_{i+1}$ and $Q \in E(X)$, then $W(Q) \leq W(Q_i)$.

Note that this construction of the sequence of best approximations does not depend on our initial hypothesis that Proposition 3.6 does not hold.

The hypothesis that $E(X)$ is not empty for $X \geq X_0$, in conjunction with the above property (iii), implies that for all $X \in [X_i, X_{i+1})$ there is a $Q \in E(X)$ with $W(Q) \leq W(Q_i)$. Thus, for any index $i \geq 0$ and for all $\epsilon > 0$ sufficiently small, we have that $Q_i \in E(X_{i+1} - \epsilon)$

and so

$$\left| Q_i^{(k)}(\xi) \right| \leq c(X_{i+1} - \epsilon)^{2k-n} \quad (k = 0, \dots, n).$$

Hence for all $i \geq 0$ we have that

$$\left| Q_i^{(k)}(\xi) \right| \leq cX_{i+1}^{2k-n} \quad (k = 0, \dots, n)$$

and thus, as $Q_i \in E(X_i)$, we have that

$$\left| Q_i^{(k)}(\xi) \right| \leq \max \{ cX_i^{2k-n}, cX_{i+1}^{2k-n} \} \quad (k = 0, \dots, n).$$

Note that by the maximality condition involved in the construction of the Q_i , we have that they are all of content 1 and that Q_i and Q_{i+1} are linearly independent.

From the theory of continued fractions (see §2.4), there are infinitely many convergents p/q of ξ such that $|q\xi - p| < q^{-1}$. Choose a convergent p/q with $q \geq X_0$, and choose $i \geq 0$ such that $X_i \leq q < X_{i+1}$. We find that

$$\begin{aligned} X_i^{2k-n} &\leq q^{2k-n} && \text{if } 2k - n \geq 0 \\ X_{i+1}^{2k-n} &\leq q^{2k-n} && \text{if } 2k - n \leq 0 \end{aligned}$$

and hence $\left| Q_i^{(k)}(\xi) \right| \leq cq^{2k-n}$ for $k = 0, \dots, n$. Let $L(T) = qT - p$. We have that $|L(\xi)| \leq q^{-1}$ and that L has content 1.

Applying Corollary 3.5 to L and Q , we get that $Q_i(\xi) = a_0(qT - p)^n$ with $a_0 \in \mathbb{Z}$. It then follows that $\left| Q_i^{(n)}(\xi) \right| = |a_0|n!q^n$, in contradiction with the assumption that $\left| Q_i^{(n)}(\xi) \right| \leq cq^{2n-n} < q^n$. This concludes the proof.

Remark. The presence of the convergents of ξ are the essential ingredient to this proof by contradiction. When ξ is badly approximable so that the convergents $(p_i/q_i)_{i \geq 0}$ are such that $q_i \gg \ll q_{i+1}$, the proof can be adapted to show that (8) admits no nonzero solution for any sufficiently large $X \in \mathbb{R}^+$, as asserted by Theorem B.

□

Proposition 3.7. *Let $\xi \in \mathbb{R}$, $n \in \mathbb{N}$ and let $c, X \in \mathbb{R}^+$. Let \mathcal{C}_X be the convex body defined by*

$$\mathcal{C}_X = \left\{ P \in \mathbb{R}[T]_{\leq n} \quad ; \quad |P^{(k)}(\xi)| \leq cX^{2k-n} \right\}.$$

If c is sufficiently large, then there are arbitrarily large values of $X \in \mathbb{R}$ such that \mathcal{C}_X contains $n + 1$ points of $\mathbb{Z}[T]_{\leq n}$ that are linearly independent over \mathbb{R} .

Proof. Consider the lattice $\mathbb{Z}[T]_{\leq n}$ in $\mathbb{R}[T]_{\leq n}$ and the bilinear form $g : \mathbb{R}[T]_{\leq n} \times \mathbb{R}[T]_{\leq n} \rightarrow \mathbb{R}$ given by (see §2.10)

$$g(P, Q) = \sum_{k=0}^n (-1)^k P^{(k)}(\xi) Q^{(n-k)}(\xi).$$

Let

$$\mathcal{D}_X = \{Q \in \mathbb{R}[T]_{\leq n}; \quad |Q^{(k)}(\xi)| \leq c^{-1} X^{-(2(n-k)-n)} = c^{-1} X^{2k-n}\}.$$

By Proposition 3.6, for c sufficiently large there are arbitrarily large values of $X \in \mathbb{R}^+$ such that $\mathcal{D}_X \cap \mathbb{Z}[T]_{\leq n} = \{0\}$. Moreover, from Proposition 2.20 we have that

$$\frac{1}{n+1} \mathcal{D}_X \subseteq \mathcal{C}_X^* \subseteq \mathcal{D}_X$$

so for those values of X we have that $\mathcal{C}_X^* \cap \mathbb{Z}[T]_{\leq n} = \{0\}$. Proposition 2.19 connects the first minimum of \mathcal{C}_X^* with the last minimum of \mathcal{C}_X . So there is a constant $c_0 = c_0(n)$ such that when $\lambda_1(\mathcal{C}_X^*) > 1$, we have that $\lambda_{n+1}(c_0 \mathcal{C}_X) < 1$. Thus if we choose c in the definition of \mathcal{C}_X to be large enough, there are arbitrarily large values of $X \in \mathbb{R}^+$ such that \mathcal{C}_X contains $n+1$ points of $\mathbb{Z}[T]_{\leq n}$ that are linearly independent over \mathbb{R} . \square

4. Preliminaries and basic results on number fields

4.1. Number fields, ring of integers and discriminant.

A *number field* is a field $K \subseteq \mathbb{C}$ of finite degree over \mathbb{Q} .

Let $n = [K : \mathbb{Q}]$ be the degree of K over \mathbb{Q} . Since \mathbb{Q} is of characteristic 0, we have n different isomorphisms of K into \mathbb{C} fixing \mathbb{Q} . Let $\sigma_1, \dots, \sigma_n$ be those \mathbb{Q} -isomorphisms. For each $x \in K$, we define

$$\begin{aligned} \text{Tr}(x) &:= \sum_{i=1}^n \sigma_i(x) \in \mathbb{Q}, & \text{called the } \textit{trace} \text{ of } x, \\ N(x) &:= \prod_{i=1}^n \sigma_i(x) \in \mathbb{Q}, & \text{called the } \textit{norm} \text{ of } x. \end{aligned}$$

Example 4.1. Let K be a number field of degree 2. Then there exists a nonzero square-free integer $d \in \mathbb{Z}$ such that $K = \mathbb{Q}(\sqrt{d})$. The two \mathbb{Q} -isomorphisms of K into \mathbb{C} are

$$\begin{array}{ccc} \text{id} : & K & \hookrightarrow \mathbb{C} \\ & a + b\sqrt{d} & \mapsto a + b\sqrt{d} \end{array} \quad \text{and} \quad \begin{array}{ccc} \sigma : & K & \hookrightarrow \mathbb{C} \\ & a + b\sqrt{d} & \mapsto a - b\sqrt{d} \end{array}$$

We find that $\text{Tr}(a + b\sqrt{d}) = 2a$ and $N(a + b\sqrt{d}) = a^2 - db^2$.

The *ring of integers* of K , denoted by \mathcal{O}_K , is the set of $x \in K$ such that x is the root of a monic polynomial with coefficients in \mathbb{Z} . As the name suggests, \mathcal{O}_K is a subring of K . It is a free \mathbb{Z} -module of rank $n = [K : \mathbb{Q}]$.

The *discriminant* of K is defined to be $D_K := \det(\sigma_i(\omega_j))^2$ where $\mathcal{B} = (\omega_1, \dots, \omega_n)$ is any basis of \mathcal{O}_K over \mathbb{Z} . It can be shown that it is independent of the choice of the basis \mathcal{B} . Moreover, we have that $D_K = \det(\text{Tr}(\omega_i \omega_j)) \in \mathbb{Z}$.

Example 4.2. Let $d \in \mathbb{Z}$ be square-free and $K = \mathbb{Q}(\sqrt{d})$ be a quadratic number field. Then

$$\mathcal{B} = \begin{cases} (1, \sqrt{d}) & \text{if } d \not\equiv 1 \pmod{4} \\ (1, \frac{1+\sqrt{d}}{2}) & \text{otherwise} \end{cases}$$

is a basis of \mathcal{O}_K over \mathbb{Z} . The discriminant of K is

$$D_K = \begin{cases} \det \begin{bmatrix} 2 & 0 \\ 0 & 2d \end{bmatrix} = 4d & \text{if } d \not\equiv 1 \pmod{4} \\ \det \begin{bmatrix} 2 & 1 \\ 1 & \frac{1+d}{2} \end{bmatrix} = d & \text{otherwise.} \end{cases}$$

Number fields of degree 2 over \mathbb{Q} are said to be *quadratic*. As mentioned in Example 4.1, they are all of the form $\mathbb{Q}(\sqrt{d})$ for some nonzero square-free $d \in \mathbb{Z}$. If $d < 0$, then $K = \mathbb{Q}(\sqrt{d})$ is said to be an *imaginary quadratic field*. In such a case, we have that \mathcal{O}_K is a discrete subgroup of \mathbb{C} of rank 2. If $d > 0$, we say that $\mathbb{Q}(\sqrt{d})$ is a *real quadratic field*.

4.2. Fractional ideals, unique factorization and norms.

A *fractional ideal* of \mathcal{O}_K is an \mathcal{O}_K -module \mathfrak{a} of K such that there exists a nonzero $t \in \mathcal{O}_K$ satisfying $t\mathfrak{a} \subseteq \mathcal{O}_K$. The product of two fractional ideals $\mathfrak{a}, \mathfrak{b}$ is defined as the set of all finite sums $\sum x_i y_i$ with $x_i \in \mathfrak{a}$ and $y_i \in \mathfrak{b}$. We denote it by $\mathfrak{a}\mathfrak{b}$. It is also a fractional ideal of \mathcal{O}_K . The set of all fractional ideals of \mathcal{O}_K is denoted by \mathbb{I}_K . The ideals of \mathcal{O}_K in the traditional sense are referred to as *integral ideals* of \mathcal{O}_K to avoid possible confusion.

The ring of integers \mathcal{O}_K is a Dedekind ring. From this we get that every fractional ideal \mathfrak{a} can be written in a unique way as a product $\mathfrak{a} = \prod_{\mathfrak{p} \in \mathcal{P}} \mathfrak{p}^{n_{\mathfrak{p}}(\mathfrak{a})}$ where \mathcal{P} is the set of all prime integral ideals of \mathcal{O}_K and the $n_{\mathfrak{p}}(\mathfrak{a}) \in \mathbb{Z}$ are almost all zero. Thus the set \mathbb{I}_K of fractional ideals of \mathcal{O}_K forms a free abelian group with respect to the product of ideals.

We define the norm of an integral ideal I of \mathcal{O}_K as $N(I) = \text{card}(\mathcal{O}_K/I)$. It is multiplicative in the sense that $N(IJ) = N(I)N(J)$ for any ideals I and J of \mathcal{O}_K . For any nonzero $x \in \mathcal{O}_K$, we note that the previous definition of the norm of x agrees with the norm of the principal ideal $x\mathcal{O}_K$ of \mathcal{O}_K in the sense that $N(x) = \text{card}(\mathcal{O}_K/x\mathcal{O}_K)$. In the case of a fractional ideal $\mathfrak{a} = \prod_{\mathfrak{p} \in \mathcal{P}} \mathfrak{p}^{n_{\mathfrak{p}}(\mathfrak{a})}$ we extend the notion of norm by putting

$$N(\mathfrak{a}) = \prod_{\mathfrak{p} \in \mathcal{P}} N(\mathfrak{p})^{n_{\mathfrak{p}}(\mathfrak{a})}$$

Then, for any two nonzero fractional ideals \mathfrak{a} and \mathfrak{b} of \mathcal{O}_K (which could be integral ideals), we have that $N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$ in the same way that for $x, y \in \mathcal{O}_K$ we have that $N(xy) =$

$N(x)N(y)$. In both those situations, we have that the norm of a nonzero integral element is a nonzero integer.

A *principal fractional ideal* is a fractional ideal generated over \mathcal{O}_K by one element of K . The set $F(K)$ of principal fractional ideals of \mathcal{O}_K forms a subgroup of \mathbb{I}_K . The quotient $\mathbb{I}_K/F(K)$ is called the *group of classes of fractional ideals of K* .

In chapter 5, we will make repeated use of the fact due to Minkowski (see §4.3 of [Sam]) that in any class of fractional ideals of K , there is an integral ideal J of \mathcal{O}_K such that $N(J) \leq \sqrt{|D_K|}$.

We now look at the multiplicative subgroup \mathcal{O}_K^* of \mathcal{O}_K formed by the invertible elements of \mathcal{O}_K . It can be shown that for $x \in \mathcal{O}_K$, we have that $x \in \mathcal{O}_K^* \iff N(x) = \pm 1$. Moreover, the group of roots of unity in K is finite and cyclic. In general, \mathcal{O}_K^* is a finitely generated abelian group (see §4.4 of [Sam]). For quadratic imaginary fields K , the group \mathcal{O}_K^* is finite and we have :

Example 4.3. Let $d \in \mathbb{N}^*$ be square-free and let $K = \mathbb{Q}(\sqrt{-d})$, then we have that

$$\mathcal{O}_K^* = \begin{cases} \pm 1 & \text{if } d \neq 1, 3 \\ \{\pm 1, \pm i\} & \text{if } d = 1 \\ \{\pm 1, \pm \rho, \pm \rho^2\} & \text{if } d = 3 \end{cases}$$

where $\rho = e^{\frac{2\pi i}{3}} = \frac{-1 + \sqrt{-3}}{2}$. See §4.5 of [Sam] for details.

4.3. Height of a subspace, orthogonal subspaces.

Let K be the field \mathbb{Q} or imaginary quadratic field and let \mathcal{O}_K be its ring of integers. Let $l \leq m$ be positive integers, let S be a subspace of K^m of dimension l , and let M be an $l \times m$ matrix with coefficients in K whose rows form a basis of S over K . Finally, let E be the set of minors of order l of M and let $\langle E \rangle_{\mathcal{O}_K}$ denote the fractional ideal generated by E over \mathcal{O}_K . We define the *height* of S as

$$H(S) := \frac{\max_{\omega \in E} |\omega|}{\sqrt{N(\langle E \rangle_{\mathcal{O}_K})}}.$$

We claim that $H(S)$ is independent of the choice of M .

Proof. For the purposes of this demonstration, let $H_M(S)$ denote the height of S computed using the matrix M .

Let M_1 be a matrix obtained from M using only elementary row operations over K (i.e. adding a row multiplied by a factor in K to another row, permuting rows). Let E_1 be the set of minors of order l of M_1 . The minors of M are unaffected by adding a multiple of a row to another row and permutations of rows may only change the sign of the minors, so $E_1 = \pm E$ as sets. It follows that $\langle E_1 \rangle_{\mathcal{O}_K} = \langle E \rangle_{\mathcal{O}_K}$ and so $H_{M_1}(S) = H_M(S)$.

Let $t \in K \setminus \{0\}$ and let M_2 be the matrix obtained from M by multiplying some row of M by t . Using the same notation as above, we have that $E_2 = tE$ and $\langle E_2 \rangle_{\mathcal{O}_K} = t \langle E \rangle_{\mathcal{O}_K}$, so

$$H_{M_2}(S) = \frac{\max_{\theta \in E_2} |\theta|}{\sqrt{N(\langle E_2 \rangle_{\mathcal{O}_K})}} = \frac{\max_{t\omega \in tE} |t\omega|}{\sqrt{N(\langle tE \rangle_{\mathcal{O}_K})}} = \frac{|t|}{\sqrt{N(t)}} \frac{\max_{\omega \in E} |\omega|}{\sqrt{N(\langle E \rangle_{\mathcal{O}_K})}} = H_M(S).$$

Finally, let M_3 be any $l \times m$ matrix with coefficients in K whose rows form a basis of S over K . We can obtain M_3 by performing elementary row operations on M and multiplying rows by factors in K^* if required. Hence the height $H(S)$ is not affected by the choice of M . Note that this also implies that, without loss of generality, we may choose the matrix M with coefficients in \mathcal{O}_K . \square

Given a subspace $S \subseteq K^m$ of dimension l , we define the orthogonal of S , denoted by S^\perp , to be

$$S^\perp := \left\{ \mathbf{y} \in K^m \mid \langle \mathbf{x}, \mathbf{y} \rangle = 0 \text{ for all } \mathbf{x} \in S \right\},$$

where $\langle \cdot, \cdot \rangle$ is the standard non-degenerate bilinear form on K^m . From classic linear algebra we know that S^\perp is a subspace of K^m with

$$\dim(S) + \dim(S^\perp) = m.$$

Moreover, from Schmidt in [ScE] we have that

$$H(S) = H(S^\perp).$$

5. Approximation over an imaginary quadratic field

5.1. Introduction.

In the first part this chapter, we extend the main result of Davenport and Schmidt's paper [DS] to the context of an imaginary quadratic field K . The original result is the following :

Theorem DS2a (1969). *Suppose that $n \geq 2$ and that $\xi \in \mathbb{R}$ is not an algebraic number of degree at most $n/2$. Let $\lambda = \lfloor n/2 \rfloor^{-1}$. Then there are arbitrarily large values of X such that the inequalities*

$$|x_0| \leq X, \quad |x_0 \xi^k - x_k| \leq cX^{-\lambda} \quad (k = 1, \dots, n)$$

where c is a suitable positive number depending on n and ξ , have no solution in integers x_0, \dots, x_n not all 0.

This result has been slightly improved by Michel Laurent in [Lau] who proved it with $\lambda = \lceil n/2 \rceil^{-1}$. His proof also simplifies that of [DS] and so we follow more closely Michel Laurent in extending the above result. Our objective is to demonstrate the following, which is the main result of this section.

Theorem 5.1. *Let K be an imaginary quadratic number field and let \mathcal{O}_K be the ring of integers of K . Let $\xi \in \mathbb{C}$ and $n \in \mathbb{N}^*$ be such that ξ is not algebraic of degree at most $n/2$ over K . Let $\lambda = \lfloor n/2 \rfloor^{-1}$. Then there are arbitrarily large values of $X \in \mathbb{R}^+$ such that the inequalities*

$$|x_0| \leq X, \quad |x_0 \xi^k - x_k| \leq cX^{-\lambda} \quad (k = 1, \dots, n)$$

where c is a suitable positive number depending on n and ξ , have no solution $x_0, \dots, x_n \in \mathcal{O}_K$ not all 0.

We will start with a few general lemmas concerning vector spaces over K and then proceed to the construction of the sequence of *best approximations*. Reasoning by contradiction, we will assume in §5.4 that Theorem 5.1 does not hold and deduce strong properties for our approximations. The lemmas on vector spaces will then lead to the required contradiction.

In the case where $n = 2$, Davenport & Schmidt had a stronger result. In their article [DS] they prove the following

Theorem DS1a (1969). *Suppose that ξ is neither rational nor a quadratic irrational. Let $\lambda = (-1 + \sqrt{5})/2 \approx 0.618$. Then there are arbitrarily large values of X such that the inequalities*

$$|x_0| \leq X \quad , \quad |x_0\xi - x_1| \leq cX^{-\lambda} \quad , \quad |x_0\xi^2 - x_2| \leq cX^{-\lambda}$$

where c is a suitable positive number depending on ξ , have no solution in integers x_0, x_1, x_2 , not all 0.

In the second part of this chapter, we will extend Theorem DS1a to the context of an imaginary quadratic field K :

Theorem 5.2. *Let K be an imaginary quadratic number field and let \mathcal{O}_K be the ring of integers of K . Let $\xi \in \mathbb{C}$ be transcendental over K or algebraic over K of degree > 2 . Let $\lambda = (-1 + \sqrt{5})/2 \approx 0.618$. Then there exists a constant $c = c(\xi, K) > 0$ for which there are arbitrarily large values of $X \in \mathbb{R}^+$ such that the inequalities*

$$(9) \quad |x_0| \leq X \quad , \quad |x_0\xi - x_1| \leq cX^{-\lambda} \quad , \quad |x_0\xi^2 - x_2| \leq cX^{-\lambda}$$

have no nonzero solution $(x_0, x_1, x_2) \in \mathcal{O}_K^3$.

D.Roy shows in [RoC] that Theorem DS1a is optimal. His result also shows the optimality of our Theorem 5.2.

We work over a quadratic imaginary number field K because, apart from \mathbb{Q} , this is the only field whose ring of integers is discrete in \mathbb{C} .

Main result of Davenport & Schmidt, general case $n \geq 2$

5.2. Some lemmas on vector spaces.

The results of this section apply in general to any number field $K \subseteq \mathbb{C}$ and its ring of integers \mathcal{O}_K . The first lemma is a special case of a result of Roy and Waldschmidt (see §5 of [RW]). Our proof, however, is different.

Lemma 5.3. *Let $a_0, \dots, a_h \in K$. Consider the matrix*

$$A = \left[\begin{array}{cccc} a_0 & \cdots & a_h & \\ & \ddots & & \ddots \\ & & a_0 & \cdots & a_h \end{array} \right] \left. \vphantom{\begin{array}{cccc} a_0 & \cdots & a_h & \\ & \ddots & & \ddots \\ & & a_0 & \cdots & a_h \end{array}} \right\} m \text{ rows}$$

with m rows, $m + h$ columns and zeros in the unspecified entries. Let \mathcal{Z} be the maximum of all the absolute values of its minors of order m . Then $\mathcal{Z} \gg \ll \max\{|a_0|, \dots, |a_h|\}^m$ for some constants depending only on m and h .

Proof. Let $M = \max\{|a_0|, \dots, |a_h|\}$. We start by noting that $\mathcal{Z} \leq m!M$ and that $\mathcal{Z} = 0$ iff $M = 0$. Thus we need only to prove that $\mathcal{Z} \gg M^m$ assuming that $M \neq 0$.

For this proof we use a function $\varphi : \{1, \dots, n\} \rightarrow \mathbb{R}$ satisfying the inequalities

$$(10) \quad 0 < \varphi(0) \leq \varphi(1) \leq \dots \leq \varphi(h) = 1$$

$$(11) \quad \varphi(k+1)^m > m! \varphi(k) \quad \text{for } k = 0, \dots, h-1.$$

An example of such a φ will be given at the end of the proof.

If $|a_0| \geq M\varphi(0)$, we have that the absolute value of the determinant of the first leftmost m columns of A is $M^m \varphi(0)^m \gg M^m$ and the lemma is proven. Hence we can assume that $|a_0| < M\varphi(0)$. Under this hypothesis let $s \leq h$ be the largest integer for which $|a_s| < M\varphi(s)$ holds.

If $s = h$, we have that $|a_k| < M\varphi(k) \leq M = \max\{|a_0|, \dots, |a_h|\}$ for all $k = 0, \dots, h$ which contradicts the fact that the maximum comes from some element among $|a_0|, \dots, |a_h|$.

As $s < h$, we now have that

$$|a_k| < M\varphi(k) \quad \text{for } k = 0, \dots, s \quad \text{and} \quad |a_{s+1}| \geq M\varphi(s+1).$$

We turn our attention to the $m \times m$ submatrix

$$A_0 = \begin{bmatrix} a_{s+1} & a_{s+2} & \cdots & & \\ a_s & a_{s+1} & \cdots & & \\ \vdots & \vdots & \ddots & & \\ & & & & \\ & & & & a_{s+1} \end{bmatrix}$$

extracted from columns $s+2$ to $s+m+1$. We expand its determinant as a sum of $m!$ terms $a_{s+1}^m - a_s a_{s+2} a_{s+1}^{m-2} + \cdots$ and we denote by M_0 the maximum over the absolute values of all terms other than the leading term a_{s+1}^m .

It is easy to see that each terms except a_{s+1}^m is a product of m coefficients of A_0 with at least one below the diagonal of A_0 . The coefficients below the diagonal are either 0 or of the form a_r for some $r < s+1$. Since $|a_r| < M\varphi(r) \leq M\varphi(s)$ for $r = 0, \dots, s$, we deduce that

$$M_0 < \varphi(s) M M^{m-1} = \varphi(s) M^m$$

Thus we have that

$$|\det(A_0)| \geq |a_{s+1}^m| - m! \varphi(s) M^m \geq M^m (\varphi(s+1)^m - m! \varphi(s)) \gg M^m$$

The constant in the last symbol \gg depends only on m, h and the choice of φ . Indeed the condition (11) ensures that

$$\min_{0 \leq k < h} (\varphi(k+1)^m - m! \varphi(k)) > 0.$$

As $\mathcal{Z} \geq |\det(A_0)|$ we conclude that $\mathcal{Z} \gg M^m$. It remains only to give an example of an appropriate function φ . We set $\varphi(h) = 1$ and define recursively

$$\varphi(h-k) := \frac{\varphi(h-k+1)^m}{2m!} \quad \text{for } k = 1, \dots, h.$$

Since

$$\varphi(h-k) < \frac{\varphi(h-k+1)^m}{m!} < \varphi(h-k+1)$$

the function φ satisfies both required inequalities (10) and (11). \square

The following lemma computes the ideal generated by the minors of maximal order of a certain matrix.

Lemma 5.4. *Let $h, m \in \mathbb{N}^*$, let $a_0, \dots, a_h \in \mathcal{O}_K$ and let $I = (a_0, \dots, a_h)$ be the ideal of \mathcal{O}_K generated by a_0, \dots, a_h . Let*

$$A = \left[\begin{array}{ccc} a_0 & \cdots & a_h \\ & \ddots & \cdots \\ & & a_0 & \cdots & a_h \end{array} \right] \Bigg\} m \text{ rows}$$

where the unspecified coefficients in A are all zeros. Let I_A be the ideal of \mathcal{O}_K generated by the minors of order m of A . Then $I_A = I^m$.

Proof. Let E be the set of all monomials of degree m in a_0, \dots, a_h with leading coefficient 1. All elements of E can be written in a unique way as $a_{r_1} \cdots a_{r_m}$ for some $0 \leq r_1 \leq \dots \leq r_m \leq h$. We use this to define the usual lexicographical ordering on E , that is

$$a_{r_1} \cdots a_{r_m} < a_{s_1} \cdots a_{s_m} \iff \text{the minimal index } j \text{ for which } r_j \neq s_j \text{ is such that } r_j < s_j.$$

We have quite trivially that $I_A \subseteq I^m$ as the minors of order m of A are homogeneous polynomials of degree m in a_0, \dots, a_h .

Suppose now that $I_A \neq I^m$ and let $a_{s_1} \cdots a_{s_m}$ be the minimal element of E with respect to our ordering which satisfies $a_{s_1} \cdots a_{s_m} \notin I_A$.

By choosing the appropriate m columns from A , it is possible to form a matrix having a_{s_1}, \dots, a_{s_m} as diagonal entries :

$$S = \begin{bmatrix} a_{s_1} & & & \\ & a_{s_2} & & \\ & & \ddots & \\ & & & a_{s_m} \end{bmatrix}.$$

For $j = 1, \dots, m$, the coefficients of the j -th column below the diagonal consists either of zeros or coefficients a_r with $r < s_j$. We expand the determinant of S along the leftmost column. Because of the particular form of S , we get that

$$\begin{vmatrix} a_{s_1} & & & \\ & a_{s_2} & & \\ & & \ddots & \\ & & & a_{s_m} \end{vmatrix} = a_{s_1} \begin{vmatrix} a_{s_2} & & \\ & \ddots & \\ & & a_{s_m} \end{vmatrix} + \left(\text{linear combination of elements of } E \text{ which} \right. \\ \left. \text{are strictly smaller than } a_{s_1} \cdots a_{s_m} \text{ with re-} \right. \\ \left. \text{spect to the ordering defined on } E. \right)$$

We repeat this process once more, again expanding the sub-determinant with respect to the leftmost column, to have that

$$a_{s_1} \begin{vmatrix} a_{s_2} & & \\ & \ddots & \\ & & a_{s_m} \end{vmatrix} = a_{s_1} a_{s_2} \begin{vmatrix} a_{s_3} & & \\ & \ddots & \\ & & a_{s_m} \end{vmatrix} + \left(\text{linear combination of elements of } E \text{ which} \right. \\ \left. \text{are strictly smaller than } a_{s_1} \cdots a_{s_m}. \right)$$

We eventually get that

$$\det(S) = a_{s_1} \cdots a_{s_m} + \left(\text{linear combination of elements of } E \text{ which} \right. \\ \left. \text{are strictly smaller than } a_{s_1} \cdots a_{s_m}. \right)$$

Since $a_{s_1} \cdots a_{s_m}$ is the minimal element of E not belonging to I_A , we have that all the other terms in the expansion of $\det(S)$ are in I_A . But $\det(S) \in I_A$ since $\det(S)$ is a minor of order m of A . Thus we get that $a_{s_1} \cdots a_{s_m} \in I_A$. This contradiction comes from the assumption $I^m \setminus I_A$ is non-empty. Hence $I_A = I^m$. \square

The next lemma is due to Michel Laurent (Lemma 2 of [Lau]).

Lemma 5.5. *Let a_0, \dots, a_h and b_0, \dots, b_h be two sequences of $h + 1$ complex numbers. Let m be a positive integer. Suppose that the two vector subspaces of \mathbb{C}^{h+m} generated over \mathbb{C} by the m rows of the $m \times (h + m)$ matrices*

$$\begin{bmatrix} a_0 & \cdots & a_h & & \\ & \ddots & & \ddots & \\ & & a_0 & \cdots & a_h \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} b_0 & \cdots & b_h & & \\ & \ddots & & \ddots & \\ & & b_0 & \cdots & b_h \end{bmatrix}$$

are equal. Then there exists a nonzero complex number ρ such that $a_k = \rho b_k$ for $0 \leq k \leq h$.

Proof. Consider the polynomials

$$A = a_0 + \dots + a_h X^h \quad \text{and} \quad B = b_0 + \dots + b_h X^h.$$

We look at the equality of the vector spaces spanned by the rows of the two above matrices as an equality between the two vector spaces

$$A \cdot \mathbb{C}[X]_{\leq m-1} = B \cdot \mathbb{C}[X]_{\leq m-1}$$

in $\mathbb{C}[X]_{\leq h+m-1}$. As $1 \in \mathbb{C}[X]_{\leq m-1}$, we have that A divides B and B divides A in $\mathbb{C}[X]$, so $A = \rho B$ for some $\rho \in \mathbb{C}$. If $\rho = 0$, we have $A = B = 0$ and we can choose $\rho' = 1$ instead of ρ to have $A = 0 = \rho' B$. So without loss of generality we can assume that $\rho \neq 0$, proving the lemma. \square

5.3. Construction of the sequence of best approximations.

For the remainder of this chapter, we let K be a quadratic imaginary number field so that its ring of integers \mathcal{O}_K is discrete in \mathbb{C} . We also fix $\xi \in \mathbb{C}$ with $[K(\xi) : K] > n/2$.

For $\mathbf{x} = (x_0, \dots, x_n) \in \mathcal{O}_K^{n+1}$, define

$$L(\mathbf{x}) = \max_{1 \leq k \leq n} |x_0 \xi^k - x_k|$$

and

$$E(X, L) = \left\{ (x_0, \dots, x_n) \in \mathcal{O}_K^{n+1} \mid 1 \leq |x_0| \leq X \quad \text{and} \quad L(x_0, \dots, x_n) < L \right\}.$$

Note that as $\xi \notin K$ we have

$$L(\mathbf{x}) \geq |x_0\xi - x_1| > 0$$

for any $\mathbf{x} \in \mathcal{O}_K^{n+1}$ such that $x_0 \neq 0$. Moreover, if $L(\mathbf{x}) < L$ for some nonzero $\mathbf{x} \in \mathcal{O}_K^{n+1}$ and some $L < 1$, then we must have that $x_0 \neq 0$ (because otherwise $L(\mathbf{x}) = \max |x_k| \geq 1$) and so, \mathbf{x} belongs to $E(X, L)$.

We start with the construction of the sequence of best approximations and deduce a few interesting properties that result from this construction. Theorem 5.1 claims that there exists a $c > 0$ such that $E(X, cX^{-\lambda}) = \emptyset$ for arbitrarily large values of X . By assuming in §5.4 that Theorem 5.1 does not hold, we obtain additional properties for the sequence of best approximations. Ultimately, these properties will lead to a contradiction.

5.3.1. General construction.

We first note the following consequence of Minkowski's first convex theorem. It shows that for some $c = c(n, K)$ we have that $E(X, cX^{-1/n})$ is not empty for any $X \geq 1$.

Lemma 5.6. *There exists $c = c(n, K) > 0$ such that the inequalities*

$$(12) \quad \begin{cases} |x_0| \leq X \\ |x_0\xi - x_1| \leq cX^{-1/n} \\ \vdots \\ |x_0\xi^n - x_n| \leq cX^{-1/n} \end{cases}$$

have a nonzero solution $(x_0, \dots, x_n) \in \mathcal{O}_K^{n+1}$ for each $X \geq 1$.

Proof. The volume of the convex body of \mathbb{C}^{n+1} defined by (12) is $\pi^{n+1}c^n$ and the co-volume of \mathcal{O}_K^{n+1} in \mathbb{C}^{n+1} is $\left(\frac{1}{2}\sqrt{|D_K|}\right)^{n+1}$. By Minkowski's first convex body theorem, (12) has a nonzero solution in \mathcal{O}_K^{n+1} if $c \geq \left(\frac{2}{\pi}\sqrt{|D_K|}\right)^{\frac{n+1}{n}}$. \square

The next lemma provides the construction of the so-called *sequence of best approximations*.

Lemma 5.7. *There exists a sequence $(\mathbf{x}_i)_{i \geq 1}$ of points of \mathcal{O}_K^{n+1} such that, if we put $X_i = |x_{i,0}|$, then the following properties hold :*

- (a) $0 < X_1 < X_2 < X_3 < \dots$
- (b) $1 > L(\mathbf{x}_1) > L(\mathbf{x}_2) > L(\mathbf{x}_3) > \dots$
- (c) *if $L(\mathbf{x}) < L(\mathbf{x}_i)$ for some $\mathbf{x} \in \mathcal{O}_K^{n+1}$ with $x_0 \neq 0$ and $i \geq 1$, then $|x_0| \geq X_{i+1}$.*

Proof. Note that, since \mathcal{O}_K is discrete in \mathbb{C} , the set $E(X, L)$ is finite for each X and L . As $\xi \in K$, we have that $L(\mathbf{x}) > 0$ for all $\mathbf{x} \in \mathcal{O}_K^{n+1}$. By Lemma 5.6 we know that for each $L > 0$ there exists $X \in \mathbb{R}^+$ sufficiently large so that $E(X, L) \neq \emptyset$.

Let $X_1 \geq 1$ be the smallest positive real X such that $E(X, 1) \neq \emptyset$. As $E(X_1, 1)$ is finite, we can choose $\mathbf{x}_1 \in E(X_1, 1)$ so that

$$L(\mathbf{x}_1) = \min_{\mathbf{x} \in E(X_1, 1)} L(\mathbf{x}).$$

There can be more than one candidate for the choice of \mathbf{x}_1 but it is of no consequence. Note that by the minimality of X_1 we have that $X_1 = |x_{1,0}|$, where $x_{1,0}$ is the first coefficient of \mathbf{x}_1 . Write $L_1 = L(\mathbf{x}_1)$ for convenience.

Since $L_1 > 0$, there exists a smallest value of $X_2 \in \mathbb{R}^+$ such that $E(X_2, L_1) \neq \emptyset$. Note the strict inequality in the definition of $E(X, L)$. By the definition of L_1 , we have that $X_2 > X_1$. We choose $\mathbf{x}_2 \in E(X_2, L_1)$ such that

$$L(\mathbf{x}_2) = \min_{\mathbf{x} \in E(X_2, L_1)} L(\mathbf{x}).$$

By the minimality of X_2 we have that $X_2 = |x_{2,0}|$, where $x_{2,0}$ is the first coefficient of \mathbf{x}_2 . We let $L_2 := L(\mathbf{x}_2)$ and we note that $L_1 > L_2$ and $X_1 < X_2$ by construction.

This process can be repeated indefinitely to produce a sequence $(\mathbf{x}_i)_{i \geq 1}$ satisfying properties (a) and (b) of the lemma. To show that it satisfies property (c) as well, let $\mathbf{x} = (x_0, \dots, x_n) \in \mathcal{O}_K^{n+1}$ with $x_0 \neq 0$ be such that $L(\mathbf{x}) < L(\mathbf{x}_i)$ for some $i \geq 1$.

Recall that X_{i+1} is defined to be smallest positive real for which we have that $E(X_{i+1}, L_i) \neq \emptyset$. As $L(\mathbf{x}) < L_i$ the minimality of X_{i+1} implies that $|x_0| \geq X_{i+1}$. This proves the last property (c) and concludes the proof of the lemma. \square

5.3.2. Special properties.

We deduce a few more interesting properties for the sequence $(\mathbf{x}_i)_{i \geq 1}$ just constructed.

Lemma 5.8. *The coordinates of $\mathbf{x}_i = (x_{i,0}, x_{i,1}, \dots, x_{i,n})$ cannot share a common factor in \mathcal{O}_K other than a root of unity. Moreover, the ideal of \mathcal{O}_K generated by the coordinates of \mathbf{x}_i has norm $\leq \sqrt{|D_K|}$.*

Proof. Suppose that a nonzero $t \in \mathcal{O}_K$ is a common factor of the coordinates of \mathbf{x}_i and write $\mathbf{x}_i = t\mathbf{z}$ with $\mathbf{z} \in \mathcal{O}_K^{n+1}$. Then

$$X_i = |t||z_0| \quad \text{and} \quad L(\mathbf{x}_i) = |t|L(\mathbf{z}).$$

Recall that $|t| \geq 1$ for any nonzero $t \in \mathcal{O}_K$ and that $|t| = 1$ only if t is a root of 1. If $|t| > 1$ we have $L(\mathbf{z}) < L(\mathbf{x}_i)$ and $|z_0| < X_i$. By property (c) of Lemma 5.7, we have that $L(\mathbf{z}) < L(\mathbf{x}_i)$ implies $|z_0| \geq X_{i+1} > X_i$ which is a contradiction. Hence $|t| = 1$ and t is a root of unity.

Let I be the ideal of \mathcal{O}_K generated by the coordinates of \mathbf{x}_i . To show that $N(I) \leq \sqrt{|D_K|}$, suppose that on the contrary we have $N(I) > \sqrt{|D_K|}$.

By a theorem of Minkowski (see §4.2), there exists an ideal J of \mathcal{O}_K of norm $N(J) \leq \sqrt{|D_K|}$ in the same class as I . Choose $a \in K^*$ such that $J = aI$ and put $\mathbf{z} = a\mathbf{x}_i$. Then \mathbf{z} belongs to \mathcal{O}_K^{n+1} since its coordinates are in J . Moreover, we have $|a| < 1$ since $N(J) = |a|^2 N(I)$ by properties of the norms and $N(J) < N(I)$ by hypothesis. This implies that $|z_0| < X_i = |x_{i,0}|$ and $L(\mathbf{z}) < L(\mathbf{x}_i)$, which gives a contradiction like that of the previous paragraph, using property (c) of Lemma 5.7. \square

Lemma 5.9. *For each $i \geq 1$, the elements \mathbf{x}_i and \mathbf{x}_{i+1} are linearly independant over K .*

Proof. Assuming this to be false, we have that $\mathbf{x}_i = t\mathbf{x}_{i+1}$ for some $t \in K$. If $|t| > 1$ we have that $X_{i+1} < X_i$ and if $|t| \leq 1$ we have that $L(\mathbf{x}_i) = |t|L(\mathbf{x}_{i+1}) \leq L(\mathbf{x}_{i+1})$, both contradicting the construction of the sequence in Lemma 5.7. \square

5.4. Specific properties coming from the negation of Theorem 5.1.

The negation of Theorem 5.1 is the statement that for any $c > 0$ there is some $X_0 \in \mathbb{R}^+$ sufficiently large so that for all $X \geq X_0$ there exists $\mathbf{x} = (x_0, \dots, x_n) \in E(X, cX^{-\lambda})$ with $1 \leq |x_0| \leq X$ and $L(\mathbf{x}) < cX^{-\lambda}$. Fix such a choice of c and X_0 .

Recall that the inequality $1 \leq |x_0|$ follows from $L(\mathbf{x}) < 1$ if $\mathbf{x} \neq 0$. The value X_0 here is not to be confused with the X_1, X_2, \dots in the sequence of best approximations. For the next result we will ask that the indices i involved are such that $X_{i+1} > X_0$.

Lemma 5.10. *For each sufficiently large i , we have*

$$(13) \quad L(\mathbf{x}_i) \leq cX_{i+1}^{-\lambda}.$$

Proof. By property (c) of Lemma 5.7 we have that $X < X_{i+1}$ and $\mathbf{x} \in E(X, 1)$ imply $L(\mathbf{x}) \geq L(\mathbf{x}_i)$. The negation of Theorem 5.1 gives in particular that for any small $\epsilon > 0$ there is some nonzero $\mathbf{x} \in E(X_{i+1} - \epsilon, c(X_{i+1} - \epsilon)^{-\lambda})$ such that $L(\mathbf{x}_i) \leq L(\mathbf{x}) < c(X_{i+1} - \epsilon)^{-\lambda}$. As this holds for all small $\epsilon > 0$, we get our result. \square

Finally, note that from $|x_{i,0}| = X_i$ and (13) we deduce that

$$\max\{|x_{i,1}|, \dots, |x_{i,n}|\} \leq (1 + \max\{|\xi|, |\xi|^n\}) X_i \leq (2 + |\xi|^n) X_i$$

and that for $0 \leq k, l \leq n$ we have

$$(14) \quad |x_{i,k}\xi^{-k} - x_{i,l}\xi^{-l}| = |x_{i,k}\xi^{-k} - x_{i,0} + x_{i,0} - x_{i,l}\xi^{-l}| \leq (|\xi|^{-k} + |\xi|^{-l}) cX_{i+1}^{-\lambda}.$$

5.5. Relations between coordinates of the best approximations.

We will now study different properties of the points $(\mathbf{x}_i)_{i \geq 1}$ forming the sequence of best approximations. As we first deal with only one such point at a time, we let $\mathbf{x}_i = (y_0, \dots, y_n)$ to lighten the notation.

For integers $h \leq n$, we define the h -th *circulant matrix* of (y_0, \dots, y_n) to be the following $(h+1) \times (n-h+1)$ matrix

$$M_h := \begin{bmatrix} y_0 & y_1 & \cdots & y_{n-h} \\ y_1 & y_2 & \cdots & y_{n-h+1} \\ \vdots & \vdots & & \vdots \\ y_h & y_{h+1} & \cdots & y_n \end{bmatrix}$$

Lemma 5.11. *Suppose that $n \geq 2h$ and $cX_{i+1}^{-\lambda} \leq 1$. Let S be a square matrix formed by taking $h + 1$ distinct columns from the h -th circulant matrix M_h . Then*

$$|\det(S)| \leq (h + 1)!c^h (2 + |\xi|^n)^{h+1} X_i X_{i+1}^{-\lambda h}$$

Proof. We can write S as

$$S = \begin{vmatrix} y_{j_0} & y_{j_1} & \cdots & y_{j_h} \\ \vdots & \vdots & & \vdots \\ y_{j_0+h} & y_{j_1+h} & \cdots & y_{j_h+h} \end{vmatrix}$$

for distinct $j_0 < \cdots < j_h \in \{0, \dots, n - h\}$. From (14) we have that

$$|y_k - y_l \xi^{k-l}| \leq (2 + |\xi|^n) cX_{i+1}^{-\lambda} \quad \text{for } 0 \leq l < k \leq n.$$

The determinant of S is unchanged if we subtract from each column (except the first) the product of the first column by an appropriate power of ξ , so

$$|\det(S)| = \left\| \begin{vmatrix} y_{j_0} & y_{j_1} - \xi^{j_1-j_0}y_{j_0} & \cdots & y_{j_h} - \xi^{j_h-j_0}y_{j_0} \\ \vdots & \vdots & & \vdots \\ y_{j_0+h} & y_{j_1+h} - \xi^{j_1-j_0}y_{j_0+h} & \cdots & y_{j_h+h} - \xi^{j_h-j_0}y_{j_0+h} \end{vmatrix} \right\|.$$

The coefficients from the first column have absolute value $\leq (2 + |\xi|^n) X_i$ and those from all the others have absolute value $\leq (2 + |\xi|^n) cX_{i+1}^{-\lambda}$, hence

$$|\det(S)| \leq (h + 1)! (2 + |\xi|^n) X_i (c(2 + |\xi|^n) X_{i+1}^{-\lambda})^h \leq (h + 1)!c^h (2 + |\xi|^n)^{h+1} X_i X_{i+1}^{-\lambda h}$$

□

Let h_i be the smallest non-negative integer h such that $\text{rank}(M_h) \leq h$. Note that if $h = 0$ the matrix M_h has rank 1, so we have at least $1 \leq h_i$.

Lemma 5.12. *Suppose that c is small in terms of n and ξ . Then for any $i \geq 1$ we have the upper bound $h_i \leq \lambda^{-1} = \lfloor n/2 \rfloor$.*

Proof. Assume that $c < (2 + |\xi|^n)^{-2} (n + 1)^{-1}$ and put $h = \lambda^{-1} = \lfloor n/2 \rfloor$. By the previous Lemma 5.11, all minors of order $(h + 1)$ of M_h have absolute value bounded above by

$$(h + 1)!c^h (2 + |\xi|^n)^{h+1} X_i X_{i+1}^{-\lambda h} \leq (h + 1)!c^h (2 + |\xi|^n)^{h+1} < 1.$$

As the minors are elements of \mathcal{O}_K , we must have that all minors of order $(h + 1)$ of M_h are zero, so $\text{rank}(M_h) \leq h$. Now h_i is the smallest integer for which this happens, so $h_i \leq \lfloor n/2 \rfloor$. □

It follows from the minimality of h_i that

$$M_{h_i} = \begin{bmatrix} y_0 & y_1 & \cdots & y_{n-h_i} \\ \vdots & \vdots & & \vdots \\ y_{h_i} & y_{h_i+1} & \cdots & y_n \end{bmatrix} \quad \text{has rank } \leq h_i$$

$$M_{h_{i-1}} = \begin{bmatrix} y_0 & y_1 & \cdots & y_{n-h_{i-1}} \\ \vdots & \vdots & & \vdots \\ y_{h_{i-1}} & y_{h_{i-1}+1} & \cdots & y_n \end{bmatrix} \quad \text{has rank } h_{i-1}.$$

Note that although these matrices share a large portion of entries, none is a submatrix of the other.

As M_{h_i} has rank $\leq h_i$, some nontrivial K -linear combination of its rows is equal to zero. Let $a_0^{(i)}, \dots, a_{h_i}^{(i)}$ be the coefficients of such a linear combination, which can be assumed without loss of generality to be in \mathcal{O}_K . Moreover, we claim that we may assume that the ideal $I = (a_0^{(i)}, \dots, a_{h_i}^{(i)})$ of \mathcal{O}_K has norm $N(I) \leq \sqrt{|D_K|}$.

Indeed, by a theorem of Minkowski (see §4.2), there is an ideal J of \mathcal{O}_K of norm $N(J) \leq \sqrt{|D_K|}$ in the same class as I . Let $t \in K^*$ be such that $J = tI$ and write $b_j = ta_j^{(i)}$ for $0 \leq j \leq h_i$. We have that $b_0, \dots, b_{h_i} \in J \subseteq \mathcal{O}_K$ and $\langle b_0, \dots, b_{h_i} \rangle_{\mathcal{O}_K} = J$. Using the coefficients b_j we get a nontrivial K -linear combination of the rows of M_{h_i} which vanishes. This proves the claim.

We have

$$a_0^{(i)} [y_0 \ y_1 \ \cdots \ y_{n-h_i}] + a_1^{(i)} [y_1 \ y_2 \ \cdots \ y_{n-h_i+1}] + \cdots + a_{h_i}^{(i)} [y_{h_i} \ y_{h_i+1} \ \cdots \ y_n] = 0$$

which can be written in a more compact form as

$$(15) \quad a_0^{(i)} y_j + a_1^{(i)} y_{j+1} + \cdots + a_{h_i}^{(i)} y_{j+h_i} = 0 \quad (j = 0, \dots, n - h_i).$$

Let $P_i(T) = a_0^{(i)} + a_1^{(i)}T + \cdots + a_{h_i}^{(i)}T^{h_i}$ so that $H(P_i) = \max \left\{ |a_0^{(i)}|, \dots, |a_{h_i}^{(i)}| \right\}$.

Lemma 5.13. *For any sufficiently large i , we have that $H(P_i) \ll X_i^{1/n}$.*

Proof. Let

$$A = \left[\begin{array}{cccc} a_0^{(h_i)} & \cdots & a_{h_i}^{(h_i)} & \\ & \ddots & & \\ & & a_0^{(h_i)} & \cdots & a_{h_i}^{(h_i)} \end{array} \right] \left. \vphantom{\begin{array}{cccc} a_0^{(h_i)} & \cdots & a_{h_i}^{(h_i)} & \\ & \ddots & & \\ & & a_0^{(h_i)} & \cdots & a_{h_i}^{(h_i)} \end{array}} \right\} \begin{array}{l} n - 2h_i + 2 \text{ rows, } \\ n - h_i + 2 \text{ columns} \end{array}$$

where the unspecified coefficients in A are all zeros. Let I be the ideal of \mathcal{O}_K generated by the $a_0^{(h_i)}, \dots, a_{h_i}^{(h_i)}$ of norm $\leq \sqrt{|D_K|}$. Let I_A be the ideal of \mathcal{O}_K generated by the minors of order $n - 2h_i + 2$ of A . By Lemma 5.4 we have that $I_A = I^{n-2h_i+2}$. Since $N(I) \leq \sqrt{|D_K|}$ we get that $N(I_A) \leq |D_K|^{(n-2h_i+2)/2} \ll 1$.

Let L_1, \dots, L_{h_i} denote the rows of M_{h_i-1} and R_1, \dots, R_{n-2h_i+2} denote the rows of A . Let $S = \langle L_1, \dots, L_{h_i} \rangle_K \subseteq K^{n-h_i+2}$. Because M_{h_i-1} has rank h_i , we have that $\dim S = h_i$ and so the orthogonal space S^\perp has dimension $n - 2h_i + 2$. The rows R_1, \dots, R_{n-2h_i+2} are linearly independent over K and they belong to S^\perp since they satisfy $L_r R_s^T = 0$ for all $1 \leq r \leq h_i$ and $1 \leq s \leq n - 2h_i + 2$ by virtue of (15). Hence $S^\perp = \langle R_1, \dots, R_{n-2h_i+2} \rangle_K$.

By Lemma 5.11 we have that the maximum of the absolute values of the minors of order h_i of M_{h_i-1} are $\ll X_i (cX_{i+1}^{-\lambda})^{h_i-1}$. Hence, using the definition of the height given in §4.3 and the fact that integral ideals have a nonzero integer norm, we have that

$$H(S) \ll X_i (cX_{i+1}^{-\lambda})^{h_i-1} \ll X_i^{1-(h_i-1)\lambda}.$$

Let \mathcal{Z} be the maximum of the absolute values of the minors of order h_i of A . By Lemma 5.3, we have that

$$\mathcal{Z} \gg \ll \max \left\{ |a_0^{(i)}|, \dots, |a_{h_i}^{(i)}| \right\}^{n-2h_i+2} = H(P_i)^{n-2h_i+2}.$$

The height of S^\perp is

$$H(S^\perp) = \frac{\mathcal{Z}}{\sqrt{N(I_A)}}.$$

As $1 \leq N(I_A) \ll 1$, we deduce that $H(S^\perp) \gg \ll \mathcal{Z}$. Again from the theory presented in §4.3, we have that $H(S) = H(S^\perp)$ and thus

$$(16) \quad H(P_i) \ll \mathcal{Z}^{1/(n-2h_i+2)} \ll X_i^{\frac{1-(h_i-1)\lambda}{n-2h_i+2}}$$

Let $f(x) = \frac{1-(x-1)\lambda}{n-2x+2}$ and compute its first derivative

$$f'(x) = \frac{-\lambda(n-2x+2) - (1-x\lambda+\lambda)(-2)}{(n-2x+2)^2} = \frac{2-n\lambda}{(n-2x+2)^2}.$$

As $\lambda = \lfloor n/2 \rfloor^{-1} \geq 2/n$, we have that $f'(x) \leq 0$ for $x \in [1, n/2]$ and so $f(x)$ is decreasing on that interval. By the inequality $h_i \leq \lfloor n/2 \rfloor$ we have

$$\frac{1 - (h_i - 1)\lambda}{n - 2h_i + 2} \leq \max_{x \in [1, n/2]} \frac{1 - (x - 1)\lambda}{n - 2x + 2} = f(1) = 1/n$$

and so by (16) we conclude that $H(P_i) \ll X_i^{1/n}$. \square

Lemma 5.14. *For any sufficiently large i , we have*

$$|P_i(\xi)| \ll cX_i^{\frac{1}{n}-1} X_{i+1}^{-\lambda}.$$

Proof. Recall that

$$\sum_{k=0}^{h_i} a_k^{(i)} y_k = 0 \quad \text{by (15).}$$

So, we can write

$$y_0 P_i(\xi) = \sum_{k=0}^{h_i} a_k^{(i)} y_0 \xi^k - \sum_{k=0}^{h_i} a_k^{(i)} y_k = \sum_{k=0}^{h_i} a_k^{(i)} (y_0 \xi^k - y_k).$$

Using the estimates

$$\begin{aligned} |y_0 \xi^k - y_k| &\leq cX_{i+1}^{-\lambda} \quad (0 \leq k \leq n), \\ |y_0| &= X_i, \\ |a_k^{(i)}| &\ll X_i^{1/n} \quad (0 \leq k \leq n) \quad (\text{coming from Lemma 5.13}) \end{aligned}$$

we deduce that $|P_i(\xi)| \ll cX_i^{-1} X_i^{1/n} X_{i+1}^{-\lambda} = cX_i^{\frac{1}{n}-1} X_{i+1}^{-\lambda}$. \square

In the same way that we wrote $\mathbf{x}_i = (y_0, \dots, y_n)$ for simplicity, we now let $\mathbf{x}_{i-1} = (z_0, \dots, z_n)$ to work on relations between \mathbf{x}_i and \mathbf{x}_{i-1} for some general index i .

Lemma 5.15. *Suppose that i is large enough. Then the coordinates of \mathbf{x}_{i-1} satisfy the same linear recurrence relations*

$$(17) \quad a_0^{(i)} z_j + a_1^{(i)} z_{j+1} + \dots + a_{h_i}^{(i)} z_{j+h_i} = 0 \quad (j = 0, \dots, n - h_i).$$

as the coordinates of \mathbf{x}_i (see (15)).

Proof. For $j = 0, \dots, n - h_i$ we have

$$z_j P_i(\xi) = a_0^{(i)} z_j + a_1^{(i)} z_{j+1} + \dots + a_{h_i}^{(i)} z_{j+h_i} + \sum_{k=0}^{h_i} a_k^{(h_i)} (z_j \xi^k - z_{j+k}).$$

It follows that

$$\begin{aligned} \left| a_0^{(i)} z_j + a_1^{(i)} z_{j+1} + \cdots + a_{h_i}^{(i)} z_{j+h_i} \right| &\ll X_{i-1} |P_i(\xi)| + H(P_i) L_{i-1} \\ &\ll c X_{i-1} X_i^{\frac{1}{n}-1} X_{i+1}^{-\lambda} + c X_i^{\frac{1}{n}} X_i^{-\lambda} \ll c \end{aligned}$$

The left side of an integer. So it must vanish if we assume that c is sufficiently small. \square

There was a priori no connection between h_{i-1} and h_i , but now that we know from (17) that the coordinates of \mathbf{x}_{i-1} satisfy the same linear relations (15) that the coordinates of \mathbf{x}_i satisfy, we have a nontrivial linear relation between the rows of

$$\begin{bmatrix} z_0 & z_1 & \cdots & z_{n-h_i} \\ \vdots & \vdots & & \vdots \\ z_{h_i} & z_{h_i+1} & \cdots & z_n \end{bmatrix}.$$

So this matrix has rank at most h_i . This implies that $h_{i-1} \leq h_i$. As the sequence $(h_i)_{i \geq 1}$ is bounded above by $\lfloor n/2 \rfloor$ (see lemma 5.12), we deduce that there exists a positive integer h such that $h_i = h$ for all sufficiently large i .

Lemma 5.16. *For all i sufficiently large, we have that*

$$P_i = \rho_i P_{i-1}$$

for some $\rho_i \in K$.

Proof. Taking i to be large enough so that we have $h_i = h_{i-1} = h$ fixed, we consider the matrix of rank h

$$Z = \begin{bmatrix} z_0 & z_1 & \cdots & z_{n-h+1} \\ \vdots & \vdots & & \vdots \\ z_{h-1} & z_h & \cdots & z_n \end{bmatrix}$$

constructed from the coordinates of (z_0, \dots, z_n) of \mathbf{x}_{i-1} . We consider the following matrices :

$$\begin{aligned} A_i &= \left[\begin{array}{cccc} a_0^{(i)} & \cdots & a_h^{(i)} & \\ & \ddots & & \ddots \\ & & a_0^{(i)} & \cdots & a_h^{(i)} \end{array} \right] \left. \vphantom{\begin{array}{cccc} a_0^{(i)} & \cdots & a_h^{(i)} & \\ & \ddots & & \ddots \\ & & a_0^{(i)} & \cdots & a_h^{(i)} \end{array}} \right\} n - 2h + 2 \text{ rows, } n - h + 2 \text{ columns} \\ A_{i-1} &= \left[\begin{array}{cccc} a_0^{(i-1)} & \cdots & a_h^{(i-1)} & \\ & \ddots & & \ddots \\ & & a_0^{(i-1)} & \cdots & a_h^{(i-1)} \end{array} \right] \left. \vphantom{\begin{array}{cccc} a_0^{(i-1)} & \cdots & a_h^{(i-1)} & \\ & \ddots & & \ddots \\ & & a_0^{(i-1)} & \cdots & a_h^{(i-1)} \end{array}} \right\} n - 2h + 2 \text{ rows, } n - h + 2 \text{ columns} \end{aligned}$$

Let V be the subspace of K^{n-h+2} generated over K by the rows of Z . The rank of Z is h so the dimension of V over K is also h . The orthogonal V^\perp in K^{n-h+2} with respect to the usual scalar product must then have dimension $(n - h + 2) - h = n - 2h + 2$.

By virtue of the relation (15) applied to $\mathbf{x}_{i-1} = \mathbf{z}$ rather than $\mathbf{x}_i = \mathbf{y}$ with i replaced by $i - 1$, we have that $ZA_{i-1}^T = 0$. As the rows of A_{i-1} are linearly independent and there are $n - 2h + 2$ of them, they must span V^\perp . Moreover, by Lemma 5.15 we have that $ZA_i^T = 0$ so we deduce in a similar way that the rows of A_i also span V^\perp .

We now apply Lemma 5.5 to A_i and A_{i-1} to get that $P_i = \rho_i P_{i-1}$ for some nonzero $\rho_i \in \mathbb{C}$. Since the coefficients of P_i and P_{i-1} are in \mathcal{O}_K so we have that $\rho_i \in K$ and this proves the lemma. \square

Now using Lemma 5.16 repeatedly, we get that for all i sufficiently large, we have that $P_i(T) = \rho_i P(T)$ for some $\rho_i \in K$ and a fixed $P(T) \in \mathcal{O}_K[T]$.

As ξ is not algebraic of degree $\leq \lfloor n/2 \rfloor$ over \mathcal{O}_K , we have that $P(\xi) \neq 0$. By Lemma 5.14 we have that $|P_i(\xi)| \rightarrow 0$ as i grows. As $|P(\xi)| > 0$ is constant, we must have that $|\rho_i| \rightarrow 0$ as i grows.

However, as the coefficients of P_i are in \mathcal{O}_K we have that $1 \leq H(P_i) = |\rho_i|H(P)$ and so $|\rho_i|$ cannot assume arbitrarily small values. This final contradiction concludes the proof of Theorem 5.1.

Main result of Davenport & Schmidt, specific case $n = 2$

We now wish to prove Theorem 5.2. We begin with a lemma. We construct the sequence of best approximations as in the first part of this section. We then assume that Theorem 5.2 does not hold and we deduce strong consequences for the sequence of best approximations. We reach a contradiction and thus we show that Theorem 5.2 holds.

5.6. A lemma on ideals.

Proposition 5.17. *Let \mathcal{O}_K be the ring of integers of a number field K and let D_K be its discriminant. Let $a, b \in \mathcal{O}_K$ with $b \neq 0$ be such that $\sqrt{a/b} \in K$. Then there exists $\alpha, \beta \in \mathcal{O}_K$ with $\beta \neq 0$ such that*

$$\sqrt{a/b} = \alpha/\beta \quad , \quad |N(\alpha)| \leq \sqrt{|D_K|}N(a)^{1/2} \quad , \quad |N(\beta)| \leq \sqrt{|D_K|}N(b)^{1/2}.$$

Proof. Let $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ be the prime ideals of \mathcal{O}_K that appear in the factorization of $a\mathcal{O}_K$ or $b\mathcal{O}_K$. We can write

$$a \mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s} \quad \text{and} \quad b \mathcal{O}_K = \mathfrak{p}_1^{f_1} \cdots \mathfrak{p}_s^{f_s}$$

for integers $e_1, \dots, e_s, f_1, \dots, f_s \geq 0$. We have

$$\frac{a}{b} \mathcal{O}_K = \mathfrak{p}_1^{g_1} \cdots \mathfrak{p}_s^{g_s} \quad \text{with} \quad g_i = e_i - f_i.$$

Without loss of generality, we may assume that the \mathfrak{p} 's are ordered so that $g_1, \dots, g_r \geq 0$ and $g_{r+1}, \dots, g_s \leq 0$. As $a/b \mathcal{O}_K = \left(\sqrt{a/b} \mathcal{O}_K\right)^2$, all the g_i 's are even. Define

$$I = \mathfrak{p}_1^{g_1/2} \cdots \mathfrak{p}_r^{g_r/2} \quad \text{and} \quad J = \mathfrak{p}_{r+1}^{-g_{r+1}/2} \cdots \mathfrak{p}_s^{-g_s/2}$$

so that I and J are ideals of \mathcal{O}_K with $\sqrt{a/b} \mathcal{O}_K = I \cdot J^{-1}$.

Let $\mathcal{R} = \{I_1, \dots, I_n\}$ be a system of representatives of the finitely many classes of fractional ideals of K . According to a theorem of Minkowski, we know that every ideal class of K contains an ideal of \mathcal{O}_K of norm $\leq \sqrt{|D_K|}$ (see [Sam] p.70 corollary 1). Without loss of generality, we can assume that I_1, \dots, I_n are ideals of \mathcal{O}_K , that I_1 belongs to the class of I^{-1} and that $N(I_1) \leq \sqrt{|D_K|}$. As $I \cdot J^{-1}$ is a principal fractional ideal, we deduce that I_1 is also in the class of J^{-1} .

We obtain

$$\sqrt{\frac{a}{b}}\mathcal{O}_K = (I_1I)(I_1J)^{-1} = \frac{\alpha}{\beta}\mathcal{O}_K$$

upon choosing $\alpha, \beta \in \mathcal{O}_K$ such that $I_1I = \alpha \mathcal{O}_K$ and $I_1J = \beta \mathcal{O}_K$. We have

$$|N(\alpha)| = N(I_1I) = N(I_1) \prod_{i=1}^r N(\mathfrak{p}_i)^{g_i/2} \leq N(I_1) \prod_{i=1}^s N(\mathfrak{p}_i)^{e_i/2} \leq |N(a)|^{1/2} \sqrt{|D_K|}$$

as $g_i \leq e_i$ for $i = 1, \dots, s$. In a similar way, we have

$$|N(\beta)| = N(I_1J) = N(I_1) \prod_{i=r+1}^s N(\mathfrak{p}_i)^{-g_i/2} \leq N(I_1) \prod_{i=1}^s N(\mathfrak{p}_i)^{f_i/2} \leq |N(b)|^{1/2} \sqrt{|D_K|}$$

as $-g_i \leq f_i$ for $i = 1, \dots, s$. Upon replacing β by βu for some unit $u \in \mathcal{O}_K^*$, we can arrange that $\alpha/\beta = \sqrt{a/b}$. This does not affect the absolute value of the norm of β . \square

5.7. The sequence of best approximations.

The construction of the sequence of best approximations found in §5.3 is valid for the case when $n = 2$. All the lemmas found in that section hold if we let $n = 2$.

Let $\lambda = (-1 + \sqrt{5})/2$ for the rest of this section. Suppose that Theorem 5.2 does not hold. This implies that for any choice of $c > 0$, there are nonzero solutions $\mathbf{x} = (x_0, x_1, x_2) \in \mathcal{O}_K^3$ to

$$1 \leq |x_0| \leq X \quad , \quad L(\mathbf{w}) = \max \{ |x_0\xi - x_1|, |x_0\xi^2 - x_2| \} \leq cX^{-\lambda}$$

for all sufficiently large values of $X \in \mathbb{R}^+$.

Section 5.3 provides us with a sequence of best approximations $(\mathbf{x}_i)_{i \geq 1}$ in \mathcal{O}_K^3 (for the choice of $n = 2$). The lemmas of §5.4 remain valid for this sequence, provided that we set $n = 2$ and $\lambda = (-1 + \sqrt{5})/2 \approx 0.618$ instead of $\lambda = \lfloor n/2 \rfloor^{-1}$.

5.8. Specific properties of the sequence of best approximations.

Lemma 5.18. *For all sufficiently large i we have that*

$$\begin{vmatrix} x_{i,0} & x_{i,1} \\ x_{i,1} & x_{i,2} \end{vmatrix} \neq 0$$

Proof. If this determinant is zero, we have that $x_{i,0}x_{i,2} = x_{i,1}^2$. This implies that $(x_{i,0}/x_{i,1})^2 = x_{i,2}/x_{i,1} \in K$ so we can use Proposition 5.17 to obtain $\alpha, \beta \in \mathcal{O}_K$ with $\beta \neq 0$ such that

$$\frac{x_{i,0}}{x_{i,1}} = \frac{\alpha}{\beta}, \quad |\alpha| \leq \sqrt{|D_K|}X_i^{1/2}, \quad |\beta| \leq \sqrt{1 + |\xi|^2}\sqrt{|D_K|}X_i^{1/2}$$

where D_K denotes the discriminant of K .

We find

$$\begin{aligned} \left| \frac{x_{i,0}}{\alpha}(\alpha\xi - \beta) \right| &= |x_{i,0}\xi - x_{i,1}| \leq cX_{i+1}^{-\lambda} \\ \Rightarrow |\alpha\xi - \beta| &\leq cX_{i+1}^{-\lambda} \frac{|\alpha|}{|x_{i,0}|} \leq c\sqrt{|D_K|}X_{i+1}^{-\lambda}X_i^{-1/2}. \end{aligned}$$

As $\mathbf{x}_{i-1}, \mathbf{x}_i$ are linearly independent over K , the matrix

$$\begin{bmatrix} x_{i-1,0} & x_{i-1,1} & x_{i-1,2} \\ x_{i,0} & x_{i,1} & x_{i,2} \end{bmatrix}$$

has rank 2. For i sufficiently large, both $x_{i-1,1}, x_{i,1}$ are nonzero, and so we must have that

either $\begin{vmatrix} x_{i-1,0} & x_{i-1,1} \\ x_{i,0} & x_{i,1} \end{vmatrix} \neq 0$ or $\begin{vmatrix} x_{i-1,1} & x_{i-1,2} \\ x_{i,1} & x_{i,2} \end{vmatrix} \neq 0$. Say the first determinant is nonzero.

This implies that $\begin{vmatrix} x_{i-1,0} & x_{i-1,1} \\ \alpha & \beta \end{vmatrix}$ is a nonzero element of \mathcal{O}_K . We look at its absolute value denoted by $\| \quad \|$ and we have that

$$\begin{aligned} 1 &\leq \left\| \begin{vmatrix} x_{i-1,0} & x_{i-1,1} \\ \alpha & \beta \end{vmatrix} \right\| = \left\| \begin{vmatrix} x_{i-1,0} & x_{i-1,1} - \xi x_{i-1,0} \\ \alpha & \beta - \alpha\xi \end{vmatrix} \right\| \\ &\ll |\alpha|L(\mathbf{x}_{i-1}) + X_{i-1}|\beta - \alpha\xi| \ll X_i^{1/2}cX_i^{-\lambda} + X_{i-1}cX_{i+1}^{-\lambda}X_i^{-1/2}. \end{aligned}$$

The above upper bound tends to 0 as i grows, providing a contradiction for i sufficiently large as $\lambda > 1/2$. A very similar calculation leads to a contradiction with the other determinant and this concludes the proof of the lemma. \square

Lemma 5.19. *For all sufficiently large i we have that*

$$(18) \quad 1 \ll cX_iX_{i+1}^{-\lambda}.$$

Proof. Consider the absolute value of the determinant $\begin{vmatrix} x_{i,0} & x_{i,1} \\ x_{i,1} & x_{i,2} \end{vmatrix} \in \mathcal{O}_K$. It is nonzero by the previous lemma, so it must be bounded below by 1. Recall that

$$|x_{i,1}\xi - x_{i,2}| \leq |x_{i,0}\xi^2 - x_{i,2} - \xi(x_{i,0}\xi - x_{i,1})| \leq c(1 + |\xi|)X_{i+1}^{-\lambda}$$

so

$$1 \leq \left\| \begin{vmatrix} x_{i,0} & x_{i,1} \\ x_{i,1} & x_{i,2} \end{vmatrix} \right\| = \left\| \begin{vmatrix} x_{i,0} & x_{i,1} - \xi x_{i,0} \\ x_{i,1} & x_{i,2} - \xi x_{i,1} \end{vmatrix} \right\| \ll cX_iX_{i+1}^{-\lambda}.$$

\square

Lemma 5.20. *Suppose that \mathbf{x}_{i-1} , \mathbf{x}_i and \mathbf{x}_{i+1} are linearly independent over \mathcal{O}_K . Then*

$$(19) \quad 1 \ll c^2 X_i^{-\lambda} X_{i+1}^{1-\lambda}.$$

Proof. By performing elementary column operations just like in the proof of Lemma 5.19 or Lemma 5.11, we get

$$\left\| \begin{array}{ccc} x_{i-1,0} & x_{i-1,1} & x_{i-1,2} \\ x_{i,0} & x_{i,1} & x_{i,2} \\ x_{i+1,0} & x_{i+1,1} & x_{i+1,2} \end{array} \right\| = \left\| \begin{array}{ccc} x_{i-1,0} & x_{i-1,1} - \xi x_{i-1,0} & x_{i-1,2} - \xi^2 x_{i-1,0} \\ x_{i,0} & x_{i,1} - \xi x_{i,0} & x_{i,2} - \xi^2 x_{i,0} \\ x_{i+1,0} & x_{i+1,1} - \xi x_{i+1,0} & x_{i+1,2} - \xi^2 x_{i+1,0} \end{array} \right\| \ll c^2 X_i^{-\lambda} X_{i+1}^{1-\lambda}.$$

The determinant itself is a nonzero element of \mathcal{O}_K and so it has absolute value ≥ 1 . Hence we get

$$1 \ll c^2 X_i^{-\lambda} X_{i+1}^{1-\lambda}$$

□

Lemma 5.21. *For infinitely many i , the minimal points \mathbf{x}_{i-1} , \mathbf{x}_i and \mathbf{x}_{i+1} are linearly independent over K .*

Proof. Assuming the contrary to be true, there is some $N \in \mathbb{N}^*$ such that for all $i \geq N$, the points $\mathbf{x}_i, \mathbf{x}_{i+1}, \mathbf{x}_{i+2}$ are linearly dependent over K . As any two consecutive minimal points are linearly independent over K by Lemma 5.9, there exists $a_i, b_i, c_i \in \mathcal{O}_K$ with $c_i \neq 0$, such that

$$a_i \mathbf{x}_i + b_i \mathbf{x}_{i+1} + c_i \mathbf{x}_{i+2} = 0.$$

This implies that $\mathbf{x}_{i+2} \in \langle \mathbf{x}_i, \mathbf{x}_{i+1} \rangle_K$ and so $\langle \mathbf{x}_i, \mathbf{x}_{i+1} \rangle_K = \langle \mathbf{x}_{i+1}, \mathbf{x}_{i+2} \rangle_K$. Using this argument repeatedly, we get that for any $i \geq N$, we have that $\langle \mathbf{x}_i, \mathbf{x}_{i+1} \rangle_K = \langle \mathbf{x}_N, \mathbf{x}_{N+1} \rangle_K$, thus $\mathbf{x}_i \in \langle \mathbf{x}_N, \mathbf{x}_{N+1} \rangle_K$ and so

$$0 = \begin{vmatrix} x_{N,0} & x_{N,1} & x_{N,2} \\ x_{N+1,0} & x_{N+1,1} & x_{N+1,2} \\ x_{i,0} & x_{i,1} & x_{i,2} \end{vmatrix} = \begin{vmatrix} x_{N,1} & x_{N,2} \\ x_{N+1,1} & x_{N+1,2} \end{vmatrix} x_{i,0} - \begin{vmatrix} x_{N,0} & x_{N,2} \\ x_{N+1,0} & x_{N+1,2} \end{vmatrix} x_{i,1} + \begin{vmatrix} x_{N,0} & x_{N,1} \\ x_{N+1,0} & x_{N+1,1} \end{vmatrix} x_{i,2}.$$

The linear independence of \mathbf{x}_h and \mathbf{x}_{h+1} implies that at least one of the above 2×2 constant determinants is nonzero. This shows the existence of $a, b, c \in \mathcal{O}_K$ not all 0 and independent from i such that

$$ax_{i,0} + bx_{i,1} + cx_{i,2} = 0 \quad \forall i \geq N.$$

Substituting $x_{i,1} = \xi x_{i,0} + \mathcal{O}(X_{i+1}^{-\lambda})$ and $x_{i,2} = \xi^2 x_{i,0} + \mathcal{O}(X_{i+1}^{-\lambda})$ in the above linear combination, we deduce that

$$\begin{aligned} & |x_{i,0} (a + b\xi + c\xi^2)| \ll X_{i+1}^{-\lambda} \\ \Rightarrow & |a + b\xi + c\xi^2| \ll X_{i+1}^{-\lambda} X_i^{-1} \quad \Rightarrow a + b\xi + c\xi^2 = 0, \end{aligned}$$

which would be possible only if ξ were algebraic of degree 2 or less over \mathcal{O}_K . \square

Now combining the previous lemmas, we have that the inequalities in (18) and (19) must hold for infinitely many i . Keeping in mind that $\lambda \approx 0.618$ and $\lambda^2 + \lambda = 1$, we find

$$X_i^{\lambda^2} \ll (c^2 X_{i+1}^{-\lambda+1})^\lambda \ll c^{2\lambda} (cX_i)^{-\lambda+1} = c^{1+\lambda} X_i^{\lambda^2}.$$

Note that the constants in the Vinogradov symbol \ll depend only on ξ and thus for our value of ξ which is fixed from the beginning, we can find some value of $c > 0$ such that the above inequality does not hold. For this choice of c , we get a contradiction. This concludes the proof of Theorem 5.2.

5.9. Optimality.

In [RoC], D. Roy shows the optimality of Theorem DS1a with the following result.

Theorem 5.22 (Roy, 2004). *Let $\lambda = (-1 + \sqrt{5})/2 \approx 0.618$. There exists a real number ξ which is neither rational nor quadratic irrational and which has the property that, for a suitable constant $c > 0$, the inequalities*

$$|x_0| \leq X \quad , \quad |x_0\xi - x_1| \leq cX^{-\lambda} \quad , \quad |x_0\xi - x_1| \leq cX^{-\lambda}$$

have a non-zero solution $(x_0, x_1, x_2) \in \mathbb{Z}^3$ for any real number $X \geq 1$. Any such number is transcendental over \mathbb{Q} and the set of those real numbers is countable.

These extremal numbers ξ are transcendental over K as well since

$$[K(\xi) : K][K : \mathbb{Q}] = [K(\xi) : \mathbb{Q}(\xi)][\mathbb{Q}(\xi) : \mathbb{Q}]$$

with $[K : \mathbb{Q}] = 2$ and $[\mathbb{Q}(\xi) : \mathbb{Q}] = \infty$. As $\mathbb{Z} \subseteq \mathcal{O}_K$, these numbers ξ are also extremal in the context of Theorem 5.2 and so the latter result is optimal.

6. Conclusion

The original results presented in Chapter 3 and the extension of Davenport and Schmidt's theorems in Chapter 5 suggest natural questions. Here are some of them, most of which seem within reach (except maybe the first one), yet one has to draw the line at some point. Mathematics generates more problems than it actually solves.

1. Optimality for part (ii) of Theorem A

In §3.4 we have shown that part (i) of Theorem A is optimal for all $\xi \in \mathbb{R} \setminus \mathbb{Q}$ and that part (ii) of Theorem A is optimal for all quadratic irrational $\xi \in \mathbb{R}$. It would be interesting to see if we could find transcendental numbers $\xi \in \mathbb{R}$ for which the exponent $-2/n$ of $H(\alpha)$ in part (ii) of Theorem A is best possible. The best we can say about a general $\xi \in \mathbb{R} \setminus \mathbb{Q}$ is that there exists a constant $c_3 > 0$ such that all algebraic integers α of degree $n + 1$ satisfy

$$c_3 H(\alpha)^{-\frac{2}{n-1}} \leq \max_{\bar{\alpha} \neq \alpha} |\xi - \bar{\alpha}|.$$

We don't know how to sharpen the exponent $-\frac{2}{n-1}$ into $-\frac{2}{n}$, if possible at all.

2. Extending Chapter 3 to any number field

In Chapter 5, we extended Davenport and Schmidt's Theorems DS1a and DS2a to quadratic imaginary fields. Our results from Chapter 3 could probably be extended in a similar way, to any number field using its canonical embedding.

3. Extension of other results of Davenport and Schmidt

In the original article by Davenport and Schmidt, Theorem DS2a is used to prove the following :

Theorem 6.1 (DS2). *Suppose that $n \geq 2$ and that $\xi \in \mathbb{R}$ is not an algebraic number of degree at most $n/2$. Then there exists $c > 0$ such that there are infinitely many algebraic integers α of degree at most $n + 1$ which satisfy*

$$0 < |\xi - \alpha| \leq cH(\alpha)^{-\theta}$$

where $\theta = \lfloor n/2 \rfloor + 1$.

Our Theorem 5.1 is an extension of Theorem DS2a. It would be interesting to provide a similar extension of the above Theorem 6.1 (DS2). We expect the following result :

“Let K be an imaginary quadratic number field and let \mathcal{O}_K be the ring of integers of K . Let $\xi \in \mathbb{C}$ and $n \in \mathbb{N}^*$ be such that ξ is not algebraic of degree at most $\lfloor n/2 \rfloor$ over K . Then there exists $c > 0$ such that there are infinitely many algebraic integers $\alpha \in \mathcal{O}_K$ of degree $n + 1$ over K which satisfy

$$0 < |\xi - \alpha| \leq cH(\alpha)^{-\theta/2}$$

where $\theta = \lfloor n/2 \rfloor + 1$.”

Davenport and Schmidt had Theorem DS1a which is stronger than Theorem DS2a when $n = 2$. They used it to show the following :

Theorem 6.2 (DS1). *Suppose that $\xi \in \mathbb{R}$ is not algebraic of degree 2 or less. Then there exists $c > 0$ such that there are infinitely many algebraic integers α of degree at most 3 which satisfy*

$$0 < |\xi - \alpha| \leq cH(\alpha)^{-\theta}$$

where $\theta = \frac{1}{2}(3 + \sqrt{5}) \approx 2.618$.

Our Theorem 5.2 is an extension of Theorem DS1a. We expect the following to hold :

“ Let K be an imaginary quadratic number field and let \mathcal{O}_K be the ring of integers of K . Then there exists $c > 0$ such that there are infinitely many algebraic integers $\alpha \in \mathcal{O}_K$ of degree 3 which satisfy

$$0 < |\xi - \alpha| \leq cH(\alpha)^{-\theta/2}$$

where $\theta = \frac{1}{2}(3 + \sqrt{5}) \approx 2.618$.”

4. Lowering the exponent λ

M. Laurent shows in [Lau] that Theorem DS2a holds when $\lambda = \lceil n/2 \rceil^{-1}$ instead of $\lfloor n/2 \rfloor^{-1}$. This is no improvement when n is even, but when n is odd it sharpens Davenport and Schmidt’s result.

We think that it should be straightforward to do the same thing concerning our Theorem 5.1.

References

- [AR] B. Arbour and D. Roy, A Gel'fond type criterion in degree two, *Acta Arith.*, **111** (2004), 97-103.
- [Bu] Y. Bugeaud, *Approximation by algebraic numbers*, Cambridge Tracts 160, Cambridge Univ. Press, 2004
- [BT] Y. Bugeaud and O. Teulié, Approximation d'un nombre réel par des nombres algébriques de degré donné, *Acta Arith.* **93** (2000), 77-86.
- [DS] H. Davenport and W. M. Schmidt, Approximation to real numbers by algebraic integers, *Acta Arith.* **15** (1969), 393-416.
- [Lau] M. Laurent, Simultaneous rational approximation to the successive powers of a real number, *Indag. Mathem.* **11** 2003 (3), 45-53.
- [Lang] S. Lang, *Algebra*, Addison Wesley, Massachusetts, 1971.
- [NiZ] I. Niven and H. S. Zuckerman, *An Introduction to the Theory of Numbers*, John Wiley & Sons, New York, 1960.
- [RoC] D. Roy, Approximation to real numbers by cubic algebraic integers I, *Proc. London Math. Soc.*, **(3) 88** (2004), 42-62.
- [RW] D. Roy and M. Waldschmidt, Diophantine approximation by conjugate algebraic integers, *Compositio Math.* **140** (2004), 595-612.
- [Sam] P. Samuel, *Théorie algébrique des nombres*, Hermann, Paris, 2003.
- [Sc] W. M. Schmidt, *Diophantine approximation*, Lecture Notes in Math. **785**, Springer-Verlag, 1980.
- [ScE] W. M. Schmidt, *Diophantine approximation and Diophantine Equations*, Lecture Notes in Math. **1467**, Springer-Verlag, New York, 1991.
- [Wae] B. L. van der Waerden, *Modern Algebra*, Frederick Ungar Publishing Co., New York, 1931.
- [Wald] M. Waldschmidt, *Nombre transcendants*, Lecture Notes in Math., **402**, Springer-Verlag, New York, 1973.
- [Wi] E. Wirsing, Approximation mit algebraischen Zahlen beschränkten Grades, *J. reine angew. Math.* **206** (1961), 67-77.