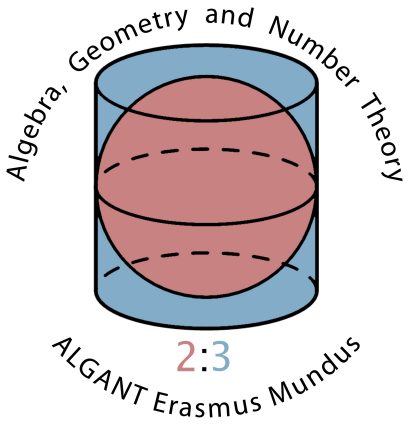

The dominant root assumption in problems with linear recurrences

Federico Zerbini

zerbini.federico@gmail.com

Advised by Prof. Yuri F. Bilu

ALGANT Master's Thesis - 7-th and 8-th of July, 2013

Università degli Studi di Milano and Université Bordeaux 1

The dominant root assumption in problems with linear recurrences

Federico ZERBINI

7-th and 8-th of July, 2013

Contents

Introduction

There are different equivalent definitions of linear recurrence, we can say that it is a complex valued function, defined on $\mathbb{N}$, of the form

$$F(n) = \sum_{i=1}^{h} c_i(n)\alpha_i^n,$$

with the *coefficients* $c_i \in \mathbb{C}[X]$ and the *roots* $\alpha_i \in \mathbb{C}$.

During the last 15 years some results in classical problems concerning linear recurrences have been obtained making use of the celebrated subspace theorem, a powerful result in diophantine approximation; above all we can cite the works of P. Corvaja and U. Zannier ([1], [4]). Unfortunately, very often these results rely on the assumption that the roots belong to a number field K, and that there exist a place v of K such that only one root has maximal absolute value with respect to v, which is widely considered not necessary for the results proved, but seems to be very difficult to remove. We will call it the *dominant root assumption*.

A breakthrough has been made in the article [3], again by Corvaja and Zannier, who managed to come over this difficulty without changing too much the approach, in the solution of a problem inspired by the so called *Pisot conjecture* (or Hadamard-quotient conjecture). Pisot conjectured that if the quotient of two linear recurrences F, G is an integer for every large $n \in \mathbb{N}$, then F/G itself is a linear recurrence. A. J. van der Poorten proved the conjecture in [15], without using the subspace theorem, but then Corvaja and Zannier tried

to go further, analysing the more general case where the quotient vanishes for not all, but infinitely many $n \in \mathbb{N}$. A first step toward the solution had already been made in [1], but they had used the dominant root assumption.

In [3] the authors basically make use of the previous methods, relying on the subspace theorem, but they find an ingenious way to simultaneously approximate the quotient F/G using all the roots with maximal absolute value (for some place v) without losing the possibility to apply the subspace theorem. It is believed that this technique could yield similar solutions in other problems usually approached assuming a dominant root, but nobody managed to do it yet.

In the first chapter, we briefly introduce the notation and the tools necessary to enunciate the subspace theorem (which is given in several different forms).

During the second chapter we give three equivalent definitions of linear recurrence, we state some important property like the *Skolem-Mahler-Lech theorem*, and we discuss some problems and results concerning linear recurrences, with a special emphasis on the problems solved using the subspace theorem.

In the third chapter, we focus our attention on two problems solved in [1] using the subspace theorem and the dominant root assumption: the already cited Hadamard-quotient problem, and a problem related to another conjecture due to Pisot, the so called d-th root conjecture. Pisot thought that if F is a linear recurrence with algebraic roots and coefficients, such that for every $n \in \mathbb{N}$ $F(n)$ is a d-th power in $\mathbb{Q}$, then there exists a linear recurrence G with algebraic roots and coefficients such that $F = G^d$. This fact has been proved for a general number field by Zannier in [16], without using the subspace theorem, but then again Corvaja and Zannier asked what happens if we have the assumptions of the conjecture only for infinitely many $n \in \mathbb{N}$, and again

for this kind of problem it works really well the subspace theorem, under the hypothesis of dominant root.

Finally, in the fourth chapter we present the proof of the Hadamard-quotient problem without using the dominant root assumption, trying to explain how the methods used are new in the context and cope with the absence of a dominant root.

Chapter 1

The subspace theorem

1.1 Places, heights and S-integers in number fields

This section is meant to be an introduction to the notation and to the objects needed to state the subspace theorem, so we will not give all the details and the proofs. References are [6] for what concerns number fields and places, and [12] for what concerns heights.

For all of this chapter we let K be a number field, i.e a finite field extension of the field $\mathbb{Q}$.

Definition 1.1.1. *An* absolute value *of K is a function $|\cdot| : K \to \mathbb{R}$ which satisfies the following conditions:*

(i) *$|x| > 0$ for every $x \in K^*$, and $|0| = 0$*

(ii) *$|xy| = |x| \cdot |y|$, for every $x, y \in K$.*

(iii) *$|x + y| \leq |x| + |y|$, for every $x, y \in K$.*

Furthermore, $|\cdot|$ is said to be non-archimedean *if, besides **(i)** and **(ii)**, it satisfies*

(iii)* $|x+y| \leq max\ \{|x|,|y|\}$, *for every* $x, y \in K$.
Obviously ***(iii)**** *is stronger than* ***(iii)***. *If* ***(iii)*** *holds but* ***(iii)**** *does not, then we say that* $|\cdot|$ *is* archimedean.

Note that any absolute value induces a metric d on the field K, defined as $d(x,y) = |x-y|$ for $x, y \in K$.

Definition 1.1.2. *Two absolute values are said to be* equivalent *if they induce equivalent metrics on* K. *This is an equivalence relation on the set of the absolute values of a field. It is possible to show that an archimedean absolute value cannot be equivalent to a non-archimedean absolute value.*

Definition 1.1.3. *A* place *of* K *is an equivalence class of absolute values, and we denote the set of places of* K *as* M_K. *Sometimes we will refer to the non-archimedean places as* finite places *and to the archimedean places as* infinite places. *We will denote the infinite places as* $M_{K,\infty}$.

Now let us consider the ring of integers $\mathcal{O}_K$ of K, it is a well known fact that for every $x \in K^*$ there exists a unique factorization of the fractional ideal $x\mathcal{O}_K$ as a product of powers of the maximal ideals of $\mathcal{O}_K$:

$$x\mathcal{O}_K = \prod \mathcal{P}^{v_{\mathcal{P}}(x)},$$

with $v_{\mathcal{P}}(x) \in \mathbb{Z}$. The uniqueness of the factorization implies that the function $v_{\mathcal{P}} : K^* \to \mathbb{Z}$ is uniquely determined by $\mathcal{P}$. We can extend $v_{\mathcal{P}}$ to K by defining $v_{\mathcal{P}}(0) := +\infty$; then for any constant $c \in (0,1)$ and for every maximal ideal $\mathcal{P}$ of $\mathcal{O}_K$ the function $|\cdot|_{\mathcal{P}} : K \to \mathcal{R}$ sending $x \mapsto c^{v_{\mathcal{P}}(x)}$ is a non-archimedean absolute value of K.

If we consider a number field extension $K \subset L$, then for a fixed prime ideal $\mathcal{P}$ of $\mathcal{O}_K$ we have again a unique factorization $\mathcal{P}\mathcal{O}_L = \mathcal{Q}_1^{e_1} \cdots \mathcal{Q}_r^{e_r}$, with $e_i \geq 1$, $\mathcal{Q}_i \neq \mathcal{Q}_j$ for $i \neq j$, and $r \geq 1$ (recall that e_i is called the *ramification index* of $\mathcal{Q}_i$ over $\mathcal{P}$). Moreover, let us fix the constant c for the absolute value $|\cdot|_{\mathcal{P}}$.

In this setting let us see, omitting the (trivial) proofs, some properties of the absolute values defined above:

Proposition 1.1.1. ***1)*** *For every i,*

$$|\cdot|_{\mathcal{Q}_i}\big|_K = |\cdot|_{\mathcal{P}}^{e_i}.$$

2) *The $|\cdot|_{\mathcal{Q}_i}$ are pairwise non equivalent.*

3) *Any non-archimedean absolute value on L whose restriction to K is equivalent to the absolute value $|\cdot|_{\mathcal{P}}$ is equivalent to $|\cdot|_{\mathcal{Q}_i}$ for some i.*

For what concerns the archimedean absolute values of a number field, to give examples let us consider the embeddings of K into $\mathbb{C}$. We list them as

$$\sigma_1, ..., \sigma_r : K \to \mathbb{R} \subset \mathbb{C}$$

real embeddings and

$$\sigma_{r+1}, \overline{\sigma}_{r+1}, ..., \sigma_{r+s}, \overline{\sigma}_{r+s} : K \to \mathbb{C}$$

complex embeddings, such that $\overline{\sigma}_j$ is the complex conjugated of σ_j, and $r+2s = [K : \mathbb{Q}]$. Then we define archimedean absolute values of K by $|x|_{\sigma_i} := |\sigma_i(x)|$, where $|\cdot|$ is the standard absolute value on $\mathbb{C}$, for $i = 1, ..., r+s$ (noting that $|\sigma_i(x)| = |\overline{\sigma}_i(x)|$), and we have that:

Proposition 1.1.2. *The $r+s$ archimedean absolute values defined above are pairwise non-equivalent.*

We want now to find a complete set of representatives for the places of our number field K. First of all, let us consider $K = \mathbb{Q}$. Here the maximal ideals are in one to one correspondence with the prime numbers, and to define the absolute value associated to every prime we choose the constants $c = c(p) = p^{-1}$. Then we have the following:

Theorem 1.1.1 (Ostrowski, 1935)**.** *The non-archimedean absolute values defined above, together with the standard (archimedean) absolute value, are a full list of representatives for the places of* $\mathbb{Q}$*.*

Note that when we consider any number field $\mathbb{Q} \subset K$, by Proposition 1.1.1 we see that the constant associated to any absolute value induced by a maximal ideal $\mathcal{P}_i$ is determined by the constant chosen for the prime p of $\mathbb{Z}$ lying below $\mathcal{P}_i$. Thus if we consider our choice of the constants for the rational primes (from now on this will be implicit), the theorem above together with the two propositions about the non-archimedean and archimedean absolute values defined before give the desired result:

Proposition 1.1.3. *The non-archimedean absolute values of* K *defined via the maximal ideals of* $\mathcal{O}_K$*, with the constants chosen as in the rational case, and the archimedean absolute values defined via the embeddings of* K *in* $\mathbb{C}$ *are a full list of representatives for the places of* K*.*

Given a valued field $(K, |\cdot|)$, where $|\cdot|$ is an absolute value, we already noticed that it can be seen as a metric space, hence we can talk about convergence of a sequence $\{a_n\} \subset K$, Cauchy sequences, completions and other analytical objects.

Definition 1.1.4. *A valued field* $(\hat{K}, ||\cdot||)$ *is called a* completion *of* $(K, |\cdot|)$ *if*

1) $K \subseteq \hat{K}$*, and* $||\cdot||$ *restricted to* K *is exactly* $|\cdot|$*.*

2) $(\hat{K}, ||\cdot||)$ *is complete.*

3) K *is dense in* $\hat{K}$*.*

Theorem 1.1.2. *A completion of* $(K, |\cdot|)$ *exists, and it is unique up to a unique isomorphism inducing the identity on* K*.*

Example 1.1.1. *If K is any number field, and $|\cdot| = |\cdot|_{\sigma_i}$ is an archimedean absolute value, then $\hat{K} = \mathbb{R}$ for $i = 1, ..., r$ (real embeddings) and $\hat{K} = \mathbb{C}$ for $i = r+1, ..., r+s$ (complex embeddings).*

Example 1.1.2. *If K is a number field, and $\mathcal{P} \subset \mathcal{O}_K$ is a maximal ideal, we denote by $\hat{K}_{\mathcal{P}}$ the completion of K with respect to the non-archimedean absolute value $|\cdot|_{\mathcal{P}}$. When $K = \mathbb{Q}$ and we consider a rational prime p, doing the completion we get $\mathbb{Q}_p := \hat{\mathbb{Q}}_p$ and we call it the field of p-adic numbers.*

Proposition 1.1.4. *Let us consider an extension of number fields $K \subset L$, and a prime ideal $\mathcal{Q}_i$ of $\mathcal{O}_L$ dividing $\mathcal{P}$ prime ideal of $\mathcal{O}_K$. If we denote by e_i the ramification index of $\mathcal{Q}_i$ over $\mathcal{P}$ and by f_i the inertial degree $[\mathcal{O}_L/\mathcal{Q}_i : \mathcal{O}_K/\mathcal{P}]$, then we have $[\hat{L}_{\mathcal{Q}_i} : \hat{K}_{\mathcal{P}}] = e_i f_i$.*

For any non-archimedean absolute value of K associated to a maximal ideal $\mathcal{P}_i$ lying over some rational prime p, with ramification index e_i and inertial degree f_i, we define the following normalization: $|\cdot|_i := |\cdot|_{\mathcal{P}_i}^{f_i}$.

Moreover, for any embedding σ_i we define the inertial degree $f_i := 1$ and the ramification index $e_i := 1$ if σ_i is a real embedding, and $e_i := 2$ if the embedding is complex. Then for any archimedean absolute value associated to an embedding of K in $\mathbb{C}$ we define the normalization: $|\cdot|_i := |\cdot|_{\sigma_i}^{e_i}$.

Let us remark that since the completion of $\mathbb{Q}$ with respect to the standard absolute value is $\mathbb{R}$, an analogous of the formula in the proposition above holds for archimedean absolute value too. Furthermore, we could have imposed this normalization in a quicker way by defining for any place v of K $d_v := [\hat{K} : \hat{\mathbb{Q}}]$, and then choosing the constant c for a finite place lying over p in such a way that $|p|_v = p^{-d_v}$, and similarly for infinite places.

Now we state one of the fundamental results of this chapter:

Theorem 1.1.3 (Product formula)**.** *With the normalization defined above for*

the places v of K, for every $x \in K^*$ we have

$$\prod_{v \in M_K} |x|_v = 1$$

Even if now, thanks to these normalizations, we have obtained a powerful tool, the product formula, we are going to see that they are not yet the final normalizations which we will deal with.

Definition 1.1.5. *Let $P = (x_0 : x_1 : ... : x_n) \in \mathbb{P}^n(K)$, we define the* (projective) field height *of P as*

$$H_K(P) := \prod_{v \in M_K} \max\{|x_0|_v, ..., |x_n|_v\}$$

where every v is normalized as in the statement of the product formula.

We want the product formula to hold because otherwise the height would not be 'projective': in fact, we need that $H_K(a\mathbf{x}) = H_K(\mathbf{x})$ for every $a \in K^*$.

One could check that for any number field extension $K \subset L$ of degree $[L : K] = d$, $H_L(P) = (H_K(P))^d$, so one solution to make the height independent of the field is to impose that $|\cdot|_v := |\cdot|_v^{1/[K:\mathbb{Q}]}$ for every $v \in M_K$, for every K. Since from now on we will always make use of this new normalization, it does not make confusion to denote these new representatives again by $|\cdot|_v$.

Definition 1.1.6. *Let $P = (x_0 : x_1 : ... : x_n) \in \mathbb{P}^n(K)$, taking into account this further normalization of the places of K we define the* (projective) height *of P as*

$$H(P) := \prod_{v \in M_K} \max\{|x_0|_v, ..., |x_n|_v\}$$

So, to resume, for any number field K we want places normalized in such a way that the product formula holds, and the height does not depend on the field. Therefore for what concerns every finite place lying over a rational prime p it suffices to choose the constant c in such a way that, if $[K : \mathbb{Q}] = d$,

$$|p|_v = p^{-d_v/d}.$$

Similarly for infinite places.

So from now on we will always consider places normalized as above.

Definition 1.1.7. *For $\alpha \in K$ we define the* height of α *as* $H(\alpha) := H(1 : \alpha)$.

Proposition 1.1.5. *The height has the following properties:*

1) *For s, r coprime integers, $r \neq 0$, it holds $H(s/r) = \max\{|s|, |r|\}$.*

2) *$H(\alpha^m) = (H(\alpha))^{|m|}$ for every $\alpha \in K$ and every $m \in \mathbb{Q}$.*

3) *For every $\alpha, \beta \in K$ it holds $H(\alpha\beta) \leq H(\alpha)H(\beta)$.*

4) *For every $\alpha \in K$, $2 \log H(\alpha) = \sum_{v \in M_K} |\log |\alpha|_v|$ where the absolute value on the right side is the standard one. Note that $\log H(\alpha) = \sum_{v \in M_K} \log^+ |\alpha|_v$: we call this quantity* logarithmic height *of α, and we denote it by $h(\alpha)$.*

5) *For every $\alpha_1, ..., \alpha_N \in K$ it holds $H(\alpha_1 + \cdots + \alpha_N) \leq N \prod_{n=1}^{N} H(\alpha_n)$.*

6) *$H(\sigma(\alpha)) = H(\alpha)$ for every $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$.*

We conclude our brief recall of the height in number fields with an important theorem:

Theorem 1.1.4 (Northcott)**.** *There exist at most finitely many algebraic numbers of bounded height and degree.*

Corollary 1.1.1 (Kronecker Theorem)**.** *The only algebraic numbers of height 1 are 0 or the roots of unity.*

Proof. It is a straightforward consequence of the theorem and of the second property in Proposition 1.1.5.

□

To conclude this preliminary section, we include a generalization of the notion of integers in number fields.

Definition 1.1.8. *For a finite set $S \subset M_K$, such that $M_{K,\infty} \subset S$, we define $\mathcal{O}_S = \mathcal{O}_{K,S} := \{x \in K : \forall\, v \notin S, |x|_v \leq 1\}$, and we call it the ring of S-*integers *(it is indeed easy to check that it is a ring).*

Note that when $S = M_{K,\infty}$, $\mathcal{O}_S = \mathcal{O}_K$. In general, $\mathcal{O}_S$ consists of those elements in K generating a fractional ideal whose denominator contains only primes from S. We recall the important generalization of the Dirichlet unit theorem:

Theorem 1.1.5. *$\mathcal{O}_S^* \simeq \mathbb{Z}^{(\#S-1)} \times T$, with T a finite group (the torsion part of $\mathcal{O}_S^*$).*

Proof. See [8].

If $S = M_{K,\infty}$, $\mathcal{O}_S^* = \mathcal{O}_K^*$ and $\#S = r + s$, so we get the classical Dirichlet theorem.

Definition 1.1.9. *We call $\mathcal{O}_S^*$ the group (with respect to the product) of S-*units *of K. It is easy to see that $\mathcal{O}_S^* = \{x \in K : \forall\, v \notin S, |x|_v = 1\}$.*

1.2 The subspace theorem, from Schmidt to Schlickewei

Again, we will not prove the majority of the results presented during this section, but we will give references for the (difficult) proofs of the main theorems.

Before formulating the celebrated subspace theorem, which is one of the most important results in diophantine approximation, we consider a theorem of Roth that a posteriori is only a particular case, but have a long and glorious history (Roth has been awarded the field medal for this), to make the general case more motivated.

Theorem 1.2.1 (Roth, 1955)**.** *Let α be an irrational real algebraic number. Then for any $\varepsilon > 0$ the inequality*

$$\left|\alpha - \frac{y}{x}\right| < \frac{1}{|x|^{2+\varepsilon}}$$

has only finitely many solutions in non-zero integers x, y.

Proof. See [9].

This is a best-possible result, in virtue of the well-known Dirichlet approximation theorem, which says that the inequality $|\alpha - y/x| \leq |x|^{-2}$ has infinitely many solutions. Sometimes Roth's theorem is known as Thue-Siegel-Roth theorem, because Roth did only the final (but very important and difficult) step of a series of results started in the first years of the 20-th century by A. Thue, who proved that $|\alpha - y/x| \leq |x|^{-n/2-1-\varepsilon}$ has finitely many solutions.

For $\mathbf{x} = (x_1, ..., x_n) \in \mathbb{Z}^n$ let us denote $||\mathbf{x}|| := \max\{|x_1|, ..., |x_n|\}$. It is easy to see that this is exactly the height of $\mathbf{x}$ introduced in the previous section, for a vector with integer and coprime coordinates. Now we are ready to state the subspace theorem:

Theorem 1.2.2 (Schmidt, 1972)**.** *Let $L_1, ..., L_n$ be linear forms in $X_1, ..., X_n$, linearly independent, with algebraic coefficients. Then for any $\varepsilon > 0$ the solutions $\mathbf{x} \in \mathbb{Z}^n$ of the inequality*

$$|L_1(\mathbf{x}) \cdots L_n(\mathbf{x})| \leq ||\mathbf{x}||^{-\varepsilon}$$

are contained in finitely many proper linear subspaces of $\mathbb{Q}^n$.

Proof. See [11].

Note that with $n = 2$, $L_1(x, y) = x\alpha - y$ and $L_2(x, y) = x$ we get that $|x| \cdot |x\alpha - y| \leq |x|^{-\varepsilon}$ has solutions x, y contained in finitely many hyperplanes of $\mathbb{Q}^2$, i.e. of the type $(x, \beta x)$; this is to say that there are only finitely many solutions $\beta = y/x$ to the inequality $|\alpha - y/x| \leq x^{-2-\varepsilon}$, which is the theorem of Roth.

We now give a generalization of the subspace theorem to any number field, due to H. P. Schlickewei, which is the one that we will need throughout our work. Let us denote $||\mathbf{x}||_v := \max\{|x_1|_v, ..., |x_n|_v\}$, for $\mathbf{x} \in K^n$ and $v \in M_K$.

Theorem 1.2.3 (Schlickewei, 1977)**.** *Let $S \subset M_K$ be a finite set of places, containing the infinite ones. Extend each $v \in S$ to $\overline{\mathbb{Q}}$ in some way. For $v \in S$ let $L_{1,v}, ..., L_{n,v}$ be linearly independent linear forms in n variables, with algebraic coefficients. Then for every $\varepsilon > 0$ the solutions $\mathbf{x} \in K^n$ of the inequality*

$$\prod_{v \in S} \prod_{i=1}^{n} \frac{|L_{i,v}(\mathbf{x})|_v}{||\mathbf{x}||_v} \leq H(\mathbf{x})^{-n-\varepsilon}$$

are contained in finitely many proper linear subspaces of K^n.

Proof. See [5].

Note that if $\mathbf{x} \in \mathcal{O}_S^n$, $||\mathbf{x}||_v \leq 1$ for $v \notin S$. It follows that

$$H(\mathbf{x}) = \prod_{v \in M_K} ||\mathbf{x}||_v \leq \prod_{v \in S} ||\mathbf{x}||_v.$$

Using this simple remark we obtain another very useful version of the subspace theorem:

Theorem 1.2.4. *Let $S \subset M_K$ be a finite set of places, containing the infinite ones. Extend each $v \in S$ to $\overline{\mathbb{Q}}$ in some way. For $v \in S$ let $L_{1,v}, ..., L_{n,v}$ be linearly independent linear forms in n variables, with algebraic coefficients. Then for every $\varepsilon > 0$ the solutions $\mathbf{x} \in \mathcal{O}_S^n$ of the inequality*

$$\prod_{v \in S} \prod_{i=1}^{n} |L_{i,v}(\mathbf{x})|_v \leq H(\mathbf{x})^{-\varepsilon}$$

are contained in finitely many proper linear subspaces of K^n.

Finally, we state one last version, a corollary of the previous one, where we want to deal with integers:

Corollary 1.2.1. *Let S be a finite set of places of $\mathbb{Q}$, containing the standard absolute value. Extend each $v \in S$ to $\overline{\mathbb{Q}}$ in some way. For $v \in S$ let $L_{1,v}, ..., L_{n,v}$ be linearly independent linear forms in n variables, with algebraic coefficients. Then for every $\varepsilon > 0$ the solutions $\mathbf{x} \in \mathbb{Z}^n$ of the inequality*

$$\prod_{v \in S} \prod_{i=1}^{n} |L_{i,v}(\mathbf{x})|_v \leq ||\mathbf{x}||^{-\varepsilon}$$

are contained in finitely many proper linear subspaces of $\mathbb{Q}^n$.

Proof. By the theorem we have that for every $\varepsilon > 0$ the solutions $\mathbf{x} \in \mathcal{O}_S^n$ of the inequality

$$\prod_{v \in S} \prod_{i=1}^{n} |L_{i,v}(\mathbf{x})|_v \leq H(\mathbf{x})^{-\varepsilon}$$

are contained in finitely many proper linear subspaces of $\mathbb{Q}^n$. Since for every $\mathbf{x} \in \mathbb{Z}^n$

$$H(\mathbf{x}) = \left(\prod_{p \text{ prime}} \max\{|x_1|_p, ..., |x_n|_p\} \right) \max\{|x_1|, ..., |x_n|\}$$

and $||\mathbf{x}|| := \max\{|x_1|, ..., |x_n|\}$, we have $H(\mathbf{x}) \leq ||\mathbf{x}||$ (and it is equal exactly when the coordinates of $\mathbf{x}$ are coprime). So we conclude, being $\mathbb{Z} \subseteq \mathcal{O}_S$ for every S, that for every $\varepsilon > 0$ also the solutions $\mathbf{x} \in \mathbb{Z}^n$ of the inequality

$$\prod_{v \in S} \prod_{i=1}^{n} |L_{i,v}(\mathbf{x})|_v \leq ||\mathbf{x}||^{-\varepsilon}$$

are contained in finitely many proper linear subspaces of $\mathbb{Q}^n$.

□

Let us remark that the Schmidt's subspace theorem is a trivial corollary of this last version, it suffices to choose S as the set containing only the infinite place.

Chapter 2

Linear recurrences

2.1 Definitions and examples

Definition 2.1.1. *A sequence* $\{F(n)\}_{n\in\mathbb{N}}$ *of complex numbers is called a* linear recurrence sequence*, or just a* linear recurrence*, if there exist* $a_0, ..., a_{r-1} \in \mathbb{C}$*, with* $r \geq 1$ *and* $a_0 \neq 0$*, such that*

$$F(n+r) = a_0F(n) + a_1F(n+1) + \cdots + a_{r-1}F(n+r-1) \tag{2.1}$$

for every $n \in \mathbb{N}$*. The minimum* r *with this property is called the* order *of the linear recurrence.*

Proposition 2.1.1. *For* $\{F(n)\}_{n\in\mathbb{N}}$ *sequence of complex numbers, the following are equivalent:*

(i) *F is a linear recurrence*

(ii) *There exists an expression, holding for every* $n \in \mathbb{N}$ *and essentially unique, of the type*

$$F(n) = \sum_{i=i}^{h} c_i(n)\alpha_i^n, \tag{2.2}$$

where the $c_i \in \mathbb{C}[X]$ *are non-zero polynomials and the* $\alpha_i \in \mathbb{C}$ *are distinct.*

(iii) *If we consider the power series* $\sum_{n\in\mathbb{N}} F(n)X^n$*, there exist polynomials* $p, q \in \mathbb{C}[X]$*, with* $\deg q < \deg p$*, such that*

$$\sum_{n=0}^{+\infty} F(n)X^n = \frac{q(X)}{p(X)}, \tag{2.3}$$

i.e. the power series above is a rational function.

Proof. (ii) ⇒ (i) Let us set $r(i) := \deg c_i$, and

$$r := \sum_{i=1}^{h} r(i).$$

Set

$$p(X) := \prod_{i=1}^{h}(1-\alpha_i X)^{r(i)} = 1 - a_0X - \cdots - a_{r-1}X^r \tag{2.4}$$

for some a_i's. Then the sequence $\{F(n)\}_{n\in\mathbb{N}}$ satisfies for every $n \in \mathbb{N}$ the linear recurrence relation

$$F(n+r) = a_0F(n) + a_1F(n+1) + \cdots + a_{r-1}F(n+r-1).$$

This because if we consider $E : F(n) \mapsto F(n+1)$ the shift operator and $\Delta := E - 1$ the difference operator, it holds

$$(E-\alpha_i)(c_i(n)\alpha_i^n) = c_i(n+1)\alpha_i^{n+1} - c_i(n)\alpha_i^{n+1} = (\Delta(c_i(n)))\alpha^{n+1},$$

and since $\Delta(c_i(n))$ has lower degree than does c_i, by linearity and induction we conclude that

$$\prod_{i=1}^{h}(E-\alpha_i)^{r(i)}$$

annihilates the sequence $\{F(n)\}_{n\in\mathbb{N}}$ as asserted.

(i) ⇒ (iii) If we consider for the polynomial $p(X) := 1 - a_0X - \cdots - a_{r-1}X^r$

$$p(X)\sum_{n=0}^{+\infty} F(n)X^n,$$

we see that the coefficients of X^m vanish for every $m \geq r$, in virtue of the equation 2.1, which holds by assumption for every $n \in \mathbb{N}$. So the product

equals $q(X)$, a polynomial with degree strictly lower than $r = \deg p$, as claimed.
(iii) ⇒ (ii) A partial fraction expansion yields[1]

$$\frac{q(X)}{p(X)} = \sum_{i=1}^{h} \sum_{j=1}^{r(i)} \frac{q_{ij}}{(1-\alpha_i X)^j} = \sum_{n=0}^{+\infty} \Big(\sum_{i=1}^{h} \sum_{j=1}^{r(i)} q_{ij} \binom{n+j-1}{j-1} \alpha_i^n \Big) X^n$$

and from this expression it is clear that the coefficients of X^n satisfy 2.2.
□

In general in the next chapters we will think linear recurrences as objects of the form 2.2; we will call *coefficients* the c_i's and *roots* the α_i's. The roots of the linear recurrence are exactly the zeros of the polynomial $X^r p(X^{-1})$, reciprocal to the polynomial 2.4, and we call it the *characteristic polynomial* of F. When the coefficients c_i are constant, we say that the linear recurrence is a *power sum*.

Note that the form 2.3 leads to interesting consequences, for example the fact that the Hadamard product

$$\sum_{n=0}^{+\infty} F(n)G(n)X^n$$

of two rational functions $\sum F(n)X^n$ and $\sum G(n)X^n$ is again a rational function: this follows from the trivial remark that the linear recurrences form a ring; to see this it suffices to consider the form 2.2.

Example 2.1.1 (Fibonacci sequence)**.** *This is probably the most famous example of linear recurrences. The Fibonacci sequence is defined by* $F(0) = 0$, $F(1) = 1$, *and obeys the rule* $F(n+2) = F(n)+F(n+1)$ *for every* $n \in \mathbb{N}$. *With the notation adopted during the proof of the proposition,* $p(X) = 1 - X - X^2$, *and we have that*

$$\sum_{n=0}^{+\infty} F(n)X^n = \frac{X}{1-X-X^2}$$

[1]Just from a formal point of view, we have the expansion $\frac{1}{(1-\alpha_i X)^j} = (\sum_{n=0}^{+\infty} \alpha_i^n X^n)^j$, then a combinatorial argument permits to express the j-th power of a series explicitly making use of some binomial coefficients.

Moreover, the characteristic polynomial is $X^2p(X^{-1}) = X^2 - X - 1$*, which has its zeros in* $(1+\sqrt{5})/2$ *and* $(1-\sqrt{5})/2$*. So we have found the roots* α_i*'s of our linear recurrence. To find the coefficients, we could again exploit the proof above, because we wrote explicitly how to pass from the form 2.3 to the form 2.2, but we prefer to use another method, not valid in general for every linear recurrence, but nice and really simple.*

Note that, for every $n \in \mathbb{N}$*,*

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} F(n+1) \\ F(n) \end{bmatrix} = \begin{bmatrix} F(n+2) \\ F(n+1) \end{bmatrix}.$$

So iterating this, and knowing the initial values of the Fibonacci sequence, we have

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^n \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} F(n+1) \\ F(n) \end{bmatrix}.$$

On the other hand, we know from linear algebra that to compute a high power of a matrix the task is fairly easy once we have diagonalized it (and this is not possible for every linear recurrence). First, we must find the eigenvalues, which are determined by the characteristic polynomial, that for

$$A = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$$

is $\lambda^2 - \lambda - 1$*, that is nothing but the characteristic polynomial that we found using the definition of characteristic polynomial of a linear recurrence! Now, call* $\alpha_1 := (1+\sqrt{5})/2$ *and* $\alpha_2 := (1-\sqrt{5})/2$ *the two eigenvalues. We know that*

$$A = S \begin{bmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{bmatrix} S^{-1} = S\Lambda S^{-1},$$

and it is not difficult to find that

$$S = \begin{bmatrix} \alpha_1 & \alpha_2 \\ 1 & 1 \end{bmatrix}.$$

Then $A^n = S\Lambda^n S^{-1}$*, so with a little work we find that* $F(n)$*, i.e. the second entry of the column vector*

$$A^n \begin{bmatrix} 1 \\ 0 \end{bmatrix},$$

is

$$\frac{1}{\sqrt{5}}(\alpha_1^n - \alpha_2^n).$$

So we have found a compact formula for the Fibonacci sequence, which is nothing but the form 2.2 of the recurrence! Moreover, we conclude that the Fibonacci sequence is a power series, because the coefficients are constant.

Definition 2.1.2. *A linear recurrence* F *is said to be* non-degenerate *if no ratio of two distinct roots is a root of unity.*

Remark 2.1.1. *We will frequently assume that our recurrences are non-degenerate, or even the stronger fact that their roots generate a torsion free multiplicative group* Γ*, but this is a kind of 'harmless' hypothesis in most of the cases, thanks to the following fact: if* q *is the order of the torsion in* Γ*, then for each* $r = 0, 1, ..., q-1$ *the recurrences* $F_r(n) := F(nq + r)$ *have roots generating a torsion-free group (they all lie in the torsion-free group* Γ^q*).*

2.2 Properties and zeros

It will be useful for future purposes to clarify the structure of this multiplicative group Γ, generated by the linear recurrences' roots:

Proposition 2.2.1. *Let* $\Gamma \subset \mathbb{C}^*$ *be a torsion-free multiplicative abelian group of rank* $t \geq 1$*. The ring of linear recurrences whose roots belong to* Γ *is isomorphic to the ring* $\mathbb{C}[X, T_1, ..., T_t, T_1^{-1}, ..., T_t^{-1}]$*.*

Proof. Let $(\beta_1, ..., \beta_t)$ be a basis of Γ. Note that $\beta_1, ..., \beta_t$ are multiplicatively independent. To each variable T_i $(i = 1, ..., t)$ we associate the

function $f_i : n \mapsto \beta_i^n$, and to the variable X we associate the identity function $I : n \mapsto n$. Hence we obtain a surjective ring homomorphism from $\mathbb{C}[X, T_1, ..., T_t, T_1^{-1}, ..., T_t^{-1}]$ to the ring of linear recurrences having their roots in Γ. Since $\beta_1, ..., \beta_t$ are multiplicatively independent, we can conclude that the functions $I, f_1, ...f_t$ are algebraically independent. This is enough to prove the injectivity of our ring homomorphism, because if it was not injective, then there would exist a non-zero polynomial $p(X_1, ..., X_{t+1})$ (which represent an element of $\mathbb{C}[X, T_1, ..., T_t, T_1^{-1}, ..., T_t^{-1}]$ which goes to zero via the morphism, and we can assume it is in fact in $\mathbb{C}[X, T_1, ..., T_t]$ multiplying it by a suitable unit of the ring) such that $p(I, f_1, ..., f_t) = 0$, i.e. we would not have the algebraic independence.

□

Remark 2.2.1. *The proposition above tells us that the ring of linear recurrences is in particular a unique factorization domain. From now on, divisibility properties in the ring of linear recurrences, such that coprimality, will be understood in this sense.*

Now we want to describe the set $\mathcal{Z} := \{n \in \mathbb{N} : F(n) = 0\}$ for a linear recurrence F. If F is degenerate, it is easy to see that $\mathcal{Z}$ may be infinite, for example we can consider $F(n) = 2^n + (-2)^n$. For what concerns non-degenerate recurrences, there are specific cases that can be studied with very elementary methods, for example it holds the following:

Proposition 2.2.2. *If F is a linear recurrence with real coefficients and real positive roots (so it is non-degenerate), the number of zeros of F is bounded by its order $r = r_1 + \cdots r_h$, where $r_i = \deg c_i$.*

Proof. We do the proof for $F(x)$ with x real variable, instead of natural, and we will therefore obtain a stronger result. The claim is clearly true for $h = 1$, by the fundamental theorem of algebra. Now let us suppose it true

for $h \leq q-1$, we want to prove it for $h = q$. Every α_i^x can be written as $e^{x\gamma_i} := e^{x \log \alpha_i}$ and every $c_i(x)$ as $\sum_{j=o}^{r_i} a_{i,j}x^j$. Suppose that for some F linear recurrence with $h = q$, the number of zeros is greater than its order r. In this case the number of zeros of the function

$$\frac{d^{r_1}}{dx^{r_1}} e^{-x\gamma_1} F(x) = \sum_{i=2}^{q} e^{x(\gamma_i - \gamma_1)} \sum_{j=0}^{r_i} b_{i,j} x^j,$$

which is a linear recurrence of the same type, with $h = q-1$, exceed its order $r' = \sum_{i=2}^{q} r_i$, because of Rolle's theorem. This is a contradiction that proves the proposition.

□

This was only a special case, but now we will state a very important theorem, discovered independently by several authors, that tells us that $\mathcal{Z}$ is always a finite set for non-degenerate linear recurrences. In fact, it tells us something more:

Theorem 2.2.1 (Skolem-Mahler-Lech)**.** *The set of zeros of a linear recurrence F is the union of a finite set with a finite union of arithmetic progressions. If F is non-degenerate, it is a finite set.*

There are different proofs of this result, we will present a very elegant one which involves p-adic analysis, taken from [14]. Since it is not our aim to give every detail of the p-adic analytic methods used, we give as a reference [7], and we will just sketch out the proof.

Proof. Let us suppose $F \neq 0$. Let us consider the field K obtained by adding to $\mathbb{Q}$ the roots α_i's and the coefficients of the polynomials c_i's of our linear recurrence F. Let us fix a prime p such that it is possible to embed K in a finite extension L_p of $\mathbb{Q}_p$, and every α_i is a p-adic unit. This is always possible, being infinite the transcendence degree of $\mathbb{Q}_p$ over $\mathbb{Q}$ (see [13]). Note that if K is a number field, it suffices to embed K into its completion K_v, for a finite place v such that $|\alpha_i|_v = 1$ for every i. So from now on we will consider

everything in L_p, with $|\cdot|_p$ defined as the (only) absolute value of L_p which extends $|\cdot|_p$ of $\mathbb{Q}_p$ (see [7], theorem 10 pag. 58).

Now for $D(y,r)$ denoting the set $\{x \in L_p : |x-y|_p < r\}$ and $r_p := p^{-1/p-1}$, let us consider the two (analytic) functions $\log_{(p)} : D(1,1) \to \Omega$, and $\exp_{(p)} : D(0,r_p) \to \Omega$, defined as

$$\begin{aligned} \log_{(p)}(x) &:= \sum_{k=1}^{+\infty} \frac{(-1)^{k+1}}{k}(x-1)^k, \\ \exp_{(p)}(x) &:= \sum_{k=0}^{+\infty} \frac{x^k}{k!}. \end{aligned}$$

It is possible to prove that in the disc $D(1,r_p)$ $\log_{(p)}$ is injective, its image is $D(0,r_p)$ and its inverse is $\exp_{(p)}$, so we can say that for $x \in D(1,r_p)$ $\exp_{(p)}(\log_{(p)}(x)) = x$ (see [7], pag 81).

It is not difficult to see that $D(1,r_p)$ is a subgroup of $D(1,1)$ of finite index, and that for every p-adic unit x, we have $x^{q-1} \in D(1,1)$, with q the cardinal of L_p. Therefore, there exist $N \in \mathbb{N}$ such that for every i, $\alpha_i^N \in D(1,r_p)$. For every $R = 0, ..., N-1$, let us define

$$F_R(m) := \sum_{i_1}^{h} c_i (mN+R)\alpha^R (\alpha_i^N)^m.$$

Being[2] $(\alpha_i^N)^m = \exp_{(p)}(m \log_{(p)}(\alpha_i^N))$, we have that F_R is an analytic function for every R, so if $F_R(m) = 0$ for infinitely many naturals m, we conclude that F_R is identically zero, because the set of p-adic integers in L_p is compact, so there is some limit point for these zeros (this is the analogous of the well-known theorem that asserts that an analytic function defined over a domain in $\mathbb{C}$ cannot have a limit point for its zeros, unless it is identically zero). Therefore some of the F_R's will be identically zero, while the remaining F_R's will have each a finite number of zeros, and this proves the first part of the theorem.

[2]It is possible to prove that for $\log_{(p)}$ and $\exp_{(p)}$ hold basically the same properties of the real logarithm and exponential.

Suppose now that $F_R = 0$, for some $R \in \{0, ..., N-1\}$. Then for every $m \in \mathbb{N}$

$$F_R(m) = \sum_{i_1}^{h} c_i(mN + R)\alpha^R(\alpha_i^N)^m = 0.$$

This means that for every i there exists at least one $j \neq i$ such that $\alpha_i^N = \alpha_j^N$, because we can assume that no c_i is identically zero, which in turn means that α_i/α_j is a root of unity, namely F is degenerate.

□

Note that if we suppose that the roots belong to a number field K, and that there is a dominant root, namely there exists a root α_i such that $|\alpha_i|_v > |\alpha_j|_v$ for every $j \neq i$ and some absolute value $v \in M_K$, then $|F(n)|_v \gg |\alpha_i|_v^n$, and so the set $\mathcal{Z}$ is finite. This is a first instance of the fact that the apparently innocent assumption, usually verified, of the existence of a dominant root for some absolute value v, can be incredibly useful in order to simplify proofs of theorems concerning linear recurrences.

2.3 Linear recurrences and the subspace theorem

If we consider two linear recurrences F and G, we can ask whether their quotient is again a linear recurrence or not. Since by 2.3 the values assumed by a linear recurrence are nothing but the coefficients of the power series expansion of a rational function, an equivalent way to formulate this question is to ask whether the Hadamard quotient of two rational functions is again a rational function or not. By the expression 2.2, a necessary condition for being a recurrence is obviously that all the values $F(n)/G(n) \in \mathcal{R}$, where $\mathcal{R}$ is a finitely generated commutative sub-ring of $\mathbb{C}$. Pisot conjectured that this condition was sufficient, and this has been proved by van der Poorten in [15]. But one

could also ask what happens when the quotient lies in a finitely generated ring for infinitely many n, which seemed to be a more difficult question.

A first partial answer has been given in [1] by Corvaja and Zannier:

Theorem 2.3.1. *For F and G power sums with rational coefficients, and roots in $\mathbb{N}$, assume that $F(n)/G(n)$ is an integer for all n in an infinite sequence $\mathcal{N}$. Then there exists a power sum of the same type Q such that $F = GQ$.*
In particular, the set of natural numbers n such that $F(n)/G(n)$ is an integer differs by a finite set from a finite union of arithmetic progressions.

In other words, if we do not have divisibility in the ring of power sums, there is no divisibility between the values, with a finite number of exceptions at most. Note that the last conclusion in the statement reminds the Skolem-Mahler-Lech theorem, stated in the previous section.

The proof of this result makes use of the subspace theorem. But why the subspace theorem?

First of all because all the values assumed by a linear recurrence (and so a power sum) F defined over a number field K are expressible as sums of a bounded number of S-units, for some finite $S \subset M_K$. Another reason comes from the fact that we are considering infinitely many values in our statements, so if these values meet the assumptions of the subspace theorem (after having defined in a clever way the other variables, and the linear forms), we conclude that infinitely many lie in the same hyperplane, which is in general the key point of this kind of proofs. Anyway, we will see the proof in details in the next chapter.

One would like to generalize theorem 2.3.1, and this is partially possible: it is not difficult to consider linear recurrences instead of power sums, to have a degenerate linear recurrence (which is not the case of the statement above, since we have positive distinct roots), to consider a finitely generated ring $\mathcal{R}$ instead of $\mathbb{Z}$ and to have roots and coefficients in a general number field

instead of $\mathbb{Q}$. Even this last assumption is harmless, because from the number field case we can get the general case, thanks to a specialization argument developed by Rumely and van der Poorten that we will see in Chapter 4. The only assumption that still has to be considered for any of these generalisations is the dominant root assumption, that obviously holds in the statement above.

Thanks to a brilliant argument, which again relies on the subspace theorem, Corvaja and Zannier in [3] finally managed to overcome this crucial difficulty, and this will be the subject of chapter 4.

Actually the method of [1] yields, more precisely, a non-trivial bound for the cancellation in the quotient $F(n)/G(n)$, i.e for the $g.c.d(F(n), G(n))$. For example a consequence of works of Bugeaud, Corvaja and Zannier in this direction is the proof of the following theorem, which is a sharp form of a conjecture of Győry-Sarkozy-Stewart.

Theorem 2.3.2. *Let $a > b > c > 0$ be integers. Then for a tending to infinity, the greatest prime factor of $(ab+1)(ac+1)$ tends to infinity.*

Proof. See [2].

Now let us consider the power series expansion of a rational function

$$y(X) = \sum_{n=0}^{+\infty} F(n)X^n,$$

with $F(n) \in \mathbb{Q}$ for all n, and suppose that it is the Hadamard d-th power of another power series with coefficients in $\mathbb{Q}$

$$z(X) = \sum_{n=0}^{+\infty} G(n)X^n.$$

Then it was conjectured, again by Pisot, that z is a rational funtion. We could re-formulate it claiming that if a linear recurrence F is such that $F(n)$ is a rational number and a d-th power for every $n \in \mathbb{N}$, then there exist another linear recurrence G such that for every n $G(n) \in \mathbb{Q}$ and $G(n)^d = F(n)$.

This conjecture became a theorem after the proof (in a more general setting, with a number field K instead of $\mathbb{Q}$) presented by Zannier in [16], that does not make use of the subspace theorem. However, again we are also interested in what happens when the assumptions of the conjecture hold for infinitely many n, but not necessarily for all $\mathbb{N}$, and in fact we can say something if we consider power sums: the subspace theorem shows off one more time his powerfulness in the proof of the following result, that appears (in a slightly different form) in [1].

Theorem 2.3.3. *Let F be a power sum with rational coefficients and positive rational roots, and let d be a positive integer. Assume that $F(n)$ is a d-th power of a rational for infinitely many $n \in \mathbb{N}$, then $F(n) = \alpha^{n+r}G(n)^d$ for all $n \in \mathbb{N}$, where α is a non-zero rational number, r is an integer and G is a power sum with rational roots and coefficients. In particular, F is a d-th power of a power sum with algebraic coefficients and rational roots.*

In fact, in [1] there is a more general version of this theorem, and a further generalizations appears in [4]:

Theorem 2.3.4. *Let F be a power sum with roots and coefficients lying in a number field K. Assume that for some absolute value v, we have $1 \neq |\alpha_1|_v > \max\{|\alpha_2|_v, ..., |\alpha_h|_v\}$. Let $g \in K[X, Y]$ be monic in Y and suppose that for an infinite sequence of $n \in \mathbb{N}$, the equation $g(F(n), Y) = 0$ has a solution $Y = y(n) \in K$. Then there exist $d_j, \beta_j \in \overline{K}^*$, $j = 1, ..., k$, and an arithmetic progression $\mathcal{N}$ such that for $n \in \mathcal{N}$ we have*

$$g\Big(\sum_{i=1}^{h} c_i\alpha_i^n, \sum_{j=1}^{k} d_j\beta_j^n\Big) = 0.$$

In the proof of this result, which involves Puiseux expansion, the authors make use of the subspace theorem and of the dominant root assumption, and nobody managed to approach successfully this problem without the dominant root.

In the next chapter, we will show in details how the subspace theorem is used to prove the results mentioned above, assuming that there is a dominant root. We do not want to enter too much in technical details, so we will just prove theorem 2.3.1 and theorem 2.3.3, where we are in very simple settings. However the proofs of the generalizations rely basically on the same ideas.

To conclude this section, let us state an obvious corollary of theorem 2.3.3:

Corollary 2.3.1. *Let F be a power sum with rational roots and coefficients, and let d be a positive integer. Assume that $F(n)$ is a d-th power of a rational for infinitely many $n \in \mathbb{N}$. Then there exist positive integers Q and R and a power sum G with rational roots and coefficients such that $F(Qn+R) = G(n)^d$ for all $n \in \mathbb{N}$.*

We cited this result because, if we compare it with the second part of theorem 2.3.1, we can remark that in both cases if the underlined property of $F(n)$ (and $G(n)$) holds for infinitely many $n \in \mathbb{N}$, then it holds for all n in suitable arithmetic progressions, similarly to the Skolem-Mahler-Lech theorem. This seems to be a rule more than a coincidence.

Chapter 3

Two problems solved using the dominant root

3.1 A fundamental lemma

We want to present through two different simple examples, i.e. theorems 2.3.1 and 2.3.3, how the subspace theorem makes his part in results concerning linear recurrences (power sums in this case). So first of all we will state a lemma, where we find the key part of the method introduced by Corvaja and Zannier, and that will be used in the proofs of the two results cited above. It is here that we will see the subspace theorem working.

Lemma 3.1.1. *Let K be a number field (embedded in $\mathbb{C}$), and $F : n \mapsto c_1\alpha_1^n + \cdots + c_h\alpha_h^n$ be a non-degenerate power sum, with coefficients lying in K and roots lying in $\mathbb{Q}$. Let $\mathcal{N}$ be an infinite subset of $\mathbb{N}$, and let $z(n) \in \mathcal{R}$ for every $n \in \mathcal{N}$, with $\mathcal{R}$ a finitely generated commutative subring of $\mathbb{Q}$. Suppose that $z(n)$ is such that $H(z(n))/\max\{1, |z(n)|\} \ll C^n$ and $|z(n) - F(n)| \ll (l/C)^n$, with C a positive real constant and $0 < l < 1$. Then there exists a power sum G with coefficients lying in $\mathbb{Q}$ such that any root of G is a root of F, and $z(n) = G(n)$ for every $n \in \mathcal{N}_1$, with $\mathcal{N}_1$ an infinite subset of $\mathcal{N}$.*

Proof. Let S be the set of absolute values of $\mathbb{Q}$ consisting of the (standard) infinite absolute value and all the primes dividing the numerator or the denominator of some α_i (i.e. such that every α_i is an S-unit). Moreover, let us enlarge S in such a way that $\mathcal{R} \subset \mathcal{O}_S$. Let us denote by ∞ the infinite absolute value.

For every $v \in S$ and every $i = 0, 1, ..., h$ we define linear forms on $\mathbb{Q}^{h+1}$ as follows:

$$L_{0,\infty}(\mathbf{X}) := X_0 - \sum_{j=1}^{h} c_j X_j,$$

and $L_{i,v}(\mathbf{X}) = X_i$ for every couple of indexes $(i, v) \neq (0, \infty)$.

Consider, for $n \in \mathcal{N}$, the vector $\mathbf{x}(n) = (z(n), \alpha_1^n, ..., \alpha_h^n) \in \mathcal{O}_S^{h+1}$. Then we have

$$\prod_{v\in S}\prod_{i=0}^{h} |L_{i,v}(\mathbf{x}(n))|_v = |z(n) - F(n)| \prod_{v\in S\setminus\{\infty\}} |z(n)|_v \prod_{i=1}^{h} \Big(\prod_{v\in S} |\alpha_i^n|_v \Big).$$

Now note that being the α_i's S-units, by the product formula we get that

$$\prod_{i=1}^{h} \Big(\prod_{v\in S} |\alpha_i^n|_v \Big) = 1.$$

Moreover, we obviously have that

$$\prod_{v\in S\setminus\{\infty\}} |z(n)|_v \leq H(z(n))/\max\{1, |z(n)|\}$$

whence we conclude that

$$\prod_{v\in S}\prod_{i=0}^{h} |L_{i,v}(\mathbf{x}(n))|_v \ll (l/C)^n C^n = l^n,$$

where we have used our assumptions on the numbers $z(n)$.

On the other hand $H(\mathbf{x}(n)) \ll A^n$ for some positive real constant A independent of n (again because of our assumptions on $z(n)$), so we have that for every $n \geq n_0$, for some $n_0 \in \mathbb{N}$, there exist k_1 and k_2 positive real constants such that $H(\mathbf{x}(n)) \leq k_1 A^n$, and

$$\prod_{v\in S}\prod_{i=0}^{h} |L_{i,v}(\mathbf{x}(n))|_v \leq k_2 l^n.$$

We can suppose that $k_1 = 1$ and $A > 1$. Then $H(\mathbf{x}(n))^{-\varepsilon} \geq A^{-n\varepsilon}$, and so for every $\varepsilon < \log(1/L)/\log A$ and $n \geq n_0$, with $L := \max\{1, k_2\} \cdot l$, we have, since $A > 1$,

$$\prod_{v \in S} \prod_{i=0}^{h} |L_{i,v}(\mathbf{x}(n))|_v \leq k_2 l^n \leq L^n < H(\mathbf{x}(n))^{-\varepsilon}.$$

So by the version 1.2.4 of the subspace theorem, considering the number field $\mathbb{Q}$, there exist finitely many non-zero rational linear forms Λ_j such that each vector $\mathbf{x}(n)$ is a zero of some Λ_j.

Suppose first that Λ_j does not depend on X_0. Then if $\Lambda_j(\mathbf{x}(n)) = 0$ we have a non-trivial relation $u_1\alpha_1^n + \cdots + u_h\alpha_h^n$, with u_i's belonging to $\mathbb{Q}$, but we are supposing that F is non-degenerate, so by the Skolem-Mahler-Lech Theorem this can happen only for a finite subset of $\mathcal{N}$.

Hence there is some rational linear form Λ, depending on X_0, such that $\Lambda(\mathbf{x}(n)) = 0$ holds for infinitely many $n \in \mathcal{N}$. We may write

$$\Lambda(\mathbf{X}) = X_0 - \sum_{i=1}^{h} v_i X_i,$$

with v_i's belonging to $\mathbb{Q}$.

Now define $G(n) := v_1\alpha_1^n + \cdots v_h\alpha_h^n$. This is a power sum with coefficients lying in $\mathbb{Q}$, and by definition every root of G is a root of F. Moreover, $G(n) = z(n)$ for n lying in an infinite subsequence $\mathcal{N}_1$ of $\mathcal{N}$, so we have our claim.
□

Now we are ready to prove the two theorems mentioned above, and in the proofs it will be crucial the dominant root assumption.

3.2 The quotient of two linear recurrences

First of all, we need another result, which is interesting in itself and simple to obtain:

Lemma 3.2.1. *Let $F(n) = c_1\alpha_1^n + \cdots + c_h\alpha_h^n$ be a non-degenerate power sum with rational coefficients and rational roots, such that $F(n) \in \mathbb{Z}$ for infinitely many $n \in \mathbb{N}$. Then the roots of F are in $\mathbb{Z}$.*

Proof. Let $F = c_1\alpha_1^n + \cdots + c_h\alpha_h^n$ be non-degenerate and suppose that its roots lie in $\mathbb{Z}$. Suppose that for infinitely many n we have that $p^n|F(n)$. Finally, suppose by contradiction that there exists $i \in \{1, ..., h\}$ such that $p \nmid \alpha_i$.

We want to apply the subspace theorem taking $N = h$ and S consisting of ∞, p and every absolute value which divides some of the α_i's. We define $L_{1,p}(\mathbf{X}) := c_1X_1 + \cdots + c_hX_h$, and for every other couple $(i, v) \neq (1, p)$, such that $i \in \{1, ..., h\}$ and $v \in S$, we define $L_{i,v}(\mathbf{X}) := X_i$.

Now for every n such that $p^n|F(n)$, consider $\mathbf{x}(n) := (\alpha_1^n, ..., \alpha_h^n)$. Then we get

$$\prod_{v\in S}\prod_{i=0}^{h}|L_{i,v}(\mathbf{x}(n))|_v = |L(\mathbf{x}(n))|_p \prod_{v\in S\setminus\{p\}}|\alpha_1^n|_v \prod_{i=2}^{h}\Big(\prod_{v\in S}|\alpha_i^n|_v\Big).$$

Being the α_i's S-units by assumption, by the product formula we get that

$$\prod_{i=2}^{h}\Big(\prod_{v\in S}|\alpha_i^n|_v\Big) = 1$$

Moreover, $|\alpha_1^n|_p = 1$ by our hypothesis of absurd (we can suppose that the i such that $p \nmid \alpha_i$ is $i = 1$), so again by the product formula

$$\prod_{v\in S\setminus\{p\}}|\alpha_1^n|_v = 1$$

Therefore

$$\prod_{v\in S}\prod_{i=0}^{h}|L_{i,v}(\mathbf{x}(n))|_v = |L(\mathbf{x}(n))|_p \leq p^{-n} < (\max\{|\alpha_i^n|\})^{-\varepsilon} = ||\mathbf{x}(n)||^{-\varepsilon}$$

for $\varepsilon < \log p/\log(\max\{|\alpha_i|\})$. Then we can apply the version 1.2.1 of the subspace theorem, obtaining that infinitely many vectors $\mathbf{x}(n)$ lie in one hyperplane, which is to say that $b_1\alpha_1^n + \cdots + b_h\alpha_h^n = 0$ has infinitely many solu-

tions, with the b_i's belonging to $\mathbb{Q}$, which is absurd by the Skolem-Mahler-Lech Theorem, because F was non-degenerate.

So we have that $p|\alpha_i$ for every i. Now let us consider F as in the statement of the Lemma. Thus we can write

$$F(n) = c_1\Big(\frac{a_1}{b_1}\Big)^n + \cdots + c_h\Big(\frac{a_h}{b_h}\Big)^n$$

Let us set $b := l.c.m.(b_1, ..., b_h)$. Then $G : n \mapsto b^n F(n)$ has roots in $\mathbb{Z}$. Being $G(n)$ an integer for infinitely many $n \in \mathbb{N}$ too, we have that for these n $p^n|G(n)$ for every p prime dividing b.

By what we have proved above, for every p dividing b we can conclude that $p|ba_1/b_i$. But for every p fixed, there exists b_i such that $p|b_i$ but $p \nmid b/b_i$, so $p|a_i$, which is absurd unless $p = 1$, since we can assume that $g.c.d.(a_i, b_i) = 1$. This means that $b = 1$, which is to say that F has roots in $\mathbb{Z}$.

□

Now we are ready to prove the Theorem 2.3.1 announced in the previous chapter:

Proof of theorem 2.3.1. Write $G(n) = c_1\alpha_1^n + \cdots + c_h\alpha_h^n$ with non-zero c_i's and $\alpha_1 > \alpha_2 > ... > \alpha_h > 0$. Set

$$K(n) := -\sum_{i=2}^{h} \frac{c_i}{c_1}\Big(\frac{\alpha_i}{\alpha_1}\Big)^n,$$

then K is a power sum with rational coefficients and positive rational roots, and we have $K(n) \ll |\alpha_2/\alpha_1|^n$, so we may write

$$\frac{1}{G(n)} = (c_1\alpha_1)^{-n}\frac{1}{1 - K(n)} = (c_1\alpha_1)^{-n}\sum_{r=0}^{\infty} K(n)^r,$$

the expansion being convergent for n large enough.

We can say that $|F(n)| \ll A^n$ for a positive real number A and pick R such that $l := A|\alpha_2/\alpha_1|^R < 1$. If we set

$$L(n) := (c_1\alpha_1)^{-n}\sum_{r=0}^{R} K(n)^r,$$

we get that $P := FL$ has rational positive roots, so it is non-degenerate.

Now let us call $z(n) := F(n)/G(n)$ for $n \in \mathcal{N}$. Being $z(n)$ integers, we have that $H(z(n))/\max\{1, |z(n)|\} \leq 1$, moreover $|z(n) - P(n)| \ll l^n$ for $0 < l < 1$, by our choice of R, so we may apply Lemma 3.1.1 obtaining that for infinitely many integers $n \in \mathcal{N}_1$ $z(n) = Q(n)$ for Q a power sum with rational coefficients and positive rational roots.

Then we can use Lemma 3.2.1 and conclude that Q has positive integer roots. This means in turn that the power sum $F - GQ$ has positive integer roots, and vanishes on an infinite set, but then it must vanishes identically, so we have proved the first part of our claim.

To get the second part, we want to show that the set $\{n \in \mathbb{N} : Q(n) \in \mathbb{Z}\}$ differs by a finite set from a finite union of arithmetic progressions, if Q is a power sum with rational coefficients and positive integer roots. In fact, it is not necessary to assume that the roots are positive. Note that

$$Q(n) = \sum_{i=1}^{h} \frac{c_i}{d_i} \alpha_i^n = k \in \mathbb{Z}$$

if and only if

$$Q'(n) := \sum_{i=1}^{h} c_i' \alpha_i^n = kd$$

where $d = l.c.m.(d_1, ..., d_h)$ and $c_i' = dc_i/d_i$, so it is enough to prove that $\{n \in \mathbb{N} : Q'(n) = 0 \bmod M\}$ differs by a finite set from a finite union of arithmetic progressions, where M is a positive integer and Q' has integer roots and integer coefficients.

Of course it is enough to consider the case $M = p^k$ for p prime. Moreover, we can assume that $n \geq k$, because we have only a finite number of n such that this is not true. Thanks to this remark, we can also assume that for every i $p \nmid \alpha_i$, because otherwise we can erase the terms divisible by p, and restart with a smaller h.

But then for every i $\alpha_i^{\Phi(p^k)} = 1 \bmod p^k$, so for every $r \in \mathbb{N}$ $Q'(n+r\Phi(p^k)) = Q'(n) \bmod p^k$, and this conclude our proof.
□

3.3 The Pisot d-th root problem

Proof of Theorem 2.3.3. Write $F(n) = c_1\alpha_1^n + \cdots + c_h\alpha_h^n$, where the α_i's are rational and such that $\alpha_1 > \alpha_2 > ... > \alpha_h > 0$. Assume first that $\alpha_1 = 1$. If we set $K(n) = b_2\alpha_2^n + \cdots + b_h\alpha_h^n$, with $b_i := c_i/c_1$, then we may write $F(n) = c_1(1 + K(n))$.

The roots of K are strictly smaller than 1, therefore $|K(n)| \ll \theta^n$ for some $0 < \theta < 1$. Since $F(n)$ is infinitely often a rational d-th power, we have $c_1 > 0$ when d is even. We may assume that $c_1 > 0$ when d is odd as well, replacing F by $-F$ is necessary. Hence for big n we can assume that $F(n) > 0$, so it has exactly one positive d-th root, which we will denote by $z(n)$.

For sufficiently large n we can express $z(n)$ using the binomial power series, obtaining:

$$z(n) = c_1^{1/d} \sum_{s=0}^{M-1} \binom{1/d}{s} K(n)^s + O(\theta^{nM})$$

for a parameter M that we will specify later.

The sum which appears in the expression above can be written as $L(n) = d_1\beta_1^n + \cdots + d_t\beta_t^n$, where the β_i's are pairwise distinct positive rational numbers, and the d_i's lie in some number field K (note that $c_1^{1/d}$ is not in $\mathbb{Q}$ in general). Thus we have $|z(n) - L(n)| \ll \theta^{nM}$.

Note now that since $z(n)^d = F(n)$, we have that $H(z(n)) = H(F(n))^{1/d} \ll C^n$ for some positive real C, because F is a power sum. So if we choose M in such a way that $l := C\theta^M < 1$, we can apply Lemma 3.1.1 (note that the numbers $z(n) \in \mathbb{Q}$ lie in a finitely generated ring, being the d-th roots of values of a power sum), obtaining that for infinitely many $n \in \mathbb{N}$ we have $z(n) = G(n)$,

where G is a power sum with rational coefficients and positive rational roots. Since $F(n) - G(n)^d$ is a power sum with positive roots as well, it can vanish infinitely often only if it vanishes identically. Therefore $F(n) = G(n)^d$, and the theorem is proved for the special case $\alpha_1 = 1$

The general case can be easily obtained now: for some r there exist infinitely many positive integers n, congruent to $-r$ modulo d such that $F(n)$ is a d-th power in $\mathbb{Q}$. Replacing $F(n)$ by $\alpha_1^{-n-r}F(n)$, we reduce the general case to the case $\alpha_1 = 1$ and we are done.

□

Chapter 4

The removal of the dominant root assumption

4.1 Introduction

The aim of this chapter is to detail and explain a method, developed by Corvaja and Zannier in [3], which permits to avoid the dominant root assumption in the application of the subspace theorem to a problem concerning linear recurrences. As anticipated in chapter 2, the problem is related to the Hadamard quotient conjecture: what happens when the values taken by the ratio of two linear recurrence are in a finitely generated ring for infinitely many $n \in \mathbb{N}$? Here is the answer:

Theorem 4.1.1. *Let F, G be linear recurrences such that their roots generate together a torsion-free multiplicative group. Let $\mathcal{R}$ be a finitely generated subring of $\mathbb{C}$ and assume that for infinitely many $n \in \mathbb{N}$ we have $G(n) \neq 0$ and $F(n)/G(n) \in \mathcal{R}$. Then there exists a nonzero polynomial $P(X) \in \mathbb{C}[X]$ such that both sequences $n \mapsto P(n)F(n)/G(n)$ and $n \mapsto G(n)/P(n)$ are linear recurrences.*

In this theorem, similarly to the theorems in chapter 3, where we assumed

the linear recurrences to be non-degenerate, we have a technical assumption about the group generated by the roots of the recurrences. Nevertheless, using the remark 2.1.1, we can see that for this kind of problems it is not really a restriction. For example, the theorem above becomes:

Corollary 4.1.1. *Let F, G be linear recurrences and let $\mathcal{R}$ be a finitely generated subring of $\mathbb{C}$. Assume that for infinitely many $n \in \mathbb{N}$ we have $G(n) \neq 0$ and $F(n)/G(n) \in \mathcal{R}$. Then there exist a nonzero polynomial $P(X) \in \mathbb{C}[X]$ and positive integers q, r such that both sequences $n \mapsto P(n)F(qn+r)/G(qn+r)$ and $n \mapsto G(qn+r)/P(n)$ are linear recurrences.*

In many cases the polynomial P turns out to be a constant, for instance it holds:

Corollary 4.1.2. *Let F, G and $\mathcal{R}$ be as in the theorem, and assume that the coefficients $d_i(n)$ are coprime polynomials. Then, if $F(n)/G(n)$ lies in $\mathcal{R}$ for infinitely many $n \in \mathbb{N}$, F/G is a linear recurrence, i.e. G divides F in the ring of linear recurrences.*

Proof. Let us write

$$G(n) = \sum_{i=1}^{r} d_i(n)\beta_i^n \tag{4.1}$$

By the theorem there exists a polynomial P such that $G/P = H$ is a linear recurrence, which we can write as

$$H(n) = \sum_{i=1}^{s} \tilde{d}_i(n)\tilde{\beta}_i^n$$

From the uniqueness of the expression 4.1 of G, we conclude that $r = s$, and $d_i = P\tilde{d}_{\sigma(j)}$ for a permutation σ of the set $\{1, ..., r\}$. But we assumed that the d_i's are coprime, so P has to be a non-zero constant c. Therefore by the theorem we have that cF/G is a linar recurrence, which implies our claim.

□

Note that this argument can be reproduced in general, and shows that P can be taken as the greatest common divisor of the coefficients of G. Moreover, let us remark that we are in the condition of the corollary when G is a power sum, so we find that an analogous of theorem 2.3.1 holds even if we remove the dominant root assumption. Finally, assuming theorem 4.1.1 it is possible to give a very easy proof of the Hadamard-quotient conjecture, which as we said has been proven by van der Poorten without using the subspace theorem (see [3], pag 436).

Let us line out the strategy of the theorem's proof. First of all, we will prove the result in the number field case, where we will see the new ideas introduced by the authors to deal with the absence of a dominant root; then, thanks to a specialisation argument due to van der Poorten and Rumely (see [10]), we will fully get the desired conclusion.

4.2 The number field case

Proposition 4.2.1. *Let K be a number field, S be a finite set of places of K containing the archimedean ones, F, G be linear recurrences with roots and coefficients in K. Suppose that the roots of F and G generate a torsion-free multiplicative subgroup Γ of K^*. Suppose also that F and G are coprime, with respect to Γ (see remark 2.2.1) and that G has more than one root. Then the set of integers*

$$\mathcal{N} := \left\{ n \in \mathbb{N} \;\middle|\; \frac{F(n)}{G(n)} \in \mathcal{O}_S \right\}$$

is finite.

Proof. Let us enlarge S in such a way that all the roots and the non-zero coefficients of F, G are S-units in K. Of course if we prove the result for this S, we get our claim for the initial smaller S.

By assumption G has at least two roots, and no ratio of two of them can be

a root of unity, otherwise Γ would not be torsion-free. Therefore there exists an absolute value v of K such that not all the roots of G has the same v-adic absolute value: if it was not true, the ratio x of any two roots would have v-adic absolute value 1 for every absolute value, which implies that $H(x) = 1$. In turn, by the Kronecker theorem cited in chapter 1 this would mean that x is a root of 1, absurd.

It is clear that such v is in S. Let us denote it by v_0. Moreover, to simplify the notation, let us replace $F(n)$ and $G(n)$ by $F(n)/\alpha^n$ and $G(n)/\alpha^n$, where α is a root of G with maximal absolute value with respect to v_0. This will not affect our conclusions. Now we can assume that the maximal v_0-adic absolute value of the roots of G is 1, and we write $G(n) = H(n) - R(n)$, where $H(n)$ is a non-zero linear recurrence whose roots have v_0-adic absolute value 1, and $R(n)$ is a non-zero linear recurrence whose roots have v_0-adic absolute value less than 1.

Let us consider the free abelian multiplicative group Γ generated by the roots of F and G, and let Λ be the free subgroup generated by the elements of v_0-adic absolute value 1. It is easy to see that Γ/Λ is torsion-free, and so if $\{\beta_1, \dots, \beta_p\}$ is a basis for Λ, we can complete it to a basis $\{\beta_1, \dots, \beta_p, \dots, \beta_t\}$ of Γ with representatives in Γ for a basis of Γ/Λ. Since the roots of H have v_0-adic absolute value 1, they lie in Λ, so by Proposition 2.2.1 we may write

$$H(n) = \gamma(n, \beta_1^n, \dots, \beta_p^n)$$

where $\gamma \in K[X, T_1, \dots, T_p, T_1^{-1}, \dots, T_p^{-1}]$. By multiplying both F and G by a suitable product of powers of $\beta_1^n, \dots, \beta_p^n$, we may assume that γ is a polynomial, and again this will not affect the conclusion. Let us suppose that the total degree of γ is $\leq D$.

Now let us look at $R(n)$: by our assumption on its roots, there exists $\rho \in (0, 1)$ such that

$$|R(n)|_{v_0} \ll \rho^n. \tag{4.2}$$

We suppose by contradiction that, for all n in an infinite set $\mathcal{N}$ of natural numbers, we have $G(n) \neq 0$ and $F(n)/G(n) \in \mathcal{O}_S$. Let us set, for $n \in \mathcal{N}$, $z_n := F(n)/G(n)$.

We fix a positive integer s, then by the Newton's formula we have

$$H(n)^s = (G(n) + R(n))^s = G(n)\left(\sum_{i=0}^{s-1} \binom{s}{i} G(n)^{s-i-1} R(n)^i \right) + R(n)^s.$$

So we have

$$\frac{F(n)}{G(n)} H(n)^s = F(n)\left(\sum_{i=0}^{s-1} \binom{s}{i} G(n)^{s-i-1} R(n)^i \right) + \frac{F(n)}{G(n)} R(n)^s,$$

whence by 4.2 we get

$$\left| z_n H(n)^s - F(n) \sum_{i=0}^{s-1} \binom{s}{i} G(n)^{s-i-1} R(n)^i \right|_{v_0} \ll \rho^{ns} |z_n|_{v_0}. \tag{4.3}$$

Further, we fix other positive integers h and k. Later we shall impose that s, h, k satisfy suitable inequalities. For every $\mathbf{d} = (d_1, \ldots, d_p) \in \mathbb{N}^p$, with $d_1 + \cdots + d_p \leq h$, and every $u \in \mathbb{N}$ with $u < k$, we consider the quantity

$$\Phi_{\mathbf{d},u}(n) := n^u \beta^{n\mathbf{d}} \left(z_n H(n)^s - F(n) \sum_{i=0}^{s-1} \binom{s}{i} G(n)^{s-i-1} R(n)^i \right), \tag{4.4}$$

where we denote $\underline{\beta}^{\mathbf{d}} = \beta_1^{d_1} \cdots \beta_p^{d_p}$. By 4.3, the fact that $|\beta_i|_{v_0} = 1$ for $i = 1, \ldots, p$ and the fact that $|n|_{v_0} \leq n$ (v_0 could be archimedean, so we cannot bound it better), we obtain

$$|\Phi_{\mathbf{d},u}(n)|_{v_0} \ll \rho^{ns} |z_n|_{v_0} n^u. \tag{4.5}$$

Let us remark that the term $n^u \underline{\beta}^{n\mathbf{d}} z_n H(n)^s$ appearing in the right side of 4.4 can be written as

$$n^u \underline{\beta}^{n\mathbf{d}} z_n H(n)^s = \sum_{\mathbf{b},l} A_{\mathbf{b},l,\mathbf{d},u} n^l \underline{\beta}^{n\mathbf{b}} z_n \tag{4.6}$$

where the coefficients $A_{\mathbf{b},l,\mathbf{d},u}$ belong to K, and the index $(\mathbf{b}, l)$ runs over the vectors $(b_1, \ldots, b_p, l) \in \mathbb{N}^{p+1}$ such that $b_1 + \cdots + b_p \leq h + sD$, and $0 \leq l < k + sD$ (we recall that H has been expressed as a polynomial of degree $\leq D$).

If we count all these possible vectors, we find out that the maximum number of non-zero terms appearing on the right side of 4.6 is $\leq N_1$, with

$$N_1 := (k + sD)\binom{p + h + sD}{p}.$$

Let us denote by $T(n)$ the recurrence $-F(n)\sum_{i=0}^{s-1}\binom{s}{i}G(n)^{s-i-1}R(n)^i$, then we call the other term on the right side of 4.4 $n^u\underline{\beta}^{n\mathbf{d}}T(n)$. It is easy to see that this is a linear combination in K of terms of the kind $n^l\alpha^n$, for suitable l's in $\mathbb{N}$ and α's in Γ, and we denote by N_2 the number of these terms.

If set $N := N_1 + N_2$, we can see $\Phi_{\mathbf{d},u}$ as a linear combination of N terms of the mentioned type, i.e if we choose some ordering for the first N_1 terms, and some ordering for the other N_2, we can write, for $n \in \mathcal{N}$,

$$\Phi_{\mathbf{d},u} = \sum_{i=1}^{n} A_{\mathbf{d},u,i}x_i(n),$$

where $x_i(n)$ are of the form $n^l\underline{\beta}^{n\mathbf{b}}z_n$ for $i = 1, \ldots, N_1$ and of the form $n^l\alpha^n$ for $i = N_1 + 1, \ldots, N$.

Note that for every $n \in \mathcal{N}$, every $x_i(n)$ is an S-integer: $z_n \in \mathcal{O}_S$ by hypothesis, and the same for every element in Γ. Finally, since S contains every archimedean absolute value, for every $v \notin S$ it is well known that $|n^l|_v \leq 1$, for every $n \in \mathbb{Z}$ and every $l \in \mathbb{N}$.

Furthermore, let us define an ordering for the vectors $(\mathbf{d}, u) \in \mathbb{N}^{p+1}$ with $d_1 + \cdots + d_p \leq h$ and $u < k$. Note that their number is $M := k\binom{p+h}{p}$, and that $M \leq N_1$.

We now define M linear forms, in order to apply subsequently the subspace theorem. For $j = 1, \ldots, M$, we set

$$L_j(X_1, \ldots, X_N) = \sum_{i=1}^{n} A_{j,i}X_i,$$

where $A_{j,i}$ corresponds to some $A_{\mathbf{d},u,i}$ via the ordering chosen for the vectors $(\mathbf{d}, u)$. It is clear that for $n \in \mathcal{N}$

$$\Phi_j(n) = L_j(x_1(n), \ldots, x_N(n)). \tag{4.7}$$

Now we claim that $L_1(X_1,\dots,X_{N_1},0,\dots,0),\dots,L_M(X_1,\dots,X_{N_1},0,\dots,0)$ are linearly independent. In fact, if by absurd they were dependent, there would be a dependence relationship holding for every vector in K^{N_1}, and in particular for every $(x_1(n),\dots,x_{N_1}(n))$ with $n\in\mathcal{N}$. So, using the identity 4.7, there would exist M coefficients in K $c_{\mathbf{d},u}$ such that for every $n\in\mathcal{N}$

$$\left(\sum_{\mathbf{d},u} c_{\mathbf{d},u} n^u \underline{\beta}^{n\mathbf{d}}\right) z_n H(n)^s = 0.$$

Since $z_n = F(n)/G(n)$, and F,H are non-degenerate, by the Skolem-Mahler-Lech theorem $z_n H(n)^s$ can vanish only for finitely many n. Also the sum in the brackets, again by the Skolem-Mahler-Lech theorem, can vanish only for finitely many n, because every $\underline{\beta}^{\mathbf{d}}$ is in Γ, which is a torsion-free multiplicative group. This is a contradiction, so our claim was true.

This means that there exist M variables $x_{i_1},\dots,x_{i_M}$ among $x_1,\dots,x_{N_1}$, which we can suppose to be $x_1,\dots,x_M$, such that
$L_1(x_1,\dots,x_M,0,\dots,0),\dots,L_M(x_1,\dots,x_M,0,\dots,0)$ are linearly independent, which in turn means that the N linear forms $L_1,\dots,L_M,X_{M+1},\dots,X_N$ are linearly independent.

Now let us define, if $\mathbf{X}=(X_1,\dots,X_N)$, $L_{v_0,j}(\mathbf{X}) := L_j(\mathbf{X})$ for every $j=1,\dots,M$, and $L_{v_0,j}(\mathbf{X}) := X_j$ for $j=M+1,\dots,N$. Moreover, for every $v\in S$, $v\neq v_0$, we define $L_{v,j}(\mathbf{X}) := X_j$ for every $j=1,\dots,N$. It is clear now that the independent assumption on the linear forms is satisfied for every $v\in S$.

In order to apply the version[1] 1.2.4 of the subspace theorem, we shall bound the quantity

$$\prod_{j=1}^{N}\prod_{v\in S} |L_{v,j}(x_1(n),\dots,x_N(n))|_v. \tag{4.8}$$

Note that for $i\le N_1$, $x_i(n) = n^l \underline{\beta}^{n\mathbf{b}} z_n$, so it could be zero if and only if it is zero z_n, that by the Skolem-Mahler-Lech theorem can happen only for finitely

[1] in fact, we will use it in its logarithmic form, substituting the standard (sometimes called exponential) height H with the logarithmic height h, defined in the proof of proposition 1.1.5

many n, so from now on we can consider only the $n \in \mathcal{N}$ such that these $x_i(n)$ are not zero, and we still have an infinite subset of $\mathbb{N}$. So we can rewrite the double product 4.8 as

$$\left(\prod_{j=1}^{N}\prod_{v\in S}|x_j(n)|_v\right)\left(\prod_{j=1}^{M}\frac{|L_{v_0,j}(x_1(n),\dots,x_N(n))|_{v_0}}{|x_j(n)|_{v_0}}\right).$$

Let L be an upper bound for the exponents l of the n's appearing in the variables $x_i(n)$ (recall that $x_i(n)$ is either of the form $n^l\underline{\beta}^{n\mathbf{b}}z_n$ or of the form $n^l\alpha^n$). Since the S-unit part disappears using the product formula, and $\sum_{v\in S}\log|z_n|_v \leq \sum_v \log^+|z_n|_v = h(z_n)$ we get the following estimate for the first factor:

$$\log\left(\prod_{j=1}^{N}\prod_{v\in S}|x_j(n)|_v\right) \leq NL\log n + N_1 h(z_n).$$

Since $M < N_1$, the terms $x_i(n)$ for $i \leq M$ are of the form $n^l\underline{\beta}^{n\mathbf{b}}z_n$, and so

$$\log|x_i(n)|_v = \log|z_n|_{v_0} + l\log|n|_{v_0}$$

for every $i = 1,\dots,M$, and for some $l \leq L$ depending on i. Then from 4.5 and 4.7 we obtain that for each $j = 1,\dots,M$, and n large enough,

$$\log\left(\frac{|L_{v_0,j}(x_1(n),\dots,x_N(n))|_{v_0}}{|x_j(n)|_{v_0}}\right) \leq sn\log\rho + 2L\log n,$$

which implies that

$$\log\left(\prod_{j=1}^{M}\frac{|L_{v_0,j}(x_1(n),\dots,x_N(n))|_{v_0}}{|x_j(n)|_{v_0}}\right) \leq M(sn\log\rho + 2L\log n).$$

So we can estimate 4.8 for n large enough:

$$\begin{aligned}&\log\left(\textstyle\prod_{j=1}^{N}\prod_{v\in S}|L_{v,j}(x_1(n),\dots,x_N(n))|_v\right)\\ &\leq M(sn\log\rho + 2L\log n) + N_1 h(z_n) + NL\log n\\ &\leq N_1 h(z_n) + Msn\log\rho + 3NL\log n. \qquad (4.9)\end{aligned}$$

Moreover, since $z_n = F(n)/G(n)$, we have for large values of n that

$$h(z_n) \leq h(F(n)) + h(G(n)) \leq nC_1,$$

where C_1 is a positive constant depending only on F and G. Using this in 4.9 we get

$$\log\Big(\prod_{j=1}^{N}\prod_{v\in S}|L_{v,j}(x_1(n),\dots,x_N(n))|_v\Big) \leq (C_1N_1 + Ms\log\rho)n + 3NL\log n. \tag{4.10}$$

Now define $C_2 := C_1/(-\log\rho)$. This is again a positive constant depending only on F and G. Now we are ready to choose our parameters s, h and k: let $s > 2C_2$, and $k > 3sD$. Then we have

$$sk > 2C_2k > \frac{3}{2}C_2(k+sD). \tag{4.11}$$

Note that the function $\binom{p+x}{p}$ is a polynomial of degree p, so for large h,

$$sk\binom{p+h}{p} > C_2(k+sD)\binom{p+sD+h}{p}, \tag{4.12}$$

because of our choice of s and k, that makes the coefficient on the left side larger than the one on the right. So h is chosen large enough to make true the inequality above.

Therefore it is satisfied the inequality $C_1N_1 < -Ms\log\rho$, so by 4.10 we get

$$\log\Big(\prod_{j=1}^{N}\prod_{v\in S}|L_{v,j}(x_1(n),\dots,x_N(n))|_v\Big) < -C_3n,$$

for large $n \in \mathcal{N}$, where C_3 is a positive real constant independent of n.

Clearly $h(\mathbf{x}(n)) \leq C_4n$, where C_4 is again a positive real constant, so we get

$$\log\Big(\prod_{j=1}^{N}\prod_{v\in S}|L_{v,j}(x_1(n),\dots,x_N(n))|_v\Big) < -\frac{C_3}{C_4}h(\mathbf{x}(n)).$$

So we can apply the subspace theorem with $\varepsilon = C_3/C_4$, concluding that our points are contained in a finite number of hyperplanes of K^N. Since we have infinite points, there exists a hyperplane that contains infinitely many of them, so we have a non-trivial linear relation

$$\lambda_1x_1(n) + \cdots + \lambda_Nx_N(n) = 0,$$

with $\lambda_i \in K$, valid for infinitely many $n \in \mathcal{N}$. Let us rewrite it as

$$\lambda_1 x_1(n) + \cdots + \lambda_{N_1} x_{N_1}(n) = -\lambda_{N_1+1} x_{N_1+1}(n) - \cdots - \lambda_N x_N(n).$$

Hence we obtain that for an infinite subsequence of $\mathcal{N}$

$$z_n A(n) = B(n),$$

where A is a linear recurrence with roots in Λ, and B is a linear recurrence with roots in Γ.

Note that $A_1, \ldots, A_{N_1}$ cannot all be zero, because otherwise by the Skolem-Mahler-Lech theorem also $A_{N_1+1}, \ldots, A_N$ would be zero, which is not possible. Therefore $A(n)$ is a non-zero linear recurrence (with roots in Λ). Since by definition $z_n = F(n)/G(n)$, we have

$$F(n)A(n) = B(n)G(n)$$

for infinitely many $n \in \mathcal{N}$, where all the recurrences A, B, F, G have roots in Γ, which is torsion-free, so are non-degenerate, so again by the Skolem-Mahler-Lech theorem this relation holds for every $n \in \mathbb{N}$. Thus by proposition 2.2.1 we can see this equality as an equality in $K[X, T_1, \ldots, T_t, T_1^{-1}, \ldots, T_t^{-1}]$, where we use to obtain the isomorphism of the proposition the basis of Γ $\{\beta_1, \ldots, \beta_p, \ldots, \beta_t\}$, and we get for $f, a, b, g \in K[X, T_1, \ldots, T_t, T_1^{-1}, \ldots, T_t^{-1}]$

$$fa = bg.$$

By assumption we know that f and g are coprime, so g divides a. But since A has roots in Λ, $a \in K[X, T_1, \ldots, T_p, T_1^{-1}, \ldots, T_p^{-1}]$, which implies that $g = \eta g_1$, where η is an invertible element of $K[X, T_1, \ldots, T_t, T_1^{-1}, \ldots, T_t^{-1}]$ and $g_1 \in K[X, T_1, \ldots, T_p, T_1^{-1}, \ldots, T_p^{-1}]$

This means that all of the roots of G have the same v_0-adic absolute value, which is a contradiction.

□

4.3 The general case

Now we shall deduce the general case from the number-field case, again following [3], where as we have said the authors basically make use of the specialisation argument developed in [10]. First of all let us consider the following general result:

Lemma 4.3.1. *Let $\mathcal{S}$ be a finitely generated subring of $\mathbb{C}$, let $\rho \in \mathcal{S}$ be non-zero and let Γ be a finitely generated torsion-free subgroup of $\mathcal{S}^*$. Then there exists a ring homomorphism $\varphi : \mathcal{S} \to \overline{\mathbb{Q}}$ such that $\varphi(\rho) \neq 0$ and such that the restriction of φ to Γ is injective.*

For a proof of this Lemma, see [10], where is proved a stronger result (Theorem 7).

Proof of Theorem 4.1.1. Let $\mathcal{N}$ be the infinite subset of $\mathbb{N}$ such that $F(n)/G(n) \in \mathcal{R}$. Let $\mathcal{S}$ be the ring generated over $\mathcal{R}$ by the coefficients of F and G, by their roots and their reciprocals. Let Γ be the (finitely generated and torsion-free) multiplicative subgroup of $\mathcal{S}^*$ generated by the roots of F and G, and let $\beta_1, \ldots, \beta_t$ be a basis for it.

Using proposition 2.2.1 we associate to F and G two elements of the ring $\mathcal{S}[X, T_1, \ldots, T_t, T_1^{-1}, \ldots, T_t^{-1}]$, say f and g, that we can assume to be coprime.

If g is a unit times an element of $\mathbb{C}[X]$, then the theorem is clearly true, so let us suppose that we are not in this situation, and we look for a contradiction. By multiplying both F and G by a suitable unit, we can assume that they are coprime polynomials in $\mathcal{S}[X, T_1, \ldots, T_t]$, and that g has more than one term as a polynomial in $T_1, \ldots, T_t$. In particular, there exists a variable, say T_1, which appears in the terms of g with at least two different degrees.

Let us consider the resultant $r(X, T_1, \ldots, T_t)$ of f and g with respect to T_1, it is non-zero and it has coefficients in $\mathcal{S}$. We denote ρ the product of the non-zero coefficients of r, f and g, and we apply lemma 4.3.1. Note that if

φ is the homomorphism prescribed by the lemma, we have that the elements $\varphi(\beta_i)$ are linearly independent, being φ injective on Γ.

If we denote f^φ and g^φ the polynomials in $\overline{\mathbb{Q}}[X, T_1, \dots, T_t, T_1^{-1}, \dots, T_t^{-1}]$ with as coefficients the images of the coefficients of f and g via φ, we still have that they are coprime with respect to T_1, because $\varphi(\rho) \neq 0$, so their resultant and leading coefficients are non-zero. Moreover, again because of our choice of ρ, the coefficients of g via φ do not vanish, so we have at least two terms in g^φ which contain the variable T_1 with different degrees. Therefore we can write $f^\varphi = hf_1$ and $g^\varphi = hg_1$, with f_1 and g_1 coprime, and h not depending on T_1, which means that g_1 contains at least two terms in T_1.

Then again by proposition 2.2.1 we can associate to f_1 and g_1 two linear recurrences F_1 and G_1, with algebraic coefficients and roots, sending every T_i to the function $n \mapsto \varphi(\beta_i)^n$. Now, being φ injective, G_1 has at least two distinct roots, because g_1 has at least two terms in T_1, and the roots of F_1 and G_1 generate a torsion-free multiplicative group. Hence by the Skolem-Mahler-Lech theorem $G_1(n) = 0$ only for finitely many $n \in \mathbb{N}$, that we shall exclude from our $\mathcal{N}$.

Therefore, for $n \in \mathcal{N}$, we have that

$$\frac{F_1(n)}{G_1(n)} = \varphi\Big(\frac{F(n)}{G(n)}\Big),$$

which implies that, for every $n \in \mathcal{N}$, $F_1(n)/G_1(n) \in \varphi(\mathcal{R})$, which is a finitely generated subring of some number field K. But we are assuming that $\mathcal{N}$ is infinite, and we saw that G_1 has at least two roots, so by proposition 4.2.1 we get a contradiction, which proves the theorem.

□

4.4 Comments

Let us resume the proof of theorem 2.3.1 presented in the last chapter: using the dominant root we expanded F/G as a convergent power series, and truncating it we obtained a power sum P which gave a good approximation to the integers $F(n)/G(n)$ for every n belonging to an infinite set. This allowed us to see the difference $(F(n)/G(n)) - P(n)$ as a small linear form, using as variables the integer $F(n)/G(n)$ and the n-th power of the roots of P. Then applying the subspace theorem we obtained our claim.

Without the dominant root assumption, we approximate $F(n)/G(n)$ by using simultaneously all the roots with maximal absolute value, as we can see in formula 4.3. But then if we try to imitate the proof above, there is one problem: in the first N_1 variables which we would 'naturally' choose to apply the subspace theorem, it appears the term $z_n := F(n)/G(n)$, which make them in some sense 'bad variables' for our purposes. Let us explain why: suppose that we have chosen our set S in the most clever way to make the method above work, then we have the product of all the linear forms defined as $L_{i,v}(\mathbf{X}) = X_i$ which gives, as one can see during the proof,

$$\log\left(\prod_{j=1}^{n}\prod_{v\in S}|x_j(n)|_v\right) \leq NL\log n + N_1\sum_{v\in S}\log|z_n|_v.$$

We would like to have this term of the same order of $\log n$, because then the other term coming from the small linear form defined by our simultaneous approximation, which is of the order of $-n$, would make the subspace theorem work. If the z_n's were S-units, we would have

$$\sum_{v\in S}\log|z_n|_v = \sum_{v\in M_k}\log|z_n|_v = 0$$

by the product formula, which would be perfect. But we cannot assume that they are S-units, being S a finite set. The best that we can do is to assume

that they are S-integers, obtaining

$$\sum_{v \in S} \log |z_n|_v \leq \sum_{v \in M_K} \log^+ |z_n|_v = h(z_n),$$

but $h(z_n) \asymp n$ so we cannot be sure that for every F, G we can apply the subspace theorem.

The authors overcome this difficulty by constructing many other small independent linear forms out from the given one, just multiplying it by suitable n-th powers of products of dominant roots, as done in 4.4. This makes raise the number N_1 of bad variables, but not that much with respect to the benefits given by the M small linear forms, because of the fundamental inequality 4.12, and so everything works.

Since we have seen that the method used in chapter 3, using the dominant root assumption, worked well also in other problems concerning linear recurrences (the proofs of the theorems 2.3.1 and 2.3.3 rely on the same lemma), one would believe that the generalization of the method presented in this chapter would work also in other problems, such as the one related to the Hadamard d-th root problem. However, it seems that at least another cardinal idea is missing, because nobody managed to do it yet.

Bibliography

[1] P. Corvaja and U. Zannier. Diophantine equations with power sums and universal Hilbert sets. *Indag. Math. (N.S.)*, 9(3):317–332, 1998.

[2] P. Corvaja and U. Zannier. On the greatest prime factor of $(ab+1)(ac+1)$. *Proc. Amer. Math. Soc.*, 131(6):1705–1709 (electronic), 2003.

[3] Pietro Corvaja and Umberto Zannier. Finiteness of integral values for the ratio of two linear recurrences. *Invent. Math.*, 149(2):431–451, 2002.

[4] Pietro Corvaja and Umberto Zannier. Some new applications of the subspace theorem. *Compositio Math.*, 131(3):319–340, 2002.

[5] Jan-Hendrik Evertse. The subspace theorem of W. M. Schmidt. In *Diophantine approximation and abelian varieties (Soesterberg, 1992)*, volume 1566 of *Lecture Notes in Math.*, pages 31–50. Springer, Berlin, 1993.

[6] Gerald J. Janusz. *Algebraic number fields*, volume 7 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, second edition, 1996.

[7] Neal Koblitz. *p-adic numbers, p-adic analysis, and zeta-functions*, volume 58 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1984.

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

[9] K. F. Roth. Rational approximations to algebraic numbers. *Mathematika*, 2:1–20; corrigendum, 168, 1955.

[10] Robert Rumely. Notes on van der Poorten's proof of the Hadamard quotient theorem. I, II. In *Séminaire de Théorie des Nombres, Paris 1986–87*, volume 75 of *Progr. Math.*, pages 349–382, 383–409. Birkhäuser Boston, Boston, MA, 1988.

[11] Wolfgang M. Schmidt. *Diophantine approximation*, volume 785 of *Lecture Notes in Mathematics*. Springer, Berlin, 1980.

[12] Wolfgang M. Schmidt. *Diophantine approximations and Diophantine equations*, volume 1467 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1991.

[13] Jean-Pierre Serre. *Algebraic groups and class fields*, volume 117 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1988. Translated from the French.

[14] A. J. van der Poorten. Some facts that should be better known, especially about rational functions. In *Number theory and applications (Banff, AB, 1988)*, volume 265 of *NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci.*, pages 497–528. Kluwer Acad. Publ., Dordrecht, 1989.

[15] Alfred J. van der Poorten. Solution de la conjecture de Pisot sur le quotient de Hadamard de deux fractions rationnelles. *C. R. Acad. Sci. Paris Sér. I Math.*, 306(3):97–102, 1988.

[16] Umberto Zannier. A proof of Pisot's dth root conjecture. *Ann. of Math. (2)*, 151(1):375–383, 2000.