Politecnico di Torino

ScuDo
Scuola di Dottorato ~ Doctoral School
WHAT YOU ARE, TAKES YOU FAR

Doctoral Dissertation
Doctoral Program in Pure and Applied Mathematics (36th cycle)

Exploring linear recurrent sequences: Theory and Applications

Candidate

Gessica Alecci

Supervisors
Prof. Danilo Bazzanella
Prof. Nadir Murru

Politecnico di Torino
2024

Declaration

I hereby declare that, the contents and organization of this dissertation constitute my own original work and does not compromise in any way the rights of third parties, including those relating to the security of personal data.
Some ideas and results have appeared previously in the following publications and preprints:

- *Zeckendorf representation of multiplicative inverses modulo a Fibonacci number,* Alecci, G., Murru, N. and Sanna, C., Monatshefte für Mathematik, 2023.
- *Some notes on the algebraic structure of linear recurrent sequences,* Alecci, G., Barbero, S. and Murru, N., Ricerche di Matematica, 2023.
- *On alternative definition of Lucas atoms and their p-adic valuations,* Alecci, G., Miska, P., Murru, N., and Romeo, G., https://arxiv.org/abs/2308.10216
- *On a criterion for algebraic independence applied to continued fractions,* Alecci, G. and Elsner, C. https://arxiv.org/abs/2311.18536

Gessica Alecci
2024

* This dissertation is presented in partial fulfillment of the requirements for **Ph.D. degree** in the Graduate School of Politecnico di Torino (ScuDo).

Abstract

In this manuscript many results about elementary number theory are presented. They mainly concern the study of linear recurrences and algebraic independence of certain continued fractions and their convergents. The set of all linear recurrent sequences can be equipped with several operations such as the binomial convolution (Hurwitz product) or the multinomial convolution (Newton product). Using elementary and combinatorial techniques, we prove that this set endowed with the termwise sum and the aforementioned products is an $R-$algebra, given any commutative ring R with identity. Moreover, we provide explicitly a characteristic polynomial of the Hurwitz product and Newton product of any two linear recurrent sequences. We also investigate whether these $R-$algebras are isomorphic, considering also the $R-$algebras obtained using the Hadamard product and the convolution product. The Lucas sequence is a specific linear recurrence of order two with characteristic polynomial $X^2 - sX - t$. When s,t are treated as variables, the definition of Lucas polynomials naturally follows. Sagan and Tirrell [57] introduced a particular factorization of these polynomials, known as Lucas atoms. We present a new approach to introducing Lucas atoms, offering straightforward proofs for their main properties. Moreover, we fully characterize the p-adic valuations of Lucas atoms for any prime p, answering to a problem left open by Sagan and Tirrell, who treated only some specific cases for $p \in \{2,3\}$. Finally, we prove that the sequence of Lucas atoms is not holonomic, contrarily to the Lucas sequence. A particular instance of Lucas sequence is the Fibonacci sequence, whose characteristic polynomial is $X^2 - X - 1$. The Zeckendorf representation of an integer is the unique way to write an integer as sum of distinct and non consecutive Fibonacci numbers. Prempreesuk, Noppakaew, and Pongsriiam [52] determined the Zeckendorf representation of the multiplicative inverse of 2 modulo F_n, for every positive integer n not divisible by 3, where F_n denotes the nth Fibonacci number. We determine the Zeckendorf representation of the multiplicative inverse of a modulo F_n, for every fixed integer $a \geq 3$ and for all positive integers n

with $\gcd(a, F_n) = 1$. Our proof makes use of the so-called base-φ expansion of real numbers.

Regarding the algebraic independence of numbers, Elsner et al. [23, 24] developed and applied a method in which the algebraic independence of n quantities $x_1, \ldots, x_n$ over a field is transferred to further n quantities $y_1, \ldots, y_n$ by means of a system of polynomials in $2n$ variables $X_1, \ldots, X_n, Y_1, \ldots, Y_n$. In this manuscript, we systematically study and explain this criterion and its variants. Moreover, we apply this criterion to periodic non-regular Hurwitz-type continued fractions, namely continued fractions with real numbers as partial quotients. We show that given a continued fraction of this type, this criterion can be applied to prove that not only the convergents are algebraically independent each other, but they are also algebraically independent from the continued fraction.

Contents

List of Tables

Chapter 1

A path into the chapters

The purpose of this manuscript is to explore linear recurrent sequences of any degree in terms of algebraic structures, and also to study some aspects of the second-order recurrences. In particular, the study focused on Lucas sequence, on a new definition of Lucas atoms, and on Fibonacci sequence. Finally, some results concern the algebraic independence of certain Hurwitz-type continued fractions and its convergents.

The first part of this dissertation is about linear recurrent sequences. Let R be an associative, commutative ring having characteristic zero and unity, let $\mathcal{S}(R)$ be the set of sequences of elements belonging to the ring R and let $\mathcal{W}(R) \subset \mathcal{S}(R)$ the set of linear recurrent sequences. Both sets can be equipped with several operations giving them interesting algebraic structures. In the case that R is a field, it is immediate to see that the element-wise sum or product (also called the Hadamard product) of two linear recurrent sequences is still a linear recurrent sequence, see, e.g., [25]. Cerruti and Vaccarino [17] proved this in the general case where R is a ring, showing that $\mathcal{W}(R)$ is an $R-$algebra and also giving explicitly the characteristic polynomial of the element-wise sum and Hadamard product of two linear recurrent sequences. Larson and Taft [43, 69] studied this algebraic structure characterizing the invertible elements and the zero divisors. Other studies about the behaviour of linear recurrent sequences under the Hadamard product can be found, e.g., in [15, 31, 38, 77]. In the same manner, $\mathcal{W}(R)$ equipped with the element-wise sum and the convolution product (or Cauchy product) has been deeply studied. In particular, $\mathcal{W}(R)$ is still an $R-$algebra and the characteristic polynomial of the convolution product between

two linear recurrent sequences can be explicitly computed [17]. The convolution product of linear recurrent sequences has been explored also from a combinatorial point of view [1] and over finite fields [36]. For other results, see, e. g., [66–68]. Another important operation between sequences is the binomial convolution (called also Hurwitz product). In [39], Keigher introduced in a systematic way the Hurwitz series ring. This has also been explored by other several authors [8, 7, 9, 10, 40, 76]. However, there are few results when focusing on linear recurrent sequences [41, 42]. In Chapter 3 we study the algebraic structure of linear recurrent sequences considering in particular the Hurwitz product and the Newton product. Moreover, in Section 3.3 we study whether isomorphisms exist between these structures.

The Lucas sequence is a specific second-order linear recurrent sequence from which Lucas polynomials are defined. Chapter 4 is devoted to the study of Lucas atoms, introduced for the first time by Sagan and Tirrel [57], that are nothing else than irreducible factors of Lucas polynomials. The main aim of the authors was to investigate, from an innovatory point of view, when some combinatorial rational functions are actually polynomials. It will be shown that Lucas atoms can be introduced in a more natural and powerful way than the original definition, providing straightforward proofs for their main properties. Specifically, in Section 4.1 we revisit some of the main properties of Lucas atoms, obtaining them with elementary proofs. The p-adic valuations of integer sequences is a well studied topic, in particular the case of Lucas sequences has been deepened by several authors (see, e.g., [6, 44, 58, 71]). Section 4.2 is devoted to the p-adic valuations of Lucas atoms. In [57], the authors dealt with Lucas atoms and some divisibility properties by $p = 2, 3$. They left open, addressing it as a hard problem, the extension of these results to arbitrary primes. In Section 4.2, we solve this problem and we completely characterize the p-adic valuations of Lucas atoms. Finally, in Section 4.3, we exploit the results on the p-adic valuations of Lucas atoms to prove that the sequence of Lucas atoms is not holonomic, i.e., it does not satisfy any recurrence relation, also considering coefficients being polynomials, contrarily to the Lucas sequence.

A particular case of Lucas sequence is the Fibonacci sequence whose elements are called Fibonacci numbers. The theorem of Zeckendorf asserts that any positive integer can be expressed in a unique manner as the sum of one or more distinct non-consecutive Fibonacci numbers [75]. These kinds of representation, called Zeckendorf representations, have been studied in several works. In particular, the Zeckendorf representation of numbers of the form f_{kn}/f_n, f_n^2/d and L_n^2/d, where

f_n are the Fibonacci numbers, L_n are the Lucas numbers and d is a Lucas or Fibonacci number, have been studied by Filipponi and Freitag [26, 28]. Whereas, the Zeckendorf representation of numbers of the form mf_n have been analyzed by Filipponi, Hart, and Sanchis [27, 35, 46]. Filipponi [27] determined the Zeckendorf representation of mf_nf_{n+k} and mL_nL_{n+k} for $m \in \{1,2,3,4\}$. The study of Zeckendorf representations has been also approached from a combinatorial point of view [4, 29, 47, 73]. Moreover, generalizations of the Zeckendorf representation to linear recurrences other than the sequence of Fibonacci numbers has been considered [18, 19, 32, 48, 51]. For all integers a and $m \geq 1$ with $\gcd(a,m) = 1$, let $(a^{-1} \bmod m)$ denote the least positive multiplicative inverse of a modulo m, that is, the unique $b \in \{1,\ldots,m\}$ such that $ab \equiv 1 \pmod{m}$. In [52], Prempreesuk, Noppakaew, and Pongsriiam determined the Zeckendorf representation of $(2^{-1} \bmod f_n)$, for every positive integer n that is not divisible by 3. (The condition $3 \nmid n$ is necessary and sufficient to have $\gcd(2, f_n) = 1$.) In particular, they showed [52, Theorem 3.2] that

$$(2^{-1} \bmod f_n) = \begin{cases} \sum_{k=0}^{(n-7)/2} f_{n-3k-2} + f_3 & \text{if } n \equiv 1 \pmod 3; \\ \sum_{k=0}^{(n-8)/2} f_{n-3k-2} + f_4 & \text{if } n \equiv 2 \pmod 3; \end{cases}$$

for every integer $n \geq 8$. In Chapter 5 we extend their result by determining the Zeckendorf representation of the multiplicative inverse of a modulo f_n, for every fixed integer $a \geq 3$ and every positive integer n with $\gcd(a, f_n) = 1$.

The last part of this dissertation focuses on the area of algebraic independence. The transcendence of π and that of e has been known since the end of the 19^{th} century, but the question of the algebraic independence of π and e over $\mathbb{Q}$ has still not been answered, i.e. the exclusion of the existence of a non-identical vanishing polynomial $P(X,Y)$ with rational coefficients such that $P(\pi,e) = 0$. The theorem of Lindemann-Weierstrass (1885), from which the transcendence of π and of e can be derived, is the beginning of a general theory on algebraic independence of complex numbers over $\mathbb{Q}$. In one of its equivalent formulations this theorem states that in the case of the *linear* independence of algebraic numbers $\alpha_1,\ldots,\alpha_n$ over $\mathbb{Q}$, the numbers $e^{\alpha_1},\ldots,e^{\alpha_n}$ are *algebraically* independent over $\mathbb{Q}$ [60]. An additional significant achievement is the theorem of Gelfond-Schneider that states the transcendence of α^β when α and β are algebraic over $\mathbb{Q}$, assuming that $\alpha \neq 0,1$ and $\beta \notin \mathbb{Q}$ [60]. Another important result is Baker's theorem on linear forms in logarithms that states that, given $\alpha_1,\ldots,\alpha_n$ algebraic numbers different from

zero such that $\log\alpha_1,\ldots,\log\alpha_n$ are linearly independent over the rational numbers, then the numbers $1,\log\alpha_1,\ldots,\log\alpha_n$ are linearly independent over the field of all algebraic numbers [5]. In 1916, S. Ramanujan [53] defined the series

$$S_{j+1}(x) := \frac{\zeta(-2j-1)}{2} + \sum_{n=1}^{\infty} \frac{n^{2j+1}x^n}{1-x^n}$$

where $\zeta(s)$ is the Riemann zeta function. Let

$$P(x) := -24S_1(x), \qquad Q(x) := 240S_3(x), \qquad R(x) := -504S_5(x). \tag{1.1}$$

In 1996, Y. Nesterenko [49] proved that for every complex number x with $0<|x|<1$, the set

$$\{x, P(x), Q(x), R(x)\}$$

contains at least three numbers that are algebraically independent over $\mathbb{Q}$. In terms of algebraic independence of continued fractions, Tanaka [70] gave a necessary and sufficient condition for the values of $\Theta(x,a,q)$ to be algebraically independent, where $\Theta(x,a,q)$ is a sort of q-hypergeometric series. In particular, he showed under which conditions the values of the continued fractions obtained when $x=a$, namely $\Theta(a,q)$, are algebraically dependent. Chapter 6 contains results on algebraic independence or dependence of number sets. A criterion and its variants will be presented, which state that, starting from a set of known algebraically independent numbers, we obtain a new set where the numbers in both sets satisfy a system of polynomial equations. Moreover, in Section 6.3 this criterion will be applied to continued fractions and a numerical example for Diophantine approximations with convergents of continued fractions with algebraically independent partial quotients is presented.

The structure of the dissertation is as follows: Chapter 2 contains some preliminary concepts and well-known results that will be useful in the subsequent chapters. New results about the algebraic structures of linear recurrent sequences will be presented in Chapter 3. The following two chapters present some results connected with second-order linear recurrent sequences: namely, Chapter 4 will be about Lucas atoms, while Chapter 5 will be about Zeckendorf representation of the inverse of an integer modulo a Fibonacci number; the final chapter focuses on the application of a criterion for algebraic independence of Hurwitz-type continued fractions and their convergents.

Chapter 2

Preliminaries and notation

2.1 About linear recurrent sequences

Given an associative and commutative ring $(R,+,\cdot)$, having characteristic zero and unity, we denote by $\mathcal{S}(R)$ the set of all sequences $\mathbf{a} := (a_n)_{n\geq 0}$ such that $a_n \in R$, for all $n \in \mathbb{N}$. A sequence $\mathbf{a} \in \mathcal{S}(R)$ is said to be a *linear recurrent sequence* of order N if its elements satisfy

$$a_n = \sum_{i=1}^{N} h_i a_{n-i}, \qquad \forall n \geq N$$

for some coefficients $h_i \in R$, $i = 1,\ldots,N$, where h_N is not a zero divisor in R. The characteristic polynomial associated to this recurrence relation is defined as

$$p_a(t) := t^N - \sum_{i=1}^{N} h_i t^{N-i}.$$

The elements $a_0,\ldots,a_{N-1}$ are called *initial conditions*. We denote by $\mathcal{W}(R) \subset \mathcal{S}(R)$ the set of all linear recurrent sequences. Moreover, given $\mathbf{a} \in \mathcal{S}(R)$, we write

$$A_o(t) := \sum_{n=0}^{\infty} a_n t^n, \quad A_e(t) := \sum_{n=0}^{\infty} \frac{a_n}{n!} t^n,$$

for the ordinary generating function (o.g.f.) and the exponential generating function (e.g.f.), respectively. For any $\mathbf{a},\mathbf{b} \in \mathcal{S}(R)$, we will deal with the following operations:

- *componentwise sum* $\oplus$, defined by

$$\mathbf{c} := \mathbf{a} \oplus \mathbf{b}, \quad c_n := a_n + b_n, \quad \forall n \geq 0;$$

- *componentwise product* or *Hadamard product* $\odot$, defined by

$$\mathbf{c} := \mathbf{a} \odot \mathbf{b}, \quad c_n := a_n \cdot b_n, \quad \forall n \geq 0;$$

- *convolution product* $*$, defined by

$$\mathbf{c} := \mathbf{a} * \mathbf{b}, \quad c_n := \sum_{i=0}^{n} a_i b_{n-i}, \quad \forall n \geq 0;$$

- *binomial convolution product* or *Hurwitz product* $\star$, defined by

$$\mathbf{c} := \mathbf{a} \star \mathbf{b}, \quad c_n := \sum_{i=0}^{n} \binom{n}{i} a_i b_{n-i}, \quad \forall n \geq 0;$$

- *multinomial convolution product* or *Newton product* $\boxtimes$, defined by

$$\mathbf{c} := \mathbf{a} \boxtimes \mathbf{b}, \quad c_n := \sum_{i=0}^{n} \sum_{j=0}^{i} \binom{n}{i} \binom{i}{j} a_i b_{n-j}, \quad \forall n \geq 0.$$

Remark 2.1.1. The Newton product is also called multinomial convolution product, because it is the natural generalization of the binomial convolution product using the multinomial coefficient. Observe indeed that $\binom{n}{i}\binom{i}{j} = \binom{n}{n-i,i-j,j}$.

Definition 2.1.2. Given two monic polynomials $f(t)$ of degree M and $g(t)$ of degree N, their resultant is $\operatorname{res}(f(t), g(t)) := \prod_{i=1}^{M} \prod_{j=1}^{N} (\alpha_i - \beta_j)$, where α_i's and β_j's are, respectively, the roots of $f(t)$ and $g(t)$, counted with their multiplicities.

After introducing general linear recurrent sequences, we now examine specific second-order sequences. Lucas sequences of the first kind $(U_n)_{n\geq 0}$ are linear recurrent sequences having characteristic polynomial $X^2 - sX - t$ with initial conditions 0 and 1, i.e., they are defined by the recurrence

$$\begin{cases} U_0 := 0, \quad U_1 := 1, \\ U_n := sU_{n-1} + tU_{n-2}, \quad \forall n \geq 2, \end{cases}$$

where s and t are usually integer numbers. If we consider s and t as two variables, then we talk about Lucas polynomials $U_n(s,t) \in \mathbb{N}[s,t]$. In [57], the authors studied a very interesting factorization for Lucas polynomials connected to cyclotomic polynomials. In particular, they introduced the *Lucas atoms* as the polynomials

$$P_1(s,t) := 1, \quad P_n(s,t) := \Gamma(\Psi_n(q)),$$

for all $n \geq 2$, where $\Psi_n(q)$ is the n–th cyclotomic polynomial and Γ a map that exploits the gamma expansion of palindromic polynomials. Given this definition, the authors proved that the following factorization of the Lucas polynomials holds:

$$U_n(s,t) = \prod_{d|n} P_d(s,t),$$

and moreover $P_n(s,t) \in \mathbb{N}[s,t]$, for all $n \geq 1$.

This study was firstly motivated by the problem of finding when the rational function

$$\frac{\prod_i U_{n_i}(s,t)}{\prod_j U_{k_j}(s,t)} \tag{2.1}$$

is actually a polynomial. For instance, it has been studied by some authors the case of the so called Lucanomial, which is the generalization of the binomial coefficient to Lucas polynomials:

$$\binom{U_n(s,t)}{U_k(s,t)} := \frac{\prod_{i=1}^{n} U_i(s,t)}{\prod_{i=1}^{k} U_i(s,t) \prod_{i=1}^{n-k} U_i(s,t)},$$

see, e.g., [11, 12]. In fact, thanks to Lucas atoms, the study of when (2.1) is a polynomial can be approached in a straightforward way exploiting the factorization of Lucas polynomials.

The idea of factorizing the Lucas polynomials dates back to 1969, when Webb and Parberry [72] employed it to discuss the irreducibility of the Lucas polynomial $U_n(s,1)$. Subsequently, Levy [45] gave the definition of fibotomic polynomials, which turn out to be the Lucas atoms for $t = \pm 1$ and he proved that they are irreducible. Moreover, he made some remarks on their connection with the two-variable homogeneous cyclotomic polynomials, which was already highlighted in a work of Brillhart et al. [14]. It is also remarkable that this approach has been

already used by Stewart et al. [61, 62, 64, 63, 65] in order to obtain estimations on the greatest prime factor of the terms of the Lucas sequence and other recurrent sequences. The definition of Lucas atoms can be simplified, avoiding the use of the Γ map.

Let us consider

$$\Phi_n(\alpha,\beta) := \prod_{\substack{j=1 \\ (j,n)=1}}^{n} (\alpha - \omega^j \beta),$$

for all $n \geq 1$, where ω is an n–th primitive root of unity. For basic properties of these polynomials we refer to [64]. From this definition, we immediately get that

$$\alpha^n - \beta^n = \prod_{d|n} \Phi_d(\alpha,\beta),$$

and

$$\beta^{\varphi(n)} \Psi_n(\alpha/\beta) = \Phi_n(\alpha,\beta),$$

where $\varphi(\cdot)$ is the Euler's totient function. Then, we can define the Lucas atoms as the polynomials

$$P_1(s,t) := 1, \quad P_n(s,t) := \Phi_n(\alpha,\beta) = \beta^{\varphi(n)} \Psi_n(\alpha/\beta), \tag{2.2}$$

for all $n \geq 2$, where $s = \alpha + \beta$ and $t = -\alpha\beta$. In this way, we obtain the factorization of the Lucas polynomials by means of the Lucas atoms (as well as with the definition given in [57]). Indeed, observing that $\Phi_1(\alpha,\beta) = \alpha - \beta$, we have

$$\alpha^n - \beta^n = (\alpha - \beta) \prod_{\substack{d|n \\ d \neq 1}} \Phi_d(\alpha,\beta) = (\alpha - \beta) \prod_{d|n} P_d(s,t),$$

remembering that $P_1(s,t) = 1$. Thus, we have

$$U_n(s,t) = \frac{\alpha^n - \beta^n}{\alpha - \beta} = \prod_{d|n} P_d(s,t) \tag{2.3}$$

where $(U_n(s,t))_{n \geq 0}$ has characteristic polynomial $X^2 - sX - t = (X - \alpha)(X - \beta)$.

In Chapter 4, it will be shown that the definition of Lucas atoms given in (2.2) is more convenient and straightforward than the original definition proposed in [57].

A particular Lucas sequence is the Fibonacci sequence, whose characteristic polynomial is $X^2 - X - 1$, so that indicating by $(f_n)_{n\geq 1}$ the sequence, then $f_n = f_{n-1} + f_{n-2}$ for $n \geq 3$ with initial conditions $f_1 = f_2 = 1$. It is well known [75] that every positive integer n can be written as a sum of distinct non-consecutive Fibonacci numbers, that is, $n = \sum_{i=1}^{m} d_i f_i$, where $m \in \mathbb{N}$, $d_i \in \{0,1\}$, and $d_i d_{i+1} = 0$ for all $i \in \{1,\ldots,m-1\}$. This is called the *Zeckendorf representation* of n and, apart from the equivalent use of f_1 instead of f_2 or vice versa, is unique.
Let us recall that for every integer $n \geq 1$ it holds the *Binet formula*

$$f_n = \frac{\varphi^n - \overline{\varphi}^n}{\sqrt{5}},$$

where $\varphi := (1+\sqrt{5})/2$ is the Golden ratio and $\overline{\varphi} := (1-\sqrt{5})/2$ is its algebraic conjugate. An interesting property of linear recurrent sequences is their periodicity modulo an integer m, $\forall m \in \mathbb{Z}$. In particular, the period of a linear recurrence is the length of the smallest subsequence that throughout the sequence. This period length, also known as the Pisano period, is denoted by $\pi(m)$. So for every integer $m \geq 1$, the Fibonacci sequence $(f_n)_{n\geq 1}$ is (purely) periodic modulo m.
The Fibonacci sequence can be studied by different prospective. In our study we see it using the so-called *base-φ expansion* of real numbers, which was introduced by Bergman [13] in 1957 (see also [56]), and which is a particular case of non-integer base expansion (see, e.g., [50, 54]). Let $\mathfrak{D}$ be the set of sequences in $\{0,1\}$ that have no two consecutive terms equal to 1, and that are not ultimately equal to the periodic sequence $0,1,0,1,\ldots$. Then for every $x \in [0,1)$ there exists a unique sequence $\boldsymbol{\delta}(x) = (\delta_i(x))_{i\in\mathbb{N}}$ in $\mathfrak{D}$ such that $x = \sum_{i=1}^{\infty} \delta_i(x)\varphi^{-i}$. Precisely, $\delta_i(x) = \lfloor \varphi \cdot T^{(i-1)}(x) \rfloor$ for every $i \in \mathbb{N}$, where $T^{(i)}$ denotes the ith iterate of the map $T : [0,1) \to [0,1)$ defined by $T(\hat{x}) := (\varphi\hat{x} \bmod 1)$ for every $\hat{x} \in [0,1)$ and $T^{(0)}$ is the identity. Furthermore, letting $\mathcal{F} := \mathbb{Q}(\varphi) \cap [0,1)$, if $x \in \mathcal{F}$ then $\boldsymbol{\delta}(x)$ is ultimately periodic. In particular, if $x \in \mathcal{F}$ is given as $x = x_1 + x_2\varphi$, where $x_1, x_2 \in \mathbb{Q}$, then the preperiod and the period of $\boldsymbol{\delta}(x)$ can be effectively computed by finding the smallest $i \in \mathbb{N}$ such that $T^{(i)}(x) = T^{(j)}(x)$ for some $j \in \mathbb{N}$ with $j < i$. Conversely, for every ultimately periodic sequence $\boldsymbol{d} = (d_i)_{i\in\mathbb{N}}$ in $\mathfrak{D}$ we have that the number $x = \sum_{i=1}^{\infty} d_i\varphi^{-i}$ belongs to $\mathcal{F}$, and $x_1, x_2 \in \mathbb{Q}$ such that $x = x_1 + x_2\varphi$ can be effectively computed in terms of the preperiod and period of $\boldsymbol{d}$ by using the formula for the sum of the geometric series. Moreover, in the case that x is a rational number in $[0,1)$ then $\boldsymbol{\delta}(x)$ is purely periodic [59].

2.2 On the theory of algebraic independence and the theory of continued fractions

The preliminaries contained in this section are mainly taken from [34] and [60].

Definition 2.2.1. A number $\alpha \in \mathbb{C}$ is said to be algebraic if it is a root of a nonzero polynomial $f(t) = a_n t^n + \cdots + a_1 t + a_0$ with rational coefficients. A number β is said to be transcendental if it is not a root of any polynomial with algebraic coefficients [60].

Two classical transcendental numbers are π and e. The transcendence of π is closely related to the problem of squaring the circle, a classical problem studied since Ancient Greek times. Some approximations of π by rational numbers were achieved in the medieval period using geometric methods, specifically through the construction of regular polygons inscribed or circumscribed about the circle. In 1873, Hermite proved the transcendence of e with a new method that Lindemann generalized proving the transcendence of π.

Definition 2.2.2. Given a field $\mathbb{K}$ and a subfield $\mathbb{L} \subseteq \mathbb{K}$, then a set of numbers $T = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ with $\alpha_i \in \mathbb{K} \quad \forall 1 \leq i \leq n$ is algebraically independent over $\mathbb{L}$ if the elements of T do not satisfy any non-trivial polynomial equation with coefficients in $\mathbb{L}$ and in n variables, namely $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is not a zero of any non-trivial polynomial in $\mathbb{L}[x_1, \ldots, x_n]$.

Definition 2.2.3. Given $\mathbb{L} \subseteq \mathbb{K}$, a derivation $\delta : \mathbb{L} \to \mathbb{K}$ is a map which satisfies $\delta(x+y) = \delta(x) + \delta(y)$ and $\delta(xy) = x\delta(y) + \delta(x)y$ for $x, y \in \mathbb{K}$. Since $\mathbb{K}$ is an extension field of $\mathbb{L}$, δ is called an $\mathbb{L}$-derivation; if in addition $\delta(x) = 0$ for all $x \in \mathbb{L}$, δ is $\mathbb{L}$-linear.

The followings theorems are classical results about the algebraic independence of certain sets of numbers.

Theorem 2.2.4 (Lindemann - Weierstrass (1885))**.** *Given $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ algebraic numbers linearly independent over $\mathbb{Q}$, then $\{e^{\alpha_1}, e^{\alpha_2}, \ldots, e^{\alpha_n}\}$ are algebraically independent over $\mathbb{Q}$.*

Theorem 2.2.5 (Gelfond - Schneider (1934))**.** *Given $\{\alpha_1, \alpha_2, \beta_1, \beta_2\}$ non-zero algebraic numbers such that $\log \alpha_1$ and $\log \alpha_2$ are linearly independent over $\mathbb{Q}$ then $\beta_1 \log \alpha_1 + \beta_2 \log \alpha_2 \neq 0$.*

One can reformulate the above theorem in a different way. If $\alpha \neq 0,1$ is an algebraic number and β is algebraic and irrational, then α^{β} is transcendental. From Theorem 2.2.5, it follows that e^{π} is transcendental. An analogous theorem holds for any arbitrary number of logarithms of algebraic numbers. In particular, Baker generalized Theorem 2.2.5.

Theorem 2.2.6 (Baker (1967))**.** *Let* $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ *non-zero algebraic numbers such that* $\{\log \alpha_1, \log \alpha_2, \ldots, \log \alpha_n\}$ *are linearly independent over the field of rationals; then, the numbers* $\{1, \log \alpha_1, \log \alpha_2, \ldots, \log \alpha_n\}$ *are linearly independent over the field of all algebraic numbers.*

Definition 2.2.7. A continued fraction is an expression of the form

$$a_1 + \cfrac{b_1}{a_2 + \cfrac{b_2}{a_3 + \cfrac{b_3}{a_3 + \cfrac{b_3}{a_4 + \ddots}}}} \tag{2.4}$$

where the numbers $a_1, a_2, a_3, \ldots, b_1, b_2, b_3, \ldots$ can be integers or complex numbers.

A continued fraction is said to be simple if $b_i = 1 \ \forall i$ in expression (2.4), so it assumes the form

$$a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \ddots}}}}$$

and it is usually denoted by $[a_1, a_2, a_3, \ldots]$. The coefficients a_i are called partial quotients of the continued fraction, whereas the numbers

$$c_1 := [a_1] = \frac{a_1}{1},$$
$$c_2 := [a_1, a_2] = a_1 + \frac{1}{a_2},$$

$$c_3 := [a_1,a_2,a_3] = a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3}},$$

$$\vdots$$

$$c_i := [a_1,a_2,a_3,\ldots,a_i] = a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_{i-1} + \cfrac{1}{a_i}}}$$

are called convergents of the continued fractions. The numbers of a_i's may be finite or infinite. In the case that the a_i's are positive integers, any finite simple continued fraction represents a rational number and conversely any rational number can be represented as a finite simple continued fraction. A very famous result due to Lagrange asserts that any real quadratic irrational number η, namely numbers that have the form $\frac{P\pm\sqrt{D}}{Q}$ with P, Q integers and D a positive integer not a square, has a continued fraction expansion which is periodic. In particular, its continued fraction is

$$\begin{aligned} \eta &:= \left[a_0,a_1,\ldots,a_{k-1},\overline{a_k,\ldots,a_{k+\ell-1}}\right] \\ &= \left[a_0,a_1,\ldots,a_{k-1},a_k,\ldots,a_{k+\ell-1},a_k,\ldots,a_{k+\ell-1},a_k,\ldots,a_{k+\ell-1},\ldots\right], \end{aligned}$$

where $a_i \in \mathbb{Z}$, $a_i > 0$ if $i \geqslant 1$ and $k \geqslant 0$ and $\ell \geqslant 0$ are positive integers. For example, $\sqrt{2} = [1,\overline{2}]$, $\sqrt{3} = [1,\overline{1,2}]$ or $\sqrt{11} = [3,\overline{3,6}]$.

Let p_m/q_m denote the convergents of $\xi \in \mathbb{R}$. They are given by the recurrence formulas

$$p_{-1} := 1,\ p_0 := a_0,\ p_m := a_m p_{m-1} + p_{m-2} \qquad (m \geq 1), \tag{2.5}$$

$$q_{-1} := 0,\ q_0 := 1,\quad q_m := a_m q_{m-1} + q_{m-2} \qquad (m \geq 1). \tag{2.6}$$

One has

$$p_{m-1}q_m - p_m q_{m-1} = (-1)^m \qquad (m \geq 0). \tag{2.7}$$

The following is a classical result about the approximation of an irrational number in terms of its convergents.

Theorem 2.2.8. *Given $\xi \in \mathbb{R}$ and $\left(\frac{p_m}{q_m}\right)_{m\geq 0}$ the sequence of convergents of its continued fraction expansion, then*

$$\frac{1}{q_m(q_m+q_{m+1})} < \left|\xi - \frac{p_m}{q_m}\right| \leq \frac{1}{q_m q_{m+1}} < \frac{1}{q_m^2}.$$

Moreover, given two integers a, b such that $1 \leq b \leq q_{m-1}$, then it holds the inequality $|q_n\eta - p_n| \leq |b\eta - a|$. This means that each convergent is closer to the irrational number than the preceding one. Moreover, continued fractions provide the best rational approximations of real numbers.

In Chapter 6, we consider non-regular Hurwitz-type continued fractions of the form

$$\xi := \left[\overline{a_0, a_1, \ldots, a_{n-1}}\right]$$

with positive partial quotients $a_0, \ldots, a_{n-1}$, which are all "or partly" algebraically independent over the rational numbers $\mathbb{Q}$. A continued fraction is said to be *non-regular* if the partial quotients a_i are real numbers, and not all integers. *Hurwitz-type* continued fractions were introduced by Hurwitz in 1887 for complex number [37]. The Hurwitz-type continued fraction of a complex number ξ is given by a sequence such that each of its elements is computed with the nearest Gaussian integer function $[\cdot]\colon \mathbb{C} \to \mathbb{Z}[i]$. This function associates to each complex number z the Gaussian integer closest to z; if there is a tie, the function takes the one with the greatest real or imaginary part.

he main difference with classical continued fractions is that the partial quotients are chosen recursevily following a particular algorithm introduced by Hurwitz.....

2.3 On the resultants between polynomials

Definition 2.3.1. Given two polynomials $f(t) = a_n t^n + \cdots + a_1 t + a_0$, $g(t) = b_m t^m + \cdots + b_1 t + b_0 \in \mathbb{K}$, their resultant with respect to the variable t is given by

$$\mathrm{Res}(f,g) = a_n^m b_n^m \prod_{i,j}(\alpha_i - \beta_j)$$

where $f(\alpha_i) = 0$ for $1 \leq i \leq n$ and $g(\alpha_j) = 0$ for $1 \leq j \leq m$. The resultant $\mathrm{Res}(f,g)$ is an element of the field of the coefficients of $f(t)$ and $g(t)$.

There are several important properties that the resultant of two polynomials exhibits: below, we will list some lemmas whose proofs will be omitted.

Lemma 2.3.2. *The resultant between two polynomials is zero if and only if two polynomials have a root in common.*

Lemma 2.3.3. *Let $f(t), g(t) \in \mathbb{K}[t]$ have degrees n and m, both greater than zero, respectively. Then $f(t)$ and $g(t)$ have a non-constant common factor if and only if there exist nonzero polynomials $A(t), B(t) \in \mathbb{K}[t]$ such that $\deg(A(t)) \leq m-1$, $\deg(B(t)) \leq n-1$, and $A(t)f(t) + B(t)g(t) = 0$.*

Lemma 2.3.4. *For $f(t), g(t) \in \mathbb{K}[t]$, there exist polynomials $A(t), B(t) \in \mathbb{K}[t]$ such that $A(t)f(t) + B(t)g(t) = Res(f,g)$.*

Lemma 2.3.5. *If $f(t)$ is the characteristic polynomial of a square matrix F, and $g(t)$ is any polynomial, then the degree of the common factor of $f(t)$ and $g(t)$ is the nullity of the matrix $g(M)$.*

Chapter 3

On new R-Algebras of linear recurrent sequences

In this chapter, we extend the studies about the algebraic structure of linear recurrent sequences [17] considering in particular the Hurwitz product and the Newton product (that can be seen as the generalization of the Hurwitz product considering multinomial coefficients). In particular, we prove that the set of linear recurrent sequences with terms in the ring R, called $\mathcal{W}(R)$, is an $R-$algebra when equipped with the element-wise sum and the Hurwitz product, as well as when we consider element-wise sum and Newton product. We also give explicitly the characteristic polynomials of the Hurwitz and Newton product of two linear recurrent sequences. For the Newton product we also find explicitly the inverses. Furthermore, we study the isomorphisms between these algebraic structures, finding that $\mathcal{W}(R)$ with element-wise sum and Hurwitz product is not isomorphic to the other algebraic structures, whereas if we consider the Newton product, there is an isomorphism with the $R-$algebra obtained using the Hadamard product. Moreover, we present an overview about the behaviour of linear recurrent sequences under all the different operations considered (element-wise sum, Hadamard product, Cauchy product, Hurwitz product, Newton product) with respect to the characteristic polynomials and their companion matrices. The results present in this chapter belong to the published paper [2].

3.1 Previous results

In [17], the authors studied the algebraic structures of the set of linear recurrent sequences equipped with the component wise sum as first operation and both the Hadamard product and the convolution product as second operation. In particular, they showed that $(\mathcal{W}(R), \oplus, \odot)$ and $(\mathcal{W}(R), \oplus, *)$ are $R-$algebras and they are never isomorphic. Moreover, given $\mathbf{a}, \mathbf{b} \in \mathcal{W}(R)$ and $\mathbf{c} = \mathbf{a} \odot \mathbf{b}$, $\mathbf{d} = \mathbf{a} * \mathbf{b}$, they proved that

$$p_c(t) = p_a(t) \otimes p_b(t), \quad p_d(t) = p_a(t) \cdot p_b(t), \tag{3.1}$$

where the operation $\otimes$ between polynomials is defined as follows. Given two polynomials $f(t)$ and $g(t)$ with coefficients in R, said F and G their companion matrices, respectively, then $f(t) \otimes g(t)$ is the characteristic polynomial of the Kronecker product between F and G. In the following, we will denote by $\otimes$ also the Kronecker product between matrices. To the best of our knowledge, similar results involving the Hurwitz product and the Newton product are still missing.

Remark 3.1.1. Let us observe that the sequences $\mathbf{c}$ and $\mathbf{d}$, defined above, recur with characteristic polynomials $p_c(t)$ and $p_d(t)$ as given in (3.1), respectively, but these polynomials are not necessarily the minimal polynomials of recurrence. In the case that R is a ring without zero divisors, see [25] for more, the minimal polynomial of a linear recurrent sequence $\mathbf{a}$ is the (unique) monic polynomial $f(t)$ such that it divides any characteristic polynomial of any linear recurrence relation satisfied by $\mathbf{a}$. In other words, it is the characteristic polynomial of the linear recurrence relation of least degree satisfied by $\mathbf{a}$. In general, it is an hard problem to find the minimal polynomials of recurrence of these sequences, for some results, see [15, 31, 43, 66].

Given a linear recurrent sequence, then its generating function is a rational function. In particular, if $A_o(t) = \sum_{n=0}^{\infty} a_n t^n$ is the o.g.f. of the sequence $a_n = \sum_{i=1}^{N} h_i a_{n-i}$, then $A_o(t) = \frac{P(t)}{1-h_1 t - h_2 t^2 - \cdots - h_n x^n}$ where $P(t) = p_0 + p_1 t + \cdots + p_{N-1} t^{N-1}$. For example, let us consider the Fibonacci sequence for which the ordinary generating function is

$$F_o(t) = 1 + t + 2t^2 + 3t^3 + 5t^4 + 8t^5 + \cdots = \frac{p_0 + p_1 t}{1 - t - t^2}.$$

With some arithmetic manipulations, in particular multiplying both sides by $1-t-t^2$, we get the condition for p_0 and p_1,

$$p_0 + p_1 t = (1-t-t^2)(1+t+2t^2+3t^3+5t^4+8t^5+\cdots) = 1+0t+0t^2+\cdots$$

which means $p_0 = 1$ and $p_1 = 0$ so the rational expression of the ordinary generating function is $F_o(t) = \frac{1}{1-t-t^2}$.

Lemma 3.1.2. *([17, Lemma 3.2]) Given* $\mathbf{a} \in \mathcal{S}(R)$*, we have that* $\mathbf{a} \in \mathcal{W}(R)$ *and* $p_a(t)$ *is its characteristic polynomial if and only if* $p_a^*(t) \cdot A_o(t)$ *is a polynomial of degree less than* $\deg(p_a(t))$*, where* $p_a^*(t)$ *denotes the reciprocal or reflected polynomial of* $p_a(t)$*.*

Proof. Let $p_a(t) := t^N - \sum_{i=1}^{N} h_i t^{N-i}$. The result of the lemma follows directly from

$$\begin{aligned} p_a^*(t) \cdot A_o(t) = & a_0 + (a_1 - h_1 a_0)t + (a_2 - h_1 a_1 - h_2 a_0)t^2 + \cdots \\ & + (a_{N-1} - h_1 a_{N-2} - \cdots h_{N-1} a_0)t^{(N-1)} \\ & + \sum_{j \geq N}^{\infty} (a_j - h_1 a_{j-1} - \cdots h_N a_{j-N})t^j. \end{aligned} \tag{3.2}$$

□

3.2 R-algebras of linear recurrent sequences

To help the reader become familiar with the operations between sequences, we present them in Table 3.1. Let $\mathbf{a} := (a_0, a_1, a_2, \dots)$ and $\mathbf{b} := (b_0, b_1, b_2, \dots) \in \mathcal{S}(R)$, then the generic n-th term of the resulting sequence, when applying one of the operations listed in the first column of Table 3.1, is shown in the third column.

Name	Symbol	Definition
Element-wise sum	$\oplus$	$a_n + b_n$
Hadamard product	$\odot$	$a_n \cdot b_n$
Convolution product	$*$	$\sum_{i=0}^{n} a_i b_{n-i}$
Hurwitz product	$\star$	$\sum_{i=0}^{n} \binom{n}{i} a_i b_{n-i}$
Newton product	$\boxtimes$	$\sum_{i=0}^{n} \sum_{j=0}^{i} \binom{n}{i}\binom{i}{j} a_i b_{n-j}$

Table 3.1 Definitions and symbols for operations between sequences.

The main results of this section are provided in Theorems 3.2.1 and 3.2.5, where we prove that $(\mathcal{W}(R),\oplus,\star)$ and $(\mathcal{W}(R),\oplus,\boxtimes)$ are $R-$algebras, finding also the characteristic polynomial of the Hurwitz and Newton product between two linear recurrent sequences.

Theorem 3.2.1. *Given* $\mathbf{a},\mathbf{b}\in\mathcal{W}(R)$*, we have that* $\mathbf{r}:=\mathbf{a}\star\mathbf{b}\in\mathcal{W}(R)$ *and the characteristic polynomial of* $\mathbf{r}$ *is* $res(p_a(x),p_b(t-x))$ *with* $p_b(t-x)$ *regarded as a polynomial in x. Moreover,* $(\mathcal{W}(R),\oplus,\star)$ *is an* $R-$*algebra.*

Proof. It is well–known that $(\mathcal{S}(R),\oplus,\star)$ is an $R-$algebra (see, e.g., [39]), thus to prove that $(\mathcal{W}(R),\oplus,\star)$ is an $R-$algebra it is sufficient to show that $\mathbf{r}$ is again in $\mathcal{W}(R)$, i.e. $\mathbf{r}$ satisfies a linear recurrence. Let M and N be the degrees of $p_a(t)$ and $p_b(t)$, respectively. We prove the theorem in the case that $p_a(t)$ and $p_b(t)$ have distinct roots denoted by $\alpha_1,\dots,\alpha_M$ and $\beta_1,\dots,\beta_N$, respectively. We consider the ordinary generating function of the sequence $\mathbf{r}=\mathbf{a}\star\mathbf{b}$,

$$\begin{aligned}R_o(t)=\sum_{n=0}^{+\infty}\left(\sum_{i=0}^{n}\binom{n}{i}a_ib_{n-i}\right)t^n&=\sum_{i=0}^{+\infty}\sum_{n=i}^{+\infty}\binom{n}{i}a_ib_{n-i}t^n\\&=\sum_{i=0}^{+\infty}a_it^i\sum_{n=i}^{+\infty}\binom{n}{i}b_{n-i}t^{n-i}\\&=\sum_{i=0}^{+\infty}a_it^i\sum_{m=0}^{+\infty}\binom{m+i}{i}b_mt^m,\end{aligned}\tag{3.3}$$

where $\sum_{m=0}^{+\infty}\binom{m+i}{i}b_mt^m$ is the ordinary generating function of the sequence obtained from the Hadamard product between $\mathbf{b}$ and $\left(\binom{m+i}{i}\right)_{m\geq0}$, i.e.,

$$\sum_{m=0}^{+\infty}\binom{m+i}{i}b_mt^m=\left(\sum_{m=0}^{+\infty}b_mt^m\right)\odot\left(\sum_{m=0}^{+\infty}\binom{m+i}{i}t^m\right)=B_o(t)\odot\frac{1}{(1-t)^{i+1}}.$$

Since $B_o(t)$ is the ordinary generating function of $\mathbf{b}\in\mathcal{W}(R)$, it is a rational function and we can write it as

$$B_o(t)=\frac{\gamma(t)}{p_b^*(t)}=\sum_{j=1}^{N}\frac{c_j}{(1-\beta_jt)},$$

for some integers c_j. Now, we have

$$\frac{1}{1-\beta_j t}\odot\frac{1}{(1-t)^{i+1}}=\sum_{m=0}^{+\infty}(\beta_j t)^m\odot\sum_{m=0}^{+\infty}\binom{m+i}{i}t^m=\sum_{m=0}^{+\infty}\binom{m+i}{i}(\beta_j t)^m=\frac{1}{(1-\beta_j t)^{i+1}},$$

and we get that

$$B_o(t)\odot\frac{1}{(1-t)^{i+1}}=\sum_{j=1}^{N}c_j\frac{1}{1-\beta_j t}\odot\frac{1}{(1-t)^{i+1}}=\sum_{j=1}^{N}\frac{c_j}{(1-\beta_j t)^{i+1}}.$$

Thus, from (3.3) we obtain

$$\begin{aligned}R_o(t)=\sum_{i=0}^{+\infty}a_i t^i\sum_{j=1}^{N}\frac{c_j}{(1-\beta_j t)^{i+1}}&=\sum_{j=1}^{N}\frac{c_j}{1-\beta_j t}\sum_{i=0}^{+\infty}a_i\frac{t^i}{(1-\beta_j t)^i}\\&=\sum_{j=1}^{N}\frac{c_j}{1-\beta_j t}A_o\left(\frac{t}{1-\beta_j t}\right)\\&=\sum_{j=1}^{N}\frac{c_j}{1-\beta_j t}\cdot\frac{\delta\left(\frac{t}{1-\beta_j t}\right)}{p_a^*\left(\frac{t}{1-\beta_j t}\right)},\end{aligned}\tag{3.4}$$

where $\delta(t)$ is a polynomial of degree less than M.

Let $p(t)=\operatorname{res}(p_a(x),p_b(t-x))$, then $p(t)=\prod_{h=1}^{M}\prod_{l=1}^{N}(t-\alpha_h-\beta_l)$ and its reciprocal polynomial is $p^*(t)=\prod_{h=1}^{M}\prod_{l=1}^{N}(1-(\alpha_h+\beta_l)t)$. In particular, it is possible to rearrange the last formula in the following way

$$\begin{aligned}p^*(t)=\prod_{h=1}^{M}\prod_{l=1}^{N}(1-\beta_l t-\alpha_h t)&=\prod_{h=1}^{M}\prod_{l=1}^{N}(1-\beta_l t)\left(1-\frac{\alpha_h t}{1-\beta_l t}\right)\\&=\prod_{h=1}^{M}\prod_{l=1}^{N}(1-\beta_l t)\prod_{l=1}^{N}\left(1-\frac{\alpha_h t}{1-\beta_l t}\right)\\&=\prod_{h=1}^{M}p_b^*(t)\prod_{l=1}^{N}\left(1-\frac{\alpha_h t}{1-\beta_l t}\right)\\&=[p_b^*(t)]^M\prod_{l=1}^{N}\prod_{h=1}^{M}\left(1-\frac{\alpha_h t}{1-\beta_l t}\right)\end{aligned}$$

$$= [p_b^*(t)]^M \prod_{l=1}^{N} p_a^* \left(\frac{t}{1-\beta_l t} \right). \tag{3.5}$$

Combining (3.4) and (3.5) we get

$$\begin{aligned} p^*(t) \cdot R_o(t) &= [p_b^*(t)]^M \prod_{l=1}^{N} p_a^* \left(\frac{t}{1-\beta_l t} \right) \left(\sum_{j=1}^{N} \frac{c_j}{(1-\beta_j t)} \cdot \frac{\delta\left(\frac{t}{1-\beta_j t}\right)}{p_a^*\left(\frac{t}{1-\beta_j t}\right)} \right) \\ &= [p_b^*(t)]^M \left(\sum_{j=1}^{N} \frac{c_j}{1-\beta_j t} \cdot \delta\left(\frac{t}{1-\beta_j t} \right) \right) \cdot \prod_{\substack{l=1 \\ l \neq j}}^{N} p_a^* \left(\frac{t}{1-\beta_l t} \right). \end{aligned} \tag{3.6}$$

Moreover, we can express the function $\delta\left(\frac{t}{1-\beta_j t}\right)$ as

$$\delta\left(\frac{t}{1-\beta_j t} \right) = \sum_{h=0}^{M-1} \delta_h \cdot \left(\frac{t}{1-\beta_j t} \right)^h = \frac{\sum_{h=0}^{M-1} \delta_h t^h (1-\beta_j t)^{M-1-h}}{(1-\beta_j t)^{M-1}} = \frac{\mu_j(t)}{(1-\beta_j t)^{M-1}},$$

with $\deg(\mu_j(t)) \leq M-1$. Applying the same reasoning, we have

$$p_a^*\left(\frac{t}{1-\beta_j t} \right) = \frac{\sum_{h=0}^{M} f_h t^h (1-\beta_j t)^{M-h}}{(1-\beta_j t)^M} = \frac{\xi_j(t)}{(1-\beta_j t)^M}$$

with $\deg(\xi_j(t)) \leq M$. Hence, equation (3.6) becomes

$$\begin{aligned} p^*(t) \cdot R_o(t) &= [p_b^*(t)]^M \sum_{j=1}^{N} \frac{c_j}{1-\beta_j t} \cdot \frac{\mu_j(t)}{(1-\beta_j t)^{M-1}} \cdot \prod_{\substack{l=1 \\ l \neq j}}^{N} \frac{\xi_j(t)}{(1-\beta_j t)^M} \\ &= [p_b^*(t)]^M \sum_{j=1}^{N} c_j \cdot \frac{\mu_j(t)}{(1-\beta_j t)^M} \cdot \frac{\prod_{\substack{l=1 \\ l \neq j}}^{N} \xi_j(t)}{\prod_{\substack{l=1 \\ l \neq j}}^{N} (1-\beta_j t)^M} \\ &= [p_b^*(t)]^M \sum_{j=1}^{N} c_j \mu_j(t) \frac{\prod_{\substack{l=1 \\ l \neq j}}^{N} \xi_j(t)}{\left[p_b^*(t)\right]^M} = \sum_{j=1}^{N} c_j \mu_j(t) \prod_{\substack{l=1 \\ l \neq j}}^{N} \xi_j(t). \end{aligned} \tag{3.7}$$

We have from (3.7)

$$\deg\left(p^*(t)R_o(t)\right)=\deg\left(\sum_{j=1}^{N}c_j\mu_j(t)\prod_{\substack{l=1\\l\neq j}}^{N}\xi_j(t)\right)\leq M-1+(N-1)M=MN-1,$$

thus, by Lemma 3.1.2, $\mathbf{r}$ is a linear recurrent sequence whose characteristic polynomial is $p(t)=\operatorname{res}(p_a(x),p_b(t-x))$. □

Remark 3.2.2. Given $\mathbf{a},\mathbf{b}\in\mathcal{W}(R)$, if $\alpha_1,\dots\alpha_M$ and $\beta_1,\dots,\beta_N$ are distinct roots of $p_a(t)$ and $p_b(t)$ respectively, then, by Theorem 3.2.1, the roots of the characteristic polynomial of $\mathbf{a}\star\mathbf{b}$ are $\alpha_i+\beta_j$, for any $i=1,\dots,M$ and $j=1,\dots,N$. The proof of Theorem 3.2.1 can be adapted also in the case of multiple roots, in this case the calculations become much longer and more onerous.

In the following proposition, we see a way for writing the Newton product in terms of the Hurwitz and Hadamard ones.

Proposition 3.2.3. *Given* $\mathbf{a},\mathbf{b}\in\mathcal{W}(R)$, *then* $\mathbf{a}\boxtimes\mathbf{b}=[(\mathbf{a}\star\mathbf{1})\odot(\mathbf{b}\star\mathbf{1})]\star\mathbf{e}$, *where* $\mathbf{1}:=(1,1,1,\dots)$ *and* $\mathbf{e}:=((-1)^n)_{n\geq0}$.

Proof. The n-th terms of $\mathbf{a}\star\mathbf{1}$ and $\mathbf{b}\star\mathbf{1}$ are by definition $\sum_{i=0}^{n}\binom{n}{i}a_i$ and $\sum_{i=0}^{n}\binom{n}{i}b_i$, respectively. Thus, the n–th term of $(\mathbf{a}\star\mathbf{1})\odot(\mathbf{b}\star\mathbf{1})$ is $\sum_{s=0}^{n}\binom{n}{s}a_s\sum_{t=0}^{n}\binom{n}{t}b_t$, and consequently

$$\sum_{i=0}^{n}\binom{n}{i}(-1)^{n-i}\sum_{s=0}^{i}\binom{i}{s}a_s\sum_{t=0}^{i}\binom{i}{t}b_t$$

is the n–th term of $[(\mathbf{a}\star\mathbf{1})\odot(\mathbf{b}\star\mathbf{1})]\star\mathbf{e}$.
Applying Newton product's definition, we need to prove the equality

$$\sum_{i=0}^{n}\binom{n}{i}(-1)^{n-i}\sum_{s=0}^{i}\binom{i}{s}a_s\sum_{t=0}^{i}\binom{i}{t}b_t=\sum_{i=0}^{n}\sum_{j=0}^{i}\binom{n}{i}\binom{i}{j}a_ib_{n-j},\quad\forall n\geq0.\tag{3.8}$$

Let $c_i:=\sum_{s=0}^{i}\binom{i}{s}a_s\sum_{t=0}^{i}\binom{i}{t}b_t$ and $d_n:=\sum_{i=0}^{n}\sum_{j=0}^{i}\binom{n}{i}\binom{i}{j}a_ib_{n-j}$, then the expression (3.8) is equivalent to

$$\sum_{i=0}^{n}\binom{n}{i}(-1)^ic_i=(-1)^nd_n.\tag{3.9}$$

Making use of the Newton's inversion formula (see, e.g., [33, Equation 5.48]),

$$\sum_{i=0}^{n}\binom{n}{i}(-1)^i f(i)=g(n)\Leftrightarrow f(n)=\sum_{i=0}^{n}\binom{n}{i}(-1)^i g(i), \tag{3.10}$$

for some arithmetic functions f and g, equation (3.9) becomes

$$\sum_{i=0}^{n}\binom{n}{i}(-1)^i(-1)^i d_i=c_n,$$

that is

$$\sum_{i=0}^{n}\binom{n}{i}\sum_{k=0}^{i}\sum_{j=0}^{k}\binom{i}{k}\binom{k}{j}a_k b_{i-j}=\sum_{s=0}^{n}\binom{n}{s}a_s\sum_{t=0}^{n}\binom{n}{t}b_t. \tag{3.11}$$

So, showing that (3.11) holds is equivalent to prove (3.8). Now, we can write the first member of (3.11) as

$$\sum_{j=0}^{n}\sum_{s=j}^{n}\sum_{i=s}^{n}\binom{n}{i}\binom{i}{s}\binom{s}{j}a_s b_{i-j}. \tag{3.12}$$

From (3.12) we have $0\leq j\leq s\leq i\leq n$, and we can rewrite (3.12) in the equivalent form

$$\sum_{s=0}^{n}\sum_{j=0}^{s}\sum_{i=s}^{n}\binom{n}{i}\binom{i}{s}\binom{s}{j}a_s b_{i-j},$$

where, setting $t=i-j$, so that $s\leq t+j\leq n$, we obtain

$$\sum_{s=0}^{n}\sum_{j=0}^{s}\sum_{t=s-j}^{n-j}\binom{n}{t+j}\binom{t+j}{s}\binom{s}{j}a_s b_t. \tag{3.13}$$

Observing that

$$\begin{aligned}\binom{n}{t+j}\binom{t+j}{s}&=\frac{n!}{(n-t-j)!(t+j-s)!s!}\\&=\frac{n!(n-s)!}{(n-s)!s!(n-t-j)!(t+j-s)!}\\&=\binom{n}{s}\binom{n-s}{n-t-j}\end{aligned}$$

the term (3.13) becomes

$$\sum_{s=0}^{n}\binom{n}{s}a_s\sum_{j=0}^{s}\sum_{t=s-j}^{n-j}\binom{n-s}{n-t-j}\binom{s}{j}b_t.$$

Finally, setting $m := s-j$, we have $0 \le m \le s$ and we get

$$\begin{aligned}
&\sum_{s=0}^{n}\binom{n}{s}a_s\sum_{m=0}^{s}\sum_{t=m}^{n-s+m}\binom{n-s}{n-s-(t-m)}\binom{s}{s-m}b_t\\
&=\sum_{s=0}^{n}\binom{n}{s}a_s\sum_{m=0}^{s}\sum_{t=m}^{n-s+m}\binom{n-s}{t-m}\binom{s}{m}b_t\\
&=\sum_{s=0}^{n}\binom{n}{s}a_s\sum_{t=0}^{n}b_t\sum_{m=0}^{t}\binom{n-s}{t-m}\binom{s}{m}\\
&=\sum_{s=0}^{n}\binom{n}{s}a_s\sum_{t=0}^{n}\binom{n}{t}b_t,
\end{aligned}$$

where the last equality is due to Vandermonde's identity $\sum_{m=0}^{t}\binom{n-s}{t-m}\binom{s}{m}=\binom{n}{t}$. □

Remark 3.2.4. The previous proposition can be proved also exploiting the umbral calculus. The techniques of umbral calculus were introduce by John Blissard around 1870. The main idea was to obtain some sequences' identities pretending that the indices of the sequence's terms were exponents. Indeed, given a sequence $(a_0,a_1,a_2,\dots)$ if we want to associate to it a new sequence $(b_0,b_1,b_2,\dots)$ such that $b_n=\sum_{k=0}^{n}\binom{n}{k}a_k$, we can mix up indices and exponents and think b_n as $b^n := (a+1)^n$. In 1930 Eric Bell tried to formulate this concept in a formal way. In particular, he associated to each sequence **a** and **b**, two variables called umbral variables such that these variables obey to a very particular algebra. In 1970 Gian-Carlo Rota and Steven Roman connected umbral calculus with linear algebra. Umbral variables can be thought as representing polynomials instead of representing sequences. Let $\mathcal{L}$ be a linear operator acting on polynomials such that $\mathcal{L}(x^n) := a_n$, then, for example, applying the binomial theorem and the linearity of $\mathcal{L}$, we get

$$\begin{aligned}
\mathcal{L}((x+1)^n) &= \mathcal{L}\Big(\sum_{k=0}^{n}\binom{n}{k}x^k\Big)\\
&=\sum_{k=0}^{n}\binom{n}{k}\mathcal{L}(x^k).
\end{aligned}$$

In order to prove Proposition 3.2.3 with the techniques of umbral calculus, we consider two linear functionals U and V defined by $U(W^n) := a_n$ and $V(Z^n) := b_n$ associated to $\mathbf{a}, \mathbf{b} \in \mathcal{S}(R)$. It follows that the n–th term given by

$$\big((\mathbf{a} \boxtimes \mathbf{b}) \star \mathbf{1}\big)_n = \sum_{i=0}^{n} \binom{n}{i} \sum_{k=0}^{i} \sum_{j=0}^{k} \binom{i}{k} \binom{k}{j} a_k b_{i-j}$$

it can be obtained using the functionals U and V in the following way

$$\begin{aligned} UV\left(\sum_{i=0}^{n} \binom{n}{i} Z^i \sum_{k=0}^{i} \binom{i}{k} W^k \sum_{j=0}^{k} \binom{k}{j} Z^{-j}\right) &= UV\left(\sum_{i=0}^{n} \binom{n}{i} Z^i \sum_{k=0}^{i} \binom{i}{k} (W + W/Z)^k\right) \\ &= UV\left(\sum_{i=0}^{n} \binom{n}{i} (ZW + W + Z)^i\right) \\ &= UV((ZW + W + Z + 1)^n). \end{aligned}$$

Now, the last quantity can be rewritten as

$$\begin{aligned} UV((Z+1)^n (W+1)^n) &= U(V(Z+1)^n (W+1)^n) \\ &= U\left(V\left(\sum_{s=0}^{n} \binom{n}{s} Z^s\right) (W+1)^n\right) \\ &= U\left(\sum_{s=0}^{n} \binom{n}{s} b_s (W+1)^n\right) \\ &= \sum_{s=0}^{n} \binom{n}{s} b_s U\left(\sum_{t=0}^{n} \binom{n}{t} W^t\right) \\ &= \sum_{s=0}^{n} \binom{n}{s} b_s \cdot \sum_{t=0}^{n} \binom{n}{s} a_t, \end{aligned}$$

which is the n–th term of the sequence $(\mathbf{a} \star \mathbf{1}) \odot (\mathbf{b} \star \mathbf{1})$.

Theorem 3.2.5. *Given $\mathbf{a}, \mathbf{b} \in \mathcal{W}(R)$, we have that $\mathbf{c} := \mathbf{a} \boxtimes \mathbf{b} \in \mathcal{W}(R)$ and the characteristic polynomial of $\mathbf{c}$ is $\prod_{i=1}^{M} \prod_{j=1}^{N} (t - (\alpha_i + \beta_j + \alpha_i \beta_j))$, where $M := \deg(p_a(t))$, $N := \deg(p_b(t))$, α_i's are the roots of $p_a(t)$ and β_j's the roots of $p_b(t)$. Moreover, $(\mathcal{W}(R), \oplus, \boxtimes)$ is an $R-$algebra.*

Proof. Firstly, we show that $(\mathcal{S}(R), \oplus, \boxtimes)$ is an $R-$algebra. This is an immediate consequence of Proposition 3.2.3. Indeed, since $\mathbf{a} \boxtimes \mathbf{b} = [(\mathbf{a} \star \mathbf{1}) \odot (\mathbf{b} \star \mathbf{1})] \star \mathbf{e}$, it is

straightforward to see that the Newton product satisfies all the properties characterizing $(\mathcal{S}(R),\oplus,\boxtimes)$ as an $R-$algebra. Moreover, since $(1,0,0,\ldots)$ is the identity element for the Hurwitz product and $\mathbf{e}$ is the inverse of $\mathbf{1}$ with respect to the Hurwitz product, we have that $(1,0,0,\ldots)$ is the identity also for the Newton product. Given $\mathbf{a},\mathbf{b}\in\mathcal{W}(R)$, we have $\mathbf{a}\boxtimes\mathbf{b}\in\mathcal{W}(R)$ by Proposition 3.2.3, thus also $(\mathcal{W}(R),\oplus,\boxtimes)$ is an $R-$algebra. By Theorem 3.2.1 and Remark 3.2.2, we can observe that, given $\mathbf{a},\mathbf{b}\in\mathcal{W}(R)$, then $\mathbf{a}\star\mathbf{1}$ and $\mathbf{b}\star\mathbf{1}$ are linear recurrent sequences whose characteristic polynomials have roots α_i+1 and β_j+1, for $i=1,\ldots,M$ and $j=1,\ldots,N$, respectively. Moreover, since $\mathbf{e}$ is a linear recurrent sequence whose characteristic polynomial is $t+1$, then $[(\mathbf{a}\star\mathbf{1})\odot(\mathbf{b}\star\mathbf{1})]\star\mathbf{e}$ has characteristic polynomial whose roots are $(\alpha_i+1)(\beta_j+1)-1=\alpha_i+\beta_j+\alpha_i\beta_j$, for $i=1,\ldots,M$ and $j=1,\ldots,N$. □

Proposition 3.2.6. *Let $\mathbf{a}\in\mathcal{S}(R)$ be invertible with respect to the Newton product, then, said $\mathbf{b}$ its inverse, we have that the generic term has the following explicit formula*

$$b_n := (-1)^n\sum_{t=0}^{n}\binom{n}{t}(-1)^t\frac{1}{\sum_{s=0}^{t}\binom{t}{s}a_s}, \tag{3.14}$$

for any $n\geq 0$.

Proof. Recalling that the identity element for the Newton product is $(1,0,0,\ldots)$, we have that a_0b_0 must be 1, i.e., $b_0=a_0^{-1}$. When $n\geq 1$, we have that

$$\sum_{i=0}^{n}\binom{n}{i}(-1)^{n-i}\sum_{s=0}^{i}\binom{i}{s}a_s\sum_{t=0}^{i}\binom{i}{t}b_t=0,$$

i.e.,

$$\sum_{i=0}^{n}\binom{n}{i}(-1)^{i}\sum_{s=0}^{i}\binom{i}{s}a_s\sum_{t=0}^{i}\binom{i}{t}b_t=0.$$

Let us define the quantities

$$f(i) := \sum_{s=0}^{i}\binom{i}{s}a_s\sum_{t=0}^{i}\binom{i}{t}b_t,\quad g(n) := \sum_{i=0}^{n}\binom{n}{i}(-1)^i f(i),$$

where $g(n)=0$, when $n\geq 1$ and $g(0)=1$. Applying Newton's inversion formula (3.10), we get

$$f(n)=\sum_{i=0}^{n}\binom{n}{i}(-1)^i g(i).$$

Since $g(i) = 0$ for all $i \geq 1$, we have $f(n) = 1$ for all $n \geq 0$, thus

$$\sum_{s=0}^{n} \binom{n}{s} a_s \sum_{t=0}^{n} \binom{n}{t} b_t = 1,$$

or, equivalently,

$$\sum_{t=0}^{n} \binom{n}{t} b_t = \frac{1}{\sum_{s=0}^{n} \binom{n}{s} a_s}.$$

Let $d_n = \frac{1}{\sum_{s=0}^{n} \binom{n}{s} a_s}$, by Newton's inversion formula, we get for all $n \geq 0$

$$d_n = \sum_{t=0}^{n} \binom{n}{t} (-1)^t (-1)^t b_t \quad \Leftrightarrow \quad (-1)^n b_n = \sum_{t=0}^{n} \binom{n}{t} (-1)^t d_t,$$

therefore

$$b_n = (-1)^n \sum_{t=0}^{n} \binom{n}{t} (-1)^t \frac{1}{\sum_{s=0}^{t} \binom{t}{s} a_s}.$$

□

Remark 3.2.7. We point out that $\mathbf{a}$ is invertible with respect to the Newton product if and only if all the elements of $\mathbf{a}$ are invertible elements of R, as well as it happens for the Hadamard product.

At each sequence $\mathbf{a} \in \mathcal{W}(R)$, it can be linked a monic characteristic polynomial $p_a \in R[t]$ and, at this polynomial a matrix A (called companion matrix) can be associated to it. Therefore, the results found for the $R-$algebras $(\mathcal{W}(R), \oplus, \odot)$, $(\mathcal{W}(R), \oplus, *)$, $(\mathcal{W}(R), \oplus, \star)$, and $(\mathcal{W}(R), \oplus, \boxtimes)$ can be seen in terms of new algebraic structures in the set of the monic polynomials $\mathcal{P}ol(R)$ with coefficients in R. Indeed, we can also observe what happens to the roots and to the companion matrices of the characteristic polynomials.

Let us consider $\mathbf{a}, \mathbf{b} \in \mathcal{W}(R)$ with characteristic polynomials of degree respectively M and N, whose roots are $\alpha_1, \ldots, \alpha_M$ and $\beta_1, \ldots \beta_N$. The sequences $\mathbf{a} + \mathbf{b}$ and $\mathbf{a} * \mathbf{b}$ both recur with characteristic polynomial $p_a(t) \cdot p_b(t)$. Regarding the Hadamard product, we have already observed that the characteristic polynomial of $\mathbf{c} = \mathbf{a} \odot \mathbf{b}$ is $p_c(t) = p_a(t) \otimes p_b(t)$, whose roots are $\alpha_i \beta_j$, for $i = 1, \ldots, M$ and $j = 1, \ldots, N$. Thus, starting from the $R-$algebra $(\mathcal{W}(R), \oplus, \odot)$, we can construct the semiring $(\mathcal{P}ol(R), \cdot, \otimes)$ whose identity element is the polynomial $t - 1$. Said A, B, and C the companion matrices of $p_a(t), p_b(t)$ and $p_c(t)$, we have that $C = A \otimes B$,

where $\otimes$ is the Kronecker product between matrices. Thus C is a $mn \times mn$ matrix with eigenvalues the products of the eigenvalues of A and B.

Similarly, starting from the Hurwitz product, we can construct a new operation in $\mathcal{P}ol(R)$. Given $\mathbf{c} = \mathbf{a} \star \mathbf{b}$, we proved that $p_c(t)$ has roots $\alpha_i + \beta_j$, for $i = 1, \dots, M$ and $j = 1, \dots, N$. The matrix $A \otimes I_n + I_m \otimes B$ is a $mn \times mn$ matrix, whose eigenvalues are the sum of the eigenvalues of A and B. Thus, we can define $p_c(t) := p_a(t) \star p_b(t)$ as the characteristic polynomial of the matrix $A \otimes I_n + I_m \otimes B$ and we get the semiring $(\mathcal{P}ol(R), \cdot, \star)$.

Finally, given $\mathbf{c} = \mathbf{a} \boxtimes \mathbf{b}$, we know that $p_c(t)$ has roots $\alpha_i + \beta_j + \alpha_i\beta_j$, for $i = 1, \dots, M$ and $j = 1, \dots, N$. In this case, we can define $p_c(t) := p_a(t) \boxtimes p_b(t)$ as the characteristic polynomial of the matrix $A \otimes I_n + I_m \otimes B + A \otimes B$, which is a $mn \times mn$ matrix, whose eigenvalues are exactly $\alpha_i + \beta_j + \alpha_i\beta_j$, for $i = 1, \dots, M$ and $j = 1, \dots, N$. Thus, we have that $(\mathcal{P}ol(R), \cdot, \boxtimes)$ is another semiring of monic polynomials.

3.3 On isomorphisms between R-algebras

In [17], Cerruti and Vaccarino proved that $(\mathcal{W}(R), \oplus, \odot)$ and $(\mathcal{W}(R), \oplus, *)$ are never isomorphic as $R-$algebras. In the following we prove similar results for the other algebraic structures that we have studied in the previous section.

Theorem 3.3.1. *The $R-$algebras $(\mathcal{W}(R), \oplus, \odot)$ and $(\mathcal{W}(R), \oplus, \star)$ are not isomorphic.*

Proof. Let us suppose that $\psi : (\mathcal{W}(R), \oplus, \odot) \to (\mathcal{W}(R), \oplus, \star)$ is an injective morphism and consider $\mathbf{a} := (1, 0, 0, 0, \dots)$ and $\mathbf{b} := (0, 1, 0, \dots)$. Since we are considering a morphism and $\mathbf{a} \odot \mathbf{b} = (0, 0, 0, \dots)$, then $\psi(\mathbf{a} \odot \mathbf{b}) = (0, 0, \dots)$ so also $\psi(\mathbf{a}) \star \psi(\mathbf{b}) = (0, 0, \dots)$ and, by injectivity, $\psi(\mathbf{a}), \psi(\mathbf{b}) \neq (0, 0, \dots)$. Let $A_e^{\psi}(t)$ and $B_e^{\psi}(t)$ be the exponential generating functions of $\psi(\mathbf{a})$ and $\psi(\mathbf{b})$, respectively. From $\psi(\mathbf{a}) \star \psi(\mathbf{b}) = (0, 0, \dots)$, it follows that $A_e^{\psi}(t) B_e^{\psi}(t) = 0$. Thanks to Lemma 3.1.2, we have

$$p^*_{\psi(\mathbf{a})}(t) A_o^{\psi}(t) = h(t) \tag{3.15}$$

with $\deg(h(t)) < \deg(p^*_{\psi(\mathbf{a})}(t))$.
Now, let us examine the map $\gamma : (R[[t]], +, \cdot) \to (R^e[[t]], +, \cdot)$, which is an isomor-

phism from the set of ordinary generating functions $R[[t]] = \{\sum_{n=0}^{\infty} a_n t^n, \forall a_n \in \mathbb{R}\}$ and the ones of exponential generating functions $R^e[[t]] = \{\sum_{n=0}^{\infty} \frac{a_n}{n!} t^n, \forall a_n \in \mathbb{R}\}$, where the sum is the usual one as the sum between polynomials. Whereas, the product of the first ring corresponds to the Cauchy product between sequences and the product of the second ring to the ones of Hurwitz. Applying γ to (3.15), we obtain

$$\gamma\left(p^*_{\psi(\mathbf{a})}(t)\right) A_e^{\psi}(t) = \gamma(h(t))$$

where $p^*_{\psi(\mathbf{a})}(t)$ can be viewed as a formal series with an infinite number of zero coefficients. Multiplying by $\gamma(p^*_{\psi(\mathbf{a})}(t))$ the equation $A_e^{\psi}(t)B_e^{\psi}(t) = 0$, it becomes

$$\gamma(h(t))B_e^{\psi}(t) = 0$$

which implies $h(t)B_o^{\psi}(t) = 0$. From this, it follows that there is a nonzero element $w \in R$, such that $wB_o^{\psi}(t) = 0$ ([30, Eq. (2.9)]) and $w\mathbf{b} = 0$, which is absurd. □

Theorem 3.3.2. *The $R-$algebras $(\mathcal{W}(R), \oplus, \odot)$ and $(\mathcal{W}(R), \oplus, \boxtimes)$ are isomorphic.*

Proof. The explicit isomorphism is $\psi : (\mathcal{W}(R), \oplus, \odot) \to (\mathcal{W}(R), \oplus, \boxtimes)$ defined by $\psi(\mathbf{a}) := \mathbf{a} \star \mathbf{e}$, where $\mathbf{e} = ((-1)^n)_{n\geq 0}$. Indeed, by Theorem 3.2.1, the map ψ is well–defined (in the sense that a linear recurrent sequence is mapped into a linear recurrent sequence). Moreover, since $\mathbf{1}$ is the inverse of $\mathbf{e}$ with respect to the Hurwitz product, it is straightforward to check injectivity and surjectivity. Finally, by Proposition 3.2.3, we have

$$\psi(\mathbf{a}) \boxtimes \psi(\mathbf{b}) = (((\mathbf{a} \star \mathbf{e}) \star \mathbf{1}) \odot ((\mathbf{b} \star \mathbf{e}) \star \mathbf{1})) \star \mathbf{e} = (\mathbf{a} \odot \mathbf{b}) \star \mathbf{e} = \psi(\mathbf{a} \odot \mathbf{b}),$$

since $\mathbf{e} \star \mathbf{1} = (1, 0, 0, \ldots)$. □

Theorem 3.3.3. *Let R be an integral domain, if $\psi : (\mathcal{W}(R), \oplus, *) \to (\mathcal{W}(R), \oplus, \star)$ is a morphism, then ψ is not injective.*

Proof. Let us suppose that $\psi : (\mathcal{W}(R), \oplus, *) \to (\mathcal{W}(R), \oplus, \star)$ is an injective morphism. Let us denote by $(\psi(\mathbf{a}))_i$ the i-th term of the sequence $\psi(\mathbf{a})$. The n-th term

of $\psi(\mathbf{a}) \star \psi(\mathbf{b})$ is

$$\sum_{i=0}^{n} \binom{n}{i} (\psi(\mathbf{a}))_i (\psi(\mathbf{b}))_{n-i} = n! \sum_{i=0}^{n} \binom{n}{i} \frac{(\psi(\mathbf{a}))_i}{i!} \frac{(\psi(\mathbf{b}))_{n-i}}{(n-i)!}.$$

Then, considering $\psi(\mathbf{a} * \mathbf{b}) = \psi(\mathbf{a}) \star \psi(\mathbf{b})$, for any $\mathbf{a}, \mathbf{b} \in \mathcal{W}(R)$, we obtain

$$\psi(\mathbf{a} * \mathbf{b}) = ((\psi(\mathbf{a}) \odot \mathbf{f}^{-1}) \star (\psi(\mathbf{b}) \odot \mathbf{f}^{-1})) \odot \mathbf{f} \tag{3.16}$$

where we define the formal sequences $\mathbf{f} := (1, 2!, 3!, \ldots)$ and $\mathbf{f}^{-1} := (1, \frac{1}{2!}, \frac{1}{3!}, \ldots)$.

We define a map $\tau : (\mathcal{W}(R), \oplus, *) \to (\mathcal{W}(R), \oplus, *)$ such that $\tau(\mathbf{a}) := \psi(\mathbf{a}) \odot \mathbf{f}^{-1}$. By definition, we have that $\tau(\mathbf{a} \oplus \mathbf{b}) = \tau(\mathbf{a}) \oplus \tau(\mathbf{b})$, $\tau(\mathbf{a} * \mathbf{b}) = \tau(\mathbf{a}) * \tau(\mathbf{b})$, for any $\mathbf{a}, \mathbf{b} \in \mathcal{W}(R)$ and $\ker(\tau) = \mathbf{0}$ where $\mathbf{0} = (0, 0, 0, \ldots)$.

Let $\tilde{\tau}$ be a map that acts over the ordinary generating functions such that if $A(t) = \sum_{n=0}^{+\infty} a_n t^n$ then $\tilde{\tau}(A(t)) = \sum_{n=0}^{+\infty} (\tau(a))_n t^n$. From the properties of τ, it follows that

$$\tilde{\tau}(A(t) + B(t)) = \tilde{\tau}(A(t)) + \tilde{\tau}(B(t)), \quad \tilde{\tau}(A(t)B(t)) = \tilde{\tau}(A(t))\tilde{\tau}(B(t))$$

and

$$\tilde{\tau}(A(t)) = \tilde{\tau}(B(t)) \quad \Leftrightarrow \quad A(t) = B(t).$$

When we consider $A(t) = 1$ and $B(t) = 1$, we clearly have

$$\tilde{\tau}(1) = \tilde{\tau}(1 \cdot 1) = \tilde{\tau}(1)\tilde{\tau}(1)$$

and this implies $\tilde{\tau}(1) = 1$. Indeed, by the injectivity of τ, we can not have $\tilde{\tau}(1) = 0$ because $\tau(1, 0, \ldots)$ should be $\mathbf{0}$. In the case that $A(t) = t$ and $B(t) = -t$, then

$$0 = \tilde{\tau}(0) = \tilde{\tau}(t - t) = \tilde{\tau}(t) + \tilde{\tau}(-t),$$

which implies $\tilde{\tau}(-t) = -\tilde{\tau}(t)$. Moreover, when $A(t) = t$ and $B(t) = t^{-1}$, then

$$1 = \tilde{\tau}(1) = \tilde{\tau}(t \cdot t^{-1}) = \tilde{\tau}(t)\tilde{\tau}(t^{-1}),$$

so $\tilde{\tau}(t^{-1}) = (\tilde{\tau}(t))^{-1}$. Lastly, if $A(t) = B(t) = t$, then

$$\tilde{\tau}(t^2) = \tilde{\tau}(t \cdot t) = \tilde{\tau}(t)\tilde{\tau}(t),$$

so $\tilde{\tau}(t^2) = (\tilde{\tau}(t))^2$ and $\tilde{\tau}(nt) = n\tilde{\tau}(t)$, $\forall n \in \mathbb{N}$.

Now, let us consider $A(t) = t$ and $\tilde{\tau}(t) = \sum_{n=0}^{+\infty} s_n t^n$, then from $\tilde{\tau}(t^2) = (\tilde{\tau}(t))^2$ it follows that

$$\left(\sum_{n=0}^{+\infty} s_n t^n\right)^2 = \sum_{n=0}^{+\infty}\left(\sum_{i=0}^{n} s_i s_{n-i}\right) t^n \Rightarrow \begin{cases} \sum_{i=0}^{2k+1} s_i s_{2k+1-i} = 0 \\ \sum_{i=0}^{2k} s_i s_{2k-i} = s_k \end{cases} \tag{3.17}$$

i.e, if we consider the square of the ordinary generating function $\tilde{\tau}(t)$, seen as the product between $\tilde{\tau}(t)$ and itself, it must be equal to $\tilde{\tau}(t^2)$, then the coefficients of the even powers are zero and the coefficients of the odd powers are s_k. From (3.17), we obtain $s_0 = s_0^2$ and we may have $s_0 = 0$ or $s_0 = 1$. In the case that $s_0 = 1$, then $s_i = 0$, $\forall i \geq 1$, and $\tilde{\tau}(t) = 1$. But this can not happen because, if so, we should have

$$\tilde{\tau}(t) = 1 = \tilde{\tau}(1),$$

which implies $\tilde{\tau}(t-1) = 0$, i. e., $t = 1$. Whereas, if $s_0 = 0$, then $s_1 = s_1^2$ and $s_1 = 0$ or $s_1 = 1$. In the case that $s_1 = 1$, then $s_i = 0$, $\forall i \geq 2$, and $\tilde{\tau}(t) = t$.
In the case that $s_1 = 0$, then $s_2 = s_2^2$ so $s_2 = 0$ or $s_2 = 1$. Repeating the same reasoning and exploiting (3.17), we get that $\tilde{\tau}(t) = t^k$ must hold for a fixed $k \geq 1$.

Let us consider $A(t) = \frac{1}{1-t}$, then

$$\tilde{\tau}((1-t)^{-1}) = (\tilde{\tau}(1) - \tilde{\tau}(t))^{-1} = (1 - \tilde{\tau}(t))^{-1} = (1 - t^k)^{-1}.$$

By definition,

$$\tilde{\tau}\left(\frac{1}{1-t}\right) = \tilde{\tau}\left(\sum_{n=0}^{+\infty} t^n\right) = \sum_{n=0}^{+\infty} (\tau(\mathbf{1}))_n t^n, \tag{3.18}$$

and, since from some $k \geq 1$ we have $\tilde{\tau}(t) = t^k$, we also have

$$\tilde{\tau}\left(\frac{1}{1-t}\right) = \sum_{n=0}^{+\infty} t^{kn}. \tag{3.19}$$

Equating the coefficients in the two equivalent power series (3.18) and (3.19), we have

$$\left(\tilde{\tau}\left(\frac{1}{1-t}\right)\right)_n = \begin{cases} 1 & \text{if } k \mid n \\ 0 & \text{if } k \nmid n. \end{cases}$$

Thus, by (3.16) and the definition of τ and $\tilde{\tau}$, we have

$$\psi(\mathbf{1})_n = (\tau(\mathbf{1}) \odot \mathbf{f})_n = \begin{cases} n! & \text{if } k \mid n \\ 0 & \text{if } k \nmid n, \end{cases}$$

which is not a linear recurrent sequence. □

Remark 3.3.4. It has been proved that $(\mathcal{W}(R), \oplus, \odot)$ and $(\mathcal{W}(R), \oplus, \boxtimes)$ are isomorphic as R-algebras (see Theorem 3.3.2). However, $(\mathcal{W}(R), \oplus, \odot)$ and $(\mathcal{W}(R), \oplus, \star)$ are not isomorphic (see Theorem 3.3.1), nor are $(\mathcal{W}(R), \oplus, \odot)$ and $(\mathcal{W}(R), \oplus, *)$ [17]. It is interesting to explore the existence of injective morphisms among these algebras. According to [17], there are no injective morphisms from $(\mathcal{W}(R), \oplus, \odot)$ to $(\mathcal{W}(R), \oplus, *)$, nor $(\mathcal{W}(R), \oplus, \boxtimes)$ to $(\mathcal{W}(R), \oplus, *)$. The existence of injective morphisms in the reverse directions remains an open problem. From the proof of Theorem 3.3.1, it follows that there are no injective morphisms from $(\mathcal{W}(R), \oplus, \odot)$ or $(\mathcal{W}(R), \oplus, \boxtimes)$ to $(\mathcal{W}(R), \oplus, \star)$. Whether the reverse injective morphisms exist is still an open problem. Finally, Theorem 3.3.3 states that there is no injective morphism from the R-algebra with the convolution product to the one with Hurwitz product, but whether the reverse is true remains an open question.

Chapter 4

Lucas atoms

In this chapter, we define Lucas atoms, originally introduced by Sagan and Tirrell [57], in a different way which is probably easier and more direct. We prove some of their main properties and we present new results on their p-adic valuations. Moreover, we solve a left open problem by Sagan and Tirrell in [57]. Finally, we exploit the results on the p-adic valuations of Lucas atoms to prove that the sequence of Lucas atoms is not holonomic.

4.1 Revisiting some properties of Lucas atoms via cyclotomic polynomials

In this section, we obtain some properties of Lucas atoms exploiting the definition (2.2). Here, we will always consider s,t,α and β as variables related by

$$s := \alpha+\beta, \quad t := -\alpha\beta.$$

First of all, we prove that the Lucas atoms are actually polynomials with natural coefficients.

Lemma 4.1.1. *For all $n \geq 0$, we have $\alpha^n+\beta^n \in \mathbb{Z}_{\geq 0}[s,t]$.*

Proof. We prove the Lemma by induction. The first steps are straightforward:

$$\alpha+\beta = s, \quad \alpha^2+\beta^2 = (\alpha+\beta)^2-2\alpha\beta = s^2+2t.$$

Now, consider an integer $n > 2$ and suppose $\alpha^i + \beta^i \in \mathbb{Z}_{\geq 0}[s,t]$ for all $i \leq n-1$. If $n = 2^k$ we want to prove that $\alpha^{2^k} + \beta^{2^k} = P_k + 2t^{2^{k-1}}$ with $P_k := P_{k-1}^2 + 4P_{k-1}t^{2^{k-2}}$. By induction, for $k = 1$ we have $\alpha^2 + \beta^2 = P_1 + 2t$, for $k > 1$

$$\begin{aligned}
\alpha^{2^k} + \beta^{2^k} &= (\alpha^{2^{k-1}} + \beta^{2^{k-1}})^2 - 2\alpha^{2^{k-1}}\beta^{2^{k-1}} \\
&= (P_{k-1} + 2t^{2^{k-2}})^2 - 2t^{2^{k-1}} \\
&= P_{k-1}^2 + 4P_{k-1}t^{2^{k-2}} + 2t^{2^{k-1}} \\
&= P_k + 2t^{2^{k-1}}.
\end{aligned}$$

Consequently we have $\alpha^{2^k} + \beta^{2^k} \in \mathbb{Z}_{\geq 0}[s,t]$. If n is odd, then

$$\begin{aligned}
\alpha^n + \beta^n &= (\alpha+\beta)\sum_{i=0}^{n-1}(-1)^i\alpha^{n-1-i}\beta^i \\
&= (\alpha+\beta)\Big(\alpha^{n-1} + \beta^{n-1} + (-\alpha\beta)^{(n-1)/2} \\
&\quad + \sum_{i=1}^{(n-3)/2}(-\alpha\beta)^i(\alpha^{n-1-2i} + \beta^{n-1-2i})\Big) \\
&= s\Big(\alpha^{n-1} + \beta^{n-1} + t^{(n-1)/2} + \sum_{i=1}^{(n-3)/2} t^i(\alpha^{n-1-2i} + \beta^{n-1-2i})\Big),
\end{aligned}$$

and by the inductive hypothesis we have $\alpha^n + \beta^n \in \mathbb{Z}_{\geq 0}[s,t]$. If $n = 2^k h$, with $k > 0$ and $h > 1$ odd, then we can write

$$\alpha^n + \beta^n = (\alpha^{2^k} + \beta^{2^k})\sum_{i=0}^{h-1}(-1)^i(\alpha^{2^k})^{h-1-i}(\beta^{2^k})^i,$$

and the thesis follows as above. □

We recall the definition 2.2 for the Lucas atoms

$$P_1(s,t) := 1, \quad P_n(s,t) := \Phi_n(\alpha,\beta) = \beta^{\varphi(n)}\Psi_n(\alpha/\beta).$$

Proposition 4.1.2. *For all $n \geq 1$, we have $P_n(s,t) \in \mathbb{Z}_{\geq 0}[s,t]$.*

Proof. From Lemma 4.1.1, we have that $P_n(s,t) \in \mathbb{Z}[s,t]$, for all $n \geq 1$. Indeed, $P_n(s,t) = \beta^{\varphi(n)}\Psi_n(\alpha/\beta)$ and by the palindromicity of the cyclotomic polynomials,

we have

$$P_n(s,t) = \alpha^{\varphi(n)} + \beta^{\varphi(n)} + \sum_{j=1}^{(\varphi(n)-2)/2} c_j(\alpha\beta)^{i_j}(\alpha^{k_j} + \beta^{k_j}),$$

where $c_j \in \mathbb{Z}$ and $i_j, k_j \in \mathbb{N}$. Moreover, we can observe that

$$P_n(s,t) = \Phi_n(\alpha,\beta) = \prod_{j=1}^{\varphi(n)/2} (\alpha^2 + \beta^2 - (\omega_j + \bar{\omega}_j)\alpha\beta),$$

where ω_j is a primitive n-th root of unity and $\bar{\omega}_j$ is its complex conjugate. Each factor in the above formula can be also written as

$$(\alpha+\beta)^2 - (\omega_j + \bar{\omega}_j + 2)\alpha\beta = s^2 + (\omega_j + \bar{\omega}_j + 2)t,$$

where $\omega_j + \bar{\omega}_j + 2 > 0$ for all j. This ensures that the coefficients of $P_n(s,t)$ must be non-negative integers. □

In [45], Levy proved the irreducibility of the univariate Lucas atoms $P_n(s,\pm 1)$. Exploiting the connection with cyclotomic polynomials $\Phi_n(\alpha,\beta)$, we are able to provide the same result for general t, i.e. for the Lucas atoms $P_n(s,t)$ in two variables.

Proposition 4.1.3. *The Lucas atoms $P_n(s,t)$ are irreducible polynomials over $\mathbb{Q}$, for all $n \in \mathbb{N}$.*

Proof. Note that $P_n(s,t) = P_n(\alpha+\beta, -\alpha\beta) = \Phi_n(\alpha,\beta)$. The polynomial Φ_n is irreducible over $\mathbb{Q}$ as the homogenization of Ψ_n, which is irreducible over $\mathbb{Q}$ as well. Then any factorization of $P_n(s,t)$ into a product of two polynomials $A_n(s,t), B_n(s,t) \in \mathbb{Q}[s,t]$ can be rewritten as

$$\Phi_n(\alpha,\beta) = P_n(\alpha+\beta,-\alpha\beta) = A_n(\alpha+\beta,-\alpha\beta)B_n(\alpha+\beta,-\alpha\beta).$$

Because of the irreducibility of $\Phi_n(\alpha,\beta)$ over $\mathbb{Q}$ we conclude that either $A_n(s,t) = A_n(\alpha+\beta,-\alpha\beta)$ or $B_n(s,t) = B_n(\alpha+\beta,-\alpha\beta)$ is a constant polynomial. This proves the irreducibility of $P_n(s,t)$ over $\mathbb{Q}$. □

From Proposition 4.1.3, using the irreducibility of the Lucas atoms $P_n(s,t)$, we obtain a simple proof of the following theorem, which is one of the main results of [57].

Theorem 4.1.4. *Let us suppose* $f(s,t) := \prod_{d\geq 2} U_{n_i}(s,t)$ *and* $g(s,t) := \prod_{d\geq 2} U_{k_j}(s,t)$, *for* $n_i, k_j \in \mathbb{N}$, *and write their atomic decompositions as*

$$f(s,t) = \prod_{d\geq 2} P_d(s,t)^{a_d}, \quad g(s,t) = \prod_{d\geq 2} P_d(s,t)^{b_d},$$

for $a_d, b_d \in \mathbb{N}$. *Then* $f(s,t)/g(s,t)$ *is a polynomial if and only if* $a_d \geq b_d$ *for all* $d \geq 2$. *Furthermore in this case* $f(s,t)/g(s,t)$ *has non-negative integer coefficients.*

Proof. The condition $a_d \geq b_d$ is clearly sufficient for $f(s,t)/g(s,t)$ being a polynomial. Conversely, since the polynomials $P_d(s,t)$ are irreducible, by Proposition 4.1.3, the Lucas atoms at the denominator cancel out only if they are present at the numerator with a greater or equal exponent. Moreover, the ratio $f(s,t)/g(s,t)$ has nonnegative integer coefficients because it is the product of the remaining Lucas atoms. □

Lucas formula and Gauss formula for cyclotomic polynomials can be easily adapted to Lucas atoms. For instance, from the Lucas formula we have that, if $n \geq 5$ odd and squarefree, then there exist two palindromic polynomials $C_n(\alpha/\beta), D_n(\alpha/\beta) \in \mathbb{Z}[\alpha/\beta]$, with degrees $\varphi(n)/2$ and $\varphi(n)/2-1$, respectively, such that

$$\Psi_n((-1)^{(n-1)/2}\alpha/\beta) = C_n^2(\alpha/\beta) - n\frac{\alpha}{\beta}D_n^2(\alpha/\beta).$$

Thus, if $n \equiv 1 \pmod 4$, we obtain

$$\beta^{\varphi(n)}\Psi_n(\alpha/\beta) = \beta^{\varphi(n)}C_n^2(\alpha/\beta) - n\alpha\beta^{\varphi(n)-1}D_n^2(\alpha/\beta) = \tilde{C}_n^2(\alpha,\beta) - n\alpha\beta\tilde{D}_n^2(\alpha,\beta),$$

where $\tilde{C}_n(\alpha,\beta), \tilde{D}_n(\alpha,\beta) \in \mathbb{Z}[\alpha,\beta]$ are palindromic with degrees $\varphi(n)/2$ and $\varphi(n)/2-1$, respectively. Then, by palindromicity of these polynomials and by Lemma 4.1.1 we get

$$P_n(s,t) = F_n^2(s,t) + ntG_n^2(s,t)$$

with $F_n(s,t), G_n(s,t) \in \mathbb{Z}[s,t]$. Similar results can be obtained for the case n even and for the Gauss formula. The same results were obtained in a simple way in [57], but with the definition (2.2) of the Lucas atoms, it becomes more clear the fact that the Lucas formula, for n odd, can not be adapted when $n \equiv 3 \pmod 4$. Indeed, in

this case we would have

$$\beta^{\varphi(n)}\Psi_n(-\alpha/\beta) = \beta^{\varphi(n)}C_n^2(\alpha/\beta) - n\alpha\beta^{\varphi(n)}D_n^2(\alpha/\beta)$$

where on the left side we have the Lucas atoms $P_n(s,t)$ but where $s = -\alpha+\beta$ and $t = \alpha\beta$ making not possible to obtain on the right hand some polynomials with these variables s and t and integer coefficients.

In [57], the authors proved also an analogue of a reduction formula for cyclotomic polynomials. In order to provide a proof of this result, the authors proved several combinatorial lemmas, claiming that a proof could not be found easily and directly from the connection with cyclotomic polynomials provided by the function Γ. Here we show that, exploiting (2.2), the proof becomes straightforward.

Theorem 4.1.5. *If $n \geq 2$ is a positive integer and p is a prime not dividing n, then*

$$P_{pn}(s,t) = \begin{cases} \dfrac{P_n(s^2+2t,-t^2)}{P_n(s,t)} & \text{if } p = 2, \\ \dfrac{P_n(sP_{2p},t^p)}{P_n(s,t)} & \text{if } p \geq 3, \end{cases}$$

where writing P_m we mean $P_m(s,t)$.

Proof. By (2.2) and the reduction formulas for cyclotomic polynomials,

$$P_{pn}(s,t) = \Phi_{pn}(\alpha,\beta) = \frac{\Phi_n(\alpha^p,\beta^p)}{\Phi_n(\alpha,\beta)} = \frac{\Phi_n(\alpha^p,\beta^p)}{P_n(s,t)}. \tag{4.1}$$

Now let us notice that α^p and β^p are the roots of the polynomial

$$(X-\alpha^p)(X-\beta^p) = X^2 - (\alpha^p+\beta^p)X + (\alpha\beta)^p,$$

hence the Lucas atom correspondent to $\Phi_n(\alpha^p,\beta^p)$ is

$$P_n(\alpha^p+\beta^p, -(\alpha\beta)^p) = P_n(\alpha^p+\beta^p, -(-t)^p).$$

If $p = 2$,

$$\Phi_n(\alpha^2,\beta^2) = P_n(\alpha^2+\beta^2,-t^2) = P_n(s^2+2t,-t^2),$$

and this concludes the proof for this case. For $p \geq 3$, let us notice that

$$U_{2p}(s,t) = \frac{\alpha^{2p} - \beta^{2p}}{\alpha - \beta} = \frac{\alpha^p - \beta^p}{\alpha - \beta}(\alpha^p + \beta^p) = P_p(s,t)(\alpha^p + \beta^p).$$

By the definition of Lucas atoms, this means that

$$\alpha^p + \beta^p = P_2 P_{2p} = (\alpha + \beta)P_{2p} = sP_{2p}.$$

Therefore,

$$\Phi_n(\alpha^p, \beta^p) = P_n(\alpha^p + \beta^p, -(-t)^p) = P_n(sP_{2p}, t^p),$$

and also the case of odd p is complete. □

Using a similar argument, it is easily obtained also the following theorem, which is the other main result of Section 5 in [57].

Theorem 4.1.6. *If $n \geq 2$ is a positive integer and p is a prime not dividing n, then,*

$$P_{p^m n}(s,t) = \begin{cases} P_{p^{m-1}n}(s^2 + 2t, -t^2) & \text{if } p = 2, \\ P_{p^{m-1}n}(sP_{2p}, t^p) & \text{if } p \geq 3, \end{cases}$$

for all $m \geq 2$.

Proof. By (2.2) and the reduction formulas for cyclotomic polynomials,

$$\begin{aligned} P_{p^m n}(s,t) &= \Phi_{p^m n}(\alpha, \beta) \\ &= \Phi_{pn}(\alpha^{p^{m-1}}, \beta^{p^{m-1}}) \\ &= \Phi_{p^{m-1}n}\left(\alpha^{\frac{p^{m-1}}{p^{m-2}}}, \beta^{\frac{p^{m-1}}{p^{m-2}}}\right) \\ &= \Phi_{p^{m-1}n}(\alpha^p, \beta^p) = P_{p^{m-1}n}(\alpha^p + \beta^p, -\alpha^p\beta^p) \end{aligned} \tag{4.2}$$

In the case that $p = 2$, the thesis follows from $\alpha^2 + \beta^2 = s^2 + 2t$. For $p \geq 3$, since $\alpha^p + \beta^p = sP_{2p}$, then $P_{p^m n}(s,t) = P_{p^{m-1}n}(sP_{2p}, -t^p)$. □

If $\Phi_n(a,b) = p$ for some index n, p prime and a, b integers, then

$$P_n(a+b, -ab) = \Phi_n(a,b) = p,$$

where $a+b$ and $-ab$ are still integers. For $b=1$, a famous conjecture of Bunyakovsky implies that, for a fixed n, $\Phi_n(a,1)=\Psi_n(a)$ is prime for infinitely many positive integers a. In light of this, we can state the following conjecture which is weaker than the Bunyakovsky's one.

Conjecture 4.1.7. *For each integer $n\geq 2$ there exist infinitely many pairs $(s,t)\in\mathbb{Z}^2$ such that $P_n(s,t)$ is prime.*

It is easy to see that the polynomials $P_2(s,t)=s$, $P_3(s,t)=s^2+t$ and $P_4(s,t)=s^2+2t$ represent all the integers, in particular all the prime numbers. The polynomial $P_6(s,t)=s^2+3t$, meanwhile, represents all the integers not congruent to 2 modulo 3, in particular all the prime numbers of this form. For remaining polynomials $P_n(s,t)$, whose degrees are at least equal to 4, we do not know any tool for proving that they represent infinitely many prime numbers.

4.2 p–adic valuations of Lucas atoms

In this section, we fully characterize the p-adic valuation of Lucas atoms. In this way we solve a problem left open in [57], which the authors addressed as hard. In particular, they treated only some cases for $p\in\{2,3\}$ (see [57, Theorems 6.3, 6.5]), leaving open the general problem of extending their results to arbitrary primes.

In the following, we consider s,t as integers and α,β as the roots of the polynomial X^2-sX-t and we will denote by Δ its discriminant.

Given an integer $n\neq 0$, let $\rho(n,U)$ be the rank of appearance of n in the sequence $(U_m)_{m\geq 0}$, i.e., the minimum positive integer k such that $n\mid U_k$. The next results are useful known properties of the rank of appearance (see, e.g., [55]). We give the proofs for completeness.

Lemma 4.2.1. *Given an integer $n\neq 0$, if $\gcd(n,t)=1$, we have that $\rho(n,U)\mid m$ if and only if $n\mid U_m$.*

Proof. Let $f(X)=X^2-sX-t$ be the characteristic polynomial of $(U_k)_{k\geq 0}$ and we also define the linear recurrent sequence $(T_k)_{k\geq 0}$ with characteristic polynomial $f(X)$ and initial conditions $(1,0)$. Furthermore, define the ring $R:=\mathbb{Z}_n[X]/(f(X))$ and the

group $G := {}^{R^*}\!/_{\mathbb{Z}_n^*}$. We denote by $[a+bX]$ the elements of G. In R, we can prove by induction that

$$X^m = T_m + U_m X$$

for all $m \geq 0$. The base cases hold:

$$X^0 = T_0 + U_0 X, \quad X^1 = T_1 + U_1 X.$$

Then,

$$X^m = X^{m-1}X = T_{m-1}X + U_{m-1}X^2 = T_{m-1}X + U_{m-1}(sX+t).$$

Considering that $T_m = tU_{m-1}$, for all $m \geq 2$, we obtain

$$X^m = tU_{m-1} + (sU_{m-1} + T_{m-1})X = T_m + (sU_{m-1} + tU_{m-2})X = T_m + U_m X.$$

Since $\gcd(n,t) = 1$, we can observe that $X \in R^*$ and we prove now that the order of $[X]$ in G is $\rho(n,U)$. Indeed,

$$\begin{aligned}\operatorname{ord}_G[X] &= \min\{k \in \mathbb{N}_+ : [X]^k = 1\} = \min\{k \in \mathbb{N}_+ : X^k \in \mathbb{Z}_n^*\} \\ &= \min\{k \in \mathbb{N}_+ : T_k + U_k X \in \mathbb{Z}_n^*\} = \min\{k \in \mathbb{N}_+ : U_k \equiv 0 \pmod{n}\} \\ &= \min\{k \in \mathbb{N}_+ : n \mid U_k\} = \rho(n,U).\end{aligned}$$

By the same reasoning we see that $n \mid U_m$ if and only if $[X]^m = 1$. By the property of the order of an element in a group we know that $[X]^m = 1$ exactly when $\operatorname{ord}_G[X] = \rho(n,U) \mid m$. The equality $\operatorname{ord}_G[X] = \rho(n,U)$ also proves that $\rho(n,U)$ exists for all n under the hypothesis of the lemma. □

Lemma 4.2.2. *Given a prime number p such that $p \nmid t$, the rank of appearance $\rho(p,U)$ divides $p - \left(\frac{\Delta}{p}\right)$, where $\left(\frac{\Delta}{p}\right)$ is the Legendre symbol.*

Proof. If $p \mid \Delta$, then $\alpha \equiv \beta \pmod{p}$ and $U_p = \sum_{j=0}^{p-1} \alpha^{p-1-j}\beta^j \equiv p\alpha^{p-1} \equiv 0 \pmod{p}$, i.e., $\rho(p,U) = p$. Considering

$$L = \begin{pmatrix} s & t \\ 1 & 0 \end{pmatrix},$$

we have that

$$L^n \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} U_{n+1} \\ U_n \end{pmatrix}$$

for all $n \geq 0$. For $p \nmid \Delta$, the matrix L is similar to the diagonal matrix

$$\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}.$$

If $\left(\frac{\Delta}{p}\right) = -1$, then by the Frobenius morphism, we have

$$\begin{pmatrix} U_{p+2} \\ U_{p+1} \end{pmatrix} = L^p \cdot L \begin{pmatrix} 1 \\ 0 \end{pmatrix} \equiv \begin{pmatrix} \alpha\beta & 0 \\ 0 & \alpha\beta \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = -t \begin{pmatrix} 1 \\ 0 \end{pmatrix} \pmod{p}$$

as $\alpha, \beta \in \mathbb{F}_{p^2} \backslash \mathbb{F}_p$ and L^p is similar to the matrix

$$\begin{pmatrix} \alpha^p & 0 \\ 0 & \beta^p \end{pmatrix} \equiv \begin{pmatrix} \beta & 0 \\ 0 & \alpha \end{pmatrix}$$

via the same similarity matrix as L and $\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$. If $\left(\frac{\Delta}{p}\right) = 1$, then by the Fermat's little theorem, we have

$$\begin{pmatrix} U_p \\ U_{p-1} \end{pmatrix} = L^{p-1} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix} \pmod{p}$$

as $\alpha, \beta \in \mathbb{F}_p$. □

Similarly to the rank of appearance of a non-zero integer in the Lucas sequence, we will denote by $\rho(n,P)$ the rank of appearance of the integer $n \neq 0$ in the sequence of Lucas atoms $(P_m)_{m \geq 1}$. In the following lemma we prove that the rank of appearance of a given prime number in a Lucas sequence is the same for the corresponding sequence of Lucas atoms.

Lemma 4.2.3. *Given a prime p, we have*

$$\rho(p,P) = \rho(p,U) =: k$$

and

$$v_p(U_k) = v_p(P_k),$$

where $v_p(\cdot)$ denotes the p-adic valuation.

Proof. Consider $k = \rho(n,U)$. By the definition of rank of appearance we have that $p \mid U_k$ and $p \nmid U_d$ for any $d < k$. If p divides P_d for some $d < k$, then it divides U_d and this is a contradiction. Therefore, the rank of appearance of p in the sequence of Lucas atoms must be greater than or equal to k. Moreover,

$$v_p(U_k) = \sum_{d|k} v_p(P_d) = v_p(P_k),$$

so that $\rho(p,P) = k$ and $v_p(U_k) = v_p(P_k)$. □

For studying the p-adic valuations of Lucas atoms, we use the following results of Ballot [6] and Sanna [58] on the p–adic valuations of Lucas sequences.

Theorem 4.2.4 ([58], Corollary 1.6)**.** *Let $p \geq 3$ be a prime number such that $p \nmid t$ and $k = \rho(p,U)$. Then,*

$$v_p(U_n) = \begin{cases} v_p(n) + v_p(U_p) - 1 & \text{if } p \mid \Delta,\ p \mid n, \\ 0 & \text{if } p \mid \Delta,\ p \nmid n, \\ v_p(n) + v_p(U_k) & \text{if } p \nmid \Delta,\ k \mid n, \\ 0 & \text{if } p \nmid \Delta,\ k \nmid n, \end{cases}$$

for each positive integer n, where $v_p(U_p) = 1$ for $p \geq 5$ if $p \mid \Delta$.

Theorem 4.2.5 ([58], Theorem 1.5 for $p = 2$)**.** *If $2 \nmid t$ and $2 \mid s$ (i.e., $2 \mid \Delta$ and $\rho(2,U) = 2$), then*

$$v_2(U_n) = \begin{cases} v_2(n) + v_2(U_2) - 1 & \text{if } 2 \mid n, \\ 0 & \text{if } 2 \nmid n. \end{cases}$$

If $2 \nmid t$ and $2 \nmid s$ (i.e., $2 \nmid \Delta$ and $\rho(2,U) = 3$), then

$$v_2(U_n) = \begin{cases} v_2(n) + v_2(U_6) - 1 & \text{if } 3 \mid n,\ 2 \mid n, \\ v_2(U_3) & \text{if } 3 \mid n,\ 2 \nmid n, \\ 0 & \text{if } 3 \nmid n. \end{cases}$$

Theorem 4.2.6 ([6], Theorem 1.2)**.** *Let p be a prime such that $s = p^a s'$ and $t = p^b t'$, where $p \nmid s't'$ and $a,b \in \mathbb{N}_+ \cup \{\infty\}$ with a,b necessarily finite in the case of $b = 2a$.*

Then for all $n \geq 1$, we have

$$v_p(U_n) = \begin{cases} (n-1)a & \text{if } \ b > 2a, \\ (n-1)a + v_p(U'_n) & \text{if } \ b = 2a, \end{cases}$$

where $(U'_n)_{n\geq 0}$ is the Lucas sequence with characteristic polynomial $X^2 - s'X - t'$. For $b < 2a$, we have that

$$\begin{cases} v_p(U_{2n}) = bn + (a-b) + v_p(n) + \lambda_n, \\ v_p(U_{2n+1}) = bn, \end{cases}$$

where

$$\lambda_n = \begin{cases} v_p(s'^2 - t') & \text{if } 2 \leq p \leq 3,\ 2a = b+1,\ p \mid n, \\ 0 & \text{otherwise.} \end{cases}$$

In the following theorems we characterize the p-adic valuations of Lucas atoms, dealing with the cases $p \nmid t$ and p divides both s and t (note that when $p \nmid s$ and $p \mid t$, the p-adic valuation of Lucas polynomials is always zero).

Theorem 4.2.7. *Let $p \geq 3$ be a prime number such that $k = \rho(p,U)$. Let us suppose that $p \nmid t$. Then*

$$v_p(P_n) = \begin{cases} v_p(U_k) & \text{if } \ n = k, \\ 1 & \text{if } \ n = kp^h,\ h \geq 1, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. First, consider $p \nmid \Delta$ and we prove by induction that

$$\begin{cases} v_p(P_n) \geq 1, & \text{if } n = kp^h,\ h \geq 0, \\ v_p(P_n) = 0, & \text{otherwise.} \end{cases} \tag{4.3}$$

By Lemmas 4.2.1 and 4.2.3 we know that $v_p(P_k) = v_p(U_k) \geq 1$ and $v_p(P_n) = 0$ for all $n < k$. Now, fixed a certain positive integer n, we suppose that (4.3) holds for all $i < n$ and we prove that it holds also for n. By (2.3), we have

$$v_p(P_n) = v_p(U_n) - \sum_{\substack{d \mid n \\ d \neq n}} v_p(P_d).$$

If $k \nmid n$, then $v_p(P_n) = 0$, since $v_p(U_n) = 0$ by Lemma 4.2.1.
If $k \mid n$ and $v_p(n) = 0$, then

$$v_p(P_n) = v_p(U_k) + v_p(n) - \sum_{\substack{d|n \\ d \neq n}} v_p(P_d),$$

by Theorem 4.2.4. Thus,

$$v_p(P_n) = - \sum_{\substack{d|n \\ d \notin \{k,n\}}} v_p(P_d) = 0,$$

since $v_p(P_k) = v_p(U_k)$ by Lemma 4.2.3 and all divisors d of n can not be of the form kp^h for some $h \geq 0$.
If $k \mid n$ and $n = kmp^h$, for some positive integer h and $m \neq 1$ with $\gcd(m, p) = 1$, then

$$v_p(P_n) = v_p(n) - \sum_{\substack{d|n \\ d \notin \{k,n\}}} v_p(P_d) = h - \sum_{i=1}^{h} v_p(P_{kp^i}),$$

since, by Lemma 4.2.2, $p \nmid k$ Moreover, by inductive hypothesis, $v_p(P_{kp^i}) \geq 1$, for all $1 \leq i \leq h$, and $v_p(P_d) = 0$ otherwise. Since the p-adic valuations of Lucas atoms can not be negative, we must have that $v_p(P_{kp^i}) = 1$, for all $1 \leq i \leq h$, and thus $v_p(P_n) = 0$.
Finally, if $k \mid n$ and $n = kp^h$ for a positive integer h, then

$$v_p(P_n) = v_p(n) - \sum_{\substack{d|n \\ d \notin \{k,n\}}} v_p(P_d) = h - \sum_{i=1}^{h-1} v_p(P_{kp^i}) = 1.$$

Now we consider the case $p \mid \Delta$ and we prove by induction that (4.3) still holds. Considering that in this case $k = p$ by Lemma 4.2.2 and $v_p(U_n) = 0$ for all $n < p$ by Theorem 4.2.4, then from Lemmas 4.2.1 and 4.2.3, the base step is true. Now, consider (4.3) true for all $i < n$, for a fixed positive integer n, and we prove that it holds also for n.
If $p \nmid n$, then $v_p(P_n) = v_p(U_n) - \sum_{\substack{d|n \\ d \neq n}} v_p(P_d) = 0$. If $p \mid n$ and $n = mp^h$, for an integer $m > 1$ such that $\gcd(m, p) = 1$, then, using the inductive hypothesis and Theorem

4.2.4, we obtain

$$v_p(P_n) = v_p(U_n) - \sum_{\substack{d|n \\ d\neq n}} v_p(P_d) = v_p(n) + v_p(U_p) - 1 - v_p(P_p) - \sum_{\substack{d|n \\ d\notin\{p,n\}}} v_p(P_d)$$
$$= h - 1 - \sum_{i=2}^{h} v_p(P_{p^i}).$$

Since $v_p(P_{p^i}) \geq 1$, and the p-adic valuation of Lucas atom is nonnegative, we must have $v_p(P_{p^i}) = 1$, for all $i \geq 2$ and thus $v_p(P_n) = 0$.
If $p \mid n$ and $n = p^h$, then

$$v_p(P_n) = v_p(U_n) - \sum_{\substack{d|n \\ d\neq n}} v_p(P_d) = v_p(n) + v_p(U_p) - 1 - v_p(P_p) - \sum_{\substack{d|n \\ d\notin\{p,n\}}} v_p(P_d)$$
$$= h - 1 - \sum_{i=2}^{h-1} v_p(P^i) = 1.$$

□

Theorem 4.2.8. *If $2 \nmid t$ and $2 \mid s$ (i.e., $2 \mid \Delta$ and $\rho(2,U) = 2$), then*

$$v_2(P_n) = \begin{cases} v_2(U_2) & \text{if } n = 2, \\ 1 & \text{if } n = 2^h,\ h \geq 2, \\ 0, & \text{otherwise}. \end{cases}$$

If $2 \nmid t$ and $2 \nmid s$ (i.e., $2 \nmid \Delta$ and $\rho(2,U) = 3$), then

$$v_2(P_n) = \begin{cases} v_2(U_3) & \text{if } n = 3, \\ v_2(U_6) - v_2(U_3) & \text{if } n = 6, \\ 1 & \text{if } n = 3 \cdot 2^h,\ h \geq 2, \\ 0 & \text{otherwise}. \end{cases}$$

Proof. The proof for the case $2 \nmid t$ and $2 \mid s$ follows as in the proof of Theorem 4.2.7. If $2 \nmid st$, we have $v_2(P_3) = v_2(U_3) \neq 0$ and $v_2(P_6) = v_2(U_6) - v_2(U_3)$, since $v_2(P_2) = 0$. Then, the other cases follow by induction as in the proof of Theorem 4.2.7. □

Theorem 4.2.9. *Let p be a prime such that $s = p^a s'$ and $t = p^b t'$, where $p \nmid s't'$, $a, b > 0$ with $b \geq 2a$ possibly infinite and a finite. Then for all $n \geq 2$, we have*

$$v_p(P_n) = \begin{cases} \varphi(n)a & \text{if } b > 2a, \\ \varphi(n)a + v_p(P'_n) & \text{if } b = 2a, \end{cases}$$

where $(P'_n)_{n\geq 1}$ is the sequence of Lucas atoms associated to the Lucas sequence $(U'_n)_{n\geq 0}$ with characteristic polynomial $X^2 - s'X - t'$.

Proof. We prove the statement by induction. If $b > 2a$, the base step is straightforward. Now suppose $v_p(P_i) = \varphi(i)a$, for all $i < n$ and then

$$v_p(P_n) = v_p(U_n) - \sum_{\substack{d|n \\ d\neq n}} v_p(P_d) = (n-1)a - \sum_{\substack{d|n \\ d\notin\{1,n\}}} \varphi(d)a = a\varphi(n),$$

where we exploited Theorem 4.2.6 and $v_p(P_1) = 0$.
Also for $b = 2a$ the base step is straightforward and supposing that the thesis is true for all the nonnegative integers less than n, we have

$$v_p(P_n) = (n-1)a + v_p(U'_n) - \sum_{\substack{d|n \\ d\neq n}} (a\varphi(d) + v_p(P'_d)) = a\varphi(n) + v_p(P'_n)$$

since $v_p(P'_n) = v_p(U'_n) - \sum_{\substack{d|n \\ d\neq n}} v_p(P'_d)$. □

Theorem 4.2.10. *Let p be a prime such that $s = p^a s'$ and $t = p^b t'$, where $a, b > 0$ and $p \nmid s't'$ and $b < 2a$ with a possibly infinite. If $p \notin \{2,3\}$ or $b < 2a+1$, then for each $n \geq 2$, we have*

$$v_p(P_n) = \begin{cases} a & \text{if } n = 2, \\ b\dfrac{\varphi(n)}{2} + 1 & \text{if } n = 2p^h,\ h \geq 1, \\ b\dfrac{\varphi(n)}{2} & \text{otherwise.} \end{cases}$$

Proof. We proceed by induction. The basis is straightforward. Now, consider $n = 2p^h$ for some $h \geq 1$ and that the thesis is true for all $i < n$. Then,

$$v_p(P_n) = v_p(U_n) - \sum_{\substack{d|n \\ d \neq n}} v_p(P_d).$$

By Theorem 4.2.6, we have

$$v_p(P_n) = bp^h + (a-b) + h - \sum_{\substack{d|n \\ d \neq n}} v_p(P_d),$$

and using the inductive hypothesis we get

$$\begin{aligned} v_p(P_n) &= bp^h + (a-b) + h - v_p(P_2) - \frac{b}{2}\sum_{i=1}^{h} \varphi(p^j) - \sum_{i=1}^{h-1} \left(b\frac{\varphi(2p^i)}{2} + 1 \right) \\ &= bp^h - b + 1 - \frac{b}{2}\left(\sum_{i=1}^{h} \varphi(p^i) + \sum_{i=1}^{h-1} \varphi(2p^i) \right) \\ &= bp^h - b + 1 - \frac{b}{2}(2p^h - 1 - \varphi(2p^h) - \varphi(2)) \\ &= b\frac{\varphi(n)}{2} + 1. \end{aligned}$$

The other cases, when $n \neq 2p^h$, follow in a similar way □

Finally, the next two theorems fully complete our analysis. The techniques of the proofs are similar to the previous ones and they exploit the results of Ballot [6].

Theorem 4.2.11. *If $s = 3^a s'$ and $t = 3^b t'$, with $a, b \in \mathbb{N}_+$, $3 \nmid s't'$ and $b = 2a - 1$, then for each $n \geq 2$, we have*

$$v_3(P_n) = \begin{cases} a & \text{if } n = 2, \\ b + 1 + v_3(s'^2 + t') & \text{if } n = 6, \\ 3^{h-1}b + 1 & \text{if } n = 2 \cdot 3^h,\ h \geq 2, \\ b\dfrac{\varphi(n)}{2} & \text{otherwise.} \end{cases}$$

Theorem 4.2.12. *If $s = 2^a s'$ and $t = 2^b t'$, with $a, b \in \mathbb{N}_+$, $2 \nmid s't'$ and $b = 2a-1$, then for each $n \geq 2$, we have*

$$v_2(P_n) = \begin{cases} a & \text{if } n = 2, \\ b+1+v_2(s'^2+t') & \text{if } n = 4, \\ 2^{h-2}b+1 & \text{if } n = 2^h,\ h \geq 3, \\ b\dfrac{\varphi(n)}{2} & \text{otherwise.} \end{cases}$$

4.2.1 Another approach for the study of the p–adic valuations of Lucas atoms

From (2.3) we derive

$$v_p(U_n) = \sum_{d|n} v_p(P_d)$$

for each prime number p and positive integer n. Hence, by Möbius transformation formula we obtain

$$v_p(P_n) = \sum_{d|n} \mu(d) v_p(U_{\frac{n}{d}}), \quad n \geq 1,$$

where μ denotes the Möbius function. From Theorems 4.2.4, 4.2.5, 4.2.6 we know that the sequence $(v_p(U_n))_{n\geq 1}$ is a linear combination of identity function, characteristic functions of some arithmetic progressions and products of functions of this form with the sequence of p-adic valuations of consecutive positive integers. By the bilinearity of Dirichlet convolution we can express p-adic valuations of Lucas atoms as linear combinations of the transformations of the mentioned functions via Dirichlet convolution with Möbius function.

For each integer $r \geq 1$ we denote by $\mathbf{1}_r$ the characteristic function of the multiplicities of r, i.e. the function given by the formula

$$\mathbf{1}_r(n) = \begin{cases} 1 & \text{if } r \mid n, \\ 0 & \text{if } r \mid n. \end{cases}$$

Now we are ready to state the crucial lemma.

Lemma 4.2.13. *Let p be a prime number and $q, r \geq 1$ be integers, where* $\gcd(q,p) = 1$. *Then, for each integer $n \geq 1$ we have:*

1. $\sum_{d|n} \mu(d) \cdot \frac{n}{d} = \varphi(n)$;
2. $\sum_{d|n} \mu(d) \cdot \mathbf{1}_r\left(\frac{n}{d}\right) = \begin{cases} 1 & \text{if } n = r, \\ 0 & \text{if } n \neq r; \end{cases}$
3. $\sum_{d|n} \mu(d) \cdot \mathbf{1}_q\left(\frac{n}{d}\right) \nu_p\left(\frac{n}{d}\right) = \begin{cases} 1 & \text{if } n = p^h q \text{ for some } h \in \mathbb{N}_+, \\ 0 & \text{otherwise.} \end{cases}$

Proof. The first identity follows from application of Möbius transformation formula to classical identity

$$\sum_{d|n} \varphi(d) = n.$$

We start the proof of remaining identities with the note that their left hand sides vanish when n is not divisible by r (q, respectively) as all the divisors of n are not divisible by r (q, respectively). From this moment on, we consider the case of n divisible by r (q, respectively). Write $n = rn'$ for some $n' \in \mathbb{N}_+$. Then,

$$\sum_{d|n} \mu(d) \cdot \mathbf{1}_r\left(\frac{n}{d}\right) = \sum_{d|n} \mu\left(\frac{n}{d}\right) \cdot \mathbf{1}_r(d) = \sum_{r|d|n} \mu\left(\frac{n}{d}\right) = \sum_{d'|n'} \mu\left(\frac{n'}{d'}\right) = \begin{cases} 1 & \text{if } n' = 1, \\ 0 & \text{if } n' \neq 1, \end{cases}$$

where we write $d = rd'$ for d divisible by r and the last equality is a well known fact. The second identity is proved. Similarly we start the proof of the last identity when $n = qn'$, $n' \in \mathbb{N}_+$. Write

$$\begin{aligned} \sum_{d|n} \mu(d) \cdot \mathbf{1}_q\left(\frac{n}{d}\right) \nu_p\left(\frac{n}{d}\right) &= \sum_{d|n} \mu\left(\frac{n}{d}\right) \cdot \mathbf{1}_q(d) \nu_p(d) \\ &= \sum_{q|d|n} \mu\left(\frac{n}{d}\right) \nu_p(d) \\ &= \sum_{d'|n'} \mu\left(\frac{n'}{d'}\right) \nu_p(d') \\ &= \sum_{d'|n'} \mu(d') \nu_p\left(\frac{n'}{d'}\right), \end{aligned} \tag{4.4}$$

where we write $d = qd'$ for d divisible by q and use the coprimality of q and p in the penultimate equality. If $n' = p^h$, $h \in \mathbb{N}_+$, then the last expression in (4.4) takes the form

$$\nu_p(p^h) - \nu_p(p^{h-1}) = 1.$$

Otherwise, $n' = p^h uw$, where $h, w \in \mathbb{N}_+$, u is a prime number, and $p \nmid uw$. Then we may write the last expression in (4.4) as follows.

$$\begin{aligned}
&\sum_{d'|pw} \left(\mu(d') \nu_p\left(\frac{n'}{d'}\right) + \mu(ud') \nu_p\left(\frac{n'}{ud'}\right) \right) \\
&= \sum_{d'|pw} \left(\mu(d') \nu_p\left(\frac{n'}{d'}\right) - \mu(d') \nu_p\left(\frac{n'}{d'}\right) \right) \\
&= 0
\end{aligned}$$

The proof of the last identity is finished. □

Now, we can reformulate Theorems 4.2.4, 4.2.5, 4.2.6.

Theorem 4.2.14 (Reformulation of Theorem 4.2.4)**.** *Let $p \geq 3$ be a prime number such that $p \nmid t$ and $k = \rho(p, U)$. Then,*

$$v_p(U_n) = \begin{cases} v_p(n) + (v_p(U_p) - 1)\mathbf{1}_p(n) & \text{if } p \mid \Delta, \\ \mathbf{1}_k(n) v_p(n) + v_p(U_k)\mathbf{1}_k(n) & \text{if } p \nmid \Delta, \end{cases}$$

for each positive integer n, where $\nu_p(U_p) = 1$ for $p \geq 5$ if $p \mid \Delta$.

Theorem 4.2.15 (Reformulation of Theorem 4.2.5)**.** *If $2 \nmid t$ and $2 \mid s$ (i.e., $2 \mid \Delta$ and $\rho(2, U) = 2$), then*

$$v_2(U_n) = v_2(n) + (v_2(U_2) - 1)\mathbf{1}_2(n).$$

If $2 \nmid t$ and $2 \nmid s$ (i.e., $2 \nmid \Delta$ and $\rho(2, U) = 3$), then

$$v_2(U_n) = v_2(n)\mathbf{1}_3(n) + v_2(U_3)\mathbf{1}_3(n) + (v_2(U_6) - v_2(U_3) - 1)\mathbf{1}_6(n).$$

Theorem 4.2.16 (Reformulation of Theorem 4.2.6)**.** *Let p be a prime such that $s = p^a s'$ and $t = p^b t'$, where $p \nmid s't'$ and $a, b \in \mathbb{N}_+ \cup \{\infty\}$ with a, b necessarily finite*

in the case of $b = 2a$. Then for all $n \geq 1$, we have

$$v_p(U_n) = \begin{cases} an - a & \text{if } \ b > 2a, \\ an - a + v_p(U'_n) & \text{if } \ b = 2a, \end{cases}$$

where $(U'_n)_{n\geq 0}$ is the Lucas sequence with characteristic polynomial $X^2 - s'X - t'$. For $b < 2a$, we have that

$$\begin{aligned} v_p(U_n) =& \frac{b}{2} \cdot n - \frac{b}{2} + \left(a - \frac{b}{2}\right) \mathbf{1}_2(n) + v_p\left(\frac{n}{2}\right) \mathbf{1}_2(n) + \lambda \mathbf{1}_{2p}(n) \\ =& \frac{b}{2} \cdot n - \frac{b}{2} + \left(a - \frac{b}{2}\right) \mathbf{1}_2(n) + v_p(n)\mathbf{1}_2(n) - \delta_{p,2}\mathbf{1}_2(n) + \lambda \mathbf{1}_{2p}(n), \end{aligned}$$

where

$$\lambda = \begin{cases} v_p(s'^2 - t') & \text{if } 2 \leq p \leq 3, \ 2a = b + 1, \\ 0 & \text{otherwise} \end{cases}$$

and

$$\delta_{p,2} = \begin{cases} 1 & \text{if } \ p = 2, \\ 0 & \text{if } \ p \neq 2. \end{cases}$$

Applying Lemma 4.2.13 to the above theorems and using bilinearity of Dirichlet convolution it is possible to obtain the main results of this section, exploiting this different approach.

4.3 Non-holonomicity of the sequence of Lucas atoms

In the striking opposition to the Lucas sequence, which is binary linearly recurrent from its definition, the sequence of Lucas atoms evaluated at any pair of integer values of variables s and $t \neq 0$ is not even holonomic, i.e. polynomially recurrent. This follows from the more general fact stated below.

Theorem 4.3.1. *For each integers s,t with $t \neq 0$ there do not exist $l \in \mathbb{N}_+$ and $G_0(X), G_1(X), \ldots, G_l(X) \in \mathbb{Q}[X]$ such that*

$$P_n(s,t) = G_0(n) + \sum_{j=1}^{l} G_j(n) P_{n-j}(s,t)$$

for sufficiently large $n \in \mathbb{N}_+$.

Proof. Fix non-zero values of s and t and assume that

$$P_n(s,t) = G_0(n) + \sum_{j=1}^{l} G_j(n) P_{n-j}(s,t)$$

for some $l, n_0 \in \mathbb{N}_+$ and $G_1(X), \ldots, G_l(X) \in \mathbb{Q}[X]$ and all $n \geq n_0$. Choose a prime number p so large that p divides neither of s, t and the denominators of the coefficients of $G_0(X), G_1(X), \ldots, G_l(X)$ written in the irreducible form. Then $G_j(n_1) \equiv G_j(n_2) \pmod{p}$ for each $j \in \{0, 1, \ldots, l\}$ and integers $n_1 \equiv n_2 \pmod{p}$. Since the set of l-tuples

$$\{(P_{mp-1}(s,t), \ldots, P_{mp-l}(s,t)) \pmod{p} : mp \geq n_0\}$$

is finite, by pigeon hole principle we find integers $m_2 > m_1 \geq \frac{n_0}{p}$ such that

$$(P_{m_1 p-1}(s,t), \ldots, P_{m_1 p-l}(s,t)) \equiv (P_{m_2 p-1}(s,t), \ldots, P_{m_2 p-l}(s,t)) \pmod{p}.$$

Putting $m_0 = m_2 - m_1$ we show by easy induction that $P_{n+m_0 p}(s,t) \equiv P_n(s,t) \pmod{p}$ for each integer $n \geq m_1 p - l$. In particular, the set of indices n such that $p \mid P_n(s,t)$ is a finite union of infinite arithmetic progressions and a finite set. Howerver, Theorems 4.2.7, 4.2.8 and 4.2.10 show that is not the case. The contradiction proves non-holonomicity of the sequence $(P_n(s,t))_{n \geq 1}$. □

As a direct consequence we get the following corollary.

Corollary 4.3.2. *There do not exist* $l \in \mathbb{N}_+$ *and* $G_0(s,t,X), G_1(s,t,X), \ldots, G_l(s,t,X) \in \mathbb{Q}[s,t,X]$ *such that*

$$P_n(s,t) = G_0(s,t,n) + \sum_{j=1}^{l} G_j(s,t,n) P_{n-j}(s,t)$$

for sufficiently large $n \in \mathbb{N}_+$.

Since a lot of number sequences having combinatorial interpretation are polynomially recurrent, Theorem 4.3.1 suggests us that the problem of finding some natural combinatorial interpretation of Lucas atoms seems to be intractable.

Let us notice that the proof of Theorem 4.3.1 is valid only if $t \neq 0$. From the definition of Lucas atoms we have $P_1(s,0) = 1$ and $P_n(s,0) = s^{\varphi(n)}$ for $n \geq 2$. Then it is quite interesting to check for which value of s the sequence $(P_n(s,0))_{n\geq 1}$ is (polynomially) recurrent.

Theorem 4.3.3. *Let $s \in \mathbb{Z}$, the sequence $(P_n(s,0))_{n\geq 1}$ is polynomially recurrent if and only if $s \in \{-1,0,1\}$.*

Proof. If $s \in \{-1,0,1\}$, the sequence $(P_n(s,0))_{n\geq 1}$ is obviously recurrent. Now, suppose $|s| > 1$ and $(P_n(s,0))_{n\geq 1}$ polynomially recurrent. Thus, there exist some polynomials $f_0(X), \ldots, f_k(X) \in \mathbb{Q}[X]$ such that

$$\sum_{j=0}^{k} f_j(n) s^{\varphi(n+j)} = 0,$$

for all $n \geq 0$. Now, let us notice that there exist infinitely many primes p such that $p \equiv 1 \pmod{(k+1)!}$. For all such p, we have that $j+1$ divides $p+j$ for all $j = 1, \ldots, k$, hence

$$\varphi(p+j) \leq (p+j)\frac{\varphi(j+1)}{j+1} \leq (p+j)\frac{j}{j+1}.$$

Therefore, since $\varphi(p) = p-1$, for all $j = 1, \ldots, k$ we have

$$\varphi(p+j) - \varphi(p) \leq (p+j)\frac{j}{j+1} - (p-1) = \frac{-p}{j+1} + \frac{j^2+j+1}{j+1}.$$

It follows that $\varphi(p+j) - \varphi(p) \to -\infty$ for $p \to +\infty$. Since

$$f_0(p) = -\sum_{j=1}^{k} f_j(p) s^{\varphi(p+j)-\varphi(p)},$$

we get that $f_0(X)$ is the null polynomial and repeating the above reasoning we get also $f_1(X) = \ldots = f_k(X) = 0$. □

Chapter 5

The Zeckendorf representation of an integer modulo a Fibonacci number

This chapter contains the study of the Zeckendorf representation of the multiplicative inverse of a fixed integer greater than 3 modulo a Fibonacci number, such that the integer and the Fibonacci number are coprime. In the first section of the chapter there are some lemmas useful to get the connection of the base-φ expansions and the Zeckendorf representation. In the second section there is the main theorem of this study regarding the Zeckendorf representation described above. The results present in this chapter belong to the published paper [3].

5.1 Preliminary lemmas for the proof of the main theorem

The next lemma gives a formula for the inverse of an integer a modulo f_n.

Lemma 5.1.1. *For all integers $a \geq 1$ and $n \geq 3$ with $\gcd(a, f_n) = 1$, we have that*

$$(a^{-1} \bmod f_n) = \frac{bf_n + 1}{a},$$

where $b := (-f_r^{-1} \bmod a)$, $r := (n \bmod \pi(a))$ and $\pi(a)$ is the period length as described in Section 2.1.

Proof. Since $r \equiv n \pmod{\pi(a)}$, we have that $f_r \equiv f_n \pmod{a}$. In particular, it follows that $\gcd(a, f_r) = \gcd(a, f_n) = 1$. Since f_r is invertible modulo a, then b is well defined. Moreover, we have that

$$bf_n + 1 \equiv -f_r^{-1} f_r + 1 \equiv 0 \pmod{a},$$

and thus $c := (bf_n + 1)/a$ is an integer. One the one have, we have that

$$ac \equiv bf_n + 1 \equiv 1 \pmod{f_n}.$$

On the other hand, since $b \leq a - 1$ and $n \geq 3$, we have that

$$0 \leq c \leq \frac{(a-1)f_n + 1}{a} = f_n - \frac{f_n - 1}{a} < f_n.$$

Therefore, we get that $c = (a^{-1} \bmod f_n)$, as desired. □

In order to introduce the next lemma, let us recall that $\mathfrak{D}$ is the set of sequences in $\{0,1\}$ that have no two consecutive terms equal to 1, and that are not ultimately equal to the periodic sequence $0,1,0,1,\ldots$. Moreover, we know that for every $x \in [0,1)$ there exists a unique sequence $\boldsymbol{\delta}(x) = (\delta_i(x))_{i\in\mathbb{N}}$ in $\mathfrak{D}$ such that $x = \sum_{i=1}^{\infty} \delta_i(x)\varphi^{-i}$. Furthermore, letting $\mathcal{F} := \mathbb{Q}(\varphi) \cap [0,1)$, if $x \in \mathcal{F}$ then $\boldsymbol{\delta}(x)$ is ultimately periodic.

The following lemma collects two easy inequalities for sums involving sequences in $\mathfrak{D}$.

Lemma 5.1.2. *For every sequence $(d_i)_{i\in\mathbb{N}}$ in $\mathfrak{D}$ and for every $m \in \mathbb{N} \cup \{\infty\}$, we have*

1. $\sum_{i=1}^{m} d_i \varphi^{-i} \in [0,1)$
2. $\sum_{i=1}^{m} d_i (-\varphi)^{-i} \in (-1, \varphi^{-1})$.

Proof. Since $(d_i)_{i\in\mathbb{N}}$ belongs to $\mathfrak{D}$, there exists $k \in \mathbb{N}$ such that $d_k = d_{k+1} = 0$. Let k be the minimum integer with such property. Then

$$\begin{aligned}\sum_{i=1}^{\infty} d_i \varphi^{-i} &= \sum_{i=1}^{k-1} d_i \varphi^{-i} + \sum_{i=k+2}^{\infty} d_i \varphi^{-i} < \sum_{j=1}^{\lfloor k/2 \rfloor} \varphi^{-(2j-1)} + \sum_{i=k+2}^{\infty} \varphi^{-i} \\ &= \left(1 - \varphi^{-2\lfloor k/2 \rfloor}\right) + \varphi^{-k} \leq 1,\end{aligned}$$

and 1 is proved. Let us prove 2. We have

$$\sum_{i=1}^{m} d_i(-\varphi)^{-i} \leq \sum_{j=1}^{m} d_{2j}\varphi^{-2j} < \sum_{j=1}^{\infty} \varphi^{-2j} = \varphi^{-1},$$

where the second inequality is strict because $\mathfrak{D}$ does not contain sequences that are ultimately equal to $(0,1,0,1,\dots)$. On the other hand, similarly, we have

$$\sum_{i=1}^{m} d_i(-\varphi)^{-i} \geq -\sum_{j=1}^{m} d_{2j-1}\varphi^{-(2j-1)} > -\sum_{j=1}^{\infty} \varphi^{-(2j-1)} = -1.$$

Thus 2. is proved. □

The next lemma relates base-φ expansion and Zeckendorf representation.

Lemma 5.1.3. *Let N be a positive integer and write $N = x\varphi^m/\sqrt{5}$ for some $x \in \mathcal{F}$ and some integer $m \geq 2$. Then the Zeckendorf representation of N is given by*

$$N = \sum_{i=1}^{m-1} \delta_{m-i}(x) f_i.$$

Moreover, we have $\delta_m(x) = 0$.

Proof. Let $R := N - \sum_{i=1}^{m-1} \delta_{m-i}(x) f_i$. We have to prove that $R = 0$. Since R is an integer, it suffices to show that $|R| < 1$. We have

$$\begin{aligned}
\sqrt{5}N = x\varphi^m &= \sum_{i=1}^{\infty} \delta_i(x)\varphi^{m-i} = \sum_{i=1}^{m} \delta_i(x)\varphi^{m-i} + \sum_{i=m+1}^{\infty} \delta_i(x)\varphi^{m-i} \\
&= \sum_{i=0}^{m-1} \delta_{m-i}(x)\varphi^i + \sum_{i=1}^{\infty} \delta_{i+m}(x)\varphi^{-i} \\
&= \sum_{i=0}^{m-1} \delta_{m-i}(x)(\varphi^i - \overline{\varphi}^i) + \sum_{i=0}^{m-1} \delta_{m-i}(x)\overline{\varphi}^i + \sum_{i=1}^{\infty} \delta_{i+m}(x)\varphi^{-i} \\
&= \sqrt{5}\sum_{i=1}^{m-1} \delta_{m-i}(x) f_i + \sum_{i=0}^{m-1} \delta_{m-i}(x)(-\varphi)^{-i} + \sum_{i=1}^{\infty} \delta_{i+m}(x)\varphi^{-i}.
\end{aligned}$$

Hence, we get that

$$\sqrt{5}R = \sum_{i=0}^{m-1} \delta_{m-i}(x)(-\varphi)^{-i} + \sum_{i=1}^{\infty} \delta_{i+m}(x)\varphi^{-i}.$$

For the sake of contradiction, suppose that $\delta_m(x) = 1$. Then $\delta_{m+1}(x) = 0$ and, by Lemma 5.1.2, it follows that

$$\begin{aligned}\sqrt{5}R &= 1 + \sum_{i=1}^{m-1} \delta_{m-i}(x)(-\varphi)^{-i} + \sum_{i=2}^{\infty} \delta_{i+m}(x)\varphi^{-i} \in (1-1+0, 1+\varphi^{-1}+\varphi^{-1}) \\ &= (0, \sqrt{5}),\end{aligned}$$

which is a contradiction, since R is an integer.

Therefore, $\delta_m(x) = 0$ and, again by Lemma 5.1.2, we have

$$\sqrt{5}R = \sum_{i=1}^{m-1} \delta_{m-i}(x)(-\varphi)^{-i} + \sum_{i=1}^{\infty} \delta_{i+m}(x)\varphi^{-i} \in (-1+0, \varphi^{-1}+1) \subseteq (-\sqrt{5}, \sqrt{5}),$$

so that $|R| < 1$, as desired. □

In the next lemma there is the explicit formula for the base-φ expansions of the sum of two numbers.

Lemma 5.1.4. *Let $x, y \in [0,1)$, $m \in \mathbb{N}$, and put $v := x + y\varphi^{-m}$. Suppose that there exists $\lambda \in \mathbb{N}$ such that $\lambda + 2 \leq m$ and $\delta_\lambda(x) = \delta_{\lambda+1}(x) = 0$. Then, putting*

$$w := \sum_{i=\lambda+2}^{\infty} \delta_i(x)\varphi^{-i} + \sum_{i=m+1}^{\infty} \delta_{i-m}(y)\varphi^{-i},$$

we have that $v, w \in [0,1)$ and

$$\delta_i(v) = \begin{cases} \delta_i(x) & \text{if } i \leq \lambda, \\ \delta_i(w) & \text{if } i > \lambda, \end{cases} \tag{5.1}$$

for every $i \in \mathbb{N}$.

Proof. From Lemma 5.1.2.1, we have that

$$0 \leq w < \varphi^{-(\lambda+1)} + \varphi^{-m} < \varphi^{-(\lambda+1)} + \varphi^{-(\lambda+2)} = \varphi^{-\lambda}.$$

Hence, $w \in [0, \varphi^{-\lambda}) \subseteq [0,1)$ and so $w = \sum_{i=\lambda+1}^{\infty} \delta_i(w)\varphi^{-i}$. Therefore, recalling that $\delta_{\lambda+1}(x) = 0$, we get that

$$v = x + y\varphi^{-m} = \sum_{i=1}^{\infty} \delta_i(x)\varphi^{-i} + \sum_{i=1}^{\infty} \delta_i(y)\varphi^{-i-m} = \sum_{i=1}^{\infty} \delta_i(x)\varphi^{-i} + \sum_{i=m+1}^{\infty} \delta_{i-m}(y)\varphi^{-i}$$
$$= \sum_{i=1}^{\lambda} \delta_i(x)\varphi^{-i} + w = \sum_{i=1}^{\lambda} \delta_i(x)\varphi^{-i} + \sum_{i=\lambda+1}^{\infty} \delta_i(w)\varphi^{-i},$$

which is the base-φ expansion of v. (Note that $\delta_\lambda(x) = 0$.) In particular, by Lemma 5.1.2.1, we have that $v \in [0,1)$. Thus (5.1) follows. □

5.2 Main theorem for the Zeckendorf representation of the inverse of an integer mod(f_n)

Theorem 5.2.1. *Let $a \geq 3$ be an integer. Then there exist integers $M, n_0, i_0 \geq 1$ and periodic sequences $\boldsymbol{z}^{(0)}, \ldots, \boldsymbol{z}^{(M-1)}$ and $\boldsymbol{w}^{(1)}, \ldots, \boldsymbol{w}^{(i_0)}$ with values in $\{0,1\}$ such that, for all integers $n \geq n_0$ with $\gcd(a, f_n) = 1$, the Zeckendorf representation of $(a^{-1} \bmod f_n)$ is given by*

$$(a^{-1} \bmod f_n) = \sum_{i=i_0}^{n-1} z_{n-i}^{(n \bmod M)} f_i + \sum_{i=1}^{i_0-1} w_n^{(i)} f_i.$$

From the proof of Theorem 5.2.1 it follows that M, n_0, i_0, $\boldsymbol{z}^{(0)}, \ldots, \boldsymbol{z}^{(M-1)}$, and $\boldsymbol{w}^{(1)}, \ldots, \boldsymbol{w}^{(i_0)}$ can be computed from a (see also Remark 5.2.2 at the end of the chapter).

Proof. Fix an integer $a \geq 3$. Let us begin by defining M, n_0, i_0, and $\boldsymbol{z}^{(0)}, \ldots, \boldsymbol{z}^{(M-1)}$. Put $M := \pi(a)$. For each $r \in \{0, \ldots, M-1\}$ with $\gcd(a, f_r) = 1$, let $b_r := (-f_r^{-1} \bmod a)$, $x_r := b_r/a$, and $\boldsymbol{z}^{(r)} := \boldsymbol{\delta}(x_r)$. Note that $x_r \in (0,1)$. Since x_r is a positive rational number, we have that $\boldsymbol{z}^{(r)}$ is a (purely) periodic sequence belonging to $\mathfrak{D}$. Let ℓ be the least common multiple of the period lengths of $\boldsymbol{z}^{(0)}, \ldots, \boldsymbol{z}^{(M-1)}$, and put $i_0 := \ell + 3$. Finally, let $n_0 := \max\{i_0 + 1, \lceil \log(2a)/\log\varphi \rceil\}$. Pick an integer $n \geq n_0$ with $\gcd(a, f_n) = 1$ and, for the sake of brevity, put $r := (n \bmod M)$. From

Lemma 5.1.1 and Binet's formula (2.1), we get that

$$(a^{-1} \bmod f_n) = \frac{b_r f_n + 1}{a} = \frac{b_r(\varphi^n - \overline{\varphi}^n)}{\sqrt{5}a} + \frac{1}{a} = (x_r + y_n \varphi^{-n}) \frac{\varphi^n}{\sqrt{5}}, \tag{5.2}$$

where

$$y_n := \frac{\sqrt{5}}{a} - x_r(-\varphi)^{-n}.$$

Since $n \geq n_0$, it follows that $y_n \in (0,1)$ and $x_r + y_n \varphi^{-n} \in (0,1)$. Therefore, from (5.2) and Lemma 5.1.3, we get that

$$(a^{-1} \bmod f_n) = \sum_{i=1}^{n-1} \delta_{n-i}(x_r + y_n \varphi^{-n}) f_i.$$

Since $\boldsymbol{\delta}(x_r)$ is (purely) periodic and belongs to $\mathfrak{D}$, we have that $\boldsymbol{\delta}(x_r)$ contains infinitely many pairs of consecutive zeros. Furthermore, since the period length of $\boldsymbol{\delta}(x_r)$ is at most ℓ, we have that among every $\ell+1$ consecutive terms of $\boldsymbol{\delta}(x_r)$ there are two consecutive zero. In particular, there exists $\lambda = \lambda(r)$ such that $n - \ell - 3 \leq \lambda \leq n-2$ and $\delta_\lambda(x_r) = \delta_{\lambda+1}(x_r) = 0$. Consequently, by Lemma 5.1.4, we get that $\delta_i(x_r + y_n \varphi^{-n}) = \delta_i(x_r)$ for each positive integer $i \leq \lambda$ and, a fortiori, for each positive integer $i \leq n - i_0$. Therefore, we have that

$$\begin{aligned}(a^{-1} \bmod f_n) &= \sum_{i=i_0}^{n-1} \delta_{n-i}(x_r) f_i + \sum_{i=1}^{i_0-1} \delta_{n-i}(x_r + y_n \varphi^{-n}) f_i \\ &= \sum_{i=i_0}^{n-1} z_{n-i}^{(r)} f_i + \sum_{i=1}^{i_0-1} w_n^{(i)} f_i,\end{aligned} \tag{5.3}$$

where $\boldsymbol{w}^{(1)}, \cdots, \boldsymbol{w}^{(i_0)}$ are the sequences defined by $w_n^{(i)} := \delta_{n-i}(x_r + y_n \varphi^{-n})$. Note that, by construction,

$$z_1^{(r)}, z_2^{(r)}, \ldots, z_{n-i_0}^{(r)}, w_n^{(i_0-1)}, w_n^{(i_0-2)}, \ldots, w_n^{(1)}$$

is a string in $\{0,1\}$ with no consecutive zeros. Hence, (5.3) is the Zeckendorf representation of $(a^{-1} \bmod f_n)$.

It remains only to prove that $\boldsymbol{w}^{(1)},\cdots,\boldsymbol{w}^{(i_0)}$ are periodic. By (5.3) and the uniqueness of the Zeckendorf representation, it suffices to prove that

$$R(n) := (a^{-1} \bmod f_n) - \sum_{i=i_0}^{n-1} z_{n-i}^{(r)} f_i = \sum_{i=1}^{i_0-1} w_n^{(i)} f_i \tag{5.4}$$

is a periodic function of n. From the last equality in (5.4), we have that $0 \le R(n) < \sum_{i=1}^{i_0-1} f_i$. (Actually, one can prove that $0 \le R(n) < f_{i_0}$, but this is not necessary for our proof.) Fix a prime number $p > \max\{a, \sum_{i=1}^{i_0-1} f_i\}$. It suffices to prove that $R(n)$ is periodic modulo p. Recalling that $(a^{-1} \bmod f_n) = (b_r f_n + 1)/a$ and that the sequence of Fibonacci numbers is periodic modulo p, it follows that $(a^{-1} \bmod f_n)$ is periodic modulo p. Hence, it suffices to prove that $R'(n) := \sum_{i=i_0}^{n-1} z_{n-i}^{(r)} f_i$ is periodic modulo p. Using that $\boldsymbol{z}^{(r)}$ has period length dividing ℓ, we get that

$$\begin{aligned}
R'(n+\ell M) - R'(n) &= \sum_{i=i_0}^{n+\ell M-1} z_{n+\ell M-i}^{((n+\ell M) \bmod M)} f_i - \sum_{i=i_0}^{n-1} z_{n-i}^{(r)} f_i \\
&= \sum_{i=i_0}^{n+\ell M-1} z_{n+\ell M-i}^{(r)} f_i - \sum_{i=i_0}^{n-1} z_{n-i}^{(r)} f_i \\
&= \sum_{i=n}^{n+\ell M-1} z_{n+\ell M-i}^{(r)} f_i + \sum_{i=i_0}^{n-1} (z_{n+\ell M-i}^{(r)} - z_{n-i}^{(r)}) f_i \\
&= \sum_{j=1}^{\ell M} z_j^{(r)} f_{n+\ell M-j},
\end{aligned}$$

which is a linear combination of sequences that are periodic modulo p. Hence $R'(n)$ is periodic modulo p. The proof is complete. □

Remark 5.2.2. The proof of Theorem 5.2.1 provides a way to compute the positive integers M, i_0, n_0 and the periods of the periodic sequences $\boldsymbol{z}^{(0)},\ldots,\boldsymbol{z}^{(M-1)}$ and $\boldsymbol{w}^{(1)},\ldots,\boldsymbol{w}^{(i_0)}$. Indeed, going through the proof, we have that: $M = \pi(a)$ is the Pisano period of a, which can be computed in an obvious way; $\boldsymbol{z}^{(r)} = \boldsymbol{\delta}\big((-f_r^{-1} \bmod a)/a\big)$ and so the period of $\boldsymbol{z}^{(r)}$ can be computed as explained at the beginning of Section 2.1; i_0 and n_0 have simple formulas in terms of ℓ, which is the least common multiple of the period lengths of $\boldsymbol{z}^{(0)},\ldots,\boldsymbol{z}^{(M-1)}$. Finally, the periods of $\boldsymbol{w}^{(1)},\ldots,\boldsymbol{w}^{(i_0)}$ can be computed from (5.4) and the fact that $R(n)$ is periodic with period length at most $\pi(p)^2 \ell M$, which follows from the arguments after (5.4). However, note that proceeding in this way might be impractical, since ℓ might be

exponential in M, and thus p might be double exponential in M; making the search for the periods of $\boldsymbol{w}^{(1)}, \ldots, \boldsymbol{w}^{(i_0)}$ extremely long.

Chapter 6

Exploring the algebraic independence with a focus on certain continued fractions and their convergents

In this chapter, we summarize a method to prove the algebraic independence of n quantities developed by C. Elsner et al. in the last years [23, 24]. Starting from n algebraic independent quantities, it is possible to transfer this property to another set of n quantities making use of a polynomial system in $2n$ variables. We provide new applications of this criterion to periodic non-regular Hurwitz type continued fractions. Specifically, given a particular continued fraction with real numbers having partial quotients that are algebraically independent from each other, then not only the convergents are algebraically independent each other, but they are also independent from the limit of the continued fraction.

6.1 A criterion for algebraic independence

In this section we summarize the different variants of the criterion developed by Elsner et al. taking into account their interconnections.

Theorem 6.1.1. *(Theorem 1, [20]) Let $\mathbb{K}$ be a field with $\mathbb{Q} \subseteq \mathbb{K} \subseteq \mathbb{C}$. Assume that the numbers $x_1, \ldots, x_n \in \mathbb{C}$ and $y_1, \ldots, y_n \in \mathbb{C}$ satisfy a system*

$$f_j(x_1, \ldots, x_n, y_1, \ldots, y_n) = 0 \qquad (j = 1, \ldots, n) \tag{6.1}$$

of equations with polynomials $f_j(X_1,\dots,X_n,Y_1,\dots,Y_n) \in \mathbb{K}[X_1,\dots,X_n,\, Y_1,\dots,Y_n]$ *for* $j = 1,\dots,n$. *If the numbers* $x_1,\dots,x_n$ *are algebraically independent over* $\mathbb{K}$ *and*

$$\det_n \left(\frac{\partial f_j}{\partial X_i}(x_1,\dots,x_n,y_1,\dots,y_n) \right) \neq 0 \tag{6.2}$$

holds, then the numbers $y_1,\dots,y_n$ *are algebraically independent over* $\mathbb{K}$.

Remark 6.1.2. We interpret j as the row number and i as the column number. From now on, we denote by capital letters the variables and by lowercase letters the numerical values they assume. Moreover, by $\det_k$ we mean the determinant of a $k \times k$ matrix.

Theorem 6.1.1 can be proved in many different ways. The proof shown below makes use of basic concepts of Commutative Algebra and of a lemma on separable algebraic field extensions. Other proofs make use respectively of the projection theorem of Tarski - Seidenberg and the concept of semi-algebraic sets (in the case of a real field $\mathbb{K}$), differential forms or isomorphism of fields, see [22, Example 1].

Proposition 6.1.3. *Let* $\mathbb{L}$ *be a field with* $\mathbb{Q} \subseteq \mathbb{L} \subseteq \mathbb{R}$. *Furthermore, let the point* $(x_1,\dots,x_n) \in \mathbb{R}^n$ *be an isolated zero of the system of equations*

$$P_j(X_1,\dots,X_n) = 0 \qquad (j = 1,\dots,n),$$

which is formed with polynomials $P_j(X_1,\dots,X_n) \in \mathbb{L}[X_1,\dots,X_n]$ *for* $j = 1,\dots,n$. *Then, the numbers* $x_1,\dots,x_n$ *are algebraic over* $\mathbb{L}$.

Proposition 6.1.3, that will be apply in the proof of Theorem 6.1.1, can be reformulated in terms of the following lemma.

Lemma 6.1.4. *Let* $\mathbb{F}$ *be an extension field of* $\mathbb{L}$ *and let* $x_1,\dots,x_n \in \mathbb{F}$ *satisfy a system of equations*

$$P_j(x_1,\dots,x_n) = 0 \qquad (\textit{for } j = 1,\dots,n) \tag{6.3}$$

with polynomials $P_j(X_1,\dots,X_n) \in \mathbb{L}[X_1,\dots,X_n]$. *If*

$$\det_n \left(\frac{\partial P_j}{\partial X_i}(x_1,\dots,x_n) \right) \neq 0$$

holds, then $\mathbb{L}(x_1,\dots,x_n)$ *is a separable algebraic field extension of* $\mathbb{L}$.

Proof. Let D be a $\mathbb{L}$-derivation of $\mathbb{F} = \mathbb{L}(x_1,\ldots,x_n)$. From 6.3, it follows that $D(P_j(x_1,\ldots,x_n) = 0$ so

$$\sum_i \left(\frac{\partial P_j}{\partial X_i}\right)(x_1,\ldots,x_n)\cdot D(x_i) = 0 \quad \text{for} = j = 1,\ldots,n$$

So we have a system of n homogeneous linear equations in $D(x_1),\ldots,D(x_n)$ with non vanishing determinant. This implies that $D(x_1) = \cdots = D(x_n) = 0$ so D is the trivial derivation. The thesis follows because a necessary and sufficient condition for a finitely generated extension field of $\mathbb{L}$ to be separable over $\mathbb{L}$ is that 0 is the only $\mathbb{L}$-derivation of $\mathbb{F}$ [74, p. 126]. □

Proof. (Theorem 6.1.1),[20] Using the polynomials $f_1,\ldots,f_n$ from Theorem 6.1.1, we define some auxiliary polynomials P_j, for $j = 1,\ldots,n$;

$$P_j(X_1,\ldots,X_n) := f_j(X_1,\ldots,X_n,y_1,\ldots,y_n) \in \mathbb{K}(y_1,\ldots,y_n)[X_1,\ldots,X_n]\,. \tag{6.4}$$

They are constructed using the variables $X_1,\ldots,X_n$, and they all vanish at the point $(x_1,\ldots,x_n)$ because of (6.1). The determinant condition (6.2) takes the form

$$\det_n\left(\frac{\partial P_j}{\partial X_i}(x_1,\ldots,x_n)\right) \neq 0\,. \tag{6.5}$$

With $\mathbb{F} = \mathbb{C}$, $\mathbb{L} = \mathbb{K}(y_1,\ldots,y_n)$ and the setting of polynomials $P_j(X_1,\ldots,X_n)$ $(j = 1,\ldots,n)$ as in (6.4), all the conditions of Lemma 6.1.4 including (6.5) are fulfilled. So, by Lemma 6.1.4, $\mathbb{L}(x_1,\ldots,x_n)$ is an algebraic field extension over $\mathbb{L}$.

We denote by $\text{tr.deg}\left(\mathbb{K}_2 : \mathbb{K}_1\right)$ the transcendence degree of the field extension $\mathbb{K}_2$ over $\mathbb{K}_1$. Then, we have

$$\text{tr.deg}\left(\mathbb{L}(x_1,\ldots,x_n) : \mathbb{L}\right) = 0 \quad \text{and} \quad \text{tr.deg}\left(\mathbb{K}(x_1,\ldots,x_n) : \mathbb{K}\right) = n\,,$$

where the latter is due to the condition on the algebraic independence of $x_1,\ldots,x_n$ over $\mathbb{K}$ in Theorem 6.1.1. Trivially, $\mathbb{K} \subseteq \mathbb{L}$ implies that $\text{tr.deg}(\mathbb{L}(x_1,\ldots,x_n) : \mathbb{K}) \geq n$. If the fields $\mathbb{K}_1$, $\mathbb{K}_2$ and $\mathbb{K}_3$ form a field tower $\mathbb{K}_1 \subseteq \mathbb{K}_2 \subseteq \mathbb{K}_3$, we know according to the chain theorem for degrees of transcendence, that

$$\text{tr.deg}\left(\mathbb{K}_3 : \mathbb{K}_1\right) = \text{tr.deg}\left(\mathbb{K}_3 : \mathbb{K}_2\right) + \text{tr.deg}\left(\mathbb{K}_2 : \mathbb{K}_1\right). \tag{6.6}$$

Applying this relation to the field tower $\mathbb{K} \subseteq \mathbb{L} = \mathbb{K}(y_1,\dots,y_n) \subseteq \mathbb{L}(x_1,\dots,x_n)$, we obtain

$$\begin{aligned} n &\leq \operatorname{tr.deg}\big(\mathbb{L}(x_1,\dots,x_n):\mathbb{K}\big) = \operatorname{tr.deg}\big(\mathbb{L}(x_1,\dots,x_n):\mathbb{L}\big) + \operatorname{tr.deg}\big(\mathbb{L}:\mathbb{K}\big) \\ &= \operatorname{tr.deg}\big(\mathbb{L}:\mathbb{K}\big) = \operatorname{tr.deg}\big(\mathbb{K}(y_1,\dots,y_n):\mathbb{K}\big) \leq n\,. \end{aligned}$$

Since $\operatorname{tr.deg}\big(\mathbb{K}(y_1,\dots,y_n):\mathbb{K}\big) = n$, the theorem is proved. □

Theorem 6.1.5. *Let $\mathbb{K}$ be a field with $\mathbb{Q} \subseteq \mathbb{K} \subseteq \mathbb{C}$. Furthermore, it is assumed that the numbers $x_1,\dots,x_n \in \mathbb{C}$ and $y_1,\dots,y_n \in \mathbb{C}$ satisfy a system*

$$y_j = T_j(x_1,\dots,x_n), \qquad (j = 1,\dots,n) \tag{6.7}$$

of equations with polynomials $T_j(X_1,\dots,X_n) \in \mathbb{K}[X_1,\dots,X_n]$ for $j = 1,\dots,n$. If the numbers $x_1,\dots,x_n$ are algebraically independent over $\mathbb{K}$ and

$$\det_n\left(\frac{\partial T_j}{\partial X_i}(x_1,\dots,x_n)\right) \neq 0 \tag{6.8}$$

holds, then the numbers $y_1,\dots,y_n$ are algebraically independent over $\mathbb{K}$.

Proof. Setting

$$f_j\big(X_1,\dots,X_n,Y_j\big) := T_j\big(X_1,\dots,X_n\big) - Y_j \qquad (1 \leqslant j \leqslant n)\,,$$

Theorem 6.1.5 follows immediately from Theorem 6.1.1. □

Remark 6.1.6. Under the conditions of Theorem 6.1.5, the non-vanishing of the determinant in (6.8) is not only sufficient but also necessary for the algebraic independence of $y_1,\dots,y_n$ over $\mathbb{K}$.

In numerous applications, each of the numbers $y_1,\dots,y_n$ can be represented as the value of a *rational function* at the point $(x_1,\dots,x_n)$, namely

$$y_j = \frac{T_j(x_1,\dots,x_n)}{U_j(x_1,\dots,x_n)} \qquad (j = 1,\dots,n)\,. \tag{6.9}$$

Here T_j and U_j are non-identical vanishing polynomials from the ring $\mathbb{K}[X_1,\ldots,X_n]$. The polynomials

$$f_j(X_1,\ldots,X_n,Y_j) := Y_jU_j(X_1,\ldots,X_n) - T_j(X_1,\ldots,X_n), \tag{6.10}$$

for $j = 1,\ldots,n$, thus vanish at the points $(x_1,\ldots,x_n,y_j)$.

Theorem 6.1.7. *Let $\mathbb{K}$ be a field with $\mathbb{Q} \subseteq \mathbb{K} \subseteq \mathbb{C}$. Furthermore, we assume that the numbers $x_1,\ldots,x_n \in \mathbb{C}$ and $y_1,\ldots,y_n \in \mathbb{C}$ satisfy a system of the form*

$$y_j = R_j(x_1,\ldots,x_n) \qquad (j = 1,\ldots,n)$$

of equations with rational functions $R_j(X_1,\ldots,X_n)$ in the extension field $\mathbb{K}(X_1,\ldots,X_n)$ for $j = 1,\ldots,n$. If the numbers $x_1,\ldots,x_n$ are algebraically independent over $\mathbb{K}$ and

$$\tilde{\Delta}_1 := \det_n\left(\frac{\partial R_j}{\partial X_i}(x_1,\ldots,x_n)\right) \neq 0 \tag{6.11}$$

holds, then the numbers $y_1,\ldots,y_n$ are algebraically independent over $\mathbb{K}$.

Proof. We denote the determinant in (6.11) by Δ_1. Let us first assume that $\Delta_1 \neq 0$; we can express the rational functions R_j by

$$R_j(X_1,\ldots,X_n) = \frac{T_j(X_1,\ldots,X_n)}{U_j(X_1,\ldots,X_n)} \qquad (j = 1,\ldots,n),$$

using the polynomials T_j and U_j already introduced in (6.9). The algebraic independence of $y_1,\ldots,y_n$ over $\mathbb{K}$ can be proven with Theorem 6.1.1, where the non-vanishing of the Jacobi determinant must be shown for the functions f_j from (6.10):

$$\begin{aligned}
\tilde{\Delta}_2 :=& \det_n\left(\frac{\partial f_j}{\partial X_i}\right)(x_1,\ldots,x_n,y_1,\ldots,y_n)\\
=& \det_n\left(y_j\frac{\partial U_j}{\partial X_i} - \frac{\partial T_j}{\partial X_i}\right)(x_1,\ldots,x_n)\\
=& \det_n\left(\frac{T_j}{U_j}\frac{\partial U_j}{\partial X_i} - \frac{\partial T_j}{\partial X_i}\right)(x_1,\ldots,x_n)
\end{aligned}$$

$$
\begin{aligned}
&= (-1)^n U_1 \cdots U_n \det_n \left(\frac{1}{U_j^2} \left(\frac{\partial T_j}{\partial X_i} U_j - T_j \frac{\partial U_j}{\partial X_i} \right) \right) (x_1, \ldots, x_n) \\
&= (-1)^n U_1 \cdots U_n \det_n \left(\frac{\partial R_j}{\partial X_i} \right) (x_1, \ldots, x_n) \\
&= (-1)^n U_1 \cdots U_n (x_1, \ldots, x_n) \tilde{\Delta}_1 \,.
\end{aligned}
$$

Since $\tilde{\Delta}_1 \neq 0$ we have $\tilde{\Delta}_2 \neq 0$. The $x_1, \ldots, x_n$ are considered as algebraically independent over $\mathbb{K}$ so that the polynomial $Q_1 \cdots Q_n$ does not vanish identically. Then, $U_1 \cdots U_n(x_1, \ldots, x_n) \neq 0$ is guaranteed. Theorem 6.1.1 thus proves the algebraic independence of $y_1, \ldots, y_n$ over $\mathbb{K}$. □

Theorem 6.1.8. *Let $\mathbb{K}$ be a field with $\mathbb{Q} \subseteq \mathbb{K} \subseteq \mathbb{C}$. Let m and n be positive integers with $1 \leq m < n$. Furthermore, assume that the numbers $x_1, \ldots, x_n \in \mathbb{C}$ and $y_1, \ldots, y_m \in \mathbb{C}$ satisfy a system*

$$
f_j(x_1, \ldots, x_n, y_1, \ldots, y_m) = 0 \qquad (j = 1, \ldots, m) \tag{6.12}
$$

of equations with polynomials $f_j(X_1, \ldots, X_n, Y_1, \ldots, Y_m) \in \mathbb{K}[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$ for $j = 1, \ldots, m$. If the numbers $x_1, \ldots, x_n$ are algebraically independent over $\mathbb{K}$ and if

$$
\det_m \left(\frac{\partial f_j}{\partial X_i} (x_1, \ldots, x_n, y_1, \ldots, y_m) \right) \neq 0 \tag{6.13}
$$

holds with $1 \leqslant i, j \leqslant m$, then the numbers $y_1, \ldots, y_m$ are algebraically independent over the field $\mathbb{K}(x_{m+1}, \ldots, x_n)$.

Proof. In addition to the equations in (6.12) we introduce the polynomials

$$
f_j(X_j, Y_j) := X_j - Y_j \in \mathbb{K}[X_j, Y_j] \qquad (j = m+1, \ldots, n)
$$

so that for $y_j := x_j$ with $j = m+1, \ldots, n$ the polynomial f_j vanishes at the point (x_j, y_j). Theorem 6.1.1 can now be applied for the proof of the algebraic independence of $y_1, \ldots, y_n$ over $\mathbb{K}$. We compute the Jacobi determinant of the functions $f_1, \ldots, f_n$ at the position $(x_1, \ldots, x_n, y_1, \ldots, y_n)$ and apply the condition from (6.13):

$$
\det_n \left(\frac{\partial f_j}{\partial X_i} (x_1, \ldots, x_n, y_1, \ldots, y_n) \right)
$$

$$
\begin{aligned}
&= \det_n \begin{pmatrix}
\frac{\partial f_1}{\partial X_1} & \cdots & \frac{\partial f_1}{\partial X_m} & \frac{\partial f_1}{\partial X_{m+1}} & \cdots & \frac{\partial f_1}{\partial X_n} \\
\vdots & \cdots & \vdots & \vdots & \cdots & \vdots \\
\frac{\partial f_m}{\partial X_1} & \cdots & \frac{\partial f_m}{\partial X_m} & \frac{\partial f_m}{\partial X_{m+1}} & \cdots & \frac{\partial f_m}{\partial X_n} \\
0 & \cdots & 0 & 1 & \cdots & 0 \\
\vdots & \cdots & \vdots & \cdots & \cdots & \vdots \\
0 & \cdots & 0 & 0 & \cdots & 1
\end{pmatrix} (x_1, \ldots, x_n, y_1, \ldots, y_m) \\
&= \det_n \begin{pmatrix}
\frac{\partial f_1}{\partial X_1} & \cdots & \frac{\partial f_1}{\partial X_m} \\
\vdots & \cdots & \vdots \\
\frac{\partial f_m}{\partial X_1} & \cdots & \frac{\partial f_m}{\partial X_m}
\end{pmatrix} (x_1, \ldots, x_n, y_1, \ldots, y_m) \quad \neq 0 .
\end{aligned}
$$

Thus, according to Theorem 6.1.1 and to $y_j = x_j$ for $j = m+1, \ldots, n$, the algebraic independence of the numbers $y_1, \ldots, y_m, x_{m+1}, \ldots, x_n$ over $\mathbb{K}$ is proven. This implies

$$\text{tr.deg}\left(\mathbb{K}(y_1, \ldots, y_m, x_{m+1}, \ldots, x_n) : \mathbb{K}\right) = n .$$

Taking into account the presupposed algebraic independence of $x_1, \ldots, x_n$ over $\mathbb{K}$, we know that the equation $\text{tr.deg}\left(\mathbb{K}(x_{m+1}, \ldots, x_n) : \mathbb{K}\right) = n - m$ holds. Again we make use of the chain rule from (6.6), applied to the fields $\mathbb{K} \subseteq \mathbb{K}(x_{m+1}, \ldots, x_n) \subseteq \mathbb{K}(y_1, \ldots, y_m, x_{m+1}, \ldots, x_n)$. Thus we obtain

$$\text{tr.deg}\left(\mathbb{K}(y_1, \ldots, y_m, x_{m+1}, \ldots, x_n) : \mathbb{K}(x_{m+1}, \ldots, x_n)\right) = m ,$$

which is the statement of Theorem 6.1.8. □

6.2 A pratical lemma for the handling of the determinant condition

In this section we want to show the method used later to get a contradiction in the proof of Theorem 6.3.1. Let X_1, X_2, Y_1, Y_2 be variables and x_1, x_2, y_1, y_2 be real numbers, where x_1 and x_2 are algebraically independent over a finite field extension

$\tilde{\mathbb{Q}}$ of $\mathbb{Q}$. Let us consider three polynomials, such that

$$\begin{aligned} P_1\big(X_1,X_2,Y_1\big) &\in \tilde{\mathbb{Q}}\big[X_1,X_2,Y_1\big]\,, \\ P_2\big(X_1,X_2,Y_2\big) &\in \tilde{\mathbb{Q}}\big[X_1,X_2,Y_2\big]\,, \\ D\big(X_1,X_2,Y_1,Y_2\big) &\in \tilde{\mathbb{Q}}\big[X_1,X_2,Y_1,Y_2\big]\,. \end{aligned}$$

We require that

$$\begin{aligned} P_1(x_1,x_2,y_1) &= 0\,, \\ P_2(x_1,x_2,y_2) &= 0\,. \end{aligned} \tag{6.14}$$

At this point, assume that

$$D(x_1,x_2,y_1,y_2) = 0\,, \tag{6.15}$$

later, in our application, we require that D is not zero. As a first step, we consider $\overline{D}(Y_1,Y_2) := D(x_1,x_2,Y_1,Y_2)$ and $\overline{P}_1(Y_1) := P_1(x_1,x_2,Y_1)$ as polynomials in the polynomial ring $\tilde{\mathbb{Q}}(x_1,x_2)[Y_1,Y_2]$. By (6.14) and (6.15), the two polynomials $\overline{D}(Y_1,Y_2)$ and $\overline{P}_1(Y_1)$ have a common root at $(Y_1,Y_2) = (y_1,y_2)$, and thus their resultant with respect to Y_1 vanishes for $Y_2 = y_2$. Therefore, we define the polynomial $\overline{P}_3(Y_2)$ as

$$\overline{P}_3(Y_2) := \mathrm{Res}_{Y_1}\big(\overline{D}(Y_1,Y_2),\overline{P}_1(Y_1)\big) = \mathrm{Res}_{Y_1}\big(D(x_1,x_2,Y_1,Y_2),P_1(x_1,x_2,Y_1)\big)$$

and, from one hand it holds the property

$$\overline{P}_3(y_2) = 0\,, \tag{6.16}$$

on the other side it is

$$\overline{P}_3(Y_2) \in \tilde{\mathbb{Q}}(x_1,x_2,Y_2)\,. \tag{6.17}$$

As a second step, we interprete $\overline{P}_2(Y_2) := P_2(x_1,x_2,Y_2)$ as a polynomial from the polynomial ring $\tilde{\mathbb{Q}}(x_1,x_2)[Y_2]$ over the field $\tilde{\mathbb{Q}}(x_1,x_2)$. Together with (6.16) and (6.17), it holds that $\overline{P}_4(x_1,x_2) = 0$ where the polynomial $\overline{P}_4(X_1,X_2)$ is defined by

$$\overline{P}_4(X_1,X_2) := \mathrm{Res}_{Y_2}\big(\overline{P}_3(Y_2),\overline{P}_2(Y_2)\big) \in \tilde{\mathbb{Q}}\big[X_1,X_2\big].$$

An algebraic conclusion argument now requires that $\overline{P}_4(X_1,X_2)$ does not vanish identically. For this we need the following lemma.

Lemma 6.2.1. *Let α_1 and α_2 be two real numbers. Set $X_1 = \alpha_1$ and $X_2 = \alpha_2$ so that we have for the above polynomials*

$$\begin{aligned} P_1(Y_1) &= \overline{P}_1(Y_1)\,, \\ P_2(Y_2) &= \overline{P}_2(Y_2)\,, \\ D(Y_1,Y_2) &= \overline{D}(Y_1,Y_2)\,, \end{aligned}$$

and all these polynomials are considered as polynomials over the field $\tilde{\mathbb{Q}}(\alpha_1,\alpha_2)$. If

$$\gamma := Res_{Y_2}\big(Res_{Y_1}\big(D(Y_1,Y_2),P_1(Y_1)\big),P_2(Y_2)\big)$$

is a non-vanishing number from the field $\tilde{\mathbb{Q}}(\alpha_1,\alpha_2)$, then the polynomial $\overline{P}_4(X_1,X_2)$ does not vanish identically.

Proof. Since there is no difference whether the resultants is computed with respect to Y_1 and Y_2 with unspecified parameters X_1 and X_2, and then assigning special values to these parameters, or whether assigning these values in the involved polynomials already at the beginning before the resultant calculations, then the proof follows. □

6.3 An application of the criterion to continued fractions

In this section we apply the above lemma to prove the algebraic independence of certain continued fractions and their convergents. In the following theorem we consider the case of a continued fractions of periods 2, and lately we show why it is not possible to prove the algebraic independence in the case of period 1.

Theorem 6.3.1. *Let $\tilde{\mathbb{Q}}$ be a real finite field extension of $\mathbb{Q}$, and let α and β be two real algebraic independent numbers over $\tilde{\mathbb{Q}}$ greater than 0. Moreover, let p_m/q_m be the convergents of $\xi := [\overline{\alpha,\beta}]$. Then, for every integer $n \geqslant 0$, the two numbers ξ and p_n/q_n are algebraically independent over the field $\tilde{\mathbb{Q}}$.*

Proof. Let us rename the following quantity as

$$y_1 := [\overline{\alpha,\beta}] = \alpha + \cfrac{1}{\beta + \cfrac{1}{y_1}} = \frac{(\alpha\beta+1)y_1+\alpha}{\beta y_1+1}.$$

Then we have

$$\beta y_1^2 - \alpha\beta y_1 - \alpha = 0. \tag{6.18}$$

This implies

$$y_1 = \frac{\alpha}{2} + \sqrt{\frac{\alpha^2}{4} + \frac{\alpha}{\beta}}, \tag{6.19}$$

but we will not need this representation of y_1. From [21, Corollary 1] we obtain three-term recurrence formulas for leaping convergents of y_1 with indices modulo 2. For $n \geqslant 2$ we have

$$p_{2n} = (\alpha\beta+2)p_{2n-2} - p_{2n-4}, \tag{6.20}$$
$$q_{2n} = (\alpha\beta+2)q_{2n-2} - q_{2n-4}; \tag{6.21}$$

and for $n \geqslant 1$,

$$p_{2n+1} = (\alpha\beta+2)p_{2n-1} - p_{2n-3}, \tag{6.22}$$
$$q_{2n+1} = (\alpha\beta+2)q_{2n-1} - q_{2n-3}. \tag{6.23}$$

The characteristic polynomial $P(x)$ of all four recursion formulas in (6.21) and (6.22) is

$$P(x) = x^2 - (\alpha\beta+2)x + 1.$$

Its roots t_1, t_2 can be easily calculated as

$$t_1 = \frac{\alpha\beta+2}{2} + \sqrt{\frac{(\alpha\beta+2)^2}{4} - 1} = \frac{\alpha\beta+2}{2} + \frac{1}{2}\sqrt{\alpha\beta(\alpha\beta+4)}, \tag{6.24}$$

and, similarly,

$$t_2 = \frac{\alpha\beta+2}{2} - \frac{1}{2}\sqrt{\alpha\beta(\alpha\beta+4)}. \tag{6.25}$$

We now determine explicit formulas for the four quantities p_{2n}, q_{2n}, p_{2n+1}, and q_{2n+1} based on the recursion formulas in (6.21) and (6.22). We start with an equation for

p_{2n}

$$p_{2n} = C_1 t_1^n + C_2 t_2^n \qquad (n \geq 0). \tag{6.26}$$

We have the initial values

$$\left.\begin{array}{lcl} p_{-1} &=& 1\,, \\ p_0 &=& \alpha\,, \\ p_1 &=& \alpha\beta + 1\,, \\ p_2 &=& \alpha^2\beta + 2\alpha\,, \\ p_3 &=& \alpha^2\beta^2 + 3\alpha\beta + 1\,. \end{array}\right\} \tag{6.27}$$

To obtain C_1 and C_2 in (6.26), we need the values for $n = 0$ and $n = 1$ from (6.27):

$$\begin{array}{lrcl} n = 0: & \alpha &=& C_1 + C_2\,, \\ n = 1: & \alpha^2\beta + 2\alpha &=& C_1 t_1 + C_2 t_2\,. \end{array}$$

Using the explicit values for t_1 and t_2 from (6.24) and (6.25), we solve this system for C_1 and C_2:

$$C_1 = \frac{\alpha}{2}\Big(1 + \frac{\alpha\beta + 2}{\sqrt{\alpha\beta(\alpha\beta+4)}}\Big)\,,$$

$$C_2 = \frac{\alpha}{2}\Big(1 - \frac{\alpha\beta + 2}{\sqrt{\alpha\beta(\alpha\beta+4)}}\Big)\,.$$

The three remaining quantities are treated in an analogous way. We continue with q_{2n}:

$$q_{2n} = C_3 t_1^n + C_4 t_2^n \qquad (n \geq 0). \tag{6.28}$$

We have the initial values

$$\begin{array}{lcl} q_{-1} &=& 0\,, \\ q_0 &=& 1\,, \\ q_1 &=& \beta\,, \\ q_2 &=& \alpha\beta + 1\,, \\ q_3 &=& \alpha\beta^2 + 2\beta\,. \end{array}$$

Hence we have

$$\begin{array}{lrcl} n = 0: & 1 &=& C_3 + C_4\,, \\ n = 1: & \alpha\beta + 1 &=& C_3 t_1 + C_4 t_2\,, \end{array}$$

and consequently,

$$C_3 = \frac{1}{2}\Big(1+\frac{\alpha\beta}{\sqrt{\alpha\beta(\alpha\beta+4)}}\Big),$$

$$C_4 = \frac{1}{2}\Big(1-\frac{\alpha\beta}{\sqrt{\alpha\beta(\alpha\beta+4)}}\Big).$$

For an explicit formula for p_{2n+1} we access values from (6.27):

$$p_{2n+1} = C_5 t_1^n + C_6 t_2^n \qquad (n \geq 0), \tag{6.29}$$

Thus, we have

$$\begin{aligned} n=0: \quad \alpha\beta+1 &= C_5+C_6, \\ n=1: \quad \alpha^2\beta^2+3\alpha\beta+1 &= C_5 t_1 + C_6 t_2, \end{aligned}$$

and consequently,

$$C_5 = \frac{\alpha\beta+1}{2} + \frac{\alpha^2\beta^2+3\alpha\beta}{2\sqrt{\alpha\beta(\alpha\beta+4)}},$$

$$C_6 = \frac{\alpha\beta+1}{2} - \frac{\alpha^2\beta^2+3\alpha\beta}{2\sqrt{\alpha\beta(\alpha\beta+4)}}.$$

Last, we are going to tackle q_{2n+1}:

$$q_{2n+1} = C_7 t_1^n + C_8 t_2^n \qquad (n \geq 0); \tag{6.30}$$

$$\begin{aligned} n=0: \quad \beta &= C_7+C_8, \\ n=1: \quad \alpha\beta^2+2\beta &= C_7 t_1 + C_8 t_2; \end{aligned}$$

$$C_7 = \frac{\beta}{2} + \frac{\alpha\beta^2+2\beta}{2\sqrt{\alpha\beta(\alpha\beta+4)}},$$

$$C_8 = \frac{\beta}{2} - \frac{\alpha\beta^2+2\beta}{2\sqrt{\alpha\beta(\alpha\beta+4)}}.$$

It is necessary to give a clearer form to the formulas (6.26), (6.28), (6.29) and (6.30), by expressing the constants by t_1 and t_2. For this purpose we first introduce

$$z := \alpha\beta\big(\alpha\beta+4\big). \tag{6.31}$$

For example, we hereby obtain for C_1 and C_2:

$$\begin{aligned} C_1 &= \frac{\alpha}{2}\cdot\frac{\alpha\beta+2+\sqrt{z}}{\sqrt{z}} = \frac{\alpha}{\sqrt{z}}\Big(\frac{\alpha\beta+2}{2}+\frac{1}{2}\sqrt{z}\Big) = \frac{\alpha t_1}{\sqrt{z}}\,, \\ C_2 &= -\frac{\alpha t_2}{\sqrt{z}}\,. \end{aligned}$$

Therefore, we can express (6.26) in the following form

$$p_{2n} = \frac{\alpha}{\sqrt{z}}\big(t_1^{n+1}-t_2^{n+1}\big)\,, \tag{6.32}$$

where

$$\begin{aligned} t_1 &= \frac{\alpha\beta+2}{2}+\frac{1}{2}\sqrt{z}, \\ t_2 &= \frac{\alpha\beta+2}{2}-\frac{1}{2}\sqrt{z}. \end{aligned}$$

Similarly, (6.28), (6.29), and (6.30) are treated, requiring intermediate calculations of greater or lesser length

$$q_{2n} = \frac{1}{\sqrt{z}}\big((t_1-1)t_1^n-(t_2-1)t_2^n\big)\,, \tag{6.33}$$

$$p_{2n+1} = \frac{1}{\sqrt{z}}\big((t_1-1)t_1^{n+1}-(t_2-1)t_2^{n+1}\big)\,, \tag{6.34}$$

$$q_{2n+1} = \frac{\beta}{\sqrt{z}}\big(t_1^{n+1}-t_2^{n+1}\big)\,. \tag{6.35}$$

By these explicit formulas for the convergents it becomes clear that the continued fraction $[\overline{\alpha,\beta}]$ converges for every pair α,β of positive real numbers: on the one side, for convergents p_{2n}/q_{2n} with even subscripts, we obtain from (6.32) and (6.33),

$$\begin{aligned} [\underbrace{\alpha,\beta,\ldots,\alpha}_{2n+1}] &= \frac{p_{2n}}{q_{2n}} \\ &= \frac{\alpha}{1-\dfrac{t_1^n\big(1-(t_2/t_1)^n\big)}{t_1^{n+1}\big(1-(t_2/t_1)^{n+1}\big)}} \overset{(n\to\infty)}{\longrightarrow} \frac{\alpha}{1-\dfrac{1}{t_1}} = \frac{\alpha}{2}+\sqrt{\frac{\alpha^2}{4}+\frac{\alpha}{\beta}} = y_1\,, \end{aligned}$$

note that the inequalities $0 < t_2 < t_1$ hold by (6.24), (6.25) and $\alpha, \beta > 0$. On the other side, a similar calculation shows for convergents p_{2n+1}/q_{2n+1} with odd subscripts by (6.34) and (6.35),

$$\begin{aligned}
[\underbrace{\alpha, \beta, \ldots, \beta}_{2n+2}] &= \frac{p_{2n+1}}{q_{2n+1}} \\
&= \frac{1}{\beta}\left(\frac{t_1^{n+2}\left(1-(t_2/t_1)^{n+2}\right)}{t_1^{n+1}\left(1-(t_2/t_1)^{n+1}\right)}\right) \overset{(n\to\infty)}{\longrightarrow} \frac{1}{\beta}\left(t_1 - 1\right) \\
&= \frac{\alpha}{2} + \sqrt{\frac{\alpha^2}{4} + \frac{\alpha}{\beta}} = y_1 \,.
\end{aligned}$$

This proves the convergence of the continued fraction $[\overline{\alpha, \beta}]$ for all positive real numbers α and β. For completeness, the convergence can also be proved applying a classical result that asserts that, taken a continued fraction with real partial quotients $[a_0, a_1, \ldots]$ such that $a_i > 0$ for $i > 0$, then it converges in $\mathbb{R}$ if and only if $\sum a_i = \infty$ (see Proposition 2.3 of [16] for a very nice and simple proof).

We first prove in Theorem 6.3.1 the algebraic independence of ξ and p_{2n}/q_{2n} for $n \geqslant 3$. In order to do that, we want to apply Theorem 6.1.1, so our look for two polynomials such that $P_{i,n}(\alpha, \beta, p_{2n}, q_{2n}) = 0$ and the functional determinant does not vanish. From now on, we omit the subscript n in $P_{i,n}$.
It makes sense to introduce also

$$w := \alpha\beta + 2 \,. \tag{6.36}$$

This allows t_1 and t_2 to be represented even more simply as

$$\begin{aligned}
t_1 &= \frac{1}{2}\left(w + \sqrt{z}\right), \\
t_2 &= \frac{1}{2}\left(w - \sqrt{z}\right).
\end{aligned}$$

These representations are used to express $t_1^m - t_2^m$ in terms of w and $\sqrt{z}$ by binomial expansions. Let

$$\begin{aligned}
\Delta_m &= \Delta_m(\alpha,\beta) := \frac{t_1^m - t_2^m}{\sqrt{z}} = \frac{1}{2^m\sqrt{z}}\left((w+z^{1/2})^m - (w-z^{1/2})^m\right) \\
&= \frac{1}{2^m\sqrt{z}}\Big(\sum_{\nu=0}^{m}\binom{m}{\nu}w^{m-\nu}z^{\nu/2} - \sum_{\nu=0}^{m}\binom{m}{\nu}w^{m-\nu}(-1)^\nu z^{\nu/2}\Big) \\
&= \frac{1}{2^m z^{1/2}}\sum_{\substack{1\le\nu\le m\\ \nu\equiv_2 1}} 2\binom{m}{\nu}w^{m-\nu}z^{\nu/2} \\
&= \frac{1}{2^{m-1}}\sum_{\mu\geqslant 1}\binom{m}{2\mu-1}w^{m-2\mu+1}z^{\mu-1} \\
&\overset{(6.31),(6.36)}{=} \frac{1}{2^{m-1}}\sum_{\mu\geqslant 1}\binom{m}{2\mu-1}(\alpha\beta+2)^{m+1-2\mu}\big(\alpha\beta(\alpha\beta+4)\big)^{\mu-1} \\
&= \frac{1}{2^{m-1}}\sum_{\mu\geqslant 1}\binom{m}{2\mu-1}(\alpha\beta)^{\mu-1}(4+\alpha\beta)^{\mu-1}(2+\alpha\beta)^{m+1-2\mu},
\end{aligned} \tag{6.37}$$

where the last expression may be considered as a polynomial in α and β with rational coefficients. Therefore, we obtain by (6.37) from (6.32), (6.33), (6.34), and (6.35):

$$\left.\begin{aligned}
p_{2n} &= \frac{\alpha(t_1^{n+1} - t_2^{n+1})}{\sqrt{z}} &&= \alpha\Delta_{n+1}, \\
q_{2n} &= \frac{(t_1^{n+1} - t_2^{n+1}) - (t_1^n - t_2^n)}{\sqrt{z}} &&= \Delta_{n+1} - \Delta_n, \\
p_{2n+1} &= \frac{(t_1^{n+2} - t_2^{n+2}) - (t_1^{n+1} - t_2^{n+1})}{\sqrt{z}} &&= \Delta_{n+2} - \Delta_{n+1}, \\
q_{2n+1} &= \frac{\beta(t_1^{n+1} - t_2^{n+1})}{\sqrt{z}} &&= \beta\Delta_{n+1}.
\end{aligned}\right\} \tag{6.38}$$

We prove Theorem 6.3.1 first for ξ and convergents p_{2n}/q_{2n} with even index $2n \geqslant 4$, so that we assume $n \geqslant 2$ in the following. Set

$$P_1(X_1, X_2, Y_1) := X_2Y_1^2 - X_1X_2Y_1 - X_1, \tag{6.39}$$

so that $P_1(x_1,x_2,y_1)=0$ for $X_1=x_1:=\alpha$, $X_2=x_2:=\beta$, and $Y_1=y_1:=\xi$ by (6.18). Moreover, let

$$y_2 := \frac{p_{2n}}{q_{2n}} \overset{(6.38)}{=} \frac{\alpha\Delta_{n+1}}{\Delta_{n+1}-\Delta_n}.$$

Hence, the polynomial

$$P_2\big(X_1,X_2,Y_2\big) := \big(\Delta_{n+1}-\Delta_n\big)Y_2-\Delta_{n+1}X_1 \tag{6.40}$$

vanishes for $(X_1,X_2,Y_2)=(x_1,x_2,y_2)$ where $\Delta_m=\Delta_m(X_1,X_2)$ with $m\in\{n,n+1\}$.

In (6.37) we replace α by X_1 and β by X_2:

$$\Delta_m\big(X_1,X_2\big) = \frac{1}{2^{m-1}}\sum_{\mu\geqslant 1}\binom{m}{2\mu-1}(X_1X_2)^{\mu-1}(4+X_1X_2)^{\mu-1}(2+X_1X_2)^{m+1-2\mu}. \tag{6.41}$$

For brevity, we again write Δ_m instead of $\Delta_m(X_1,X_2)$, and we set

$$\Delta_m^{(X_j)} := \frac{\partial\Delta_m}{\partial X_j} \qquad (j=1,2).$$

Then we obtain

$$\frac{\partial P_1}{\partial X_1} \overset{(6.39)}{=} -X_2Y_1-1,$$

$$\frac{\partial P_1}{\partial X_2} \overset{(6.39)}{=} Y_1^2-X_1Y_1,$$

$$\frac{\partial P_2}{\partial X_1} \overset{(6.40)}{=} \big(\Delta_{n+1}^{(X_1)}-\Delta_n^{(X_1)}\big)Y_2-\Delta_{n+1}^{(X_1)}X_1-\Delta_{n+1},$$

$$\frac{\partial P_2}{\partial X_2} \overset{(6.40)}{=} \big(\Delta_{n+1}^{(X_2)}-\Delta_n^{(X_2)}\big)Y_2-\Delta_{n+1}^{(X_2)}X_1.$$

With these partial derivatives we calculate the following functional determinant

$$\begin{aligned} D_1 &= D_1(X_1,X_2,Y_1,Y_2) := \begin{vmatrix} \dfrac{\partial P_1}{\partial X_1} & \dfrac{\partial P_1}{\partial X_2} \\ \dfrac{\partial P_2}{\partial X_1} & \dfrac{\partial P_2}{\partial X_2} \end{vmatrix} \\ &= -(1+X_2Y_1)\Big((\Delta_{n+1}^{(X_2)}-\Delta_n^{(X_2)})Y_2-\Delta_{n+1}^{(X_2)}X_1\Big) \\ &\quad -(Y_1^2-X_1Y_1)\Big((\Delta_{n+1}^{(X_1)}-\Delta_n^{(X_1)})Y_2-\Delta_{n+1}^{(X_1)}X_1-\Delta_{n+1}\Big). \end{aligned} \tag{6.42}$$

For $1 \leqslant \mu \leqslant \lfloor (m+1)/2 \rfloor$ let

$$H_{m,\mu} = H_{m,\mu}(X_1,X_2) = \frac{1}{2^{m-1}}\binom{m}{2\mu-1}(X_1X_2)^{\mu-1}(4+X_1X_2)^{\mu-1}(2+X_1X_2)^{m+1-2\mu}. \tag{6.43}$$

Then we obtain from (6.41)

$$\Delta_m = \sum_{\mu \geqslant 1} H_{m,\mu}. \tag{6.44}$$

Note that

$$\Delta_1 = H_{1,1} = 1 \qquad \text{and} \qquad \Delta_2 = H_{2,1} = 2+X_1X_2.$$

Thus $m=2$ is the smallest index for which neither $\Delta_m^{(X_1)}$ nor $\Delta_m^{(X_2)}$ vanishes identically. Therefore, in (6.42) the same holds for $n \geq 2$, and the calculations made below do not require a case distinction. The statements of Theorem 6.3.1 for p_2/q_2 and p_0/q_0 have to be proved separately later. We have from (6.41) and (6.42) to (6.44):

$$\begin{aligned} D_1 = -\sum_{\mu=1}^{\lfloor (n+2)/2 \rfloor} \Big(& (1+X_2Y_1)Y_2(H_{n+1,\mu}^{(X_2)}-H_{n,\mu}^{(X_2)}) - (1+X_2Y_1)X_1H_{n+1,\mu}^{(X_2)} \\ & + (Y_1-X_1)Y_1Y_2(H_{n+1,\mu}^{(X_1)}-H_{n,\mu}^{(X_1)}) - (Y_1-X_1)X_1Y_1H_{n+1,\mu}^{(X_1)} \\ & - (Y_1-X_1)Y_1H_{n+1,\mu}\Big) \end{aligned} \tag{6.45}$$

In the following, let $m \geqslant 2$ and $1 \leqslant \mu \leqslant (m+1)/2$ (if m is odd) and $1 \leqslant \mu \leqslant m/2$ (if m is even). We obtain from (6.43):

$$\begin{aligned} H_{m,\mu}^{(X_1)} &= H_{m,\mu}^{(X_1)}(X_1,X_2) := \frac{\partial H_{m,\mu}(X_1,X_2)}{\partial X_1} \\ &= \frac{1}{2^{m-1}}\binom{m}{2\mu-1}\big((\mu-1)X_2(X_1X_2)^{\mu-2}(4+X_1X_2)^{\mu-1}(2+X_1X_2)^{m+1-2\mu} \\ &\quad +(\mu-1)(X_1X_2)^{\mu-1}X_2(4+X_1X_2)^{\mu-2}(2+X_1X_2)^{m+1-2\mu} \\ &\quad +(m+1-2\mu)(X_1X_2)^{\mu-1}(4+X_1X_2)^{\mu-1}X_2(2+X_1X_2)^{m-2\mu}\big)\,. \end{aligned} \tag{6.46}$$

Note that for $\mu = 1$ the formula for the partial derivative of $H_{m,1}(X_1,X_2)$ with respect to X_1 takes the form

$$H_{m,1}^{(X_1)} = \frac{m(m-1)}{2^{m-1}}X_2(2+X_1X_2)^{m-2}\,. \tag{6.47}$$

Additionally we obtain the identity

$$X_1H_{m,\mu}^{(X_1)}(X_1,X_2) = X_2H_{m,\mu}^{(X_2)}(X_1,X_2)\,, \tag{6.48}$$

which follows from (6.43) by the chain rule for derivatives.

In the following we prepare a procedure as described in the section 6.2. Here we will choose $\alpha_1 = 2$ and $\alpha_2 = -2$. We obtain from (6.43), (6.46), (6.47) and (6.48):

$$H_{m,1}(2,-2) = \frac{1}{2^{m-1}}\binom{m}{1}(-2)^{m-1} = (-1)^{m-1}m\,, \tag{6.49}$$

$$H_{m,\mu}(2,-2) = 0 \qquad (\mu \geqslant 2)\,, \tag{6.50}$$

$$H_{m,1}^{(X_1)}(2,-2) = \frac{m(m-1)}{2^{m-1}}(-2)(-2)^{m-2} = (-1)^{m-1}m(m-1)\,, \tag{6.51}$$

$$H_{m,1}^{(X_2)}(2,-2) = (-1)^m m(m-1)\,, \tag{6.52}$$

$$H_{m,2}^{(X_1)}(2,-2) = \frac{1}{2^{m-1}}\binom{m}{3}(-4)(-2)(-2)^{m-3} = 2(-1)^{m-1}\binom{m}{3}, \tag{6.53}$$

$$H_{m,2}^{(X_2)}(2,-2) = 2(-1)^m\binom{m}{3}, \tag{6.54}$$

$$H_{m,\mu}^{(X_j)}(2,-2) = 0 \qquad (\mu \geqslant 3,\ j=1,2)\,. \tag{6.55}$$

Next, we substitute the values from (6.49) to (6.55) into (6.45), where m is replaced by n and $n+1$, respectively. Note that $\lfloor (m+1)/2 \rfloor = \lfloor (n+2)/2 \rfloor \geqslant 2$ holds by our assumption $n \geq 2$. We obtain

$$
\begin{aligned}
D_1(2,-2) &= -(1-2Y_1)Y_2(H^{(X_2)}_{n+1,1}+H^{(X_2)}_{n+1,2}-H^{(X_2)}_{n,1}-H^{(X_2)}_{n,2}) \\
&\quad +2(1-2Y_1)(H^{(X_2)}_{n+1,1}+H^{(X_2)}_{n+1,2}) \\
&\quad -(Y_1-2)Y_1Y_2(H^{(X_1)}_{n+1,1}+H^{(X_1)}_{n+1,2}-H^{(X_1)}_{n,1}-H^{(X_1)}_{n,2}) \\
&\quad +2(Y_1-2)Y_1(H^{(X_1)}_{n+1,1}+H^{(X_1)}_{n+1,2}) \\
&\quad +(Y_1-2)Y_1H_{n+1,1} \\
&= (2Y_1-1)Y_2\left((-1)^{n+1}n(n+1)+2(-1)^{n+1}\binom{n+1}{3}\right. \\
&\quad \left.-(-1)^n(n-1)n-2(-1)^n\binom{n}{3}\right) \\
&\quad +2(1-2Y_1)\left((-1)^{n+1}n(n+1)+2(-1)^{n+1}\binom{n+1}{3}\right) \\
&\quad -(Y_1-2)Y_1Y_2\left((-1)^{n}n(n+1)+2(-1)^{n}\binom{n+1}{3}\right. \\
&\quad \left.-(-1)^{n-1}(n-1)n-2(-1)^{n-1}\binom{n}{3}\right) \\
&\quad +2(Y_1-2)Y_1\left((-1)^{n}n(n+1)+2(-1)^{n}\binom{n+1}{3}\right) \\
&\quad +(Y_1-2)Y_1(-1)^n(n+1)(-1)^{n+1} \\
&\quad \left((2Y_1-1)Y_2\left(n(n+1)+2\binom{n+1}{3}+(n-1)n+2\binom{n}{3}\right)\right. \\
&\quad +2(1-2Y_1)\left(n(n+1)+2\binom{n+1}{3}\right) \\
&\quad +(Y_1-2)Y_1Y_2\left(n(n+1)+2\binom{n+1}{3}+(n-1)n+2\binom{n}{3}\right) \\
&\quad -2(Y_1-2)Y_1\left(n(n+1)+2\binom{n+1}{3}\right) \\
&\quad \left.-(Y_1-2)Y_1(n+1)\right) \\
&= \frac{(-1)^{n+1}(n+1)}{3}\left((Y_1^2Y_2-Y_2)n(2n+1)\right. \\
&\quad \left.+(2-2Y_1^2)n(n+2)+3(2Y_1-Y_1^2)\right) \qquad (6.56)
\end{aligned}
$$

We need to evaluate the polynomials P_1 and P_2 from (6.39) and (6.40), respectively, at the point $(X_1, X_2) = (2, -2)$. For the polynomial P_1 we get immediately

$$P_1(2, -2, Y_1) = 4Y_1 - 2Y_1^2 - 2\,. \tag{6.57}$$

For P_2, we obtain from (6.41), (6.43), (6.49) and (6.50) that

$$\begin{aligned} \Delta_{n+1}(2,-2) &= (-1)^n(n+1)\,, \\ \Delta_n(2,-2) &= (-1)^{n-1}n\,. \end{aligned}$$

Therefore,

$$P_2(2,-2,Y_2) = (-1)^n\big((2n+1)Y_2 - 2(n+1)\big)\,.$$

Now we assume for the functional determinant D_1 in (6.42) that

$$D_1(x_1, x_2, y_1, y_2) = 0 \tag{6.58}$$

holds. Additionally, we know from (6.39) and (6.40) that

$$\left.\begin{aligned} P_1(x_1, x_2, y_1) &= 0\,, \\ P_2(x_1, x_2, y_2) &= 0\,. \end{aligned}\right\} \tag{6.59}$$

Now we consider the following polynomials in one variable each (for Δ_m from (6.37) with α and β replaced respectively by x_1 and x_2):

$$\left.\begin{aligned} D_1(x_1, x_2, Y_1, y_2) &\in \mathbb{Q}(x_1, x_2, y_2)[Y_1] \subseteq \tilde{\mathbb{Q}}(x_1, x_2, y_2)[Y_1]\,, \\ P_1(x_1, x_2, Y_1) &\in \mathbb{Q}(x_1, x_2)[Y_1] \subseteq \tilde{\mathbb{Q}}(x_1, x_2)[Y_1]\,, \\ P_2(x_1, x_2, Y_2) &\in \mathbb{Q}(x_1, x_2)[Y_2] \subseteq \tilde{\mathbb{Q}}(x_1, x_2)[Y_2]\,. \end{aligned}\right\} \tag{6.60}$$

Thus, a situation is now given as described at the beginning of subsection 6.2. It now will be necessary to guarantee the non-vanishing of $D_1(x_1, x_2, y_1, y_2)$ with the help of Lemma 6.2.1. Because of (6.58) to (6.60) we obtain by using resultants

$$P_3(x_1, x_2, y_2) := \mathrm{Res}_{Y_1}\big(D_1(x_1, x_2, Y_1, y_2), P_1(x_1, x_2, Y_1)\big) = 0\,,$$

and

$$P_4(x_1, x_2) := \mathrm{Res}_{Y_2}\big(P_3(x_1, x_2, Y_2), P_2(x_1, x_2, Y_2)\big) = 0\,.$$

Because of $P_4(x_1,x_2) \in \tilde{\mathbb{Q}}(x_1,x_2)$ and the presupposed algebraic independence of x_1 and x_2 over $\tilde{\mathbb{Q}}$, the latter is possible only for $P_4 \equiv 0$.

In particular, we can rewrite (6.56) in terms of the coefficients

$$\begin{aligned} C_n &= \frac{(-1)^{n+1}(n+1)}{3}, \\ A_n &= n(2n+1)Y_2 - 2n(n+2) - 3, \\ B_n &= -n(2n+1)Y_2 + 2n(n+2) \end{aligned} \tag{6.61}$$

obtaining $D_1 = A_nC_nY_1^2 + 6C_nY_1 + B_nC_n$.
The solutions of (6.56) can be written using (6.61) obtaining

$$\begin{aligned} a_1 &= -\frac{3}{A_n} + \sqrt{\frac{9}{A_n^2} - \frac{B_n}{A_n}}, \\ a_2 &= -\frac{3}{A_n} - \sqrt{\frac{9}{A_n^2} - \frac{B_n}{A_n}}, \end{aligned}$$

whereas the solutions of the polynomial P_1 are $b_1 = b_2 = 1$.
Applying the definition of the resultants, it follows

$$\begin{aligned} P_3\big(2,-2,Y_2\big) &= (A_nC_n)^2(-2)^2(a_1-b_1)(a_1-b_2)(a_2-b_1)(a_2-b_2) \\ &= 4A_n^2C_n^2\left(-\frac{3}{A_n} - 1 + \sqrt{\frac{9}{A_n^2} - \frac{B_n}{A_n}}\right)^2\left(-\frac{3}{A_n} - 1 - \sqrt{\frac{9}{A_n^2} - \frac{B_n}{A_n}}\right)^2 \\ &= 4A_n^2C_n^2\left(\frac{6-3}{A_n}\right)^2 \\ &= 4(n+1)^2. \end{aligned}$$

Applying the same reasoning for $Res_{Y_2}(P_2,P_3)$ we have

$$P_4\big(2,-2\big) = 4(n+1)^2 \neq 0. \tag{6.62}$$

Formula (6.62) contradicts $P_4 \equiv 0$. So $D_1(x_1,x_2,y_1,y_2)$ does not vanish in (6.58), and so the algebraic independence of $\xi = [\overline{\alpha,\beta}]$ and p_{2n}/q_{2n} over $\tilde{\mathbb{Q}}$ for $n \geqslant 2$ follows by Theorem 6.1.1 with $\mathbb{K} = \tilde{\mathbb{Q}}$. Now we prove Theorem 6.3.1 for ξ and convergents p_{2n+1}/q_{2n+1} with odd index, so that we assume $n \geqslant 1$ in the following.

As the argument is similar to the even case, we omit some calculations.
The polynomial $P_1\left(X_1,X_2,Y_1\right)$ does not change, whereas since now we are considering convergents with odd index we define a new polynomial. Let

$$y_2 := \frac{p_{2n+1}}{q_{2n+1}} \overset{(6.38)}{=} \frac{\Delta_{n+2}-\Delta_{n+1}}{\beta\Delta_{n+1}}.$$

Hence, the polynomial

$$P_2\left(X_1,X_2,Y_2\right) := \Delta_{n+1}X_2Y_2 - \left(\Delta_{n+2}-\Delta_{n+1}\right) \tag{6.63}$$

vanishes for $X_1 = x_1$, $X_2 = x_2$, and $Y_2 = y_2$, where $\Delta_m = \Delta_m(X_1,X_2)$ with $m \in \{n+1, n+2\}$.
Applying the same reasoning of the case of the convergents with even indexes, we obtain

$$\frac{\partial P_1}{\partial X_1} \overset{(6.39)}{=} -X_2Y_1 - 1\,,$$

$$\frac{\partial P_1}{\partial X_2} \overset{(6.39)}{=} Y_1^2 - X_1Y_1\,,$$

$$\frac{\partial P_2}{\partial X_1} \overset{(6.63)}{=} X_2Y_2\Delta_{n+1}^{(X_1)} - \Delta_{n+2}^{(X_1)} + \Delta_{n+1}^{(X_1)}\,,$$

$$\frac{\partial P_2}{\partial X_2} \overset{(6.63)}{=} Y_2\Delta_{n+1} + X_2Y_2\Delta_{n+1}^{(X_2)} - \Delta_{n+2}^{(X_2)} + \Delta_{n+1}^{(X_2)}\,.$$

With these partial derivatives we calculate the following functional determinant

$$\begin{aligned} D_2 = D_2\left(X_1,X_2,Y_1,Y_2\right) &:= -(1+X_2Y_1)\left(Y_2\Delta_{n+1} + X_2Y_2\Delta_{n+1}^{(X_2)} - \Delta_{n+2}^{(X_2)} + \Delta_{n+1}^{(X_2)}\right) \\ &\quad -\left(Y_1^2 - X_1Y_1\right)\left(X_2Y_2\Delta_{n+1}^{(X_1)} - \Delta_{n+2}^{(X_1)} + \Delta_{n+1}^{(X_1)}\right). \end{aligned} \tag{6.64}$$

Next, we substitute the values from (6.49) to (6.55) into (6.64), where m is replaced by $n+1$ and $n+2$, respectively and we obtain

$$\begin{aligned} D_2(2,-2) &= -(1-2Y_1)Y_2H_{n+1,1} + 2(1-Y_2)(H_{n+1,1}^{(X_2)} + H_{n+1,2}^{(X_2)}) \\ &\quad + (1-2Y_1)(H_{n+2,1}^{(X_2)} + H_{n+2,2}^{(X_2)} - H_{n+1,1}^{(X_2)} - H_{n+1,2}^{(X_2)}) \end{aligned}$$

$$
\begin{aligned}
&+ 2(Y_1^2 - 2Y_1)Y_2(H_{n+1,1}^{(X_1)} + H_{n+1,2}^{(X_1)}) \\
&+ (Y_1^2 - 2Y_1)(H_{n+2,1}^{(X_1)} + H_{n+2,2}^{(X_1)}) \\
&- (Y_1^2 - 2Y_1)(H_{n+1,1}^{(X_1)} + H_{n+1,2}^{(X_1)}) \\
&= \frac{(-1)^n(n+1)}{3}\big(6 - 6Y_1^2 + 2n^2(-1+Y_1^2)(-1+Y_2) \\
&- 3Y_2 + 6Y_1Y_2 + n(-1+Y_1^2)(-7+4Y_2)\big)
\end{aligned} \tag{6.65}
$$

We need to evaluate the polynomials P_1 and P_2 from (6.39) and (6.40), respectively, at the point $(X_1, X_2) = (2, -2)$. For the polynomial P_1 we have the result (6.57). For P_2, we obtain from (6.41), (6.43), (6.49) and (6.50) that

$$
\begin{aligned}
\Delta_{n+1}(2,-2) &= (-1)^n(n+1)\,, \\
\Delta_{n+2}(2,-2) &= (-1)^{n-1}(n+2)\,.
\end{aligned}
$$

Therefore,

$$
P_2(2,-2,Y_2) = (-1)^n\big(-(n+1)Y_2 + 2n + 3\big)\,. \tag{6.66}
$$

Now we assume for the functional determinant D_2 in (6.64) that

$$
D_2(x_1, x_2, y_1, y_2) = 0 \tag{6.67}
$$

holds. Additionally, we know from (6.39) and (6.40) that

$$
\left.
\begin{aligned}
P_1(x_1, x_2, y_1) &= 0\,, \\
P_2(x_1, x_2, y_2) &= 0\,.
\end{aligned}
\right\} \tag{6.68}
$$

Now we consider the following polynomials in one variable each (for $\Delta_m \in \mathbb{Q}[x_1, x_2]$ see (6.37)):

$$
\left.
\begin{aligned}
D_2(x_1, x_2, Y_1, y_2) &\in \mathbb{Q}(x_1, x_2, y_2)[Y_1] \subseteq (x_1, x_2, y_2)[Y_1]\,, \\
P_1(x_1, x_2, Y_1) &\in \mathbb{Q}(x_1, x_2)[Y_1] \subseteq \tilde{\mathbb{Q}}(x_1, x_2)[Y_1]\,, \\
P_2(x_1, x_2, Y_2) &\in \mathbb{Q}(x_1, x_2)[Y_2] \subseteq \tilde{\mathbb{Q}}(x_1, x_2)[Y_2]\,.
\end{aligned}
\right\} \tag{6.69}
$$

Also in this case, a situation is now given as described at the beginning of subsection 6.2. It now will be necessary to guarantee the non-vanishing of $D_2(x_1, x_2, y_1, y_2)$ with the help of Lemma 6.2.1. Because of (6.67) to (6.69) we obtain by using

resultants

$$P_3(x_1,x_2,y_2) := \mathrm{Res}_{Y_1}\big(D_2(x_1,x_2,Y_1,y_2), P_1(x_1,x_2,Y_1)\big) = 0\,,$$

and

$$P_4(x_1,x_2) := \mathrm{Res}_{Y_2}\big(P_3(x_1,x_2,Y_2), P_2(x_1,x_2,Y_2)\big) = 0\,.$$

Because of $P_4(x_1,x_2) \in \tilde{\mathbb{Q}}(x_1,x_2)$ and the presupposed algebraic independence of x_1 and x_2 over $\tilde{\mathbb{Q}}$, the latter is possible only for $P_4 \equiv 0$.

However, we obtain with (6.65), (6.57) and (6.66):

$$P_3\big(2,-2,Y_2\big) = 4(n+1)^2Y_2^2\,,$$

and hereby finally

$$P_4\big(2,-2\big) = 4(3+5n+2n^2)^2 \neq 0\,. \tag{6.70}$$

Formula (6.70) contradicts $P_4 \equiv 0$. So $D_2(x_1,x_2,y_1,y_2)$ does not vanish in (6.58), and so it follows by Theorem 6.1.1 with $\mathbb{K} = \tilde{\mathbb{Q}}$ the algebraic independence of $\xi = [\overline{\alpha,\beta}]$ and p_{2n+1}/q_{2n+1} over $\tilde{\mathbb{Q}}$ for $n \geqslant 0$.

In the following we want to study the particular cases of the convergents p_0/q_0, p_1/q_1 and p_2/q_2.

In particular, from equations (2.5) and (2.6) we have

$$y_2 := \frac{p_0}{q_0} = \alpha$$

so we can define the polynomial

$$P_2\big(X_1,X_2,Y_2\big) := X_1 - Y_2.$$

From the fact that $y_1 > 1$ and $x_1 - y_1 < 0$, we have

$$D_3 = D_3\big(X_1,X_2,Y_1,Y_2\big) := -\big(Y_1^2 - X_1Y_1\big) = Y_1(X_1 - Y_1) < 0.$$

For the case of p_1/q_1 we have

$$y_2 := \frac{p_1}{q_1} = \frac{\alpha\beta+1}{\beta}$$

so we can define the polynomials

$$P_2\big(X_1,X_2,Y_2\big) := X_2Y_2 - X_1X_2 - 1,$$

$$D_4 = D_4\big(X_1,X_2,Y_1,Y_2\big) := X_1 + X_2Y_1^2 - Y_2 - X_2Y_1Y_2.$$

In particular, it follows that

$$D_4(2,-2,Y_1,Y_2) = 2 - 2Y_1^2 - Y_2 + 2Y_1Y_2$$

and that

$$P_2(2,-2,Y_1,Y_2) = 3 - 2Y_2.$$

Repeating the same reasoning of the convergents with even or odd indexes, we have

$$P_3(2,-2,Y_2) = 4Y_2^2,$$

$$P_4(2,-2,Y_2) = 36 \neq 0.$$

For the case of p_2/q_2 we have

$$y_2 := \frac{p_2}{q_2} = \frac{\alpha^2\beta + 2\alpha}{\alpha\beta + 1}$$

the corresponding polynomial is

$$P_2\big(X_1,X_2,Y_2\big) := (X_1X_2 + 1)Y_2 - (X_1^2X_2 + 2X_1).$$

We have

$$D_5 = D_5\big(X_1,X_2,Y_1,Y_2\big) := X_1^2 - 2X_1Y_1 - X_1Y_2 - X_1^2X_2Y_1 + 2X_1X_2Y_1^2 - X_2Y_1^2Y_2 + 2Y_1^2.$$

In particular, it follows that

$$D_5(2,-2,Y_1,Y_2) = 4 + 4Y_1 - 6Y_1^2 - 2Y_2 + 2Y_1^2Y_2$$

and that

$$P_2(2,-2,Y_1,Y_2) = -3Y_2 + 4.$$

Repeating the same reasoning of the convergents with even or odd indexes, we have

$$P_3(2,-2,Y_2) = 16\,,$$

$$P_4(2,-2,Y_2) = 16 \neq 0\,.$$

This completes the proof of Theorem 6.3.1. □

Remark 6.3.2. Theorem 6.3.1 can also be proved in a short and alternative way, without using the criterion set out in the Theorem 6.1.1. The main idea of this alternative proof is to define rational functions from equations 6.21, 6.22, 6.27, from which it follows that $\text{tr.deg}\,(\tilde{\mathbb{Q}}(\alpha,\beta,\xi,p_{2n}/q_{2n}) : \tilde{\mathbb{Q}}(\xi,p_{2n}/q_{2n})) = 0$ that implies the following degree of transcendence $\text{tr.deg}\,(\tilde{\mathbb{Q}}(\xi,p_{2n}/q_{2n}) : \tilde{\mathbb{Q}}) = 2$. However, the proof of Theorem 6.3.1 presented in this manuscript, which uses the algebraic independence criterion, also allows for handling the more general case $\xi := [\overline{T_1(\alpha,\beta),\ldots,T_w(\alpha,\beta)}]$ with $w \geq 2$, $T_1,\ldots,T_w \in \mathbb{Q}[X_1,X_2]$ and $\alpha,\beta \in \mathbb{R}$ algebraically independent numbers over the field $\mathbb{Q}$. In this dissertation, we choose to present this proof, rather than the shorter one, to provide the reader with an idea of how to apply the criterion to prove the algebraic independence between ξ and its convergents also in the more general case $\xi := [\overline{T_1(\alpha,\beta),\ldots,T_w(\alpha,\beta)}]$.

Remark 6.3.3. Theorem 6.3.1 does not longer hold in the case of period 1, so when

$$y_1 = [\overline{\alpha}] = \frac{\alpha}{2} + \frac{1}{2}\sqrt{4+\alpha^2}\,.$$

In this case we have

$$y_2 = \frac{p_0}{q_0} = \frac{\alpha}{1} = \alpha,$$

so there is an algebraic dependence over $\mathbb{Q}$ between y_1 and y_2 due to the following relation

$$y_1^2 - y_1 y_2 - 1 = 0\,.$$

Let $n \geq 2$, and let $a_0,\ldots,a_{n-1}$ be positive real numbers, where $a_0 \geqslant 1$. Asuume that, among $a_0,\ldots,a_{n-1}$ there are at least two numbers, a_μ and a_ν with $0 \leqslant \mu < \nu \leqslant n-1$, say, which are algebraically independent over $\mathbb{Q}$. In terms of the transcendence

degree, this means that

$$\text{tr.deg}\,(\mathbb{Q}(a_0,\ldots,a_{n-1}):\mathbb{Q}) \geqslant 2\,. \tag{6.71}$$

Next, we introduce the field $\tilde{\mathbb{Q}}$ by the field extension

$$\tilde{\mathbb{Q}} := \mathbb{Q}\big(a_0,\ldots,a_{\mu-1},a_{\mu+1},\ldots,a_{\nu-1},a_{\nu+1},\ldots,a_{n-1}\big)\,.$$

Let p_m^*/q_m^* be the mth convergent of the number

$$\xi := \big[\overline{a_0,\ldots,a_{n-1}}\big]\,. \tag{6.72}$$

Since $a_0 \geqslant 1$ and $a_k > 0$ for $k = 1,\ldots,n-1$, we have

$$\frac{p_m^*}{q_m^*} > 1 \qquad (m \geqslant 1)\,. \tag{6.73}$$

Both, the terms p_m^* and q_m^*, depend on $a_0,\ldots,a_m$ for all $m \geqslant 0$. We write

$$\begin{aligned} p_m^* &= p_m^*(x_0,\ldots,x_m), \qquad \text{for} \quad x_k = a_k \quad (0 \leqslant k \leqslant m)\,,\\ q_m^* &= q_m^*(x_0,\ldots,x_m), \qquad \text{for} \quad x_k = a_k \quad (0 \leqslant k \leqslant m)\,. \end{aligned}$$

Finally, we assume that

$$\det\left(\begin{array}{cc} \dfrac{\partial}{\partial x_\mu}\left(\dfrac{p_{n-1}^*-q_{n-2}^*}{q_{n-1}^*}\right) & \dfrac{\partial}{\partial x_\nu}\left(\dfrac{p_{n-1}^*-q_{n-2}^*}{q_{n-1}^*}\right) \\[2ex] \dfrac{\partial}{\partial x_\mu}\left(\dfrac{p_{n-1}^*-q_{n-2}^*}{p_{n-2}^*}\right) & \dfrac{\partial}{\partial x_\nu}\left(\dfrac{p_{n-1}^*-q_{n-2}^*}{p_{n-2}^*}\right) \end{array}\right)_{\substack{x_\nu = a_\nu \\ 0 \leqslant \nu \leqslant n-1}} \neq 0\,, \tag{6.74}$$

where

$$\frac{p_{n-1}^*}{q_{n-1}^*} = [a_0,a_1,\ldots,a_{n-1}] \quad \text{and} \quad \frac{p_{n-2}^*}{q_{n-2}^*} = [a_0,a_1,\ldots,a_{n-2}]\,. \tag{6.75}$$

In the following theorem, using the results obtained in Theorem 6.3.1, we derive further results regarding algebraic independence.

Theorem 6.3.4. *Let all the quantities defined above satisfy the conditions in (6.71) to (6.75). Then there exist two positive real numbers α and β such that α and β are algebraically independent over $\tilde{\mathbb{Q}}$, and the two numbers ξ and p_n/q_n are algebraically independent over $\tilde{\mathbb{Q}}$ for every integer $n \geqslant 0$.*

Proof. From (6.72) we have the identity

$$\xi = \frac{p_{n-1}^*\xi + p_{n-2}^*}{q_{n-1}^*\xi + q_{n-2}^*},$$

which can be rearranged to the quadratic equation

$$q_{n-1}^*\xi^2 - (p_{n-1}^* - q_{n-2}^*)\xi - p_{n-2}^* = 0.$$

Solving this equation for the positive number ξ yields

$$\xi = \frac{p_{n-1}^* - q_{n-2}^*}{2q_{n-1}^*} + \sqrt{\frac{(p_{n-1}^* - q_{n-2}^*)^2}{4q_{n-1}^{*2}} + \frac{p_{n-2}^*}{q_{n-1}^*}} = R_1 + \sqrt{R_2}, \tag{6.76}$$

where

$$R_1 := \frac{p_{n-1}^* - q_{n-2}^*}{2q_{n-1}^*} \quad \text{and} \quad R_2 := R_1^2 + \frac{p_{n-2}^*}{q_{n-1}^*}.$$

Set

$$\alpha := \frac{p_{n-1}^* - q_{n-2}^*}{q_{n-1}^*} \quad \text{and} \quad \beta := \frac{p_{n-1}^* - q_{n-2}^*}{p_{n-2}^*}. \tag{6.77}$$

We obtain from (6.73) for $m = n-1 \geqslant 1$ that $p_{n-1}^* > q_{n-1}^* \geqslant q_{n-2}^*$. Therefore, α and β are positive real numbers. From the combination of Theorem 6.1.7 and 6.1.8, due to the assumed nonvanishing of the determinant in (6.74), we have the algebraic independence of the two numbers α and β over $\tilde{\mathbb{Q}}$.

Since

$$R_1 = \frac{\alpha}{2} \quad \text{and} \quad R_2 = \frac{\alpha^2}{4} + \frac{\alpha}{\beta},$$

we obtain from the equations (6.76) and (6.19) that

$$\xi = R_1 + \sqrt{R_2} = \frac{\alpha}{2} + \sqrt{\frac{\alpha^2}{4} + \frac{\alpha}{\beta}} = y_1 = [\overline{\alpha, \beta}]. \tag{6.78}$$

The remaining statement in Theorem 6.3.4 on the algebraic independence of ξ and p_n/q_n over $\tilde{\mathbb{Q}}$ for $n \geqslant 0$ follows from Theorem 6.3.1. □

Remark 6.3.5. The convergents p_m^*/q_m^* of ξ depend on $a_0, \ldots, a_{n-1}$, while the convergents p_m/q_m of ξ depend only on α and β. The convergents p_m^*/q_m^* are in general completely different from the convergents p_m/q_m, although they approximate the same number ξ. This effect occurs because we are not dealing with continued fractions whose partial quotients are natural numbers. If one tries to generalize Theorem 6.3.1 to a continued fraction with period length greater than two, our method of prove will become very complicated. Theorem 6.3.4 reduces this type of continued fraction to one with period length two and we obtain such a result for the convergents p_m/q_m instead of p_m^*/q_m^*.

6.3.1 Some supplementary results and their proofs

From the formulas (6.72), (6.75), (6.77) and (6.78) we obtain an explicit formula to transform the regular continued fraction $\xi = [b_0, \overline{b_1, \ldots, b_n}]$ of a quadratic irrational number ξ into a non-regular continued fraction with a small preperiod and a period of length one. Here, b_0 and $b_\nu \geqslant 1$ for $1 \leqslant \nu \leqslant n$ are integers.

For this result, we additionally need an identity between a periodic regular continued fraction with rational partial quotients and a non-regular continued fraction with integer denominators and numerators.
Let a/b and c/d be rationals with $a, c \in \mathbb{Z} \setminus \{0\}$ and $b, d \in \mathbb{N}$. Then, we have

$$\left[\overline{\frac{a}{b}, \frac{c}{d}}\right] = \frac{a}{b} + \cfrac{1}{\frac{c}{d} + \cfrac{1}{\frac{a}{b} + \cfrac{1}{\frac{c}{d} + \ddots}}}$$

$$
\begin{aligned}
&= \frac{a}{b} + \cfrac{d}{c + \cfrac{bd}{a + \cfrac{bd}{c + \cfrac{bd}{\ddots}}}} \\
&= \frac{a}{b} + \cfrac{d}{c + \left[\overline{\frac{bd}{a}, \frac{bd}{c}}\right]} \\
&= \frac{a}{b} + \left[\overline{\frac{d}{c}, \frac{bd}{a}, \frac{bd}{c}}\right].
\end{aligned}
$$

In the special case of $a = c$ this identity assumes the simple form

$$
\left[\overline{\frac{a}{b}, \frac{a}{d}}\right] = \frac{a}{b} + \left[\overline{\frac{d}{a}, \frac{bd}{a}}\right]. \tag{6.79}
$$

Shifting the index in (6.75), we have with

$$
\frac{p_n^*}{q_n^*} = \left[b_1, \ldots, b_n\right] \quad \text{and} \quad \frac{p_{n-1}^*}{q_{n-1}^*} = \left[b_1, \ldots, b_{n-1}\right]
$$

the equation

$$
\left[\overline{b_1, \ldots, b_n}\right] = \left[\overline{\frac{p_n^* - q_{n-1}^*}{q_n^*}, \frac{p_n^* - q_{n-1}^*}{p_{n-1}^*}}\right], \tag{6.80}
$$

which results from (6.72), (6.77) and (6.78). Combining (6.79) and (6.80), we obtain

$$
\begin{aligned}
\xi &= \left[b_0, \overline{b_1, \ldots, b_n}\right] \\
&= b_0 + \left[0, \overline{b_1, \ldots, b_n}\right] \\
&= b_0 + \frac{1}{\left[\overline{b_1, \ldots, b_n}\right]}
\end{aligned}
$$

$$
\begin{aligned}
&\overset{(6.80)}{=} b_0 + \frac{1}{\left[\overline{\frac{p_n^* - q_{n-1}^*}{q_n^*}, \frac{p_n^* - q_{n-1}^*}{p_{n-1}^*}}\right]} \\
&\overset{(6.79)}{=} b_0 + \frac{1}{\frac{p_n^* - q_{n-1}^*}{q_n^*} + \left[\frac{p_{n-1}^*}{p_n^* - q_{n-1}^*} + \overline{\frac{p_{n-1}^* q_n^*}{p_n^* - q_{n-1}^*}}\right]} \\
&= b_0 + \frac{q_n^*}{p_n^* - q_{n-1}^* + \left[\frac{p_{n-1}^* q_n^*}{p_n^* - q_{n-1}^*} + \overline{\frac{p_{n-1}^* q_n^*}{p_n^* - q_{n-1}^*}}\right]} \\
&= b_0 + \left[\frac{q_n^*}{p_n^* - q_{n-1}^*} + \overline{\frac{p_{n-1}^* q_n^*}{p_n^* - q_{n-1}^*}}\right] \\
&= b_0 + \cfrac{q_n^*}{p_n^* - q_{n-1}^* + \cfrac{p_{n-1}^* q_n^*}{p_n^* - q_{n-1}^* + \cfrac{p_{n-1}^* q_n^*}{p_n^* - q_{n-1}^* + \ddots}}}.
\end{aligned}
$$

For example,

$$
\sqrt{19} = \left[4, \overline{2,1,3,1,2,8}\right] = 4 + \cfrac{117}{312 + \cfrac{4563}{312 + \cfrac{4563}{312 + \ddots}}} = 4 + \left[\frac{117}{312} + \overline{\frac{4563}{312}}\right],
$$

since

$$
\frac{p_6}{q_6} = \left[2,1,3,1,2,8\right] = \frac{326}{117} \quad \text{and} \quad \frac{p_5}{q_5} = \left[2,1,3,1,2\right] = \frac{39}{14}.
$$

Example 6.3.6. An interesting special case of Theorem 6.3.4 is given when the Hurwitz period of ξ is composed of only two algebraically independent numbers α^*

and β^* over $\mathbb{Q}$. For this we consider the following two examples.

(i) Let $\xi := [\overline{\alpha^*, \beta^*, \beta^*, \alpha^*}]$.
With $n = 4$ we have by $a_0 = a_3 = \alpha$ and $a_1 = a_2 = \beta$. Then, we obtain with (6.77),

$$\alpha := \frac{p_3^* - q_2^*}{q_3^*} = \frac{\alpha^{*2}\beta^{*2} + \alpha^{*2} - \beta^{*2} + 2\alpha^*\beta^*}{\alpha^*\beta^{*2} + \alpha^* + \beta^*} = \frac{p_3^* - q_2^*}{p_2^*} =: \beta\,.$$

Due to $\alpha = \beta$, the algebraic independence of these two quantities is not given; the determinant in (6.74) vanishes. Theorem 6.3.4 is not applicable to this situation.

(ii) Next, let $\xi := [\overline{\alpha^*, \beta^*, \beta^*}]$.
With $n = 3$ we obtain

$$\begin{aligned} \alpha &:= \frac{p_2^* - q_1^*}{q_2^*} = \frac{\alpha^*\beta^{*2} + \alpha^*}{\beta^{*2} + 1} = \alpha^*\,, \\ \beta &:= \frac{p_2^* - q_1^*}{p_1^*} = \frac{\alpha^*\beta^{*2} + \alpha^*}{\alpha^*\beta^* + 1}\,. \end{aligned}$$

The determinant in (6.74) takes the value

$$\det \begin{pmatrix} \dfrac{\partial}{\partial x_0}(x_0) & \dfrac{\partial}{\partial x_1}(x_0) \\[2ex] \dfrac{\partial}{\partial x_0}\left(\dfrac{x_0x_1^2 + x_0}{x_0x_1 + 1}\right) & \dfrac{\partial}{\partial x_1}\left(\dfrac{x_0x_1^2 + x_0}{x_0x_1 + 1}\right) \end{pmatrix}_{\substack{x_0 = \alpha^* \\ x_1 = \beta^*}} = \frac{\alpha^*\left(\alpha^*\beta^{*2} - \alpha^* + 2\beta^*\right)}{\left(\alpha^*\beta^* + 1\right)^2}\,,$$

which does not vanish by the algebraic independence of α^* and β^* over $\tilde{\mathbb{Q}}$. Thus, Theorem 6.3.4 is applicable with

$$\xi = \left[\overline{\alpha^*, \beta^*, \beta^*}\right] = \left[\overline{\alpha^*, \frac{\alpha^*(\beta^{*2} + 1)}{\alpha^*\beta^* + 1}}\right].$$

We complete the application of the algebraic independence criterion to non regular continued fractions by the following proposition, for which we provide two different proofs.

Proposition 6.3.7. *Let $n \geq 1$ and let $a_0, \ldots, a_{n-1}$ be real algebraic independent numbers greater than 1. Then the convergents*

$$\frac{p_m}{q_m} = [a_0, a_1, \ldots, a_m] \qquad (0 \leq m \leq n-1) \tag{6.81}$$

of the continued fraction $[\overline{a_0, a_1, \ldots, a_{n-1}}]$ are algebraically independent over the field $\mathbb{Q}$ of rational numbers.

Proof. The first proof makes use of Theorem 6.1.7. We may consider p_m/q_m as a rational function formed by integer polynomials at the places $a_0, \ldots, a_m$. We compute these rational functions using the recurrence formulas (2.5) and (2.6). We have for $m = 0$ and $m = 1$

$$\frac{p_0}{q_0} = a_0\,, \qquad \frac{p_1}{q_1} = \frac{a_0 a_1 + 1}{a_1}\,, \tag{6.82}$$

for $m \geq 2$

$$\frac{p_m}{q_m} = \frac{a_m p_{m-1} + p_{m-2}}{a_m q_{m-1} + q_{m-2}}\,. \tag{6.83}$$

Note that by (6.81) the four numbers p_{m-1}, q_{m-1}, p_{m-2} and q_{m-2} do not depend on a_μ for $\mu = m+1, \ldots, n$. Since p_m/q_m is a rational function $R_m(X_0, \ldots, X_m)$ at the places $a_0, \ldots, a_m$, we have[1]

$$y_j := \frac{p_j}{q_j} = R_j\big(a_0, a_1, \ldots, a_j\big) \qquad (j = 0, \ldots, n-1)\,.$$

In order to prove the algebraic independence of $y_0, \ldots, y_{n-1}$ over $\mathbb{Q}$ we apply Theorem 6.1.7

$$\det_n\left(\frac{\partial R_j}{\partial X_i}(a_0, \ldots, a_{n-1})\right) = \begin{vmatrix} \dfrac{\partial R_0}{\partial X_0} & \cdots & \dfrac{\partial R_0}{\partial X_{n-1}} \\ \vdots & \vdots & \vdots \\ \dfrac{\partial R_{n-1}}{\partial X_0} & \cdots & \dfrac{\partial R_{n-1}}{\partial X_{n-1}} \end{vmatrix} (a_0, \ldots, a_{n-1})$$

[1] We change the index from m to j to adjust to the notation in Theorem 6.1.7.

$$
\begin{aligned}
&= \begin{vmatrix}
\frac{\partial R_0}{\partial X_0} & 0 & 0 & \dots & 0 \\
\frac{\partial R_1}{\partial X_0} & \frac{\partial R_1}{\partial X_1} & 0 & \dots & 0 \\
\frac{\partial R_2}{\partial X_0} & \frac{\partial R_2}{\partial X_1} & \frac{\partial R_2}{\partial X_2} & \dots & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots \\
\frac{\partial R_{n-1}}{\partial X_0} & \frac{\partial R_{n-1}}{\partial X_1} & \frac{\partial R_{n-1}}{\partial X_2} & \dots & \frac{\partial R_{n-1}}{\partial X_{n-1}}
\end{vmatrix} (a_0,\dots,a_n) \\
&= \prod_{j=0}^{n-1} \frac{\partial R_j}{\partial X_j}(a_0,\dots,a_j)\,. \qquad (6.84)
\end{aligned}
$$

We obtain from (6.82):

$$
\frac{\partial R_0(a_0)}{\partial X_0} = 1 = \frac{1}{q_0^2}\,, \qquad \frac{\partial R_1(a_0,a_1)}{\partial X_1} = \frac{a_0a_1-(a_0a_1+1)}{a_1^2} = -\frac{1}{a_1^2} = -\frac{1}{q_1^2}\,. \qquad (6.85)
$$

Similarly, using the quotient rule for the derivative in (6.83), we get for $j \geq 2$, respecting the remark made about (6.83):

$$
\begin{aligned}
\frac{\partial R_j(a_0,\dots,a_j)}{\partial X_j} &= \frac{p_{j-1}(a_jq_{j-1}+q_{j-2})-(a_jp_{j-1}+p_{j-2})q_{j-1}}{(a_jq_{j-1}+q_{j-2})^2} \\
&= \frac{p_{j-1}q_{j-2}-p_{j-2}q_{j-1}}{q_j^2} \\
&\overset{(2.7)}{=} \frac{(-1)^j}{q_j^2}\,. \qquad (6.86)
\end{aligned}
$$

With (6.85) and (6.86) the formula (6.84) changes into:

$$
\det_n\Big(\frac{\partial R_j}{\partial X_i}(a_0,\dots,a_{n-1})\Big) = \prod_{j=0}^{n-1}\frac{(-1)^j}{q_j^2} = (-1)^{(n-1)n/2}\prod_{j=0}^{n-1} q_j^{-2}\,. \qquad (6.87)
$$

At this point we insert a brief consideration of the nonvanishing of the q_j for $j = 0,\dots,n-1$. It is clear that $q_0 = 1$ and $q_1 = a_1 > 1$ do not vanish. By induction on

the index m, it then follows from the recurrence formula (2.6) that all denominators q_m are positive and thus nonzero.

The determinant in (6.87) does not vanish either, and with Theorem 6.1.7 the proof of our Proposition 6.3.7 is completed.

Now we prove the Proposition with no use of Theorem 6.1.7, but only with the use of some algebra notions. In particular, since the degree of transcendence of the field $\mathbb{Q}(a_0,\dots,a_{n-1})$ over $\mathbb{Q}$ is n, we have a chain of transcendental field extensions

$$\mathbb{Q} \subset \mathbb{Q}(a_0) \subset \mathbb{Q}(a_0,a_1) \subset \cdots \subset \mathbb{Q}(a_0,\dots,a_{n-2}) \subset \mathbb{Q}(a_0,\dots,a_{n-1}).$$

From the recurrence formulas of p_m and q_m we know for the generic convergents p_m/q_m that

$$c_m := \frac{p_m}{q_m} \in \mathbb{Q}(a_0,\dots,a_m) \setminus \mathbb{Q}(a_0,\dots,a_{m-1}) \qquad (0 \le m \le n).$$

By induction we will show that

$$\text{tr.deg}\left(\mathbb{Q}(c_0,\dots,c_\nu) : \mathbb{Q}\right) = \nu+1 \qquad (0 \le \nu \le n). \tag{6.88}$$

For $\nu = 0$ it follows that $\text{tr.deg}\left(\mathbb{Q}(c_0) : \mathbb{Q}\right) = \text{tr.deg}\left(\mathbb{Q}(a_0) : \mathbb{Q}\right) = 1$. Let us suppose that equation (6.88) is true for $0 \le \nu \le n-2$ and we want to prove that

$$\text{tr.deg}\left(\mathbb{Q}(c_0,\dots,c_{\nu+1}) : \mathbb{Q}\right) = \nu+2.$$

Let us assume the contrary, so there exists a polynomial $P \in \mathbb{Q}[X_0,\dots,X_{\nu+1}] \setminus \{0\}$ such that $P(c_0,\dots,c_{\nu+1}) = 0$. From the algebraic independence of $c_0,\dots,c_\nu$, it follows that the degree of the polynomial P with respect to the variable $X_{\nu+1}$ is greater than 0, otherwise we would have $P(c_0,\dots,c_\nu,0) = 0$, which is impossible. Now, let us consider the polynomial $\bar{P}(X_{\nu+1}) := P(c_0,\dots,c_\nu,X_{\nu+1}) \in \mathbb{Q}(c_0,\dots,c_\nu)[X_{\nu+1}]$. From the consideration above, the leading coefficient of $\bar{P}$ is a non-vanishing polynomial from $\mathbb{Q}[X_0,\dots,X_\nu]$, and when computed for $c_0,\dots,c_\nu$, it does not vanish. In other words,

$$\bar{P}[X_{\nu+1}] = P(c_0,\dots,c_\nu,X_{\nu+1}) \in \mathbb{Q}(a_0,\dots,a_\nu)[X_{\nu+1}] \setminus \{0\}. \tag{6.89}$$

From $P(c_0,\dots,c_{\nu+1})=0$ it should follow that $\bar{P}(c_{\nu+1})=P(c_0,\dots,c_\nu,c_{\nu+1})=0$, but this is not possible by (6.89) and the fact that $c_{\nu+1}=p_{\nu+1}/q_{\nu+1}$ is transcendental over $\mathbb{Q}(a_0,\dots,a_\nu)$. □

6.4 A numerical example

We want to show an interesting example about the Diophantine approximations with convergents of continued fractions having algebraic independent partial quotients. The four numbers $\sqrt{2},\sqrt{3},\sqrt{5},\sqrt{7}$ are linear independent over the rationals. By Lindemann's theorem it follows that the numbers $a_0=e^{\sqrt{2}}>1$, $a_1=e^{\sqrt{3}}>1$, $a_2=e^{\sqrt{5}}>1$, and $a_3=e^{\sqrt{7}}>1$ are algebraically independent over the rationals [60, page 71]. Let $n=4$, and set

$$\xi=[\overline{a_0,a_1,a_2,a_3}]=4.286912134558658401198114599 5\dots$$

where ξ is the positive root of the polynomial

$$P(x)=(a_1a_2a_3+a_1+a_3)x^2+(a_1a_2-a_0a_1a_2a_3-a_0a_1-a_0a_3-a_2a_3)x-a_0a_1a_2-a_0-a_2.$$

Its first four convergents are

$$\begin{aligned}
\frac{p_0}{q_0} &= e^{\sqrt{2}}=4.113250\dots,\\
\frac{p_1}{q_1} &= e^{\sqrt{2}}\bigl(1+e^{-\sqrt{2}-\sqrt{3}}\bigr)=4.290171\dots,\\
\frac{p_2}{q_2} &= e^{\sqrt{2}}\Bigl(1+\frac{e^{-\sqrt{2}-\sqrt{3}}}{1+e^{-\sqrt{3}-\sqrt{5}}}\Bigr)=4.286888\dots,\\
\frac{p_3}{q_3} &= e^{\sqrt{2}}\Bigl(1+\frac{e^{-\sqrt{2}-\sqrt{3}}+e^{-\sqrt{2}-\sqrt{3}-\sqrt{5}-\sqrt{7}}}{1+e^{-\sqrt{3}-\sqrt{5}}+e^{-\sqrt{5}-\sqrt{7}}}\Bigr)=4.286912\dots.
\end{aligned}$$

From the theory of regular continued fractions, in particular applying Theorem 2.2.8, one knows the following approximation quality of the convergents p_m/q_m

$$\Bigl|\xi-\frac{p_m}{q_m}\Bigr|\leqslant\frac{1}{q_mq_{m+1}}\qquad(m\geqslant 0)\,. \tag{6.90}$$

For example, we check (6.90) for $m = 2$ and $m = 3$

$$0.238634221\cdots\cdot 10^{-4} = \left|\xi - \frac{p_2}{q_2}\right| \leqslant \frac{1}{q_2 q_3} = 0.242554642\cdots\cdot 10^{-4},$$

$$0.392042084\cdots\cdot 10^{-6} = \left|\xi - \frac{p_3}{q_3}\right| \leqslant \frac{1}{q_3 q_4} = 0.408315495\cdots\cdot 10^{-6}.$$

References

[1] M. Abrate, S. Barbero, U. Cerruti, and N. Murru. Colored compositions, invert operator and elegant compositions with the "black tie". *Discrete Mathematics*, 335:1–7, 2014.

[2] G. Alecci, S. Barbero, and N. Murru. Some notes on the algebraic structure of linear recurrent sequences. *Ricerche di Matematica*, pages 1–17, 2023.

[3] G. Alecci, N. Murru, and C. Sanna. Zeckendorf representation of multiplicative inverses modulo a Fibonacci number. *Monatshefte für Mathematik*, 201(1):1–9, 2023.

[4] J. Artz and M. Rowell. A tiling approach to Fibonacci product identities. *Involve, a Journal of Mathematics*, 2(5):581–587, 2010.

[5] A. Baker. *Transcendental number theory*. Cambridge university press, 2022.

[6] C. Ballot. The p-adic valuation of Lucas sequences when p is a special prime, Fibonacci quart. 57 (2019), no. 3, 265–275. *Fibonacci Quart*, 57(3):265–275, 2019.

[7] S. Barbero, U. Cerruti, and N. Murru. On the operations of sequences in rings and binomial type sequences. *Ricerche di Matematica*, 67(2):911–927, 2018.

[8] S. Barbero, U. Cerruti, and N. Murru. Some combinatorial properties of the Hurwitz series ring. *Ricerche di Matematica*, 67:491–507, 2018.

[9] A. Benhissi. Ideal structure of Hurwitz series rings. *Beiträge zur Algebra und Geometrie*, 48(1):251–256, 2007.

[10] A. Benhissi and F. Koja. Basic properties of Hurwitz series rings. *Ricerche di matematica*, 61(2):255, 2012.

[11] A. T. Benjamin and S. S. Plott. A combinatorial approach to Fibonomial coefficients. *Fibonacci Quart.*, 46/47(1):7–9, 2008/09.

[12] C. Bennett, J. Carrillo, J. Machacek, and B. E. Sagan. Combinatorial interpretations of Lucas analogues of binomial coefficients and catalan numbers. *Annals of Combinatorics*, 24(3):503–530, 2020.

[13] G. Bergman. A number system with an irrational base. *Mathematics magazine*, 31(2):98–110, 1957.

[14] J. Brillhart, P. L. Montgomery, and R. D. Silverman. Tables of Fibonacci and Lucas factorizations. *Mathematics of Computation*, 50(181):251–260, 1988.

[15] E. Çakçak. A remark on the minimal polynomial of the product of linear recurring sequences. *Finite Fields and Their Applications*, 4(1):87–97, 1998.

[16] L. Capuano, F. Veneziano, and U. Zannier. An effective criterion for periodicity of ℓ-adic continued fractions. *Mathematics of Computation*, 88(318):1851–1882, 2019.

[17] U. Cerruti and F. Vaccarino. R-algebras of linear recurrent sequences. *Journal of Algebra*, 175(1):332–338, 1995.

[18] D. E. Daykin. Representation of natural numbers as sums of generalised Fibonacci numbers. *Journal of the London Mathematical Society*, 1(2):143–160, 1960.

[19] P. Demontigny, T. Do, A. Kulkarni, S. J. Miller, D. Moon, and U. Varma. Generalizing Zeckendorf's theorem to f-decompositions. *Journal of Number Theory*, 141:136–158, 2014.

[20] C. Elsner. Varianten eines kriteriums zum nachweis algebraischer unabhängigkeitem. *Forschungsberichte der FHDW Hannover*, pages 1–22, 2012.

[21] C. Elsner and T. Komatsu. A recurrence formula for leaping convergents of non-regular continued fractions. *Linear algebra and its applications*, 428(4):824–833, 2008.

[22] C. Elsner, S. Shimomura, and I. Shiokawa. A remark on Nesterenko's theorem for Ramanujan functions. *The Ramanujan Journal*, 21(2):211–221, 2010.

[23] C. Elsner, S. Shimomura, and I. Shiokawa. Algebraic independence results for reciprocal sums of Fibonacci numbers. *Acta Arith*, 148(3):205–223, 2011.

[24] C. Elsner, S. Shimomura, I. Shiokawa, and Y. Tachiya. Algebraic independence results for the sixteen families of q-series. *The Ramanujan Journal*, 22:315–344, 2010.

[25] G. Everest, A. J. van der Poorten, I. Shparlinski, T. Ward, et al. *Recurrence sequences*, volume 104. American Mathematical Society Providence, RI, 2003.

[26] P. Filipponi and H. T. Freitag. The Zeckendorf representation of f_{kn}/f_n. In *Applications of Fibonacci Numbers: Volume 5 Proceedings of 'The Fifth International Conference on Fibonacci Numbers and Their Applications', The University of St. Andrews, Scotland, July 20–July 24, 1992*, pages 217–219. Springer, 1993.

[27] P. Filipponi and E. L. Hart. The Zeckendorf decomposition of certain Fibonacci-Lucas products. *Fibonacci Quarterly*, 36:240–247, 1998.

[28] H. T. Freitag and P. Filipponi. On the f-representation of integral sequences f_n^2/d and l_n^2/d where d is either a fibonacci or a lucas number. *Fibonacci Quarterly*, 27(3):276–282, 1989.

[29] D. Gerdemann. Combinatorial proofs of Zeckendorf family identities, Fibonacci quart. 46/47 (2008/2009), no. 3, 249–260. *Fibonacci Quart*, 46(47):2009, 2008.

[30] R. Gilmer. On polynomial and power series rings over a commutative ring. *The Rocky Mountain Journal of Mathematics*, 5(2):157–175, 1975.

[31] R. Göttfert and H. Niederreiter. On the minimal polynomial of the product of linear recurring sequences. *Finite Fields and Their Applications*, 1(2):204–218, 1995.

[32] P. Grabner and R. Tichy. Contributions to digit expansions with respect to linear recurrences. *Journal of Number Theory*, 36(2):160–169, 1990.

[33] R. L. Graham, D. E. Knuth, O. Patashnik, and S. Liu. Concrete mathematics: a foundation for computer science. *Computers in Physics*, 3(5):106–107, 1989.

[34] G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers*. Oxford university press, 1979.

[35] E. Hart and L. Sanchis. On the occurrence of f_n in the Zeckendorf decomposition of nf_n. *Fibonacci Quart*, 37:21–33, 1999.

[36] P. Haukkanen. On a convolution of linear recurring sequences over finite fields. *J. Algebra*, 149(1):179–182, 1992.

[37] A. Hurwitz. *Über die Entwicklung complexer Grössen in Kettenbrüchen*. Springer, 1888.

[38] S. D. Kazenas. The Hadamard product and recursively defined sequences. *Open J. Discrete Math.*, 3(1):20–24, 2020.

[39] W. F. Keigher. On the ring of Hurwitz series. *Communications in Algebra*, 25(6):1845–1859, 1997.

[40] W. F. Keigher and F. L. Pritchard. Hurwitz series as formal functions. *Journal of Pure and Applied Algebra*, 146(3):291–304, 2000.

[41] V. L. Kurakin. Convolution of linear recurrent sequences. *Russian Mathematical Surveys*, 48(4):249, 1993.

[42] V. L. Kurakin. Structure of the Hopf algebras of linear recurrent sequences. *Russian Mathematical Surveys*, 48(5):177, 1993.

[43] R. G. Larson and E. J. Taft. The algebraic structure of linearly recursive sequences under Hadamard product. *Israel Journal of Mathematics*, 72:118–132, 1990.

[44] T. Lengyel. The order of the Fibonacci and Lucas numbers. *Fibonacci Quart*, 33(3):234–239, 1995.

[45] D. Levy. The irreducible factorization of Fibonacci polynomials over q. *Fibonacci Quarterly*, 39(4):309–319, 2001.

[46] D. McGregor and M. J. Rowell. On using patterns in beta-expansions to study Fibonacci-Lucas products. *Fibonacci Quarterly*, 36(1):396–406, 1998.

[47] D. McGregor and M. J. Rowell. Combinatorial proofs of Zeckendorf representations of Fibonacci and Lucas products. *Involve*, 4(1):75–89, 2011.

[48] I. Nemes and A. Peth. Generalized Zeckendorf expansions. *Appl. Math. Lett*, 7(2):25–28, 1994.

[49] Y. Nesterenko. Modular functions and transcendence problems. *Comptes rendus de l'Académie des sciences. Série 1, Mathématique*, 322(10):909–914, 1996.

[50] W. Parry. On the β-expansions of real numbers. *Acta Mathematica Hungarica*, 11(3-4):401–416, 1960.

[51] A. Pethö and R. R. Tichy. On digit expansions with respect to linear recurrences. *Journal of Number Theory*, 33(2):243–256, 1989.

[52] B. Prempreesuk, P. Noppakaew, and P. Pongsriiam. Zeckendorf representation and multiplicative inverse of f_m mod f_n. *Int. J. Math. Comput. Sci*, 15(1):17–25, 2020.

[53] S. Ramanujan. On certain arithmetical functions. *Collected papers of Srinivasa Ramanujan*, pages 137–162, 1916.

[54] A. Rényi. Representations for real numbers and their ergodic properties. *Acta Math. Acad. Sci. Hungar*, 8(3-4):477–493, 1957.

[55] P. Ribenboim. *The little book of bigger primes*, volume 811. Springer, 2004.

[56] C. Rousseau. The phi number system revisited. *Mathematics Magazine*, 68(4):283–284, 1995.

[57] B. E. Sagan and J. Tirrell. Lucas atoms. *Advances in Mathematics*, 374:107387, 2020.

[58] C. Sanna. The p-adic valuation of Lucas sequences. *Fibonacci Quart*, 54(2):118–124, 2016.

[59] K. Schmidt. On periodic expansions of Pisot numbers and salem numbers. *Bulletin of the London Mathematical Society*, 12(4):269–278, 1980.

[60] A. B. Shidlovskii. *Transcendental numbers*, volume 12. Walter de Gruyter, 2011.

[61] T. Shorey and C. Stewart. On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers, ii. *Journal of the London Mathematical Society*, 2(1):17–23, 1981.

[62] C. Stewart. The greatest prime factor of $a^n - b^n$. *Acta Arithmetica*, 26(4):427–433, 1975.

[63] C. Stewart. On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers, iii. *Journal of the London Mathematical Society*, 2(2):211–217, 1983.

[64] C. L. Stewart. On divisors of Fermat, Fibonacci, Lucas, and Lehmer numbers. *Proceedings of the London Mathematical Society*, 3(3):425–447, 1977.

[65] C. L. Stewart. On divisors of Lucas and Lehmer numbers. 2013.

[66] M. Stoll. Bounds for the length of recurrence relations for convolutions of p-recursive sequences. *European Journal of Combinatorics*, 18(6):707–712, 1997.

[67] T. Szakács. Convolution of second order linear recursive sequences i. In *Annales Mathematicae et Informaticae*, volume 46, pages 205–216, 2016.

[68] T. Szakács. Convolution of second order linear recursive sequences ii. *Communications in Mathematics*, 25, 2018.

[69] E. J. Taft. Hadamard invertibility of linearly recursive sequences in several variables. *Discrete mathematics*, 139(1-3):393–397, 1995.

[70] T.-a. Tanaka. Conditions for the algebraic independence of certain series involving continued fractions and generated by linear recurrences. *Journal of Number Theory*, 129(12):3081–3093, 2009.

[71] M. Ward. The linear p-adic recurrence of order two. *Illinois Journal of Mathematics*, 6(1):40–52, 1962.

[72] W. Webb and E. Parberry. Divisibility properties of Fibonacci polynomials. *Fibonacci Quart*, 7(5):457–463, 1969.

[73] P. M. Wood. Bijective proofs for Fibonacci identities related to Zeckendorf's theorem. *Fibonacci Quarterly*, 45(2):138, 2007.

[74] O. Zariski and P. Samuel. Commutative Algebra, vol. 1. 1975.

[75] É. Zeckendorf. Representations des nombres naturels par une somme de nombres de Fibonacci on de nombres de lucas. *Bulletin de La Society Royale des Sciences de Liege*, pages 179–182, 1972.

[76] L. Zhongkui. Hermite and ps-rings of Hurwitz series. *Communications in Algebra*, 28(1):299–305, 2000.

[77] N. Zierler and W. Mills. Products of linear recurring sequences. *Journal of Algebra*, 27(1):147–157, 1973.