Characterisation of Divisibility Sequences

Ambi Dikeledi Oosterhout (0479306)
Supervised by Frits Beukers

Utrecht University
Department of Mathematics
Master's Thesis

June 2011

Dedication and Acknowledgements

I would like to dedicate this thesis to my parents, who supported me during my whole study and never pressured me, and to my grandmothers, who both wanted to study, but were never able to, because in their time women weren't allowed to do so.

Special thanks to Allard, for all his love, comfort and support, to Douwe, Mariska, Kelly and Anouk, for taking my mind off of things when I needed it, and to my mother, for reading my thesis. Many thanks to all my friends in Amsterdam, Diemen and Utrecht, and finally, special thanks to my supervisor Frits Beukers, for all his time, support and interest.

Knobbels

De talenknobbel had ik, manifest
Geen knobbel dus voor mathematica?
Ik zou dat bijgeloof niet honoreren
Integendeel, ik hield van algebra

Aan weinig vakken had ik echt de pest
Chemie, dat vond ik maar zo zo la la
Pipetten, kolven, lakmoesproef, titreren
Nee - potlood en papier en algebra!

Daar werd een puriteinse dorst gelest
Door orde, denktechniek et cetera
Formules kon je leren en hanteren
Jazeker, ik genoot van algebra

En u? Misschien vond u het vak funest
(Gebrek aan knobbel of aan goed doceren?)
En zag u het als algeblablabla

Drs. P & Marjolein Kool, *Wis- en Natuurlyriek, met Chemisch Supplement* (2008)

Abstract

Certain linear recurrence sequences have a divisibility property, namely that a term u_n divides another term u_m if n divides m (e.g., the Fibonacci sequence). Such *divisibility sequences* can be characterised, namely they can often be written as a product of second order divisibility sequences. E.g., a power of the Fibonacci sequence will again give a divisibility sequence, but of a higher order. In this thesis we characterise divisibility sequences of orders 2, 3 and 4. A theoretical basis is provided by Ritt's theorem on factorisation of exponential polynomials.

Contents

CHAPTER 1

Introduction

A linear recurrence $\boldsymbol{u}$ in $\mathbb{Z}$ of order n is a sequence of integers $u_0, u_1, u_2, \ldots$ with the property that $u_{k+n} = A_1 u_{k+n-1} + \cdots + A_{n-1} u_{k+1} + A_n u_k$, for $A_1, \ldots, A_n \in \mathbb{Z}$ fixed ($A_n \neq 0$) and $u_0, \ldots, u_{n-1}$ chosen. The characteristic polynomial of a linear recurrence with such a recurrence relation is the polynomial $X^n - A_1 X^{n-1} - \cdots - A_{n-1} X - A_n$. If we assume the characteristic polynomial has n distinct roots $\theta_1, \ldots, \theta_n$, then for all $k \in \mathbb{Z}_{\geqslant 0}$ the terms of $\boldsymbol{u}$ are of the form $u_k = \lambda_1 \theta_1^k + \cdots + \lambda_n \theta_n^k$, for algebraic numbers $\lambda_1, \ldots, \lambda_n$ and algebraic integers $\theta_1, \ldots, \theta_n$ [1].

A linear recurrence is called nondegenerate if none of the quotients θ_i/θ_j (for $1 \leqslant i < j \leqslant n$) is a root of unity. A *divisibility sequence* is a nondegenerate linear recurrence $\boldsymbol{u}$ in $\mathbb{Z}$ such that if $k \mid \ell$ and $u_k \neq 0$, then $u_k \mid u_\ell$. An example is the famous Fibonacci sequence F_k (with initial values $F_0 = 0$ and $F_1 = 1$), which has recurrence relation $F_{k+2} = F_{k+1} + F_k$. To illustrate the divisibility property, we give the first ten terms of the Fibonacci sequence:

k	0	1	2	3	4	5	6	7	8	9	10
F_k	0	1	1	2	3	5	8	13	21	34	55

Furthermore, the characteristic polynomial of the Fibonacci sequence is $X^2 - X - 1$ and it has roots $\theta_1 = \frac{1}{2} + \frac{1}{2}\sqrt{5}$ and $\theta_2 = \frac{1}{2} - \frac{1}{2}\sqrt{5}$. The terms are of the form $F_k = (\theta_1^k - \theta_2^k)/(\theta_1 - \theta_2)$, so indeed $F_0 = 0$ and $F_1 = 1$. Sequences of this form $(\alpha^k - \beta^k)/(\alpha - \beta)$ for $\alpha, \beta \in \overline{\mathbb{Z}}$ are called Lucas sequences, named after the 19th century French mathematician Édouard Lucas. Like Lucas [2] and Ward [3], we wonder whether all divisibility sequences can be written in such a form.

This thesis consists of two parts: In the first part (Chapter 2) we connect linear recurrence sequences to *exponential polynomials*. In particular, we prove the unique factorisation of such polynomials, a theorem due to Joseph Ritt [4], given in Section 2.1. In the second part (Chapter 3) we relate divisibility sequences to Lucas sequences and actually characterise them. Theorems 3.3.1 and 3.4.1 give the characterisation of divisibility sequences of orders 2 and 3, respectively. There are a number of cases for divisibility sequences of order 4, which are treated in Section 3.5.

CHAPTER 2

The ring of exponential polynomials

In this chapter we study the ring of exponential polynomials. In Section 2.1 we treat closure under addition and multiplication, associativity and distributivity, units, the zero element and zero divisors. In Sections 2.2 through 2.6 we study unique factorisation of exponential polynomials.

2.1 Definition and properties

Definition 2.1.1
An exponential polynomial over $\mathbb{C}$ *is an expression of the form*

$$a_0 e^{\alpha_0 x} + \cdots + a_n e^{\alpha_n x}, \tag{2.1.1}$$

with $a_0, \ldots, a_n \in \mathbb{C}$ *and* $\alpha_0, \ldots, \alpha_n \in \mathbb{C}$ *distinct.*

From now on we speak of *exponential polynomials* instead of *exponential polynomials over* $\mathbb{C}$, unless mentioned otherwise. We show that the ring of exponential polynomials is closed under multiplication and addition: consider two exponential polynomials:

$$P = \sum_{i=0}^{n} a_i e^{\alpha_i x}, \quad Q = \sum_{j=0}^{m} b_j e^{\beta_j x}.$$

Then their product is:

$$\begin{aligned} PQ &= \sum_{i=0}^{n}\sum_{j=0}^{m} a_i b_j e^{(\alpha_i+\beta_j)x} \\ &= \sum_{i=0}^{n}\sum_{j=0}^{m} d_{ij} e^{\delta_{ij} x} \\ &= \sum_{\ell=0}^{p} c_\ell e^{\gamma_\ell x}, \end{aligned} \tag{2.1.2}$$

where $d_{ij} = a_i b_j$ and $\delta_{ij} = \alpha_i + \beta_j$. Since the δ_{ij} are not necessarily distinct, we can collect the terms with the same exponent and obtain the exponential polynomial (2.1.2), for $c_\ell \in \mathbb{C}$ and $\gamma_\ell \in \mathbb{C}$ distinct, and where $p \leqslant mn$. Hence exponential polynomials are closed under multiplication.

We also consider the sum of P and Q:

$$P + Q = \sum_{\ell=0}^{n+m+1} d_\ell e^{\delta_\ell x},$$

where

$$d_\ell = \begin{cases} a_\ell & \text{for} \quad 0 \leqslant \ell \leqslant n \\ b_{\ell-n-1} & \text{for} \quad n < \ell \leqslant n+m+1, \end{cases}$$

and

$$\delta_\ell = \begin{cases} \alpha_\ell & \text{for} \quad 0 \leqslant \ell \leqslant n \\ \beta_{\ell-n-1} & \text{for} \quad n < \ell \leqslant n+m+1. \end{cases}$$

Note that $d_\ell, \delta_\ell \in \mathbb{C}$, but the δ_ℓ are not necessarily distinct. Again we can collect the terms with the same exponent and obtain an exponential polynomial with $p+1$ terms, where $p \leqslant mn$. Hence the sum of two exponential polynomials is again an exponential polynomial. The associative and distributive properties are easily checked. In the following lemma we find the units of exponential polynomials:

Lemma 2.1.2

Unit elements of exponential polynomials are expressions of the form $ae^{\alpha x}$ with $a \in \mathbb{C}^*$ and $\alpha \in \mathbb{C}$.

PROOF First note that the multiplicative identity element is $1e^{0x}$ and that multiplication in the ring of exponential polynomials is commutative. We denote the identity element by 1. The set of units consists of all exponential polynomials P such that $PQ = QP = 1$ for some exponential polynomial Q. Consider two exponential polynomials P, Q:

$$P = \sum_{i=0}^{n} a_i e^{\alpha_i x}, \quad Q = \sum_{j=0}^{m} b_j e^{\beta_j x}.$$

Consider their product:

$$\begin{aligned} PQ &= \left(\sum_{i=0}^{n} a_i e^{\alpha_i x} \right) \left(\sum_{j=0}^{m} b_j e^{\beta_j x} \right) \\ &= \sum_{i=0}^{n} \sum_{j=0}^{m} d_{ij} e^{\delta_{ij} x} \\ &= \sum_{\ell=0}^{p} c_\ell e^{\gamma_\ell x}, \end{aligned}$$

where $c_\ell \in \mathbb{C}$ and $\gamma_\ell \in \mathbb{C}$ distinct as before. Assume $PQ = 1$. It then follows that $\gamma_0 = \cdots = \gamma_p = 0$,

i.e. $p = 0$ and $\gamma_0 = 0$. Then $c_0 = \cdots = c_p = 1$. As each γ_ℓ coincides with a δ_{ij} for some $0 \leqslant i \leqslant n$ and $0 \leqslant j \leqslant m$, it follows that $\delta_{ij} = 0$ for every i, j. Recall that $\delta_{ij} = \alpha_i + \beta_j$. Since for $i = 0, \ldots, n$ the α_i are distinct and for $j = 0, \ldots, m$ the β_j are distinct, it follows that $n = m = 0$. So write $\alpha_i = \alpha$ and $a_i = a$ for every i and $\beta_j = \beta$ and $b_j = b$ for every j. Then $\beta = -\alpha$ and from $c_0 = 1$ it follows that $ab = 1$. Hence $b = \frac{1}{a}$. We conclude that units are expressions of the form $ae^{\alpha x}$ with $a \in \mathbb{C}^*$ and $\alpha \in \mathbb{C}$. ∎

For the zero element we consider the following lemma:

Lemma 2.1.3
Let $a_0, \ldots, a_n \in \mathbb{C}$ and $\alpha_0, \ldots, \alpha_n \in \mathbb{C}$ distinct. Then $a_0 e^{\alpha_0 x} + \cdots + a_n e^{\alpha_n x} = 0$ for all $x \in \mathbb{C}$ if and only if $a_0 = \cdots = a_n = 0$.

PROOF Assume $a_0 = \cdots = a_n = 0$. Then, for any $x \in \mathbb{C}$, $a_0 e^{\alpha_0 x} + \cdots + a_n e^{\alpha_n x} = 0$. Conversely, assume $a_0 e^{\alpha_0 x} + \cdots + a_n e^{\alpha_n x} = 0$ for all $x \in \mathbb{C}$. We substitute e^x by its power series and obtain:

$$a_0 e^{\alpha_0 x} + \cdots + a_n e^{\alpha_n x} = \sum_{k=0}^{\infty} \left(a_0 \alpha_0^k + \cdots + a_n \alpha_n^k\right) \frac{x^k}{k!}.$$

This can only be equal to zero if its coefficients are zero, i.e. $a_0 \alpha_0^k + \cdots + a_n \alpha_n^k = 0$ for all $k \geqslant 0$. Consider these coefficients for $k = 0, \ldots, n$:

$$(a_0, \ldots, a_n) \begin{pmatrix} 1 & \alpha_0 & \cdots & \alpha_0^n \\ 1 & \alpha_1 & \cdots & \alpha_1^n \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \cdots & \alpha_n^n \end{pmatrix} = (a_0, \ldots, a_n)A = (0, \ldots, 0).$$

So $(a_0, \ldots, a_n)A = (0, \ldots, 0)$, which implies that either $\det(A) = 0$ or $(a_0, \ldots, a_n) = (0, \ldots, 0)$. Note that A is a Vandermonde matrix, hence its determinant [5] is of the following form:

$$\det(A) = \prod_{0 \leqslant i < j \leqslant n} (\alpha_j - \alpha_i).$$

If $\det(A) = 0$, then there are $0 \leqslant i, j \leqslant n$ distinct such that $\alpha_i = \alpha_j$, which contradicts the assumption that $\alpha_0, \ldots, \alpha_n$ are distinct. It follows that the coefficients of the exponential polynomial are all zero: $a_0 = \cdots = a_n = 0$. ∎

It follows from Lemma 2.1.3 that the zero element of the ring of exponential polynomials is the element $a_0 e^{\alpha_0 x} + \cdots + a_n e^{\alpha_n x}$ with all coefficients equal to zero.

We arrange the terms of an exponential polynomial as Ritt [4] does, namely in the following manner: α_i comes before α_j when $\mathrm{Re}(\alpha_i) < \mathrm{Re}(\alpha_j)$, or when $\mathrm{Re}(\alpha_i) = \mathrm{Re}(\alpha_j)$ and $\mathrm{Im}(\alpha_i) < \mathrm{Im}(\alpha_j)$. We use this to prove the following proposition:

Proposition 2.1.4
The ring of exponential polynomials has no zero divisors.

PROOF Let P and Q be two nonzero exponential polynomials, so that after ordering:

$$\begin{aligned} P &= a_0 e^{\alpha_0 x} + \cdots + a_n e^{\alpha_n x} \\ Q &= b_0 e^{\beta_0 x} + \cdots + b_m e^{\beta_m x}, \end{aligned}$$

where the coefficients are nonzero. By the ordering given above, the product of the last terms of P and Q gives the last term of the product PQ, i.e. the last term of PQ is $a_n b_m e^{(\alpha_n+\beta_m)x}$. Now suppose that $PQ = 0$. By Lemma 2.1.3 all the coefficients of PQ must be equal to zero, hence also $a_n b_m = 0$. But $a_n, b_m \in \mathbb{C}^*$, and since $\mathbb{C}^*$ has no zero divisors, either $a_n = 0$ or $b_m = 0$. But this contradicts the assumption that P and Q have nonzero coefficients. Hence $PQ \neq 0$, so indeed there are no zero divisors in the ring of exponential polynomials. ∎

Next we look at factorisation of exponential polynomials. It will appear that not every exponential polynomial factors into irreducible polynomials. These turn out to be so-called simple exponential polynomials.

Definition 2.1.5
A simple exponential polynomial over $\mathbb{C}$ is a polynomial of the form $1 - ae^{\alpha x}$, with $a, \alpha \in \mathbb{C}^*$.

Proposition 2.1.6
A simple exponential polynomial has an infinite number of factors.

PROOF Let $1 - ae^{\alpha x}$ be a simple exponential polynomial. Then we can view it as a Laurent polynomial in the variable $e^{\alpha x/t}$, for any $t \in \mathbb{Z}$. Therefore it has degree at least t. Let ζ be a tth primitive root of unity and let $a_k = \zeta^k a^{1/t}$. We see that:

$$\left(1 - a_1 e^{\alpha x/t}\right) \cdots \left(1 - a_t e^{\alpha x/t}\right) \;\Big|\; \left(1 - ae^{\alpha x}\right),$$

for any $t \in \mathbb{Z}$. Hence $1 - ae^{\alpha x}$ has an infinite number of factors. ∎

Clearly, an irreducible exponential polynomial cannot be simple. Therefore we consider factorisation of exponential polynomials into simple factors and irreducible factors. In order to do this, we only need to look at nonzero elements. Following Ritts approach [4], we can multiply a nonzero exponential polynomial of the form (2.1.1) by units such that $a_0 = 1$ and $\alpha_0 = 0$, i.e. it is of the form

$$1 + \sum_{i=1}^{n} a_i e^{\alpha_i x}, \tag{2.1.3}$$

with $a_1, \ldots, a_n \in \mathbb{C}$ and $\alpha_1, \ldots, \alpha_n \in \mathbb{C}^*$ distinct. This form with first term unity is useful because then factorisation gives factors that also have first term unity. We prove the following theorem [4]:

Theorem 2.1.7 (Ritt)
An exponential polynomial P (distinct from unity) can be factored uniquely (up to units) as a finite product of simple exponential polynomials and irreducible exponential polynomials. Irreducible polynomials are unique up to units and simple exponential polynomials are unique if we require that they do not divide other simple divisors of the exponential polynomial P.

To prove this theorem, we use an approach that is similar to the one by Ritt [4], but some parts are substituted by more modern mathematics. It is clear from Ritts approach that in 1926 linear algebra was not what it is today. For example, Ritt goes through a lot of trouble to show that every set of complex numbers can be written as a linear combination of rational numbers, i.e. every $\mathbb{C}$-vector space has a $\mathbb{Q}$-basis. Our approach begins as that of Ritt: we transform exponential polynomials into Laurent polynomials. Then we use unique factorisation of Laurent polynomials into Puiseux polynomials, which is treated in a different manner than by Ritt. This is worked out in the next four sections. In Section 2.6 the proof of Ritts theorem is completed. Ritts article [4] starts with the following proposition on the shape of the factors of an exponential polynomial:

Proposition 2.1.8
Consider an exponential polynomial of the form

$$1 + \sum_{i=1}^{n} a_i e^{\alpha_i x},$$

with $a_i \in \mathbb{C}$ and where each $\alpha_i \in \mathbb{C}^*$ is a $\mathbb{Z}$-linear combination of a $\mathbb{Q}$-linearly independent set $\{\mu_1, \ldots, \mu_p\}$. Suppose the polynomial factors into two exponential polynomials:

$$1 + \sum_{i=1}^{n} a_i e^{\alpha_i x} = \left(1 + \sum_{k=1}^{m} b_k e^{\beta_k x}\right)\left(1 + \sum_{\ell=1}^{r} c_\ell e^{\gamma_\ell x}\right). \tag{2.1.4}$$

Then for every $k = 1, \ldots, m$, β_k is a $\mathbb{Q}$-linear combination of $\alpha_1, \ldots, \alpha_n$.

PROOF We follow Ritts proof: Suppose there is a β_k that is not a $\mathbb{Q}$-linear combination of $\alpha_1, \ldots, \alpha_n$, say β. As the α_i are $\mathbb{Z}$-linear combinations of $\mu_1, \ldots, \mu_p$, it follows that $\beta, \mu_1, \ldots, \mu_p$ are $\mathbb{Q}$-linearly independent. Therefore we write $\beta = \mu_0$. Expand the independent set $\{\mu_0, \ldots, \mu_p\}$ to an independent set $\{\mu_0, \ldots, \mu_t\}$, for some $t \geqslant p$, such that every α_i, β_k and γ_ℓ is $\mathbb{Q}$-linearly independent in $\mu_0, \ldots, \mu_t$.

We can order the terms of $1+b_1e^{\beta_1 x}+\cdots+b_m e^{\beta_m x}$ such that the frequency of the last term, say it has frequency B, has the largest coefficient of μ_0. If there are other terms that have the same coefficient of μ_0, then B has the largest coefficient of μ_1, etc. Then $B = u_0\mu_0 + \cdots + u_t\mu_t$ with $u_0 \geqslant 1$.

Similarly, if we introduce $c_0 e^{\gamma_0 x} = 1$ (i.e. $c_0 = 1$ and $\gamma_0 = 0$), then we can order the polynomial $1 + c_1 e^{\gamma_1 x} + \cdots + c_r e^{\gamma_r x}$ such that the frequency of the last term, say with frequency C, is of the

form $C = v_0\mu_0 + \cdots + v_t\mu_t$ with $v_0 \geqslant 0$. Then the frequency of the last term of the product (2.1.4) is $B + C$, which is unequal to every other $\beta_k + \gamma_\ell$. Hence $B + C$ does not cancel out and must equal one of the α_i.

Now $B + C = (u_0 + v_0)\mu_0 + \ldots + (u_t + v_t)\mu_t$ equals an α_i, and $u_0 + v_0 \geqslant 1$. But the $\alpha_1, \ldots, \alpha_n$ only depend on $\mu_1, \ldots, \mu_p$. This implies that $\mu_1, \ldots, \mu_p$ are not independent, which contradicts our assumption that they are. Therefore, $\beta = \mu_0$ is also a $\mathbb{Q}$-linear combination of $\alpha_1, \ldots, \alpha_n$. ∎

By the argument given in the above proof, we conclude that for every $k = 1, \ldots, m$ and every $\ell = 1, \ldots, r$, the β_k and γ_ℓ are $\mathbb{Q}$-linear combinations of $\alpha_1, \ldots, \alpha_n$, and therefore also $\mathbb{Q}$-linear combinations of $\mu_1, \ldots, \mu_p$.

2.2 From exponential polynomials to Laurent polynomials

In this section we show how exponential polynomials can be viewed as Laurent polynomials. Let $1 + a_1 e^{\alpha_1 x} + \cdots + a_n e^{\alpha_n x}$ be an exponential polynomial. Consider the $\mathbb{Q}$-vector space $\langle \alpha_1, \ldots, \alpha_n \rangle_{\mathbb{Q}}$, spanned by the coefficients of x. Let $\{\mu_1, \ldots, \mu_p\}$ be a basis for this vector space. Then every α_i for $i = 1, \ldots, n$ can be written as a $\mathbb{Q}$-linear combination of $\mu_1, \ldots, \mu_p$:

$$\alpha_i = q_{i1}\mu_1 + \cdots + q_{ip}\mu_p$$

with $q_{ij} \in \mathbb{Q}$ (for $j = 1, \ldots, p$). We can even choose the basis $\{\mu_1, \ldots, \mu_p\}$ such that the α_i are $\mathbb{Z}$-linear combinations, i.e. $q_{ij} \in \mathbb{Z}$. Then:

$$1 + \sum_{i=1}^{n} a_i e^{\alpha_i x} = 1 + \sum_{i=1}^{n} a_i e^{(q_{i1}\mu_1 + \cdots + q_{ip}\mu_p)x} = 1 + \sum_{i=1}^{n} a_i \prod_{j=1}^{p} e^{q_{ij}\mu_j x},$$

with $\mu_j \in \mathbb{C}^*$ and $q_{ij} \in \mathbb{Z}$ for $i = 1, \ldots, n$ and $j = 1, \ldots, p$. In other words, we can write and exponential polynomial of the form (2.1.3) as a Laurent polynomial in the variables $e^{\mu_1 x}, \ldots, e^{\mu_p x}$.

In the following lemma we show that there is an isomorphism between the ring of exponential polynomials and the ring of Laurent polynomials.

Lemma 2.2.1
Let $\mu_1, \ldots, \mu_p \in \mathbb{C}^*$ be $\mathbb{Q}$-linearly independent. Then there is an isomorphism between the rings $\mathbb{C}\left[e^{\pm\mu_1 x}, \ldots, e^{\pm\mu_p x}\right]$ and $\mathbb{C}\left[y_1^{\pm 1}, \ldots, y_p^{\pm 1}\right]$.

PROOF Let $\varphi : \mathbb{C}\left[y_1^{\pm 1}, \ldots, y_p^{\pm 1}\right] \to \mathbb{C}\left[e^{\pm\mu_1 x}, \ldots, e^{\pm\mu_p x}\right]$ be given by $y_j \mapsto e^{\mu_j x}$ for $j = 1, \ldots, p$. Then φ is surjective: let $P \in \mathbb{C}\left[e^{\pm\mu_1 x}, \ldots, e^{\pm\mu_p x}\right]$. Then P is of the form

$$P\left(e^{\mu_1 x}, \ldots, e^{\mu_p x}\right) = \sum_{i=1}^{n} a_i \prod_{j=1}^{p} e^{q_{ij}\mu_j x}.$$

Then, for

$$Q(y_1,\ldots,y_p)=\sum_{i=1}^{n}a_i\prod_{j=1}^{p}y_j^{q_{ij}}\in\mathbb{C}\left[y_1^{\pm1},\ldots,y_p^{\pm1}\right]$$

we obtain:

$$\begin{aligned}\varphi\left(Q(y_1,\ldots,y_p)\right) &= \sum_{i=1}^{n}a_i\prod_{j=1}^{p}\varphi(y_j)^{q_{ij}}\\ &= \sum_{i=1}^{n}a_i\prod_{j=1}^{p}e^{q_{ij}\mu_j x}\\ &= P\left(e^{\mu_1 x},\ldots,e^{\mu_p x}\right).\end{aligned}$$

So for all $P\in\mathbb{C}\left[e^{\pm\mu_1 x},\ldots,e^{\pm\mu_p x}\right]$ there is a $Q\in\mathbb{C}\left[y_1^{\pm1},\ldots,y_p^{\pm1}\right]$ such that $\varphi(Q)=P$. Recall that φ is injective if its kernel contains only the zero element, i.e. if

$$\ker(\varphi)=\{Q\in\mathbb{C}\left[y_1^{\pm1},\ldots,y_p^{\pm1}\right]\mid\varphi(Q)=0\}=\{0\}.$$

Note that indeed $0\in\ker(\varphi)$. Let $Q\in\mathbb{C}\left[y_1^{\pm1},\ldots,y_p^{\pm1}\right]$ be nonzero. Then:

$$\begin{aligned}\varphi(Q(y_1,\ldots,y_p)) &= \varphi\left(\sum_{i=1}^{n}a_i\prod_{j=1}^{p}y_j^{q_{ij}}\right)\\ &= \sum_{i=1}^{n}a_i\prod_{j=1}^{p}e^{q_{ij}\mu_j x}\\ &= u_1e^{v_1x}+\cdots+u_se^{v_sx},\end{aligned}$$

with $u_1,\ldots,u_s\in\mathbb{C}^*$ for some $s\in\mathbb{Z}_{\geqslant1}$ and $v_1,\ldots,v_s\in\mathbb{C}$ distinct. Hence:

$$u_1e^{v_1x}+\cdots+u_se^{v_sx}=0\text{ implies }u_1=\cdots=u_s=0.$$

This is a contradiction of $u_1,\ldots,u_s\in\mathbb{C}^*$, so the kernel of φ indeed consists only of the zero polynomial, i.e. φ is injective. Hence φ is an isomorphism. ∎

We conclude that an exponential polynomial can be written as a Laurent polynomial:

$$\begin{aligned}1+\sum_{i=1}^{n}a_ie^{\alpha_i x} &= 1+\sum_{i=1}^{n}a_i\prod_{j=1}^{p}e^{q_{ij}\mu_j x}\\ &= 1+\sum_{i=1}^{n}a_i\prod_{j=1}^{p}y_j^{q_{ij}}.\end{aligned}$$

We have thus transformed exponential polynomials to Laurent polynomials, which was the goal of this section. We end this section with an important theorem, but first we give the following definition of a *Puiseux polynomial*.

Definition 2.2.2
A Puiseux polynomial over $\mathbb{C}$ in p variables is an element of $\bigcup_{t\geqslant 1} \mathbb{C}\left[y_1^{\pm 1/t}, \ldots, y_p^{\pm 1/t}\right]$.

From now on we speak of *Puiseux polynomials* instead of *Puiseux polynomials over* $\mathbb{C}$. The units are elements of the form $a y_1^{q_1/t} \cdots y_p^{q_p/t}$, for $a \in \mathbb{C}^*$ and $q_1, \ldots, q_p \in \mathbb{Z}$. The identity element is the element with $a = 1$ and $q_1 = \cdots = q_p = 0$.

Definition 2.2.3
A simple Puiseux polynomial over $\mathbb{C}$ in p variables is a Puiseux polynomial with two terms.

To prove Theorem 2.1.7, we want to factor Laurent polynomials into Puiseux polynomials. The approach is as follows: since the ring of Laurent polynomials is a unique factorisation domain, we start with a Laurent polynomial and split it into a finite product of simple Laurent polynomials (i.e. Laurent polynomials with two terms) and irreducible Laurent polynomials. We set aside the simple factors and consider an irreducible factor:

$$Q(y_1, \ldots, y_p) = 1 + \sum_{i=1}^{n} a_i \prod_{j=1}^{p} y_j^{q_{ij}}.$$

Suppose that $Q(y_1, \ldots, y_p)$ has a non-trivial Puiseux divisor $P\left(y_1^{1/t}, \ldots, y_p^{1/t}\right)$. Then $Q(y_1^t, \ldots, y_p^t)$ has a non-trivial Laurent divisor $P(y_1, \ldots, y_p)$. According to Ritt [4] "the problem thus becomes: Given an irreducible polynomial $Q(y_1, \ldots, y_p)$, to determine for which positive integers $t_1, \ldots, t_p$ the polynomial $Q(y_1^{t_1}, \ldots, y_p^{t_p})$ is reducible."

Let $t = \operatorname{lcm}(t_1, \ldots, t_p)$. If we can find $t_1, \ldots, t_p$ such that $Q(y_1^{t_1}, \ldots, y_p^{t_p})$ is reducible, then certainly $Q(y_1^t, \ldots, y_p^t)$ is reducible (in the ring $\mathbb{C}\left[y_1^{\pm 1}, \ldots, y_p^{\pm 1}\right]$). Consequently, $Q(y_1, \ldots, y_p)$ is reducible in the ring $\mathbb{C}\left[y_1^{\pm 1/t}, \ldots, y_p^{\pm 1/t}\right]$. So choose a $t \in \mathbb{Z}$ such that $Q(y_1^t, \ldots, y_p^t)$ splits into T irreducible Laurent polynomials $Q_\ell(y_1, \ldots, y_p)$ for $\ell = 1, \ldots, T$. To prove that t and T are bounded we follow a different direction than Ritt. We will prove the following theorem:

Theorem 2.2.4
A Laurent polynomial P can be factored uniquely (up to units) into a finite product of simple Puiseux polynomials and irreducible Puiseux polynomials. Irreducible Puiseux polynomials are unique up to units and simple Puiseux polynomials are unique if we require that they do not divide other simple divisors of the Puiseux polynomial P.

We will prove this theorem in Section 2.5. To do this we need some background information, which will be treated in the next two sections.

Note that since $Q(y_1^t, \ldots, y_p^t) = Q_1(y_1, \ldots, y_p) \cdots Q_T(y_1, \ldots, y_p)$, for any $N \in \mathbb{Z}_{\geqslant 1}$ there exist Laurent polynomials $Q'_1, \ldots, Q'_T$ such that:

$$\begin{aligned} Q(y_1^{Nt}, \ldots, y_p^{Nt}) &= Q_1(y_1^N, \ldots, y_p^N) \cdots Q_T(y_1^N, \ldots, y_p^N) \\ &= Q'_1(y_1, \ldots, y_p) \cdots Q'_T(y_1, \ldots, y_p). \end{aligned}$$

It seems as if there are infinitely many $t \in \mathbb{Z}_{\geqslant 1}$ such that $Q(y_1^t, \ldots, y_p^t)$ is reducible. In Section 2.4 we will make an assumption that eliminates this problem. First we need to know more about the support and Newton polytope of Laurent polynomials.

2.3 Support and Newton polytope

In this section we give the definitions of support and Newton polytope of a Laurent polynomial and we show two properties of Newton polytopes [6].

Definition 2.3.1
Consider a Laurent polynomial

$$P(y_1, \ldots, y_p) = \sum_{(k_1, \ldots, k_p) \in \mathbb{Z}^p} a_{k_1 \cdots k_p} y_1^{k_1} \cdots y_p^{k_p},$$

for $a_{k_1 \cdots k_p} \in \mathbb{C}$ and $k_1, \ldots, k_p \in \mathbb{Z}$, where $a_{k_1 \cdots k_p} = 0$ for all $k_1, \ldots, k_p$ but finitely many. The support of P is defined as:

$$\operatorname{supp}(P) = \{(k_1, \ldots, k_p) \in \mathbb{Z}^p \mid a_{k_1 \cdots k_p} \neq 0\}.$$

Definition 2.3.2
Let P and Q be Laurent polynomials. The joint support of P and Q is $\operatorname{supp}(P) \cup \operatorname{supp}(Q)$. *Notation:* $\operatorname{supp}(P, Q)$.

Definition 2.3.3
The Newton polytope of a Laurent polynomial P is the convex closure of its support, denoted by $N(P) = \operatorname{conv}(\operatorname{supp}(P))$.

The following proposition from [7] states one of the two properties of Newton polytopes that we need for the proof of Theorem 2.2.4.

Proposition 2.3.4
Let P and Q be Laurent polynomials. Then $N(PQ)$ is the Minkowski sum of $N(P)$ and $N(Q)$, i.e. $N(PQ) = N(P) + N(Q)$ in the sense that $r \in N(PQ)$ is of the form $p + q$ with $p \in N(P)$ and $q \in N(Q)$.

PROOF Consider two Laurent polynomials P and Q and their product PQ:

$$\begin{aligned} P &= \sum_{(k_1,\ldots,k_p)\in\mathbb{Z}^p} a_{k_1\cdots k_p} y_1^{k_1}\cdots y_p^{k_p}, \\ Q &= \sum_{(\ell_1,\ldots,\ell_p)\in\mathbb{Z}^p} b_{\ell_1\cdots\ell_p} y_1^{\ell_1}\cdots y_p^{\ell_p}, \\ PQ &= \sum_{(k_1,\ldots,k_p)} \sum_{(\ell_1,\ldots,\ell_p)} a_{k_1\cdots k_p} b_{\ell_1\cdots\ell_p} y_1^{k_1+\ell_1}\cdots y_p^{k_p+\ell_p}. \end{aligned}$$

Then the support of PQ is:

$$\begin{aligned} \operatorname{supp}(PQ) &= \{(k_1+\ell_1,\ldots,k_p+\ell_p)\in\mathbb{Z}^p \mid a_{k_1\cdots k_p} b_{\ell_1\cdots\ell_p}\neq 0\} \\ &= \{(k_1,\ldots,k_p)+(\ell_1,\ldots,\ell_p)\in\mathbb{Z}^p \mid a_{k_1\cdots k_p} b_{\ell_1\cdots\ell_p}\neq 0\} \\ &\subseteq \{(k_1,\ldots,k_p)\in\mathbb{Z}^p \mid a_{k_1\cdots k_p}\neq 0\} + \{(\ell_1,\ldots,\ell_p)\in\mathbb{Z}^p \mid b_{\ell_1\cdots\ell_p}\neq 0\} \\ &= \operatorname{supp}(P)+\operatorname{supp}(Q) \\ &\subseteq N(P)+N(Q). \end{aligned}$$

So $\operatorname{supp}(PQ)\subseteq N(P)+N(Q)$ and therefore also $N(PQ)\subseteq N(P)+N(Q)$. Conversely, let v be any vertex of $N(P)+N(Q)$. Then there are vertices v_1 and v_2 of $N(P)$ and $N(Q)$, respectively, such that $v=v_1+v_2$. Note that v_1 and v_2 must be vertices, for otherwise their sum would not be a vertex.

We now show that v_1 and v_2 are unique for any $v\in N(P)+N(Q)$: Let $v_1'\in N(P)$ and $v_2'\in N(Q)$ be vertices such that also $v_1'+v_2'=v$. Then:

$$v=\frac{1}{2}(v_1+v_2)+\frac{1}{2}(v_1'+v_2')=\frac{1}{2}(v_1+v_2')+\frac{1}{2}(v_1'+v_2).$$

Since both v_1+v_2' and $v_1'+v_2$ are elements of $N(P)+N(Q)$, it follows that v is the average of these two points, i.e. v is a point on the line segment between v_1+v_2' and $v_1'+v_2$. But v is a vertex, so it cannot be a point on a line segment in $N(P)+N(Q)$. Therefore we have $v_1+v_2'=v_1'+v_2=v$. Recall that also $v_1+v_2=v_1'+v_2'=v$. Subtracting this equality from the latter gives $v_1=v_1'$ and $v_2=v_2'$.

So indeed, for $v\in N(P)+N(Q)$ there are unique vertices $v_1\in N(P)$ and $v_2\in N(Q)$ such that $v=v_1+v_2$. Hence there are corresponding $(k_1,\ldots,k_p),(\ell_1,\ldots,\ell_p)\in\mathbb{Z}^p$ with $a_{k_1\cdots k_p}\neq 0$ and $b_{\ell_1\cdots\ell_p}\neq 0$ such that:

$$\begin{aligned} v &= v_1+v_2 \\ &= (k_1,\ldots,k_p)+(\ell_1,\ldots,\ell_p) \text{ with } a_{k_1\cdots k_p}, b_{\ell_1\cdots\ell_p}\neq 0 \\ &= (k_1+\ell_1,\ldots,k_p+\ell_p)\in\mathbb{Z}^p \text{ with } a_{k_1\cdots k_p} b_{\ell_1\cdots\ell_p}\neq 0, \end{aligned}$$

i.e. $v\in N(PQ)$ so that also $N(P)+N(Q)\subseteq N(PQ)$. Hence $N(PQ)=N(P)+N(Q)$. ∎

Another important property is treated in the following proposition:

Proposition 2.3.5
Let $P(y_1, \ldots, y_p)$ be a Laurent polynomial. Then, for any $t \in \mathbb{Z}$:

$$N\left(P\left(y_1^t, \ldots, y_p^t\right)\right) = t \cdot N(P(y_1, \ldots, y_p)).$$

PROOF The support and Newton polytope of $P(y_1, \ldots, y_p)$ are:

$$\begin{aligned} \operatorname{supp}(P(y_1, \ldots, y_p)) &= \{(k_1, \ldots, k_p) \in \mathbb{Z}^p \mid a_{k_1 \cdots k_p} \neq 0\}, \\ N(P(y_1, \ldots, y_p)) &= \operatorname{conv}(\operatorname{supp}(P(y_1, \ldots, y_p))). \end{aligned}$$

For $P\left(y_1^t, \ldots, y_p^t\right) = \sum_{(k_1, \ldots, k_p)} a_{k_1 \cdots k_p} y_1^{k_1 t} \cdots y_p^{k_p t}$, we find the support and Newton polytope:

$$\begin{aligned} \operatorname{supp}\left(P\left(y_1^t, \ldots, y_p^t\right)\right) &= \{(k_1 t, \ldots, k_p t) \in \mathbb{Z}^p \mid a_{k_1 \cdots k_p} \neq 0\} \\ &= \{t(k_1, \ldots, k_p) \in \mathbb{Z}^p \mid a_{k_1 \cdots k_p} \neq 0\} \\ N\left(P\left(y_1^t, \ldots, y_p^t\right)\right) &= \operatorname{conv}\left(\operatorname{supp}\left(P\left(y_1^t, \ldots, y_p^t\right)\right)\right) \\ &= t \cdot \operatorname{conv}(\operatorname{supp}(P(y_1, \ldots, y_p))) \\ &= t \cdot N(P(y_1, \ldots, y_p)). \end{aligned}$$

■

We continue our quest for an upper bound of T, where T is the number of irreducible Laurent polynomials into which $Q(y_1^t, \ldots, y_p^t)$ factors. We do this in the next section, by bounding t and finding a relation between T and t.

2.4 Finding an upper bound for T

The situation is as follows: Let $Q(y_1, \ldots, y_p)$ be an irreducible Laurent polynomial and let $t \in \mathbb{Z}_{\geqslant 1}$ such that $Q\left(y_1^t, \ldots, y_p^t\right)$ factors into a finite product of irreducible (non-unitary) Laurent polynomials in the variables $y_1, \ldots, y_p$:

$$Q\left(y_1^t, \ldots, y_p^t\right) = \prod_{\ell=1}^{T} Q_\ell(y_1, \ldots, y_p). \tag{2.4.1}$$

In this section we prove that both T and t are bounded.

Theorem 2.4.1
Let $Q(y_1, \ldots, y_p)$ be an irreducible Laurent polynomial and let $t \in \mathbb{Z}_{\geqslant 1}$ such that $Q(y_1^t, \ldots, y_p^t)$ factors into T irreducible Laurent polynomials $Q_1(y_1, \ldots, y_p), \ldots, Q_T(y_1, \ldots, y_p)$. Then T has an upper bound depending only on Q.

As the proof contains many steps, in order to maintain an overview, each step is formulated as a proposition.

Let ζ be a tth primitive root of unity and consider $Q_1(\zeta^{\sigma_1}y_1,\ldots,\zeta^{\sigma_p}y_p)$ for $\sigma_1,\ldots,\sigma_p \in [0,t-1]$. Note that $Q_1(\zeta^{\sigma_1}y_1,\ldots,\zeta^{\sigma_p}y_p)$ is also irreducible as a Laurent polynomial. Since $Q_1(y_1,\ldots,y_p)$ is a divisor of $Q(y_1^t,\ldots,y_p^t)$, it follows that

$$Q_1\left(\zeta^{\sigma_1}y_1,\ldots,\zeta^{\sigma_p}y_p\right) \mid Q\left((\zeta^{\sigma_1}y_1)^t,\ldots,(\zeta^{\sigma_p}y_p)^t\right) = Q\left(y_1^t,\ldots,y_p^t\right).$$

Therefore, $Q_1(\zeta^{\sigma_1}y_1,\ldots,\zeta^{\sigma_p}y_p)$ must be equal to some $Q_\ell(y_1,\ldots,y_p)$. We conclude that for every $(\sigma_1,\ldots,\sigma_p)\in[0,t-1]^p$ there is an $\ell\in[1,T]$ such that $Q_1\left(\zeta^{\sigma_1}y_1,\ldots,\zeta^{\sigma_p}y_p\right)=Q_\ell(y_1,\ldots,y_p)$.

For the converse, consider the following proposition:

Proposition 2.4.2
For every $\ell=1,\ldots,T$ there is at least one $(\sigma_1,\ldots,\sigma_p)\in[0,t-1]^p$ such that

$$Q_1\left(\zeta^{\sigma_1}y_1,\ldots,\zeta^{\sigma_p}y_p\right)=Q_\ell(y_1,\ldots,y_p).$$

PROOF Consider the product:

$$\prod_{\sigma_1,\ldots,\sigma_p=0}^{t-1} Q_1\left(\zeta^{\sigma_1}y_1,\ldots,\zeta^{\sigma_p}y_p\right).$$

Expanding this product gives a Laurent polynomial in the variables $y_1^t,\ldots,y_p^t$. Therefore, define

$$P\left(y_1^t,\ldots,y_p^t\right) := \prod_{\sigma_1,\ldots,\sigma_p=0}^{t-1} Q_1\left(\zeta^{\sigma_1}y_1,\ldots,\zeta^{\sigma_p}y_p\right). \tag{2.4.2}$$

For $\sigma_1=\cdots=\sigma_p=0$ we have $Q_1\left(\zeta^{\sigma_1}y_1,\ldots,\zeta^{\sigma_p}y_p\right)=Q_1(y_1,\ldots,y_p)$, from which it follows that $Q_1(y_1,\ldots,y_p)$ is a divisor of $P\left(y_1^t,\ldots,y_p^t\right)$. From definition (2.4.1) we know that $Q_1(y_1,\ldots,y_p)$ is also a divisor of $Q\left(y_1^t,\ldots,y_p^t\right)$. Therefore,

$$Q_1(y_1,\ldots,y_p) \mid \gcd\left(P\left(y_1^t,\ldots,y_p^t\right), Q\left(y_1^t,\ldots,y_p^t\right)\right).$$

We know that $Q\left(y_1^t,\ldots,y_p^t\right)$ is irreducible in $\mathbb{C}\left[y_1^{\pm t},\ldots,y_p^{\pm t}\right]$. So either the gcd is one or $Q\left(y_1^t,\ldots,y_p^t\right)$ divides $P\left(y_1^t,\ldots,y_p^t\right)$. But $Q_1(y_1,\ldots,y_p)$ is non-unitary, hence indeed $Q\left(y_1^t,\ldots,y_p^t\right) \mid P\left(y_1^t,\ldots,y_p^t\right)$, i.e.

$$\prod_{\ell=1}^{T} Q_\ell(y_1,\ldots,y_p) \;\Bigg|\; \prod_{\sigma_1,\ldots,\sigma_p=0}^{t-1} Q_1\left(\zeta^{\sigma_1}y_1,\ldots,\zeta^{\sigma_p}y_p\right).$$

Consequently, for every $\ell=1,\ldots,T$ there is at least one $(\sigma_1,\ldots,\sigma_p)\in[0,t-1]^p$ such that

$$Q_1\left(\zeta^{\sigma_1}y_1,\ldots,\zeta^{\sigma_p}y_p\right)=Q_\ell(y_1,\ldots,y_p).$$

■

We know that every $\ell = 1, \ldots, T$ corresponds to at least one p-tuple $(\sigma_1, \ldots, \sigma_p)$. Now we want to know how many of such p-tuples correspond to each ℓ. Suppose there are $m \in \mathbb{Z}_{\geqslant 1}$ p-tuples $(\sigma_1, \ldots, \sigma_p) \in [0, t-1]^p$ for which $Q_1(\zeta^{\sigma_1} y_1, \ldots, \zeta^{\sigma_p} y_p) = Q_1(y_1, \ldots, y_p)$. We will show that for every ℓ there are m corresponding p-tuples in $[0, t-1]^p$.

Let G be the group consisting of all $(\sigma_1, \ldots, \sigma_p)$ such that $Q_1\left(\zeta^{\sigma_1} y_1, \ldots, \zeta^{\sigma_p} y_p\right) = Q_1(y_1, \ldots, y_p)$. E.g., $(0, \ldots, 0)$ is an element of G. Then m is the order of G. By G_ℓ denote the set consisting of all p-tuples $(\rho_1, \ldots, \rho_p) \in [0, t-1]^p$ such that $Q_1\left(\zeta^{\rho_1} y_1, \ldots, \zeta^{\rho_p} y_p\right) = Q_\ell(y_1, \ldots, y_p)$ for $\ell = 1, \ldots, T$. In the next proposition we show that m is also the cardinality of G_ℓ.

Proposition 2.4.3
For every $\ell = 1, \ldots, T$, the set G_ℓ has m elements.

PROOF Let $\ell \in [1, T]$ and let $(\rho_1, \ldots, \rho_p) \in G_\ell$. Then $Q_1\left(\zeta^{\rho_1} y_1, \ldots, \zeta^{\rho_p} y_p\right) = Q_\ell(y_1, \ldots, y_p)$ and:

$$\begin{aligned}
(\sigma_1, \ldots, \sigma_p) \in G \quad &\Leftrightarrow \quad Q_1\left(\zeta^{\sigma_1} y_1, \ldots, \zeta^{\sigma_p} y_p\right) = Q_1(y_1, \ldots, y_p) \\
&\Leftrightarrow \quad Q_1\left(\zeta^{\sigma_1+\rho_1} y_1, \ldots, \zeta^{\sigma_p+\rho_p} y_p\right) = Q_1(\zeta^{\rho_1} y_1, \ldots, \zeta^{\rho_p} y_p) \\
&\Leftrightarrow \quad Q_1\left(\zeta^{\sigma_1+\rho_1} y_1, \ldots, \zeta^{\sigma_p+\rho_p} y_p\right) = Q_\ell(y_1, \ldots, y_p) \\
&\Leftrightarrow \quad (\sigma_1 + \rho_1, \ldots, \sigma_p + \rho_p) \in G_\ell.
\end{aligned}$$

Since G has m elements and $(0, \ldots, 0) \in G$, every G_ℓ also has m elements. ∎

From Proposition 2.4.3 it follows that every $\ell = 1, \ldots, T$ corresponds to m p-tuples $(\sigma_1, \ldots, \sigma_p)$. Therefore,

$$\prod_{\sigma_1, \ldots, \sigma_p = 0}^{t-1} Q_1\left(\zeta^{\sigma_1} y_1, \ldots, \zeta^{\sigma_p} y_p\right) = \left(\prod_{\ell=1}^{T} Q_\ell(y_1, \ldots, y_p)\right)^m.$$

From definitions (2.4.1) and (2.4.2) it follows that:

$$P\left(y_1^t, \ldots, y_p^t\right) = \left(Q\left(y_1^t, \ldots, y_p^t\right)\right)^m.$$

Next we compare the Newton polytopes of $P\left(y_1^t, \ldots, y_p^t\right)$ and $\left(Q\left(y_1^t, \ldots, y_p^t\right)\right)^m$ to bound t.

Proposition 2.4.4
Let m be the number of $(\sigma_1, \ldots, \sigma_p) \in [0, t-1]^p$ such that $Q_1(\zeta^{\sigma_1} y_1, \ldots, \zeta^{\sigma_p} y_p) = Q_1(y_1, \ldots, y_p)$. The Newton polytopes of $Q_1(y_1, \ldots, y_p)$ and $Q(y_1, \ldots, y_p)$ have the following relation:

$$N(Q_1) = \frac{m}{t^{p-1}} \cdot N(Q). \tag{2.4.3}$$

PROOF By multiplying $Q_1(y_1, \ldots, y_p)$ with units, we can assure it has constant term 1. Then:

$$Q_1(y_1, \ldots, y_p) = \sum_{(k_1, \ldots, k_p) \in \operatorname{supp}(Q_1)} a_{k_1 \cdots k_p} y_1^{k_1} \cdots y_p^{k_p}, \tag{2.4.4}$$

with $a_{0\cdots 0} = 1$. Now:

$$Q_1\left(\zeta^{\sigma_1} y_1, \ldots, \zeta^{\sigma_p} y_p\right) = \sum_{(k_1,\ldots,k_p)\in \mathrm{supp}(Q_1)} a_{k_1\cdots k_p} y_1^{k_1}\cdots y_p^{k_p} \zeta^{k_1\sigma_1+\cdots+k_p\sigma_p}. \tag{2.4.5}$$

Since $\zeta^{k_1\sigma_1+\cdots+k_p\sigma_p} \neq 0$,

$$\mathrm{supp}\left(Q_1\left(\zeta^{\sigma_1} y_1, \ldots, \zeta^{\sigma_p} y_p\right)\right) = \mathrm{supp}\left(Q_1(y_1,\ldots,y_p)\right) \tag{2.4.6}$$

for every $(\sigma_1,\ldots,\sigma_p) \in [0, t-1]^p$. We combine equality (2.4.6) with definition (2.4.2) and Proposition 2.3.4, so that $N\left(P\left(y_1^t,\ldots,y_p^t\right)\right) = t^p \cdot N(Q_1(y_1,\ldots,y_p))$. Using Proposition 2.3.5 we moreover find that $N\left(\left(Q\left(y_1^t,\ldots,y_p^t\right)\right)^m\right) = m\cdot t\cdot N(Q(y_1,\ldots,y_p))$. Since $P(y_1^t,\ldots,y_p^t) = (Q(y_1^t,\ldots,y_p^t))^m$, it follows that $N(Q_1) = \frac{m}{t^{p-1}}\cdot N(Q)$. ∎

To bound t, we need to know more about m. Recall that m is the number of p-tuples $(\sigma_1,\ldots,\sigma_p)$ in $[0, t-1]^p$ such that $Q_1\left(\zeta^{\sigma_1} y_1, \ldots, \zeta^{\sigma_p} y_p\right) = Q_1(y_1,\ldots,y_p)$. From equalities (2.4.4) and (2.4.5) it thus follows that m is the number of $(\sigma_1,\ldots,\sigma_p)$ such that for all $(k_1,\ldots,k_p) \in \mathrm{supp}(Q_1)$, $\zeta^{k_1\sigma_1+\cdots+k_p\sigma_p} = 1$. Since ζ is a tth primitive root of unity, $\zeta^{k_1\sigma_1+\cdots+k_p\sigma_p} = 1$ is equivalent to $k_1\sigma_1+\cdots+k_p\sigma_p \equiv 0 \pmod{t}$.

Before we continue to find out more about m, we introduce the following definitions:

Definition 2.4.5
Let $Z \subseteq \mathbb{Z}^p$. The content of Z is the largest $N \in \mathbb{Z}_{\geqslant 1}$ such that $Z \subset N\,\mathbb{Z}^p$. Notation: $\mathrm{content}(Z)$.

From equality (2.4.6) and Proposition 2.4.2 it follows that $\mathrm{supp}(Q_\ell) = \mathrm{supp}(Q_1)$ for every $\ell \in [1, T]$. The following proposition states the assumption mentioned at the end of Section 2.2:

Proposition 2.4.6
For $Q(y_1^t,\ldots,y_p^t)$ and $Q_1(y_1,\ldots,y_p)$ as above we may assume that $\gcd(\mathrm{content}(\mathrm{supp}(Q_1)), t) = 1$.

PROOF Assume $\gcd(\mathrm{content}(\mathrm{supp}(Q_1)), t) = d \in \mathbb{Z}_{\geqslant 1}$, and let $t = d\cdot t'$. Since $d \mid \mathrm{content}(\mathrm{supp}(Q_1))$ and $\mathrm{supp}(Q_\ell) = \mathrm{supp}(Q_1)$ for every $\ell = 1,\ldots,T$, it follows that there are Laurent polynomials Q'_ℓ such that $Q_\ell(y_1,\ldots,y_p) = Q'_\ell(y_1^d,\ldots,y_p^d)$ for every ℓ. Therefore, we can rewrite (2.4.1) as:

$$Q(y_1^{d\cdot t'},\ldots,y_p^{d\cdot t'}) = Q'_1(y_1^d,\ldots,y_p^d)\cdots Q'_T(y_1^d,\ldots,y_p^d).$$

Consequently, $Q(y_1^{t'},\ldots,y_p^{t'}) = Q'_1(y_1,\ldots,y_p)\cdots Q'_T(y_1,\ldots,y_p)$. Hence we may as well assume that $d = \gcd(\mathrm{content}(\mathrm{supp}(Q_1)), t) = 1$. ∎

We conclude that if $Q(y_1^t,\ldots,y_p^t)$ is reducible for $t \in \mathbb{Z}_{\geqslant 1}$, then t is maximal.

Define the lattice $\Lambda := \langle (k_1,\ldots,k_p)\rangle_{(k_1,\ldots,k_p)\in\mathrm{supp}(Q_1)}$, i.e. the lattice generated by the elements of the support of Q_1. As $\Lambda \subseteq \mathbb{Z}^p$, we denote by $\Lambda_{\mathbb{Q}}$ the extension of Λ to $\mathbb{Q}^p$, so that $\Lambda \subset \Lambda_{\mathbb{Q}}$. Let

$\delta = |(\Lambda_{\mathbb{Q}} \cap \mathbb{Z}^p)/\Lambda|$, i.e. the index of $\Lambda_{\mathbb{Q}} \cap \mathbb{Z}^p$ over Λ, where $\Lambda_{\mathbb{Q}} \cap \mathbb{Z}^p$ is the plane spanned by the lattice Λ and can contain more points with integer coordinates than Λ. We call $\Lambda_{\mathbb{Q}} \cap \mathbb{Z}^p$ the *saturated lattice* or *saturation* of Λ.

We can find an s-dimensional basis (with $s \leqslant p$) of Λ, say

$$\{\boldsymbol{k}_1, \ldots, \boldsymbol{k}_s\} = \{(k_{11}, \ldots, k_{1p}), (k_{21}, \ldots, k_{2p}), \ldots, (k_{s1}, \ldots, k_{sp})\}.$$

Recall from the beginning of the proof of Proposition 2.4.4 that $a_{0\cdots0} = 1$. It follows that $(0, \ldots, 0)$ is a point on the lattice Λ. Suppose $(0, \ldots, 0)$ is a vertex of $N(Q_1)$. Recall that m is the number of p-tuples $(\sigma_1, \ldots, \sigma_p)$ such that for all $(k_1, \ldots, k_p) \in \Lambda$, $k_1\sigma_1 + \cdots + k_p\sigma_p \equiv 0 \pmod{t}$. Since Λ has basis $\{\boldsymbol{k}_1, \ldots, \boldsymbol{k}_s\}$ (for $s \leqslant p$), every $(k_1, \ldots, k_p) \in \Lambda$ is a linear combination of $\boldsymbol{k}_1, \ldots, \boldsymbol{k}_s$. Hence $k_1\sigma_1 + \cdots + k_p\sigma_p \equiv 0 \pmod{t}$ is equivalent to:

$$\begin{array}{ccccccc} k_{11}\sigma_1 & + & \cdots & + & k_{1p}\sigma_p & \equiv & 0 \pmod{t} \\ k_{21}\sigma_1 & + & \cdots & + & k_{2p}\sigma_p & \equiv & 0 \pmod{t} \\ \vdots & & & & \vdots & & \vdots \\ k_{s1}\sigma_1 & + & \cdots & + & k_{sp}\sigma_p & \equiv & 0 \pmod{t} \end{array}$$

In short, $K\boldsymbol{\sigma} \equiv \mathbf{0} \pmod{t}$, where K is the matrix (k_{ij}) for $i = 1, \ldots, s$ and $j = 1, \ldots, p$, and where $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_p)$ and $\mathbf{0} = (0, \ldots, 0)$.

We can normalise the matrix K to its Smith normal form [8]: there exist invertible $s \times s$ and $p \times p$ matrices Σ and Π, respectively, with integer entries, such that the Smith normal form $\Sigma K \Pi$ of K is an $s \times p$ matrix

$$\begin{pmatrix} \eta_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & \eta_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \eta_s & 0 & \cdots & 0 \end{pmatrix} \tag{2.4.7}$$

where $\eta_1 \mid \eta_2$, $\eta_2 \mid \eta_3, \ldots, \eta_{s-1} \mid \eta_s$. After applying Σ and Π, the lattice Λ lies in a new coordinate system with a new basis. The s rows of the matrix (2.4.7) represent the new basis of Λ, with respect to Σ and Π, which we denote by Λ':

$$\Lambda' = \Sigma\Lambda\Pi = \langle(\eta_1, 0, \ldots, 0), (0, \eta_2, 0, \ldots, 0), \ldots, (0, \ldots, 0, \eta_s, 0, \ldots, 0)\rangle. \tag{2.4.8}$$

Proposition 2.4.7
Let δ, Λ and $\Lambda_{\mathbb{Q}} \cap \mathbb{Z}^p$ as before and let Λ' as (2.4.8). Then $\delta = \eta_1 \cdots \eta_s$.

PROOF We can also apply Σ and Π to $\Lambda_{\mathbb{Q}}$: $\Sigma(\Lambda_{\mathbb{Q}} \cap \mathbb{Z}^p)\Pi = \Lambda'_{\mathbb{Q}} \cap \mathbb{Z}^p$, since $\Sigma\,\mathbb{Z}^p\,\Pi = \mathbb{Z}^p$. Then:

$$\Lambda'_{\mathbb{Q}} \cap \mathbb{Z}^p = \langle(1, 0, \ldots, 0), (0, 1, 0, \ldots, 0), \ldots, (0, \ldots, 0, 1, 0, \ldots, 0)\rangle.$$

Consider the homomorphism:

$$\begin{array}{rcl} \psi: \Lambda'_{\mathbb{Q}} \cap \mathbb{Z}^p & \to & \mathbb{Z}/\eta_1\mathbb{Z} \times \cdots \times \mathbb{Z}/\eta_s\mathbb{Z} \\ (a_1, \ldots, a_s, 0, \ldots, 0) & \mapsto & (a_1 (\mathrm{mod}\ \eta_1), \ldots, a_s (\mathrm{mod}\ \eta_s)). \end{array}$$

Then the kernel of ψ is precisely Λ' and obviously ψ is surjective, so by the First Isomorphism Theorem [9] the image of ψ is isomorphic to $(\Lambda'_{\mathbb{Q}} \cap \mathbb{Z}^p)/\ker(\psi)$, i.e.:

$$(\Lambda'_{\mathbb{Q}} \cap \mathbb{Z}^p)/\Lambda' \simeq \mathbb{Z}/\eta_1\mathbb{Z} \times \cdots \times \mathbb{Z}/\eta_s\mathbb{Z},$$

and therefore:

$$\delta = |(\Lambda_{\mathbb{Q}} \cap \mathbb{Z}^p)/\Lambda| = |(\Lambda'_{\mathbb{Q}} \cap \mathbb{Z}^p)/\Lambda'| = \eta_1 \cdots \eta_s.$$

■

Proposition 2.4.8
Let K, Σ and Π as before, and let m be the number of p-tuples $(\sigma_1, \ldots, \sigma_p) \in [0, t-1]^p$ such that for all $(k_1, \ldots, k_p) \in \mathrm{supp}(Q_1)$, $K\boldsymbol{\sigma} \equiv \mathbf{0} \pmod t$. Then $m \mid \gcd(\delta, t^{s-1}) \cdot t^{p-s}$.

PROOF Let $\boldsymbol{z} = (z_1, \ldots, z_p) \in \mathbb{Z}^p$ such that $\boldsymbol{\sigma} = \Pi\boldsymbol{z}$. Then:

$$\Sigma K\boldsymbol{\sigma} = \Sigma K\Pi\boldsymbol{z} = \begin{pmatrix} \eta_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & \eta_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \eta_s & 0 & \cdots & 0 \end{pmatrix} \begin{pmatrix} z_1 \\ \vdots \\ z_s \\ \vdots \\ z_p \end{pmatrix} = \begin{pmatrix} \eta_1 z_1 \\ \vdots \\ \eta_s z_s \end{pmatrix}$$

We see that there is no restriction modulo t on the variables $z_{s+1}, \ldots, z_p$. Therefore each of these has t possible values. In total we thus have t^{p-s} choices for the variables $z_{s+1}, \ldots, z_p$.

In general, an equation of the form $\eta z \equiv 0 \pmod t$ has $\gcd(\eta, t)$ solutions modulo t. The total number of solutions $\boldsymbol{z}$ to $\Sigma K\Pi\boldsymbol{z} \equiv \mathbf{0} \pmod t$ is therefore

$$\gcd(\eta_1, t) \cdots \gcd(\eta_s, t) \cdot t^{p-s}. \tag{2.4.9}$$

As the lattice Λ is generated by the elements of $\mathrm{supp}(Q_1)$, its basis $\{\boldsymbol{k}_1, \ldots, \boldsymbol{k}_s\}$ is a subset of $\mathrm{supp}(Q_1)$. Recall from Proposition 2.4.6 that $\gcd(\mathrm{content}(\mathrm{supp}(Q_1)), t) = 1$. Therefore we also have that $\gcd(\mathrm{content}(\text{basis of } \Lambda), t) = 1$, hence also $\gcd(\mathrm{content}(\text{basis of } \Lambda'), t) = 1$, i.e.

$$\gcd(\mathrm{content}(\{(\eta_1, 0, \ldots, 0), (0, \eta_2, 0, \ldots, 0), \ldots, (0, \ldots, 0, \eta_s, 0, \ldots, 0)\}), t) = \gcd(\eta_1, t) = 1,$$

since $\eta_1 \mid \eta_i$ for all $i = 2, \ldots, s$. Therefore,

$$\gcd(\eta_1, t) \cdots \gcd(\eta_s, t) = \gcd(\eta_2, t) \cdots \gcd(\eta_s, t),$$

which divides $\gcd(\eta_2 \cdots \eta_s, t^{s-1})$. Recall from Proposition 2.4.7 that $\delta = \eta_1 \cdots \eta_s$. Since $\gcd \eta_1, t = 1$, it follows that $\gcd(\eta_1, t) \cdots \gcd(\eta_s, t) \mid \gcd(\delta, t^{s-1})$.

Now we see that the number of solutions (2.4.9) of $\boldsymbol{z}$ to the equation $\Sigma K \Pi \boldsymbol{z} \equiv \mathbf{0} \pmod t$ is a divisor of $\gcd(\delta, t^{s-1}) \cdot t^{p-s}$. Since m is the number of $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_p) \in [0, t-1]^p$ such that $K\boldsymbol{\sigma} \equiv \mathbf{0} \pmod t$, it follows that m is also the number of solutions $\boldsymbol{\sigma}$ to the equation $\Sigma K \boldsymbol{\sigma} \equiv \mathbf{0} \pmod t$, which corresponds to the solutions $\boldsymbol{z}$ to $\Sigma K \Pi \boldsymbol{z} \equiv \mathbf{0} \pmod t$. Hence:

$$m \mid \gcd(\delta, t^{s-1}) \cdot t^{p-s}. \tag{2.4.10}$$

■

In particular, $m \mid t^{s-1} \cdot t^{p-s} = t^{p-1}$.

Proposition 2.4.9
Let $Q(y_1^t, \ldots, y_p^t)$, $Q_1(y_1, \ldots, y_p)$, Λ and δ as above. Then δ depends only on Q.

PROOF Define $\Lambda(Q_1) := \langle \text{vertices of } N(Q_1) \rangle$ and $\Lambda(Q) := \langle \text{vertices of } N(Q) \rangle$. By equality (2.4.3), $\Lambda(Q) = \rho \cdot \Lambda(Q_1)$ for $\rho = \frac{t^{p-1}}{m}$. Hence $\Lambda(Q)$ is a sublattice of $\Lambda(Q_1)$ and $\Lambda(Q_1)$ is a sublattice of Λ. Moreover, $\Lambda(Q)_{\mathbb{Q}} = \Lambda(Q_1)_{\mathbb{Q}} = \Lambda_{\mathbb{Q}}$. Now consider δ:

$$\begin{aligned} \delta &= |(\Lambda_{\mathbb{Q}} \cap \mathbb{Z}^p)/\Lambda| \\ &\leqslant |(\Lambda(Q_1)_{\mathbb{Q}} \cap \mathbb{Z}^p)/\Lambda(Q_1)| \\ &= |(\Lambda(Q)_{\mathbb{Q}} \cap \mathbb{Z}^p)/(\rho^{-1} \cdot \Lambda(Q))| \\ &= \rho^{-s} \cdot |(\Lambda(Q)_{\mathbb{Q}} \cap \mathbb{Z}^p)/\Lambda(Q)|, \end{aligned}$$

where s is the dimension of the basis of Λ, hence of $\Lambda(Q)$. It follows that δ depends only on Q. ■

In equality (2.4.3) we saw that the size of $N(Q_1)$ depends on $N(Q)$ by a factor $\frac{m}{t^{p-1}}$. Since $m \mid t^{p-1}$, there is a constant $c_Q \in \mathbb{Z}_{\geqslant 1}$ depending on Q, such that

$$\frac{t^{p-1}}{m} \leqslant c_Q. \tag{2.4.11}$$

Combine this with equation (2.4.10):

$$t^{p-1} \leqslant c_Q \cdot m \leqslant c_Q \cdot \gcd(\delta, t^{s-1}) \cdot t^{p-s},$$

so that $t^{s-1} \leqslant c_Q \cdot \gcd(\delta, t^{s-1}) \leqslant c_Q \cdot \delta$.

For the final stage of bounding t, we eliminate the case where $s = 1$. Namely, if $s = 1$, then the lattice Λ has only one basiselement, so the support of Q_1 is one-dimensional. This means that for $(k_1, \ldots, k_p), (k'_1, \ldots, k'_p) \in \text{supp}(Q_1)$, $(k'_1, \ldots, k'_p) = c(k_1, \ldots, k_p)$ for some $c \in \mathbb{Z}$. As explained in Section 2.1, it follows that Q_1 is simple. But at the beginning of this section we assumed Q_1 to be irreducible, i.e. it cannot be simple. Therefore $s \geqslant 2$, and we conclude that

$$t \leqslant t^{s-1} \leqslant c_Q \cdot \delta, \tag{2.4.12}$$

where $c_Q \in \mathbb{Z}$ and $\delta = |(\Lambda_{\mathbb{Q}} \cap \mathbb{Z}^p)/\Lambda|$. Hence t only depends on Q.

We have found an upper bound for t. In the next proposition we find a relation between t and T, the number of Laurent polynomials into which $Q(y_1^t, \ldots, y_p^t)$ factors.

Proposition 2.4.10
Let T be the number of Laurent polynomials in which $Q(y_1^t, \ldots, y_p^t)$ factors. Then $T = \frac{t^p}{m}$.

PROOF Using Proposition 2.4.2 and equality (2.4.6), we have that for all $\ell = 1, \ldots, T$:

$$N\left(Q_\ell(y_1, \ldots, y_p)\right) = N\left(Q_1\left(\zeta^{\sigma_1} y_1, \ldots, \zeta^{\sigma_p} y_p\right)\right) = N(Q_1(y_1, \ldots, y_p)).$$

Moreover, by definition (2.4.1) and Proposition 2.3.5,

$$\begin{aligned} t \cdot N(Q(y_1, \ldots, y_p)) &= N\left(Q\left(y_1^t, \ldots, y_p^t\right)\right) \\ &= N\left(\prod_{\ell=1}^{T} Q_\ell(y_1, \ldots, y_p)\right) \\ &= T \cdot N(Q_1(y_1, \ldots, y_p)). \end{aligned}$$

By equality (2.4.3) it then follows that

$$T = \frac{t \cdot N(Q)}{N(Q_1)} = \frac{t^p \cdot N(Q)}{m \cdot N(Q)} = \frac{t^p}{m}.$$

■

Finally, we can prove Theorem 2.4.1:

PROOF In Proposition 2.4.10 we found a relation between T and t, namely $T = \frac{t^p}{m}$. By equations (2.4.11) and (2.4.12) it follows that:

$$T = \frac{t^p}{m} \leqslant c_Q^2 \cdot \delta, \tag{2.4.13}$$

where both c_Q and δ only depend on the known Laurent polynomial $Q(y_1^t, \ldots, y_p^t)$. ■

2.5 Factorisation of Laurent polynomials into Puiseux polynomials

We now return to the situation of Theorem 2.2.4: We need to factor an irreducible Laurent polynomial $Q(y_1, \ldots, y_p)$ into a finite product of irreducible Puiseux polynomials. Suppose $Q(y_1, \ldots, y_p)$ splits into M Puiseux polynomials $Q_\ell\left(y_1^{1/t}, \ldots, y_p^{1/t}\right)$ for $\ell = 1, \ldots, M$ and for some $t \in \mathbb{Z}_{\geqslant 1}$. Then:

$$Q(y_1^t, \ldots, y_p^t) = \prod_{\ell=1}^{M} Q_\ell(y_1, \ldots, y_p).$$

From the previous section it follows that $M \leqslant c_Q^2 \cdot \delta$ (see equation (2.4.13)). Consequently, the number of Puiseux polynomials into which $Q(y_1, \ldots, y_p)$ factors is bounded. We want these Puiseux polynomials to be irreducible, so consider the following lemma:

Lemma 2.5.1
Suppose $Q(y_1, \ldots, y_p)$ factors into M Puiseux polynomials and M is maximal in this respect. Then the polynomials $Q_\ell\left(y_1^{1/t}, \ldots, y_p^{1/t}\right)$ for $\ell = 1, \ldots, M$ are irreducible as Puiseux polynomials.

PROOF Suppose there is an $\ell \in [1, M]$ for which $Q_\ell\left(y_1^{1/t}, \ldots, y_p^{1/t}\right)$ is reducible. Without loss of generality we assume $\ell = 1$. Then there are Puiseux polynomials A and B into which Q_1 factors:

$$Q_1\left(y_1^{1/t}, \ldots, y_p^{1/t}\right) = A\left(y_1^{1/t'}, \ldots, y_p^{1/t'}\right) B\left(y_1^{1/t'}, \ldots, y_p^{1/t'}\right),$$

where $t \mid t'$. Then we obtain:

$$\begin{aligned} Q(y_1, \ldots, y_p) &= \prod_{\ell=1}^{M} Q_\ell\left(y_1^{1/t}, \ldots, y_p^{1/t}\right) \\ &= A\left(y_1^{1/t'}, \ldots, y_p^{1/t'}\right) B\left(y_1^{1/t'}, \ldots, y_p^{1/t'}\right) \prod_{\ell=2}^{M} Q_\ell\left(y_1^{1/t}, \ldots, y_p^{1/t}\right). \end{aligned}$$

Now $Q(y_1, \ldots, y_p)$ factors into $M + 1$ Puiseux polynomials, which contradicts M being maximal. Hence all $Q_\ell\left(y_1^{1/t}, \ldots, y_p^{1/t}\right)$ for $\ell = 1, \ldots, M$ are irreducible as Puiseux polynomials. ∎

Now we can prove Theorem 2.2.4:

PROOF At the end of Section 2.2 we explained the following: Start with a Laurent polynomial, and factor it into simple Laurent polynomials and irreducible Laurent polynomials. The simple Laurent polynomials can be factored infinitely into simple Puiseux polynomials. Moreover, in Section 2.4 we saw that irreducible Laurent polynomials can be factored into a finite number of Puiseux polynomials, and from Lemma 2.5.1 it follows that these Puiseux polynomials are in fact irreducible. ∎

2.6 Unique factorisation of exponential polynomials

Finally, we can prove Theorem 2.1.7:

PROOF From the isomorphism proved in Lemma 2.2.1, it follows that exponential polynomials can be written as Laurent polynomials. By Theorem 2.2.4 we can factor Laurent polynomials uniquely into a finite product of simple Puiseux polynomials and irreducible Puiseux polynomials. Therefore, exponential polynomials can be factored into simple exponential Puiseux polynomials and irreducible exponential Puiseux polynomials. Since exponential Puiseux polynomials are just exponential polynomials, the statement of the theorem follows. ∎

CHAPTER 3

Divisibility sequences

In this chapter, we use $\overline{\mathbb{Q}}$ to denote the algebraic numbers, i.e. roots of polynomials with integer coefficients. Furthermore, we use $\overline{\mathbb{Z}}$ to denote the algebraic integers, i.e. roots of *monic* polynomials with integer coefficients. Integers are roots of monic polynomials of degree 1, hence algebraic. As rational numbers are roots of polynomials of degree 1, an algebraic integer is a normal integer if and only if it is a rational number: $\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$.

3.1 Properties

Recall from Chapter 1 that a divisibility sequence is a nondegenerate linear recurrence sequence $\boldsymbol{u}$ with the property that if $k \mid \ell$ and $u_k \neq 0$, then $u_k \mid u_\ell$. Furthermore, if $\theta_1, \ldots, \theta_n$ are the n distinct roots of the characteristic polynomial of a divisibility sequence $\boldsymbol{u}$, then the sequence can be written as $u_k = \lambda_1\theta_1^k + \cdots + \lambda_n\theta_n^k$ for every $k \in \mathbb{Z}_{\geqslant 0}$, with $\lambda_1, \ldots, \lambda_n \in \overline{\mathbb{Q}}$. Note that $\theta_1 \cdots \theta_n$ is the constant term of the characteristic polynomial, hence it is nonzero. Therefore $\theta_i \neq 0$ for every $i = 1, \ldots, n$. We can rewrite the sequence as

$$u_k = \sum_{i=1}^{n} \lambda_i \theta_i^k = \sum_{i=1}^{n} \lambda_i e^{k \log \theta_i} = \sum_{i=1}^{n} \lambda_i e^{k\alpha_i},$$

where $\alpha_i = \log \theta_i$ for all $i = 1, \ldots, n$.

Now u_k is an exponential polynomial over $\mathbb{C}$, restricted to $\mathbb{N}$ (where we assume $0 \in \mathbb{N}$). We say that u_k is an exponential polynomial over $\mathbb{N}$. Furthermore, note that since we can multiply u_k by scalars, we may assume that not only $\theta_i \in \overline{\mathbb{Z}}$, but also $\lambda_i \in \overline{\mathbb{Z}}$, for $i = 1, \ldots, n$.

By the definition of a divisibility sequence given in Chapter 1, divisibility sequences are sequences in $\mathbb{Z}$. For the characterisation of such sequences, we extend the concept of divisibility sequences to $\overline{\mathbb{Z}}$: a sequence is a divisibility sequence in $\overline{\mathbb{Z}}$ if the divisibility property (if $k \mid \ell$ and $u_k \neq 0$, then $u_k \mid u_\ell$) holds in $\overline{\mathbb{Z}}$.

Lemma 3.1.1

Let $\boldsymbol{u}$ be a divisibility sequence in $\mathbb{Z}$ as above. Then, for every k such that $u_k \neq 0$ and for every $i = 1, \ldots, n$, u_k divides

$$\lambda_i \theta_1^k \cdots \theta_n^k \prod_{1 \leqslant i < j \leqslant n} \left(\theta_j^k - \theta_i^k\right).$$

PROOF Let u_k be a nonzero term of $\boldsymbol{u}$. Then u_k is of the form $u_k = \lambda_1 \theta_1^k + \cdots + \lambda_n \theta_n^k$, with $\lambda_1, \ldots, \lambda_n \in \overline{\mathbb{Z}}$ and $\theta_1, \ldots, \theta_n \in \overline{\mathbb{Z}}$ distinct. Consider the following determinant:

$$\det(\Theta) = \begin{vmatrix} \theta_1^k & \theta_1^{2k} & \cdots & \theta_1^{nk} \\ \theta_2^k & \theta_2^{2k} & \cdots & \theta_2^{nk} \\ \vdots & \vdots & \ddots & \vdots \\ \theta_n^k & \theta_n^{2k} & \cdots & \theta_n^{nk} \end{vmatrix} = \theta_1^k \cdots \theta_n^k \begin{vmatrix} 1 & \theta_1^k & \cdots & \theta_1^{(n-1)k} \\ 1 & \theta_2^k & \cdots & \theta_2^{(n-1)k} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \theta_n^k & \cdots & \theta_n^{(n-1)k} \end{vmatrix},$$

which is a Vandermonde determinant, hence:

$$\det(\Theta) = \theta_1^k \cdots \theta_n^k \prod_{1 \leqslant i < j \leqslant n} (\theta_j^k - \theta_i^k).$$

Note that, since divisibility sequences are nondegenerate and every $\theta_i \neq 0$, the determinant of Θ is nonzero. Now consider $\lambda_1 \det(\Theta)$:

$$\begin{aligned} \lambda_1 \det(\Theta) &= \begin{vmatrix} \lambda_1\theta_1^k & \lambda_1\theta_1^{2k} & \cdots & \lambda_1\theta_1^{nk} \\ \theta_2^k & \theta_2^{2k} & \cdots & \theta_2^{nk} \\ \vdots & \vdots & \ddots & \vdots \\ \theta_n^k & \theta_n^{2k} & \cdots & \theta_n^{nk} \end{vmatrix} \\ &= \begin{vmatrix} u_k & u_{2k} & \cdots & u_{nk} \\ \theta_2^k & \theta_2^{2k} & \cdots & \theta_2^{nk} \\ \vdots & \vdots & \ddots & \vdots \\ \theta_n^k & \theta_n^{2k} & \cdots & \theta_n^{nk} \end{vmatrix} \equiv 0 \pmod{u_k}. \end{aligned}$$

Obviously, replacing λ_1 by any λ_i gives $\lambda_i \det(\Theta) \equiv 0 \pmod{u_k}$. Therefore,

$$u_k \mid \lambda_i \det(\Theta) = \lambda_i \theta_1^k \cdots \theta_n^k \prod_{1 \leqslant i < j \leqslant n} \left(\theta_j^k - \theta_i^k\right).$$

■

From Lemma 3.1.1 it follows that $\lambda_i \det(\Theta)$ is a linear recurrence sequence divisible by u_k for every $i = 1, \ldots, n$ and $k \geqslant 0$. We would therefore like to know more about factorisation of linear recurrence sequences. For this we can use the Hadamard Quotient Theorem:

Theorem 3.1.2 (Pourchet-Van der Poorten)
Let $\boldsymbol{u}$ and $\boldsymbol{v}$ be two nondegenerate linear recurrence sequences of (algebraic) integers and suppose that u_k divides v_k whenever $u_k \neq 0$. Then there exists a linear recurrence sequence $\boldsymbol{w}$ such that $v_k = u_k w_k$ for all $k \geqslant 0$.

According to Rumely [10]: "The Hadamard Quotient Theorem in its general form was first considered by Charles Pisot in 1959" (see [11]), and "Van der Poorten's proof is independent of [Pisot's approach,] the dominant-root method, but its last step relies crucially on the Pólya-Cantor lemma" [12]. Van der Poorten's proof is based on an incomplete argument by Pourchet [13]. For this reason, we credit the Hadamard Quotient Theorem to Pourchet and Van der Poorten.

Combining the result of Lemma 3.1.1 with Theorem 3.1.2, we find that there exists a linear recurrence sequence $\boldsymbol{v}$ such that $\lambda_i \det(\Theta) = u_k v_k$ for all $k \geqslant 0$. As linear recurrence sequences are exponential polynomials over $\mathbb{N}$, it seems possible that Theorem 3.1.2 can be lifted to exponential polynomials. However, the following example shows that this is not always easy:

Example 3.1.3
Let $\boldsymbol{u}$ and $\boldsymbol{v}$ be linear recurrence sequences:

$$\begin{aligned} u_k &= \alpha^k + (-\beta)^k \\ v_k &= \alpha^{2k} + 2(-\alpha\beta)^k + \beta^{2k}. \end{aligned}$$

Then $u_k^2 = v_k$, so $\boldsymbol{u}$ and $\boldsymbol{v}$ satisfy Theorem 3.1.2. Lift these linear recurrence sequences to exponential polynomials, and we obtain:

$$\begin{aligned} u_x &= e^{ax} + e^{(\pi i + b)x} \\ v_x &= e^{2ax} + 2e^{(\pi i + a + b)x} + e^{2bx}. \end{aligned}$$

Then u_x^2 has last term $e^{2(\pi i+b)x} = e^{2\pi i} e^{2bx}$, whereas v_x has last term e^{2bx}.

We see that we can not easily lift Theorem 3.1.2 to exponential polynomials over $\mathbb{C}$. But since u_k is a divisor of $\lambda_i \det(\Theta)$, which is a product of constants and simple exponential polynomials over $\mathbb{N}$, it seems likely that u_k is itself a product of simple exponential polynomials over $\mathbb{N}$. However, the following example shows that there are irreducible exponential polynomials that are divisors of simple exponential polynomials:

$$\alpha + \beta \mid \alpha^2 - \beta^2. \tag{3.1.1}$$

Therefore, u_k can be a product of irreducible exponential polynomials and simple exponential polynomials. As we are uncertain of the shape of u_k, we consider the obvious divisors of $\lambda_i \det(\Theta)$, namely sequences of the form $\prod_{j=1}^{r} \left(\alpha_j^k - \beta_j^k\right)$, where α_j, β_j are algebraic integers and $j = 1, \ldots, r$.

In the next sections we will relate this form to Lucas sequences and characterise divisibility sequences in $\mathbb{Z}$ of orders 2, 3 and 4. We will also present an example of a fourth order divisibility sequence that is not a product of simple exponential polynomials over $\mathbb{N}$.

3.2 (General) Lucas sequences

Definition 3.2.1
A Lucas sequence is a nondegenerate linear recurrence sequence $\boldsymbol{u}$ in $\mathbb{Z}$ of order 2 with terms u_k of the following form:

$$u_k = \frac{\alpha^k - \beta^k}{\alpha - \beta}, \tag{3.2.1}$$

for $k \geqslant 0$ and where α, β are distinct algebraic integers.

Note that the terms of a Lucas sequence are integers. Lucas sequences are useful when considering divisibility sequences in $\mathbb{Z}$. Ward [3] even speaks of *Lucasian sequences* instead of divisibility sequences. He also remarks that "it appears probable that all Lucasian sequences may be exhibited as resultant sequences or divisors of resultant sequences", where resultant sequences are divisibility sequences of the form $\prod_{i,j}(\alpha_i^k - \beta_i^k)/(\alpha_i - \beta_i)$. This is what we found as a result of Lemma 3.1.1.

For the construction of third and fourth order divisibility sequences, we use a generalisation of Lucas sequences to $\overline{\mathbb{Z}}$.

Definition 3.2.2
A general Lucas sequence is a nondegenerate linear recurrence sequence $\boldsymbol{u}$ in $\overline{\mathbb{Z}}$ of order 2 with terms u_k of the following form:

$$u_k = \frac{\alpha^k - \beta^k}{\alpha - \beta},$$

for $k \geqslant 0$ and where α, β are distinct algebraic integers.

The initial values of a (general) Lucas sequence $\boldsymbol{u}$ are $u_0 = 0$ and $u_1 = 1$.

Let $M = \alpha + \beta$ and $N = \alpha\beta$. Then α, β are roots of the polynomial $X^2 - MX + N$. This is the characteristic polynomial of the sequence, as the recurrence relation is given by:

$$\begin{aligned} u_{k+2} &= \frac{\alpha^{k+2} - \beta^{k+2}}{\alpha - \beta} \\ &= \frac{(\alpha+\beta)(\alpha^{k+1} - \beta^{k+1}) - \alpha\beta(\alpha^k - \beta^k)}{\alpha - \beta} \\ &= Mu_{k+1} - Nu_k. \end{aligned}$$

Note that if $\boldsymbol{u}$ is a Lucas sequence, M and N are integers. In the general case: $M, N \in \overline{\mathbb{Z}}$.

A famous example of a Lucas sequence is the Fibonacci sequence:

Example 3.2.3

For $M = 1$ and $N = -1$, the Lucas sequence with terms u_k is the Fibonacci sequence, with recurrence relation $u_{k+2} = u_{k+1} + u_k$ and initial values $u_0 = 0$ and $u_1 = 1$. The characteristic polynomial is $X^2 - X - 1$, with roots

$$\alpha = \frac{1+\sqrt{5}}{2}, \quad \beta = \frac{1-\sqrt{5}}{2}.$$

As mentioned in Chapter 1, the Fibonacci sequence is a divisibility sequence. Its first ten terms are:

k	0	1	2	3	4	5	6	7	8	9	10
u_k	0	1	1	2	3	5	8	13	21	34	55

Indeed we can see that if $k \mid \ell$, then $u_k \mid u_\ell$.

Another example is the sequence of Mersenne numbers:

Example 3.2.4

For $M = 3$ and $N = 2$, the Lucas sequence with terms u_k is the sequence of Mersenne numbers: $u_{k+2} = 3u_{k+1} - 2u_k$, with $u_0 = 0$ and $u_1 = 1$. The roots of the characteristic polynomial $X^2 - 3X + 2$ are $\alpha = 2$ and $\beta = 1$. Therefore, Mersenne numbers are given by

$$u_k = \frac{\alpha^k - \beta^k}{\alpha - \beta} = 2^k - 1.$$

Williams [2] remarks that "Lucas discovered that primality testing for certain integers could be effected (...) without having to perform a very large number of trial divisions". One of the numbers Lucas proved is prime, is the 127th Mersenne number. Later, Lehmer simplified Lucas's test, which is nowadays known as the Lucas-Lehmer primality test. In [14], Lehmer defines an extension of Lucas sequences, i.e. he defines a particular form of general Lucas sequences, which in this thesis we call *Lucas-Lehmer sequences*.

Definition 3.2.5

A Lucas-Lehmer sequence is a general Lucas sequence $\boldsymbol{u}$ with terms u_k as (3.2.1), but with the following recurrence relation:

$$u_{k+2} = \sqrt{M}u_{k+1} - Nu_k,$$

where $\sqrt{M} = \alpha + \beta$ and $N = \alpha\beta$ for α, β distinct algebraic integers such that $M, N \in \mathbb{Z}$. The initial values still are $u_0 = 0$ and $u_1 = 1$.

Note that the terms of a Lucas-Lehmer sequence satisfy:

$$u_k = \frac{\alpha^k - \beta^k}{\alpha - \beta} \in \begin{cases} \mathbb{Z} & \text{for } k \text{ odd} \\ \sqrt{M}\,\mathbb{Z} & \text{for } k \text{ even.} \end{cases}$$

Proposition 3.2.6
General Lucas sequences are divisibility sequences in $\overline{\mathbb{Z}}$.

PROOF Let $\boldsymbol{u}$ be a general Lucas sequence. Then the terms u_k, for $k \geqslant 0$, are of the form:

$$u_k = \frac{\alpha^k - \beta^k}{\alpha - \beta},$$

where α, β are distinct algebraic integers. Suppose $k \mid \ell$ for $k, \ell \geqslant 1$ and $u_k \neq 0$. Then:

$$\frac{u_\ell}{u_k} = \frac{\alpha^\ell - \beta^\ell}{\alpha^k - \beta^k} = \sum_{i=1}^{\frac{\ell}{k}} \alpha^{\ell - ik} \beta^{(i-1)k} \in \overline{\mathbb{Z}},$$

so indeed $u_k \mid u_\ell$ in $\overline{\mathbb{Z}}$. ∎

From Proposition 3.2.6 it follows that products of general Lucas sequences are divisibility sequences in $\overline{\mathbb{Z}}$. Moreover:

Corollary 3.2.7
Lucas sequences, i.e. general Lucas sequences with terms in $\mathbb{Z}$, are divisibility sequences in $\mathbb{Z}$.

PROOF Let $\boldsymbol{u}$ be a Lucas sequence and suppose $k \mid \ell$ for $k, \ell \geqslant 1$ and $u_k \neq 0$. From the proof of Proposition 3.2.6 it follows that $u_\ell / u_k \in \overline{\mathbb{Z}}$. Moreover, since the terms of a Lucas sequence are integers, $u_\ell / u_k \in \mathbb{Q}$. As explained at the beginning of this chapter, therefore $u_\ell / u_k \in \mathbb{Z}$, hence $\boldsymbol{u}$ is a divisibility sequence in $\mathbb{Z}$. ∎

Clearly, products of Lucas sequences are divisibility sequences in $\mathbb{Z}$, but we can also construct divisibility sequences in $\mathbb{Z}$ from products of general Lucas sequences. These are sequences $\boldsymbol{u}$ in $\mathbb{Z}$ with terms of the form

$$u_k = \prod_{j=1}^{r} \frac{\alpha_j^k - \beta_j^k}{\alpha_j - \beta_j}, \tag{3.2.2}$$

where $\alpha_j, \beta_j \in \overline{\mathbb{Z}}$ such that $\alpha_j \neq \beta_j$ for every $j = 1, \ldots, r$, and where $r \in \mathbb{Z}$.

In the following theorem we connect the integer r to the order n of the sequence $\boldsymbol{u}$.

Theorem 3.2.8
For a divisibility sequence $\boldsymbol{u}$ of which the terms u_k are of the form (3.2.2), the order n of $\boldsymbol{u}$ is restricted by the length r of the product as follows: $r + 1 \leqslant n \leqslant 2^r$.

PROOF Recall that the order n of a divisibility sequence $\boldsymbol{u}$ is the number of terms of which u_k consists. Consider the case where the order is the largest, and where it is the smallest. The largest possible order is attained when all α_j, β_j in the product (3.2.2) are distinct. In that case, the product has 2^r terms, so $n = 2^r$. The sequence has the smallest possible order when $\alpha_1 = \cdots = \alpha_r = \alpha$ and

$\beta_1 = \cdots = \beta_r = \beta$. This gives:

$$u_k = \left(\frac{\alpha^k - \beta^k}{\alpha - \beta}\right)^r$$

and by the Binomial Theorem u_k has $r+1$ terms. Hence $r + 1 \leqslant n \leqslant 2^r$. ∎

As we are interested in divisibility sequences of orders 2, 3 and 4, using Theorem 3.2.8 we conclude the following:

Order n	Length of the product r
2	1
3	2
4	2 or 3

In the next sections we consider divisibility sequences of abovementioned orders separately. There we find what restrictions on the coefficients of the general Lucas sequences are necessary so that the resulting divisibility sequences are in $\mathbb{Z}$.

3.3 Divisibility sequences of order 2

Let $\boldsymbol{u}$ be a divisibility sequence of order 2 that is a product of general Lucas sequences. From the previous section we know that $\boldsymbol{u}$ has terms u_k for $k \geqslant 0$ of the form

$$u_k = \frac{\alpha^k - \beta^k}{\alpha - \beta},$$

where α, β are distinct algebraic integers. The initial values are $u_0 = 0$ and $u_1 = 1$. So $\boldsymbol{u}$ is itself a general Lucas sequence. For $\boldsymbol{u}$ to be a divisibility sequence in $\mathbb{Z}$ we need the coefficients of the recurrence relation to be integers, i.e. $\boldsymbol{u}$ is a Lucas sequence. Since divisibility sequences are non-degenerate, this is the only form of second order divisibility sequences. This is proven in [15] by Hall. We have thus proven the following theorem:

Theorem 3.3.1
Divisibility sequences in $\mathbb{Z}$ of order 2 are Lucas sequences.

3.4 Divisibility sequences of order 3

Let $\boldsymbol{u}$ be a divisibility sequence of order 3 that is a product of general Lucas sequences. In the table at the end of Section 3.2 we find that the terms u_k for $k \geqslant 0$ are a product of two general Lucas sequences ($r = 2$ for $n = 3$):

$$\begin{aligned} u_k &= \frac{\alpha_1^k - \beta_1^k}{\alpha_1 - \beta_1} \cdot \frac{\alpha_2^k - \beta_2^k}{\alpha_2 - \beta_2} \\ &= \frac{(\alpha_1\alpha_2)^k - (\alpha_1\beta_2)^k - (\alpha_2\beta_1)^k + (\beta_1\beta_2)^k}{(\alpha_1 - \beta_1)(\alpha_2 - \beta_2)}, \end{aligned}$$

where $\alpha_i, \beta_i \in \overline{\mathbb{Z}}$ and since $\boldsymbol{u}$ is nondegenerate, $\alpha_1 \neq \beta_1$ and $\alpha_2 \neq \beta_2$. As $\boldsymbol{u}$ has order 3, it follows that $\alpha_1\beta_2 = \alpha_2\beta_1$. Let $\lambda = \sqrt{\alpha_2/\alpha_1}$. Then $\alpha_1\lambda = \sqrt{\alpha_1\alpha_2} = \alpha_2\lambda^{-1}$. So we may as well assume $\alpha_1 = \alpha_2 =: \alpha$. Then also $\beta_1 = \beta_2 =: \beta$. The terms are therefore of the form

$$u_k = \left(\frac{\alpha^k - \beta^k}{\alpha - \beta}\right)^2 = \frac{(\alpha^2)^k - 2(\alpha\beta)^k + (\beta^2)^k}{(\alpha - \beta)^2}.$$

The initial values are $u_0 = 0$, $u_1 = 1$ and $u_2 = (\alpha + \beta)^2$. So $\boldsymbol{u}$ is not only the product of two general Lucas sequences, it is the square of one general Lucas sequence. But we still need to figure out which conditions on the coefficients of the general Lucas sequence are necessary to be sure that $\boldsymbol{u}$ has terms in $\mathbb{Z}$. For this we consider the characteristic polynomial:

$$(X - \alpha^2)(X - \alpha\beta)(X - \beta^2) = X^3 - (\alpha^2 + \alpha\beta + \beta^2)X^2 + \alpha\beta(\alpha^2 + \alpha\beta + \beta^2)X - (\alpha\beta)^3.$$

Define $P = \alpha^2 + \alpha\beta + \beta^2$ and $Q = \alpha\beta$. Then $P \in \mathbb{Z}$ as it is the coefficient of X^2 and since Q is the quotient of the coefficient of X and P, it follows that $Q \in \mathbb{Q}$. But since the constant coefficient is $Q^3 \in \mathbb{Z}$, it follows that $Q \in \mathbb{Z}$. So both $P, Q \in \mathbb{Z}$. Now the characteristic polynomial becomes:

$$X^3 - PX^2 + PQX - Q^3,$$

so the recurrence relation of the terms of $\boldsymbol{u}$ is:

$$u_{k+3} = Pu_{k+2} - PQu_{k+1} + Q^3u_k,$$

where $P, Q \in \mathbb{Z}$. The sequence $\boldsymbol{u}$ has initial values $u_0 = 0$, $u_1 = 1$ and $u_2 = (\alpha + \beta)^2 = P + Q$. Note that the characteristic polynomial splits into a linear factor and an irreducible quadratic factor:

$$X^3 - PX^2 + PQX - Q^3 = (X - Q)(X^2 + (Q - P)X + Q^2).$$

It follows that third order divisibility sequences cannot have an irreducible characteristic polynomial. This is one of the properties of divisibility sequences that Hall shows in [15]. Now let

$R = P+Q = (\alpha+\beta)^2 \in \mathbb{Z}$. Then $\alpha+\beta = \sqrt{R}$ and since $\alpha\beta = Q$, we see that α and β are roots of the polynomial $X^2 - \sqrt{R}X + Q$, which is the characteristic polynomial of the Lucas-Lehmer sequence $v_{k+2} = \sqrt{R}v_{k+1} - Qv_k$ with initial values $v_0 = 0$ and $v_1 = 1$. Hence $u_k = v_k^2$. Hall [15] explains that this is the only possibility for third order divisibility sequences, i.e. he proves the following theorem:

Theorem 3.4.1
Divisibility sequences in $\mathbb{Z}$ of order 3 are squares of Lucas-Lehmer sequences.

3.5 Divisibility sequences of order 4

In Sections 3.3 and 3.4 we saw that divisibility sequences in $\mathbb{Z}$ of orders 2 and 3 are always products of (general) Lucas sequences. At the beginning of this chapter, we made clear that for fourth order divisibility sequences, this is not necessarily the case. First we study divisibility sequences that are indeed products of general Lucas sequences, then we show an example where this is not the case.

At the end of Section 3.2 we saw that if a divisibility sequence is the product of general Lucas sequences, then this product consists of either two or three general Lucas sequences ($r = 2$ or $r = 3$ for $n = 4$). For $r = 2$,

$$\begin{aligned} u_k &= \frac{\alpha_1^k - \beta_1^k}{\alpha_1 - \beta_1} \cdot \frac{\alpha_2^k - \beta_2^k}{\alpha_2 - \beta_2} \\ &= \frac{(\alpha_1\alpha_2)^k - (\alpha_1\beta_2)^k - (\beta_1\alpha_2)^k + (\beta_1\beta_2)^k}{(\alpha_1 - \beta_1)(\alpha_2 - \beta_2)}, \end{aligned}$$

for $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \overline{\mathbb{Z}}$ distinct. This is the case where $u_k = v_k w_k$, the product of two general Lucas sequences $\boldsymbol{v}$ and $\boldsymbol{w}$, treated in Section 3.5.3. For $r = 3$, the terms u_k are of the form

$$u_k = \frac{\alpha_1^k - \beta_1^k}{\alpha_1 - \beta_1} \cdot \frac{\alpha_2^k - \beta_2^k}{\alpha_2 - \beta_2} \cdot \frac{\alpha_3^k - \beta_3^k}{\alpha_3 - \beta_3}$$

and after expanding:

$$\frac{(\alpha_1\alpha_2\alpha_3)^k - (\alpha_1\alpha_2\beta_3)^k - (\alpha_1\beta_2\alpha_3)^k + (\alpha_1\beta_2\beta_3)^k - (\beta_1\alpha_2\alpha_3)^k + (\beta_1\alpha_2\beta_3)^k + (\beta_1\beta_2\alpha_3)^k - (\beta_1\beta_2\beta_3)^k}{(\alpha_1 - \beta_1)(\alpha_2 - \beta_2)(\alpha_3 - \beta_3)}.$$

For u_k to have four terms, there are two possibilities. The first possibility is the following:

$$\begin{aligned} \alpha_1\alpha_2\beta_3 &= \alpha_1\beta_2\alpha_3 = \beta_1\alpha_2\alpha_3 \\ \alpha_1\beta_2\beta_3 &= \beta_1\alpha_2\beta_3 = \beta_1\beta_2\alpha_3, \end{aligned}$$

which results in $\alpha_1 = \alpha_2 = \alpha_3$ and $\beta_1 = \beta_2 = \beta_3$ so that $u_k = v_k^3$, i.e. $\boldsymbol{u}$ is the cube of a general Lucas sequence $\boldsymbol{v}$.

The second possibility is

$$\begin{aligned}\alpha_1\beta_2\alpha_3 &= \beta_1\alpha_2\alpha_3\\ \alpha_1\beta_2\beta_3 &= \beta_1\beta_2\alpha_3\\ \alpha_1\alpha_2\beta_3 &= \beta_1\alpha_2\beta_3,\end{aligned}$$

so that $\alpha_1 = \alpha_2$, $\alpha_3 = \alpha_1^2$, $\beta_1 = \beta_2$ and $\beta_3 = \beta_1^2$. In this case $u_k = v_k^2 v_{2k}/v_2$, for v_k a general Lucas sequence.

In the following sections, we therefore disinguish the abovementioned three cases: For each case we construct the characteristic polynomial to find the conditions on the coefficients of the general Lucas sequences $\boldsymbol{v}$ and $\boldsymbol{w}$ of which the sequence $\boldsymbol{u}$ is a product. After that, we show an example of a fourth order divisibility sequence that is not the product of general Lucas sequences.

3.5.1 Case 1: $u_k = v_k^2 v_{2k}/v_2$

Let $\boldsymbol{u}$ be of the form $u_k = v_k^2 v_{2k}/v_2$, where v_k are the terms of a general Lucas sequence $\boldsymbol{v}$:

$$v_k = \frac{\alpha^k - \beta^k}{\alpha - \beta},$$

for α, β distinct algebraic integers. Note that $v_2 = \alpha + \beta$. Let $\alpha + \beta = M$ and $\alpha\beta = N$, and let the corresponding characteristic polynomial of $\boldsymbol{v}$ be $X^2 - MX + N$. The recurrence relation of $\boldsymbol{v}$ is then $v_{k+2} = Mv_{k+1} - Nv_k$. The terms u_k are:

$$\begin{aligned}u_k &= \frac{v_k^2 v_{2k}}{v_2}\\ &= \left(\frac{\alpha^k - \beta^k}{\alpha - \beta}\right)^2 \cdot \frac{\alpha^{2k} - \beta^{2k}}{\alpha - \beta} \cdot \frac{1}{\alpha + \beta}\\ &= \frac{(\alpha^4)^k - 2(\alpha^3\beta)^k + 2(\alpha\beta^3)^k - (\beta^4)^k}{(\alpha - \beta)^2(\alpha^2 - \beta^2)}. \qquad (3.5.1)\end{aligned}$$

From the form (3.5.1) we derive the characteristic polynomial of $\boldsymbol{u}$:

$$\begin{aligned}&(X - \alpha^4)(X - \alpha^3\beta)(X - \alpha\beta^3)(X - \beta^4)\\ =\ &\alpha^2\beta^2(X - \alpha^4)(X - \beta^4)\left(\frac{X}{\alpha\beta} - \alpha^2\right)\left(\frac{X}{\alpha\beta} - \beta^2\right)\\ =\ &\alpha^2\beta^2\left(X^2 - (\alpha^4 + \beta^4)X + (\alpha\beta)^4\right)\left(\left(\frac{X}{\alpha\beta}\right)^2 - (M^2 - 2N)\frac{X}{\alpha\beta} + N^2\right)\\ =\ &(X^2 - (M^4 - 4M^2N + 2N^2)X + N^4)(X^2 - \alpha\beta(M^2 - 2N)X + (\alpha\beta N)^2)\\ =\ &X^4 - M^2(M^2 - 3N)X^3 + (M^6N - 6M^4N^2 + 10M^2N^3 - 2N^4)X^2 - M^2N^4(M^2 - 3N)X + N^8.\end{aligned}$$

The initial values are $u_0 = 0$, $u_1 = 1$ and

$$\begin{aligned} u_2 &= (\alpha+\beta)^2(\alpha^2+\beta^2) = M^2(M^2-2N) \\ u_3 &= (\alpha^2+\alpha\beta+\beta^2)^2(\alpha^4+\alpha^2\beta^2+\beta^4) = M^8 - 6M^6N + 12M^4N^2 - 10M^2N^3 + 3N^4. \end{aligned}$$

For $\boldsymbol{u}$ to be in $\mathbb{Z}$, we need the initial values and the coefficients of the characteristic polynomial to be integers. The coefficient of X divided by the coefficient of X^3 is N^4, hence $N^4 \in \mathbb{Q}$. But the constant coefficient is $(N^4)^2 \in \mathbb{Z}$, so $N^4 \in \mathbb{Z}$. Subtracting the coefficient of X^3 from u_2 gives $M^2N \in \mathbb{Z}$. Subtracting this from the coefficient of X^3 gives $M^4 \in \mathbb{Z}$. As $M^2N \in \mathbb{Z}$, also $M^4N^2 \in \mathbb{Z}$. Hence $N^2 \in \mathbb{Q}$. But we already saw that $N^4 \in \mathbb{Z}$, hence $N^2 \in \mathbb{Z}$. We therefore define $P = M^4$ and $Q = M^2N$. Then $P, Q \in \mathbb{Z}$ such that $P \mid Q^2$. The characteristic polynomial now becomes:

$$X^4 - (P-3Q)X^3 + \frac{Q}{P^2}(P^3 - 6P^2 + 10PQ^2 - 2Q^3)X^2 - \frac{Q^2}{P}(P-3Q)X + \frac{Q^8}{P^4}$$

and the initial values are $u_0 = 0$, $u_1 = 1$ and

$$\begin{aligned} u_2 &= P - 2Q \\ u_3 &= \frac{(P-Q)^3(P-3Q)}{P^2}. \end{aligned}$$

This proves the following theorem:

Theorem 3.5.1
For divisibility sequences $\boldsymbol{u}$ in $\mathbb{Z}$ of order 4 with terms $u_k = v_k^2 v_{2k}/v_2$, where v_k are the terms of a general Lucas sequence $\boldsymbol{v}$, the terms u_k satisfy the recurrence relation:

$$u_{k+4} = (P-3Q)u_{k+3} - \frac{Q}{P^2}(P^3 - 6P^2 + 10PQ^2 - 2Q^3)u_{k+2} + \frac{Q^2}{P}(P-3Q)u_{k+1} - \frac{Q^8}{P^4}u_k, \quad (3.5.2)$$

for $P, Q \in \mathbb{Z}$ such that $P \mid Q^2$. Hence the conditions on the coefficients of the general Lucas sequence $\boldsymbol{v}$, with recurrence relation $v_{k+2} = Mv_{k+1} - Nv_k$, are: $M = \sqrt[4]{P}$ and $N = \frac{Q}{\sqrt{P}}$.

3.5.2 Case 2: $u_k = v_k^3$

Let $\boldsymbol{u}$ be of the form $u_k = v_k^3$, where v_k are the terms of a general Lucas sequence $\boldsymbol{v}$ of the form

$$v_k = \frac{\alpha^k - \beta^k}{\alpha - \beta},$$

where α, β are distinct algebraic integers. Let the corresponding characteristic polynomial of $\boldsymbol{v}$ be $X^2 - MX + N$ with roots α, β. The recurrence relation of $\boldsymbol{v}$ is then $v_{k+2} = Mv_{k+1} - Nv_k$ and the

terms u_k are

$$\begin{aligned} u_k &= \left(\frac{\alpha^k - \beta^k}{\alpha - \beta}\right)^3 \\ &= \frac{(\alpha^3)^k - 3(\alpha^2\beta)^k + 3(\alpha\beta^2)^k - (\beta^3)^k}{(\alpha-\beta)^3}, \end{aligned}$$

and the initial values are $u_0 = 0$, $u_1 = 1$ and

$$\begin{aligned} u_2 &= (\alpha+\beta)^3 = M^3 \\ u_3 &= (\alpha^2 + \alpha\beta + \beta^2)^3 = M^6 - 3M^4N + 3M^2N^2 - N^3. \end{aligned}$$

Using the integrality of the coefficients of the characteristic polynomial of $\boldsymbol{u}$, we can find conditions on M and N. The characteristic polynomial is

$$\begin{aligned} & (X-\alpha^3)(X-\alpha^2\beta)(X-\alpha\beta^2)(X-\beta^3) \\ = \;& \alpha^4\beta^4\left(\frac{X}{\alpha^2}-\alpha\right)\left(\frac{X}{\alpha^2}-\beta\right)\left(\frac{X}{\beta^2}-\alpha\right)\left(\frac{X}{\beta^2}-\beta\right) \\ = \;& \alpha^4\beta^4\left(\left(\frac{X}{\alpha^2}\right)^2 - M\frac{X}{\alpha^2} + N\right)\left(\left(\frac{X}{\beta^2}\right)^2 - M\frac{X}{\beta^2} + N\right) \\ = \;& (X^2 - \alpha^2 MX + \alpha^4 N)(X^2 - \beta^2 MX + \beta^4 N) \\ = \;& X^4 - M(\alpha^2+\beta^2)X^3 + (N(\alpha^4+\beta^4) + (\alpha\beta M)^2)X^2 - MN(\alpha\beta)^2(\alpha^2+\beta^2)X + (\alpha\beta)^4N^2 \\ = \;& X^4 - M(M^2-2N)X^3 + (M^4N - 3M^2N^2 + 2N^3)X^2 - MN^3(M^2-2N)X + N^6. \end{aligned}$$

The coefficient of X divided by the coefficient of X^3 is N^3, hence $N^3 \in \mathbb{Q}$. But the constant coefficient is $(N^3)^2 \in \mathbb{Z}$, so $N^3 \in \mathbb{Z}$. Subtracting the coefficient of X^3 from the value of u_2 gives $2MN \in \mathbb{Z}$, hence $MN \in \mathbb{Q}$. The value of u_2 is M^3, so $M^3 \in \mathbb{Z}$. Thus we see that $M^3N^3 = (MN)^3 \in \mathbb{Z}$, so also $MN \in \mathbb{Z}$. Therefore we define $P = M^3$ and $Q = MN$. Then $P, Q \in \mathbb{Z}$ such that $P \mid Q^3$.

The characteristic polynomial now becomes

$$X^4 - (P-2Q)X^3 + \frac{Q}{P}(P-Q)(P-2Q)X^2 - \frac{Q^3}{P}(P-2Q)X + \frac{Q^6}{P^2},$$

and the initial values are $u_0 = 0$, $u_1 = 1$ and

$$\begin{aligned} u_2 &= P \\ u_3 &= \frac{(P-Q)^3}{P}. \end{aligned}$$

We have thus proven the following theorem:

Theorem 3.5.2

For a fourth order divisibility sequence $\boldsymbol{u}$ in $\mathbb{Z}$ with terms $u_k = v_k^3$, where v_k are the terms of a general Lucas sequence $\boldsymbol{v}$, we see that the terms u_k satisfy the recurrence relation:

$$u_{k+4} = (P-2Q)u_{k+3} - \frac{Q}{P}(P-Q)(P-2Q)u_{k+2} + \frac{Q^3}{P}(P-2Q)u_{k+1} - \frac{Q^6}{P^2}u_k, \tag{3.5.3}$$

for $P, Q \in \mathbb{Z}$ such that $P \mid Q^3$. So the conditions on the coefficients of the general Lucas sequence $\boldsymbol{v}$, of which the recurrence relation is $v_{k+2} = Mv_{k+1} - Nv_k$, are the following: $M = \sqrt[3]{P}$ and $N = \frac{Q}{\sqrt[3]{P}}$.

3.5.3 Case 3: $u_k = v_k w_k$

Let $\boldsymbol{u}$ have terms of the form $u_k = v_k w_k$, where v_k and w_k are the terms of two general Lucas sequences $\boldsymbol{v}$ and $\boldsymbol{w}$:

$$v_k = \frac{\alpha^k - \beta^k}{\alpha - \beta}, \quad w_k = \frac{\gamma^k - \delta^k}{\gamma - \delta},$$

where $\alpha, \beta, \gamma, \delta$ are distinct algebraic integers. Let the corresponding characteristic polynomials of $\boldsymbol{v}$ and $\boldsymbol{w}$ be $X^2 - M_1X + N_1$ with roots α, β and $X^2 - M_2X + N_2$ with roots γ, δ. Note that, as long as the product $v_k w_k$ is unchanged, we can multiply v_k by a scalar λ^k and w_k by λ^{-k}. Therefore we can assume that $M_1 = M_2$ (unless $M_1 = 0$ or $M_2 = 0$), say $M_1 = M_2 = M$. The recurrence relations are then $v_{k+2} = Mv_{k+1} - N_1 v_k$ and $w_{k+2} = Mw_{k+1} - N_2 w_k$. The terms u_k are

$$\begin{aligned} u_k &= v_k w_k \\ &= \frac{\alpha^k - \beta^k}{\alpha - \beta} \cdot \frac{\gamma^k - \delta^k}{\gamma - \delta} \\ &= \frac{(\alpha\gamma)^k - (\alpha\delta)^k - (\beta\gamma)^k + (\beta\delta)^k}{(\alpha - \beta)(\gamma - \delta)}, \end{aligned} \tag{3.5.4}$$

with characteristic polynomial

$$\begin{aligned} & (X - \alpha\gamma)(X - \alpha\delta)(X - \beta\gamma)(X - \beta\delta) \\ = \; & \alpha^2\beta^2 \left(\left(\frac{X}{\alpha} \right)^2 - M\frac{X}{\alpha} + N_2 \right) \left(\left(\frac{X}{\beta} \right)^2 - M\frac{X}{\beta} + N_2 \right) \\ = \; & (X^2 - \alpha M X + \alpha^2 N_2)(X^2 - \beta M X + \beta^2 N_2) \\ = \; & X^4 - (\alpha + \beta)MX^3 + ((\alpha^2 + \beta^2)N_2 + \alpha\beta M^2)X^2 - \alpha\beta(\alpha + \beta)MN_2X + (\alpha\beta N_2)^2 \\ = \; & X^4 - M^2X^3 + (M^2(N_1 + N_2) - 2N_1N_2)X^2 - M^2N_1N_2X + (N_1N_2)^2. \end{aligned}$$

The initial values are $u_0 = 0$, $u_1 = 1$ and

$$\begin{aligned} u_2 &= (\alpha + \beta)(\gamma + \delta) = M^2 \\ u_3 &= (\alpha^2 + \alpha\beta + \beta^2)(\gamma^2 + \gamma\delta + \delta^2) = (M^2 - N_1)(M^2 - N_2). \end{aligned}$$

For $\boldsymbol{u}$ to be in $\mathbb{Z}$, we need the initial values and the coefficients of the characteristic polynomial to be integers. The coefficient of X divided by the value of u_1 is N_1N_2, so $N_1N_2 \in \mathbb{Q}$. But the constant coefficient is $(N_1N_2)^2$, so $N_1N_2 \in \mathbb{Z}$. From the coefficient of X^2 we derive that $M^2(N_1 + N_2) \in \mathbb{Z}$. We therefore define

$$\begin{aligned} P &= M^2 \\ Q &= M^2(N_1 + N_2) \\ R &= N_1N_2. \end{aligned}$$

Then $P, Q, R \in \mathbb{Z}$. The characteristic polynomial now becomes

$$X^4 - PX^3 + (Q - 2R)X^2 - PRX + R^2,$$

i.e. the recurrence relation of the terms u_k is

$$u_{k+4} = Pu_{k+3} - (Q - 2R)u_{k+2} + PRu_{k+1} - R^2u_k. \tag{3.5.5}$$

This relation is not the same as given by Williams [16], due to a different choice of Q. It does however not affect the conditions on M and N. The sequence has initial values $u_0 = 0$, $u_1 = 1$ and

$$\begin{aligned} u_2 &= P \\ u_3 &= P^2 - Q + R. \end{aligned}$$

As $R = N_1N_2$ and $Q = P(N_1 + N_2)$, it follows that N_1, N_2 are roots of the polynomial $Y^2 - \frac{Q}{P}Y + R$. So far, we know the following about the coefficients of the recurrence relations of the general Lucas sequences $\boldsymbol{v}$ and $\boldsymbol{w}$:

- $M^2 \in \mathbb{Z}$
- $N_1N_2 \in \mathbb{Z}$
- $N_1 + N_2 \in \mathbb{Q}$

We see that $\boldsymbol{v}$ and $\boldsymbol{w}$ are similar to Lucas-Lehmer sequences, since their recurrence relations are of the form

$$\begin{aligned} v_{k+2} &= \sqrt{P}v_{k+1} - N_1v_k \\ w_{k+2} &= \sqrt{P}w_{k+1} - N_2w_k \end{aligned}$$

with $P \in \mathbb{Z}$. However, since N_1, N_2 are roots of $Y^2 - \frac{Q}{P}Y + R$, we are not sure whether N_1, N_2 are integers; they aren't even necessariy algebraic integers. In Section 3.6 we find a possible solution to this problem using so-called twists of the general Lucas sequences $\boldsymbol{v}$ and $\boldsymbol{w}$.

3.5.4 Another case

We have characterised the divisibility sequences in $\mathbb{Z}$ of order 4 that are products of general Lucas sequences. However, these are not all possible divisibility sequences in $\mathbb{Z}$ of order 4. At the beginning of this chapter we saw and example (3.1.1) of an irreducible exponential polynomial dividing a simple exponential polynomial. Similarly we find the following example of a fourth order divisibility sequence $\boldsymbol{u}$ with terms that are not a product of general Lucas sequences:

$$u_k = (\alpha^k + \beta^k)(\alpha^{dk} - \beta^{dk}), \tag{3.5.6}$$

where α, β are distinct algebraic integers and $d \in \mathbb{Z}$ odd.

We cannot confirm the integrality of the sequence yet, so for the time being we let it be in $\overline{\mathbb{Z}}$. Therefore we also only consider divisibility in $\overline{\mathbb{Z}}$. First we check $\boldsymbol{u}$ is indeed a divisibility sequence. To do this, consider the following proposition:

Proposition 3.5.3
Let $d \in \mathbb{Z}$ be odd. For every $m \in \mathbb{Z}$, $(x+y)(x^d - y^d)$ divides $(x^m + y^m)(x^{dm} - y^{dm})$ in $\overline{\mathbb{Z}}$.

PROOF If m is odd, then $x + y \mid x^m + y^m$ and $x^d - y^d \mid x^{dm} - y^{dm}$, so the statement holds for $m \in \mathbb{Z}$ odd. If m is even, then, since d is odd, both $x + y \mid x^{dm} - y^{dm}$ and $x^d - y^d \mid x^{dm} - y^{dm}$. Hence also for $m \in \mathbb{Z}$ odd, the proposition holds. ∎

Assume $k \mid \ell$ and $u_k \neq 0$ and write $\ell = km$. Then by Proposition 3.5.3:

$$(\alpha^k + \beta^k)(\alpha^{dk} - \beta^{dk}) \mid (\alpha^{km} + \beta^{km})(\alpha^{dkm} - \beta^{dkm}),$$

hence $u_k \mid u_\ell$ in $\overline{\mathbb{Z}}$. We conclude that linear recurrence sequences with terms of the form (3.5.6) with d odd are divisibility sequences in $\overline{\mathbb{Z}}$. It follows that $u_1 \mid u_k$ for all $k \geqslant 1$, so we can normalise the sequence by dividing every term by u_1. The terms of $\boldsymbol{u}$ then become:

$$u_k = \frac{\alpha^k + \beta^k}{\alpha + \beta} \cdot \frac{\alpha^{dk} - \beta^{dk}}{\alpha^d - \beta^d},$$

where d is odd and the initial values are $u_0 = 0$, $u_1 = 1$ and

$$\begin{aligned} u_2 &= (\alpha^2 + \beta^2) \cdot \frac{\alpha^d + \beta^d}{\alpha + \beta} \\ u_3 &= (\alpha^2 - \alpha\beta + \beta^2)(\alpha^{2d} + \alpha^d\beta^d + \beta^{2d}). \end{aligned}$$

Example 3.5.4
Let $d = 3$. Then $\boldsymbol{u}$ is a divisibility sequence with terms

$$u_k = \frac{\alpha^k + \beta^k}{\alpha + \beta} \cdot \frac{\alpha^{3k} - \beta^{3k}}{\alpha^3 - \beta^3},$$

for $\alpha, \beta \in \overline{\mathbb{Z}}$ distinct. If we let $\alpha + \beta = M \in \mathbb{Z}$ and $\alpha\beta = N \in \mathbb{Z}$, then the initial values are $u_0 = 0$, $u_1 = 1$ and

$$\begin{aligned} u_2 &= (\alpha^2 + \beta^2)(\alpha^2 - \alpha\beta + \beta^2) = (M^2 - 2N)(M^2 - N) \\ u_3 &= (\alpha^2 - \alpha\beta + \beta^2)(\alpha^6 + \alpha^3\beta^3 + \beta^6) = M^8 + 7M^6N + 15M^4N^2 + 12M^2N^3 + 3N^4. \end{aligned}$$

Note that:

$$u_k = \frac{v_{2k}}{v_k \cdot v_2} \cdot \frac{v_{3k}}{v_3},$$

where v_k is a Lucas sequence (3.2.1). The characteristic polynomial of $\boldsymbol{u}$ is the same as that of Section 3.5.1:

$$X^4 - M^2(M^2 - 3N)X^3 + (M^6N - 6M^4N^2 + 10M^2N^3 - 2N^4)X^2 - M^2N^4(M^2 - 3N)X + N^8.$$

As the coefficients of the characteristic polynomial and the initial values are integers, $\boldsymbol{u}$ is in $\mathbb{Z}$, hence $u_\ell/u_k \in \mathbb{Q}$. Moreover, since $u_k \mid u_\ell$ in $\overline{\mathbb{Z}}$, it follows that $u_k \mid u_\ell$ in $\mathbb{Z}$. Hence $\boldsymbol{u}$ is a divisibility sequence in $\mathbb{Z}$. The differences with the case from Section 3.5.1 are the initial values, and therefore this sequence is of a different shape.

Theorem 3.5.5
For divisibility sequences in $\mathbb{Z}$ of order 4 with terms

$$u_k = \frac{v_{2k}}{v_k \cdot v_2} \cdot \frac{v_{dk}}{v_d},$$

for d odd, and where v_k are the terms of a Lucas sequence $\boldsymbol{v}$, we see that the terms u_k satisfy the recurrence relation:

$$u_{k+4} = M^2(M^2-3N)u_{k+3} - (M^6N - 6M^4N^2 + 10M^2N^3 - 2N^4)u_{k+2} + (M^2N^4(M^2-3N)u_{k+1} - N^8u_k,$$

for $M, N \in \mathbb{Z}$ the coefficients of the Lucas sequence $\boldsymbol{v}$: $v_{k+2} = Mv_{k+1} - Nv_k$.

In conclusion: divisibility sequences in $\mathbb{Z}$ of orders 2 and 3 are always products of (general) Lucas sequences (see Section 3.3 and Section 3.4, respectively), there are three forms of fourth order divisibility sequences in $\mathbb{Z}$ that are products of general Lucas sequences (see Sections 3.5.1, 3.5.2 and 3.5.3), but there are also forms where this is not the case (an example is shown in this section).

The following conjecture covers all possibilities of divisibility sequences:

Conjecture 3.5.6

Suppose $\boldsymbol{u}$ is a (nondegenerate) divisibility sequence with terms u_k for $k \geqslant 0$ and let $\theta_1, \ldots, \theta_n$ be the roots of its characteristic polynomial. Let Γ be the subgroup of $\overline{\mathbb{Q}}^*$ generated by the θ_i. Then there exists a $c \in \overline{\mathbb{Q}}$, elements $A, \gamma_1, \ldots, \gamma_m \in \Gamma$ and Lucas polynomials $p_1, \ldots, p_m$ such that

$$u_k = cA^k p_1(\gamma_1^k) \cdots p_m(\gamma_m^k),$$

for all $k \geqslant 0$.

Lucas polynomials are polynomials $p \in \overline{\mathbb{Q}}[x]$ such that $p(x)$ divides $p(x^k)$ for every $k \in \mathbb{Z}_{\geqslant 1}$. For example, $x - 1$ or $x^d - 1$ for $d \in \mathbb{Z}$.

Example 3.5.7

Let $\boldsymbol{u}$ be a third order divisibility sequence, i.e. with terms

$$u_k = \left(\frac{\alpha^k - \beta^k}{\alpha - \beta} \right)^2,$$

for α, β distinct algebraic integers and for every $k \geqslant 0$. We saw in Section 3.4 that the roots of the characteristic polynomial of $\boldsymbol{u}$ are $\alpha^2, \alpha\beta, \beta^2$. So $\Gamma = \langle \alpha^2, \alpha\beta, \beta^2 \rangle \subseteq \overline{\mathbb{Q}}^*$. Rewrite the terms as

$$\begin{aligned} u_k &= \frac{1}{(\alpha - \beta)^2} \beta^{2k} \left(\left(\frac{\alpha}{\beta} \right)^k - 1 \right)^2 \\ &= cA^k (\gamma^k - 1)^2, \end{aligned}$$

for $c \in \overline{\mathbb{Q}}$, $A = \beta^2 \in \Gamma$ and $\gamma = \alpha/\beta = \alpha^2 \cdot (\alpha\beta)^{-1} \in \Gamma$. The Lucas polynomial is $p(x) = (x - 1)$. And indeed, $u_k = cA^k p(\gamma^k)^2$ for every $k \geqslant 0$.

3.6 Twists of divisibility sequences

As promised at the end of Section 3.5.3, we introduce twists of divisibility sequences. These twists change general Lucas sequences into Lucas sequences, and simplify the cases of fourth order divisibility sequences in $\mathbb{Z}$ treated in Section 3.5. Namely, products of Lucas sequences are already divisibility sequences in $\mathbb{Z}$. In Section 3.6.3 we twist the divisibility sequence of Section 3.5.3 so that it becomes a proper product of general Lucas sequences, instead of something that looks like a product of two Lucas-Lehmer sequences.

Definition 3.6.1
Let $\boldsymbol{u}$ be a divisibility sequence in $\overline{\mathbb{Z}}$ with terms u_k for $k \geqslant 0$ satisfying the recurrence relation:

$$u_{k+n} = A_1 u_{k+n-1} + \cdots + A_{n-1} u_{k+1} + A_n u_k,$$

for $A_1, \ldots, A_n \in \overline{\mathbb{Z}}$. A twist of $\boldsymbol{u}$ is a divisibility sequence $\tilde{\boldsymbol{u}}$ with terms $\tilde{u}_k = \tau^k u_k$ for some $\tau \in \overline{\mathbb{Z}}$.

It is obvious that $\tilde{\boldsymbol{u}}$ itself is a divisibility sequence, but not necessarily in $\mathbb{Z}$. However, τ can be chosen such that $\tilde{\boldsymbol{u}}$ is in $\mathbb{Z}$. The terms $\tilde{u}_k$ of the twist satisfy the recurrence relation:

$$\begin{aligned}
\tilde{u}_{k+n} &= \tau^{k+n} u_{k+n} \\
&= \tau A_1(\tau^{k+n-1} u_{k+n-1}) + \cdots + \tau^{n-1} A_{n-1}(\tau^{k+1} u_{k+1}) + \tau^n A_n(\tau^k u_k) \\
&= \tau A_1 \tilde{u}_{k+n-1} + \cdots + \tau^{n-1} A_{n-1} \tilde{u}_{k+1} + \tau^n A_n \tilde{u}_k.
\end{aligned}$$

3.6.1 Twist of $u_k = v_k^2 v_{2k}/v_2$

Consider the fourth order divisibility sequence $\boldsymbol{u}$ with terms $u_k = v_k^2 v_{2k}/v_2$ from Section 3.5.1. Here $\boldsymbol{v}$ is a general Lucas sequence with recurrence relation $v_{k+2} = Mv_{k+1} - Nv_k$, where $M = P^{\frac{1}{4}}$ and $N = P^{-\frac{1}{2}}Q$ for $P, Q \in \mathbb{Z}$ such that $P \mid Q^2$. We twist this general Lucas sequence $\boldsymbol{v}$ with $\tau = P^{\frac{3}{4}}$, obtaining the twist $\tilde{\boldsymbol{v}}$ with terms $\tilde{v}_k = P^{\frac{3}{4}k} v_k$, satisfying the recurrence relation

$$\begin{aligned}
\tilde{v}_{k+2} &= \tau M \tilde{v}_{k+1} - \tau^2 N \tilde{v}_k \\
&= P\tilde{v}_{k+1} - PQ\tilde{v}_k.
\end{aligned}$$

Since $P, Q \in \mathbb{Z}$, $\tilde{\boldsymbol{v}}$ is a Lucas sequence. We twist the fourth order divisibility sequence u_k as follows:

$$(\tau^k v_k)^2 (\tau^{2k} v_{2k})/v_2 = \tau^{4k} v_k^2 v_{2k}/v_2 = \tau^{4k} u_k = P^{3k} u_k.$$

So for the fourth order divisibility sequence $\boldsymbol{u}$ in $\mathbb{Z}$, there is another fourth order divisibility sequence in $\mathbb{Z}$ corresponding to $\boldsymbol{u}$, namely the twist $\tilde{\boldsymbol{u}}$, with terms $\tilde{u}_k = P^{3k} u_k \in \mathbb{Z}$. In particular, while u_k is a product of general Lucas sequences, $\tilde{u}_k$ is a product of Lucas sequences.

Recall the recurrence relation (3.5.2) of the terms u_k:

$$u_{k+4} = (P-3Q)u_{k+3} - \frac{Q}{P^2}(P^3 - 6P^2 + 10PQ^2 - 2Q^3)u_{k+2} + \frac{Q^2}{P}(P-3Q)u_{k+1} - \frac{Q^8}{P^4}u_k.$$

By Definition 3.6.1 the terms $\tilde{u}_k$ then satisfy the following recurrence relation:

$$\tilde{u}_{k+4} = P^3(P-3Q)\tilde{u}_{k+3} - P^4Q(P^3 - 6P^2 + 10PQ^2 - 2Q^3)\tilde{u}_{k+2} + P^8Q^2(P-3Q)\tilde{u}_{k+1} - P^8Q^8\tilde{u}_k.$$

3.6.2 Twist of $u_k = v_k^3$

Consider the fourth order divisibility sequence $\boldsymbol{u}$ with terms $u_k = v_k^3$ from Section 3.5.2. Here $\boldsymbol{v}$ is a general Lucas sequence with recurrence relation $v_{k+2} = Mv_{k+1} - Nv_k$, where $M = P^{\frac{1}{3}}$ and $N = P^{-\frac{1}{3}}Q$ for $P, Q \in \mathbb{Z}$ such that $P \mid Q^3$. We twist this general Lucas sequence $\boldsymbol{v}$ with $\tau = P^{\frac{2}{3}}$, obtaining the twist $\tilde{\boldsymbol{v}}$ with terms $\tilde{v}_k = P^{\frac{2}{3}k}v_k$, satisfying the recurrence relation

$$\begin{aligned} \tilde{v}_{k+2} &= \tau M\tilde{v}_{k+1} - \tau^2 N\tilde{v}_k \\ &= P\tilde{v}_{k+1} - PQ\tilde{v}_k. \end{aligned}$$

Since $P, Q \in \mathbb{Z}$, $\tilde{\boldsymbol{v}}$ is a Lucas sequence. We twist the fourth order divisibility sequence u_k as follows:

$$(\tau^k v_k)^3 = \tau^{3k}v_k^3 = \tau^{3k}u_k = P^{2k}u_k.$$

As in the previous section, the divisibility sequence $\boldsymbol{u}$ in $\mathbb{Z}$ corresponds to the twist $\tilde{\boldsymbol{u}}$, with terms $\tilde{u}_k = P^{2k}u_k = (\tau^k v_k)^3 = \tilde{v}_k^3$. Since $\tilde{v}$ is a Lucas sequence, $\tilde{u}_k \in \mathbb{Z}$. While u_k is a product of general Lucas sequences, $\tilde{u}_k$ is a product of Lucas sequences. Recall the recurrence relation (3.5.3) of the terms u_k:

$$u_{k+4} = (P-2Q)u_{k+3} - \frac{Q}{P}(P-Q)(P-2Q)u_{k+2} + \frac{Q^3}{P}(P-2Q)u_{k+1} - \frac{Q^6}{P^2}u_k.$$

By Definition 3.6.1 the terms $\tilde{u}_k$ then satisfy the following recurrence relation:

$$\tilde{u}_{k+4} = P^2(P-2Q)\tilde{u}_{k+3} - P^3Q(P-Q)(P-2Q)\tilde{u}_{k+2} + P^5Q^3(P-2Q)\tilde{u}_{k+1} - P^6Q^6\tilde{u}_k.$$

3.6.3 Twist of $u_k = v_k w_k$

Consider the fourth order divisibility sequence $\boldsymbol{u}$ with terms $u_k = v_k w_k$ from Section 3.5.3. Here $\boldsymbol{v}$ and $\boldsymbol{w}$ are general Lucas sequences with recurrence relations

$$\begin{aligned} v_{k+2} &= Mv_{k+1} - N_1 v_k \\ w_{k+2} &= Mw_{k+1} - N_2 w_k, \end{aligned}$$

where $M = \sqrt{P}$, $N_1 + N_2 = \frac{Q}{P}$ and $N_1 N_2 = R$. We twist these general Lucas sequences $\boldsymbol{v}$ and $\boldsymbol{w}$ with $\tau = \sqrt{P}$, obtaining the twists $\tilde{\boldsymbol{v}}$ and $\tilde{\boldsymbol{w}}$ with terms $\tilde{v}_k = P^{\frac{k}{2}} v_k$ and $\tilde{w} = P^{\frac{k}{2}} w_k$, respectively, satisfying the recurrence relations

$$\begin{aligned} \tilde{v}_{k+2} &= \tau M \tilde{v}_{k+1} - \tau^2 N_1 \tilde{v}_k \\ &= P\tilde{v}_{k+1} - PN_1 \tilde{v}_k \end{aligned}$$

and

$$\begin{aligned} \tilde{w}_{k+2} &= \tau M \tilde{w}_{k+1} - \tau^2 N_2 \tilde{w}_k \\ &= P\tilde{w}_{k+1} - PN_2 \tilde{w}_k. \end{aligned}$$

Recall that N_1, N_2 are roots of $Y^2 - \frac{Q}{P}Y + R$. Then PN_1, PN_2 are roots of $Y^2 - QY + P^2R$. So now we are certain that PN_1, PN_2 are algebraic integers. So the twists $\tilde{\boldsymbol{v}}$ and $\tilde{\boldsymbol{w}}$ are general Lucas sequences. We can twist the divisibility sequence u_k as follows:

$$(\tau^k v_k)(\tau^k w_k) = \tau^{2k} v_k w_k = \tau^{2k} u_k = P^k u_k.$$

Recall the recurrence relation (3.5.5) of the terms u_k:

$$u_{k+4} = Pu_{k+3} - (Q - 2R)u_{k+2} + PRu_{k+1} - R^2 u_k.$$

By Definition 3.6.1 the terms $\tilde{u}_k$ then satisfy the following recurrence relation:

$$\tilde{u}_{k+4} = P^2 \tilde{u}_{k+3} - P^2(Q - 2R)\tilde{u}_{k+2} + P^4 R\tilde{u}_{k+1} - P^4 R^2 \tilde{u}_k.$$

So for the fourth order divisibility sequence $\boldsymbol{u}$ in $\mathbb{Z}$, there is also the fourth order divisibility sequence $\tilde{\boldsymbol{u}}$ in $\mathbb{Z}$, with terms $\tilde{u}_k = P^k u_k = (\tau^k v_k)(\tau^k w_k) = \tilde{v}_k \tilde{w}_k$. In particular, while u_k is a product of second order sequences that look a lot like Lucas-Lehmer sequences, $\tilde{u}_k$ is the product of two general Lucas sequences, $\tilde{v}_k$ and $\tilde{w}_k$.

References

[1] E. Croot. Notes on linear recurrence sequences. `http://people.math.gatech.edu/~ecroot/recurrence_notes2.pdf`, 2005.

[2] H. C. Williams. *Édouard Lucas and Primality Testing*. Canadian Mathematical Society series of monographs and advanced texts, 1998. ISBN 0-471-14852-4.

[3] M. Ward. The law of apparition of primes in a Lucasian sequence. *Transactions of the American Mathematical Society*, 44:68–86, 1938.

[4] J. F. Ritt. A factorization theory for functions $\sum_{i=1}^{n} a_i e^{\alpha_i x}$. *Transactions of the American Mathematical Society*, 29(3):584–596, 1927.

[5] L. Mirsky. *An Introduction to Linear Algebra*. Dover Publications, 1990. ISBN 0-486-66434-1.

[6] B. Sturmfels. Polynomial equations and convex polytopes. *American Mathematical Monthly*, 105:907–922, December 1998.

[7] I. M. Gelfand, M. M. Kapranov, and A. V. Zelevinsky. *Discriminants, Resultants, and Multidimensional Discriminants*. Birkhäuser Boston, 1994. ISBN 0-8176-4770-4.

[8] H. J. S. Smith. On systems of linear indeterminate equations and congruences. *Philosophical Transactions of the Royal Society of London*, 151:293–326, 1861.

[9] M. A. Armstrong. *Groups and Symmetry*. Springer-Verlag, 1988. ISBN 0-387-96675-7.

[10] R. S. Rumely. Notes on van der Poorten's proof of the Hadamard Quotient Theorem. *Séminaire de Théorie des Nombres, Paris 1986-87*, pages 349–409, 1989.

[11] C. Pisot. Conférences données à l'Institut Fourier de Grenoble, 1959.

[12] D. G. Cantor. On arithmetic properties of the Taylor series of rational functions II. *Pacific Journal of Mathematics*, 41:329–334, 1972.

[13] Y. Pourchet. Solution du problème arithmetique du quotient de Hadamard de deux fractions rationelles. *Comptes-rendus de l'Académie des Sciences Paris*, 288:1055–1057, 1979.

[14] D. H. Lehmer. An extended theory of Lucas' functions. *The Annals of Mathematics*, 31(3):419–448, 1930.

[15] M. Hall. Divisibility sequences of third order. *American Journal of Mathematics*, 58(3):577–584, 1936.

[16] H. C. Williams. A problem concerning divisibility sequences. Slides from the Ottawa-Carleton Number Theory Seminar at Carleton University of Canada, March 2010.