# On problems related to multiple solutions of Pell's equation and continued fractions over function fields

*Nikoleta Dianova Kalaydzhieva*

A dissertation submitted in partial fulfillment

of the requirements for the degree of

**Doctor of Philosophy**

of

**University College London**.

Department of Mathematics

University College London

November 30, 2020

I, Nikoleta Dianova Kalaydzhieva, confirm that the work presented in this thesis is my own. Where information has been derived from other sources, I confirm that this has been indicated in the work.

# Abstract

We study old problems, connected to the theory of continued fractions, with a new twist: changing the setting from the real numbers to the field of formal Laurent series in $1/t$.

In the classical theory, a famous by-product of the continued fraction expansion of quadratic irrational numbers $\sqrt{D}$ is the solution to Pell's equation for $D$. It is well-known that, once an integer solution to Pell's equation exists, we can use it to generate all other solutions $(u_n, v_n)_{n\in\mathbb{Z}}$. Our object of interest is the polynomial version of Pell's equation, where the integers are replaced by polynomials with complex coefficients. We then investigate the factors of $v_n(t)$. In particular, we show that over the complex polynomials, there are only finitely many values of $n$ for which $v_n(t)$ has a repeated root. Restricting our analysis to $\mathbb{Q}[t]$, we give an upper bound on the number of "new" factors of $v_n(t)$ of degree at most $N$. Furthermore, we show that all "new" linear rational factors of $v_n(t)$ can be found when $n \leq 3$, and all "new" quadratic rational factors when $n \leq 6$.

Another application of continued fractions arises from the theory of rational approximations to real irrational numbers. There, if we truncate the continued fraction expansion of $\alpha \in \mathbb{R}$, the resulting rational number "best" approximates it. This consequence remains true when we replace real numbers by formal Laurent series in $1/t$. In the framework of power series over the rational numbers, we define the Lagrange spectrum, related to Diophantine approximation of irrationals, and the Markov spectrum, related to elements represented by indefinite binary quadratic forms. We compute both spectra, by showing they equal sets whose elements are quantities attached to doubly infinite sequences of non-constant polynomials. Moreover, we prove that Lagrange and Markov spectra coincide and exhibit no gaps, contrary to what happens over the real numbers.

# Impact Statement

Continued fractions are special representations of numbers and, more generally, power series with coefficients in a given field. They have long been of interest to the mathematical community, but also have applications in areas such as cyber security, cryptography and image processing.

This thesis primarily impacts the study of Pellian polynomials. In particular, through understanding the factorisation of the solutions to Pell's equation for such polynomials, we are able to give a method of constructing new polynomials for which Pell's equation is solvable. We also contribute to the areas of Diophantine approximation and binary quadratic forms by explicitly describing the spectrum of Markov, related to representations of indefinite binary quadratic forms with coefficients formal Laurent series, and the spectrum of Lagrange, related to rational approximations of irrational power series.

Outside of mathematics, results from number theory are often utilised to answer questions on cyber security. A typical problem of interest is that of the breakability of the crypto algorithm used when sending sensitive data. For example, for RSA, Wiener showed that the theory of continued fractions can be employed to determine the private key generated by the algorithm and used for decryption, provided that it is smaller than a certain bound, yielding a computationally efficient attack on public-key cryptosystems. Furthermore, the continued fraction expansion for Laurent series can be applied to the theory of stream ciphers. There, Niederreiter showed that Laurent series with coefficients in a finite field, with bounded partial quotients are directly connected to linear complexity profiles of sequences and pseudorandom number generation. The results in this thesis do not have a particular cryptography problem in mind; however the theory developed could be of use.

# Acknowledgements

First, I would like to thank my supervisor Andrew Granville for giving me the opportunity to explore the beauty of Mathematics; for making me an independent researcher and thinker; for his support and patience with all my extra interests, and for always pushing me to be better!

I would like to thank Luciano Rila, for being the one who inspired me to pursue Mathematics all those years ago, for the many years of friendship and support and for all the opportunities to share my love of Mathematics with the public. To my academic family and the analytic number theory group for our numerous seminars and study group and for making conference trips so much more enjoyable. I am indebted to Oleksey Klurman and Ardavan Afshar, for the lovely discussions, both mathematical and not, for the motivational words and always knowing how to make my worries and frustration go away. I would like to thank the department of Mathematics at UCL for being so warm, welcoming and supportive and making me feel like home for 8 years, and lastly for letting me organise a lot of fun social activities. Special thanks to David Sheard for pointing out all my rogue uses of punctuation and obsession with furthermore.

I would like to acknowledge the SuperKLB for the hours wasted in the pub, park, and various other locations, discussing anything and everything from paper cup spheres and triangles to Nutela addictions. You made my PhD experience super awesome! To Chalkdust – the magazine for the mathematically curious – for showing me how fun it is to work in a team and giving me the feeling of being part of something special. I would also like to thank my lunchtime crew for many enjoyable lunches and bizarre conversations, mostly concerning fruit. To Udhav Fowdar for trying to make me a machine, dude, during our coffee breaks. To Sally Said for supporting my shoe addiction and Carmen Cabrera Arnau for trying to create my

gym addiction. To Alberto Lazzari for the wild nights, infused by tequila, making me feel/act like a teenager, followed by the best brunches. To my travel companion, partner in crime and cheerleader, Giulia Luise, we did it!

To my urban family - my flatmates Asli and Ashley for being nothing but supportive, nothing but wild fun, and definitely not dull and tired.

To my parmegianos – Boryana and Marina – for the lovely beach holidays which kept me sane, tanned and thoroughly hydrated – one can only be so lucky to have friends to share the best and the worst with, for over 15 years!

And last but definitely not least, I could not have done this without my family – I am eternally indebted for their love, support and encouragement to follow my chosen path.

It has been a journey – Don’t stop believing.

# Contents

## Chapter 1

# Introductory materials

## 1.1 Introduction

Pell's equation is defined to be

$$x^2 - Dy^2 = 1, \tag{1.1}$$

and classically solved in positive integers $x = u,\ y = v$, for a given non-zero positive integer $D$, which is not a square.

If we take the solution $(u, v)$ in which $v$ is the smallest positive integer, then we can use it to generate all other solutions to (1.1) by

$$u_n \pm v_n\sqrt{D} = \pm\left(u + v\sqrt{D}\right)^n. \tag{1.2}$$

In this thesis we are interested in the polynomial analogue to the integers case. Indeed, we study solutions $u(t), v(t) \in \mathbb{C}[t]$, with $v \neq 0$, to Pell's equation for a polynomial $D(t)$ with coefficients in $\mathbb{C}$. If (1.1) is solvable, we take its *fundamental solution*, the one in which $v$ has minimal degree, and obtain all other solutions $(u_n(t), v_n(t))_{n\in\mathbb{Z}}$ in the same way as in the classical case, using (1.2).

Our goal, in the first part of the thesis, is to better understand the polynomials $v_n(t)$ that arise in the solutions of Pell's equation when $D(t) \in \mathbb{Q}[t]$. In the classical case, when $D$ is a square-free, positive integer, it has been of great interest to factor $v_n \in \mathbb{Z}$, see [5]. Additionally, Lehmer [20] showed that in certain cases $v_n \in \mathbb{Z}$ factors into many parts. However, we will see that in the polynomial case the factors over $\mathbb{Q}[t]$ of $v_n(t)$ are very controlled.

Similar to the integers case, we have that $gcd(v_n(t), v_m(t)) = v_{gcd(m,n)}(t)$. In particular, if $m \mid n$ then $v_m(t) \mid v_n(t)$, and $v_1(t) \mid v_n(t)$, for all $n$. Furthermore, we will also show that $gcd\,(v_m(t),\ v_n(t)/v_m(t)) = 1$, which is not always the case over the integers: there, if a prime $p \mid v_n$, but $p^2 \nmid v_n$, then $p^2 \mid v_{np}$; in other words $p \mid gcd\,(v_n,\ v_{np}/v_n)$.

Over $\mathbb{C}[t]$, we can write $v_n(t) = v_n^{\text{old}}(t) v_n^{\text{new}}(t)$, where $v_n^{\text{old}}(t)$ is a product of the factors of $v_n(t)$ that also divide $v_m(t)$ for some $m < n$, and $v_n^{\text{new}}(t)$ are the remaining factors, including multiplicity. Then we obtain

$$v_n(t) = \prod_{m|n} v_m^{\text{new}}(t) \text{ and}$$
$$v_n^{\text{new}}(t) = \prod_{m|n} v_m^{\mu\left(\frac{n}{m}\right)}(t),$$

where the latter follows from the product form of Möbius inversion. Furthermore, the $v_n^{\text{new}}$ are pairwise co-prime, so we study their factors. Our first goal is to understand whether $v_n^{\text{new}}(t)$ ever has any repeated factors. It turns out that for any fixed $D(t) \in \mathbb{C}[t]$, there are only finitely many $n$ for which $v_n^{\text{new}}(t)$ has repeated factors. This comes out as a consequence of

**Theorem 1.1.1.** *For any polynomial $D(t) \in \mathbb{C}[t]$, for which the associated Pell's equation has a fundamental solution $(u(t), v(t))$, we define*

$$R(D) := \{\alpha \in \mathbb{C} : (t-\alpha)^2 \mid v_n^{new}(t) \text{ for some } n\}.$$

*Then $\#R(D) \leq \deg u - 1$.*

The proof actually gives us a finite algorithm that yields all repeated roots of $v_n^{\text{new}}$ for all $n$. It turns out that they come from the factors of $u'(t)$. Suppose $(t-\alpha)^k \parallel u'(t)$, for $k \geq 1$. We show that if $u(\alpha) = \cos\frac{\pi r}{n}$, for some $r < n$, with $(r,n) = 1$, then $(t-\alpha)^{k+1} \parallel v_n^{\text{new}}(t)$.

If we then restrict ourselves to working over $\mathbb{Q}[t]$, the repeated root $\alpha$ must come from a field extension of degree $d_\alpha$, satisfying $\varphi(2n)/2 < d_\alpha < \deg u$. So using results on the growth order of the Euler totient function [40] we show that if $v_n^{\mathrm{new}}(t)$ has a repeated root, we must have $n \ll d \log\log d$, where $d = \deg u$.

We then proceed to look at the degrees of the irreducible factors of $v_n^{\mathrm{new}}(t)$ when $u, v, D \in \mathbb{Q}[t]$, and obtain various Galois theoretic results.

**Theorem 1.1.2.** *Let $N$ be a positive integer, and define*

$$I(N) := \{P(t) \in \mathbb{Q}[t],\ \textit{irreducible}: \deg P \leq N,\ P(t) \mid v_m^{new}(t) \textit{ for some } m\}.$$

*Then $\#I(N) \leq 10N \deg u$, for $N$ large enough.*

If we want a result that holds for all $N$, we can get $\#I(N) \leq 4N^2 \deg u$.

Specialising to factors of certain degree, we show:

**Theorem 1.1.3.**

1. *There are no linear polynomials with coefficients in $\mathbb{Q}$ that divide $v_n^{new}(t)$, for $n \geq 4$.*

2. *There are no quadratic polynomials with coefficients in $\mathbb{Q}$ that divide $v_n^{new}(t)$, for $n \geq 7$.*

Both of these results are best possible. To see this, we present the following example:

**Example.** Let $D(t) = t^2 - 1$, then its Pell's equation has a fundamental solution $(t, 1)$. The only linear factors of $v_n(t)$, are $v_2^{\mathrm{new}} = 2t$, $v_3^{\mathrm{new}} = 2t \pm 1$. For $n \geq 4$, there are no linear factors over the rational numbers. Furthermore, the only quadratic irreducible factors are $v_4^{\mathrm{new}} = 2t^2 - 1$, $v_5^{\mathrm{new}} = 4t^2 \pm 2t - 1$ and $v_6^{\mathrm{new}} = 4t^2 - 3$. For $n \geq 7$, $v_n^{\mathrm{new}}$ has no irreducible quadratic factors in $\mathbb{Q}[t]$. We will give examples for all possibilities in section 3.3.1.

Moreover, we show that for a repeated root of $v_n^{\mathrm{new}}(t)$ to be of a prime degree $p$, then $p$ lies in a subset of the primes that has density 0.

**Theorem 1.1.4.** *Suppose $D(t) \in \mathbb{Q}[t]$, which has Pell's equation with fundamental solution $(u,v)$. If the polynomials $v_n^{new}(t)$ for $n > 3$ have a repeated root $\alpha$ of an odd prime degree $d_\alpha$, then either $n = 2d_\alpha + 1$ is also prime, or $n = 9$ in which case $\alpha$ is cubic.*

Restricting our investigation to polynomials with integer coefficients:

**Corollary 1.1.5.** *For $u,v,D \in \mathbb{Z}[t]$, the polynomials $v_n^{new}(t)$ for $n > 3$ have no repeated factors that are quadratic polynomials with integer coefficients.*

Solving the polynomial Pell's equation is not completely analogous to the classical case: for instance, there are certain $D(t) \in \mathbb{C}[t]$ with corresponding Pell's equation that has no non-trivial solutions. This is obvious when $D(t)$ has odd degree, since the term of highest degree cannot be cancelled. Therefore, we fix $D(t)$ to be a polynomial of degree $2d$ and look for solutions to (1.1) amongst polynomials with complex coefficients. However, there are examples when $D(t)$ has even degree, for instance $D(t) = t^4 + t + 1$, where it is less obvious why the corresponding Pell's equation is not solvable. We will call polynomials $D(t)$ for which (1.1) has a non-trivial solution *Pellian.*

We can use our understanding of the factors of $v_n(t)$, for a given Pellian polynomial $D(t)$, together with the following lemma, to construct new Pellian polynomials.

**Lemma 1.1.6.** *The polynomial $F^2D(t)$ is Pellian if and only if $D(t)$ is a Pellian polynomial with solutions $(u_n(t), v_n(t))_{n\in\mathbb{Z}}$, and $F(t) \mid v_n(t)$, for some $n$.*

Furthermore, recall that if we restrict $D(t)$, $u(t)$ and $v(t) \in \mathbb{Q}[t]$, then there are only finitely many factors $F(t) \in \mathbb{Q}[t]$ of $v_n(t)$, of a given degree. Therefore, there are infinitely many families of infinitely many polynomials of the form $F^2D(t)$ that are not Pellian. This contrasts with the situation over the integers, where for any non-square positive integer of the form $F^2D$, Pell's equation is solvable.

The discrepancy of there being solutions for every non-square, positive integer $D$, but not for every polynomial $D(t)$, arises from the underlying relation with the theory of continued fraction expansions for quadratic irrationals. In particular, Pell's equation is solvable for all non-square, positive integers $D$ because the continued fraction of $\sqrt{D}$ is always periodic.

Abel [1] was the first one to consider the continued fraction expansion for $\sqrt{D(t)}$ for monic, non-square polynomials $D(t) \in \mathbb{Q}[t]$ of even degree, and thus he extended the theory to $\mathbb{Q}((1/t))$. The field $\mathbb{Q}((1/t))$ plays the role of $\mathbb{R}$, and is the completion of $\mathbb{Q}(t)$, under the valuation $-\partial eg$ , where for an element $\alpha = \sum_{-\infty}^{m} a_i t^i \in \mathbb{Q}((1/t))$, with $a_m \neq 0$, we define $\partial eg\ \alpha := m$. Any formal Laurent series $\alpha \in \mathbb{Q}((1/t))$ can be written as a continued fraction:

$$\alpha = [a_0, a_1, a_2, \ldots] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots}},$$

where the *partial quotients* $a_i$ are polynomials with rational coefficients, and the truncated continued fraction is a rational function of polynomials with rational coefficients, called a *convergent*. Moreover, Abel showed that the connection between solutions to Pell's equation and continued fractions carries over to the polynomial setting:

**Theorem.** (Abel) *A monic polynomial* $D(t) \in \mathbb{Q}[t]$ *is Pellian if and only if the continued fraction of* $\sqrt{D(t)}$ *is periodic.*

We have seen, however, that not every polynomial $D(t) \in \mathbb{Q}[t]$ is Pellian, hence $\sqrt{D(t)}$ is not always periodic, which highlights a major discrepancy with the theory of continued fractions for real irrational numbers. However, if there are solutions to Pell's equation for $D(t)$, then they can be found amongst the convergents of the continued fractions expansion of $\sqrt{D(t)}$, similarly to the classical case. Moreover, this method of finding solutions to Pell's equation arises from the fact that the convergents $p(t)/q(t)$ best approximate $\alpha \in \mathbb{Q}((1/t))$.

To quantify the idea of good, in the classical case, we say that a rational number $p/q$ is a *best approximation* for $r \in \mathbb{R}$ if for every other pair of integers

$P,Q$, such that $Q \leq q$, then $|r-p/q| < |r-P/Q|$. Furthermore, we know that if $|r-p/q| < 1/2q^2$, then $p/q$ must be a convergent of $\alpha$, and that all convergents of $r$ satisfy $|r-p/q| < 1/q^2$. Observe that as $q$ grows, the distance from $r$ to the convergent can be arbitrarily reduced. So it is more natural to consider the quantity $q^2|r-p/q|$ as a measure of accuracy.

A consequence of a theorem of Dirichlet then states:

**Theorem.** *For every algebraic real number $r$, the inequality*

$$q^2\left|r-\frac{p}{q}\right| < 1$$

*is satisfied by infinitely many pairs of integers $p,q$, with $q \neq 0$.*

In 1903 this was further improved by Borel when he proves that infinitely many rational numbers $p/q$ satisfy

$$q^2\left|r-\frac{p}{q}\right| < \frac{1}{\sqrt{5}}.$$

A theorem of Hurwitz from 1891 asserts that $\sqrt{5}$ is the largest constant that works for all real irrational numbers. That means that if we increase the constant in the denominator further, the statement no longer holds, for example, for $r=(1+\sqrt{5})/2$. However, if we exclude $\sqrt{5}$ (and numbers 'equivalent to it') we can reduce the upper bound further to $1/\sqrt{8}$. This process, in some sense, yields the 'best' constant of Diophantine approximation for a given real number. That is, for $r \in \mathbb{R}/\mathbb{Q}$, we define the *Lagrange constant*, $l(r) = \sup L$, where the supremum is taken over all real numbers $L$, for which the inequality

$$q^2\left|r-\frac{p}{q}\right| < \frac{1}{L} \tag{1.3}$$

is satisfied by infinitely many rational numbers $p/q$, $q>0$. Running through all real irrationals, we obtain the *Lagrange spectrum*:

$$\mathbf{L} = \{l(\alpha) \ : \ \alpha \in \mathbb{R}/\mathbb{Q}\}.$$

The results on approximating irrational numbers by rationals can be translated to the setting of $\mathbb{Q}((1/t))$, which is the focus of this thesis. Unsurprisingly, we can also extend the definition of the Lagrange constant to formal Laurent series. For $\alpha \in \mathbb{Q}((1/t))$, not a rational function, we let the Lagrange constant, $l(\alpha)$, be the supremum over integers $k$ such that

$$\partial eg \left(\alpha - \frac{p(t)}{q(t)}\right) \leq -2\partial eg\ q(t) - k$$

is satisfied by infinitely many polynomials $p(t), q(t) \in \mathbb{Q}[t]$, with $q(t) \neq 0$. Observe that taking logs of (1.3) and replacing the absolute value by $\partial eg\ (\cdot)$ shows that the definition of $l(\alpha)$ is analogous to that of $l(r)$. Moreover, the Lagrange spectrum for formal Laurent series in $1/t$ is defined as

$$\mathscr{L} := \{l(\alpha)\ :\ \alpha \text{ a formal Laurent series in } 1/t\text{, not a rational function}\}.$$

Recently, some work has been done on the Lagrange spectrum in the setting of formal Laurent series in $1/t$, with coefficients in finite fields, by Parkkonen and Paulin in [33] and Bugeaud in [6]. In particular, they give analogies to the well-known results over the real numbers about the closedness and boundedness of the spectrum, as well as computations of its maximum.

We, however, study the Lagrange spectrum for formal Laurent series in $1/t$, with coefficients in $\mathbb{Q}$ and prove:

**Theorem 1.1.7.** *The Lagrange spectrum $\mathscr{L}$ for $\mathbb{Q}((1/t))$ is equal to $\mathbb{N} \cup \{\infty\}$.*

Furthermore, for each $l \in \mathscr{L}$, we construct an element $\alpha \in \mathbb{Q}((1/t))$, such that $l = l(\alpha)$.

Going back to the real case, Perron [35], using properties of the convergents of $r = [a_0, a_1, \ldots]$, showed that the Lagrange constant

$$l(r) = \limsup_{n\to\infty} (q_n|q_n r - p_n|)^{-1}$$

can be re-written as

$$l(r) = \limsup_{n\to\infty}(a_n + [0, a_{n-1}, \ldots, a_0] + [0, a_{n+1}, \ldots]). \tag{1.4}$$

Moreover, given a sequence of positive integers $A = \ldots, a_{-1},\ a_0,\ a_1, \ldots$ let

$$\lambda_n(A) = [a_{n+1},\ a_{n+2}, \ldots] + [0,\ a_n,\ a_{n-1}, \ldots].$$

In other words, using (1.4), we can prove that the set obtained from the $\limsup_{n\to\infty} \lambda_n(A)$, as we run through all such sequences $A$, is equal to the Lagrange spectrum. Interestingly, if we just consider the supremum of $\lambda_n(A)$ for all integers $n$, then the set

$$\mathfrak{M} := \{\sup_{n\in\mathbb{Z}} \lambda_n(A)\ :\ A \text{ doubly infinite sequence of positive integers}\}$$

is in one-to-one correspondence with the Markov spectrum $\mathbf{M}$, classically related to binary quadratic forms. Namely, given a real binary quadratic form $q = q(x,y) = ax^2 + bxy + cy^2$, of discriminant $d(q) = b^2 - 4ac > 0$, we let

$$\mu(q) := \inf_{\substack{x,y\in\mathbb{Z}\\(x,y)\neq(0,0)}} |q(x,y)|$$

be its arithmetic minimum. Then

$$\mathbf{M} := \left\{ \frac{\sqrt{d(q)}}{\mu(q)}\ :\ q \text{ a real binary quadratic form with positive discriminant} \right\}.$$

Markov [26] exhaustively studied the part of the spectrum below 3, showing that it is a discrete set. His methods involved proving that for each element $m \in \mathbf{M}$ we can find a doubly infinite sequence of positive integers $A$ such that $\sup_{n\in\mathbb{Z}} \lambda_n(A) = m$ and that the converse is also true. Hurwitz [14] noted that techniques of Markov can be used to show that $\mathbf{L} \cap [0,3] = \mathbf{M} \cap [0,3]$. However if we consider the two spectra for numbers greater than 3, we have $\mathbf{L} \subsetneq \mathbf{M}$, see [13] and [44]. In [44] and [10], Delone together with Fuks and Vinogradov showed that there exists some $\mu > 3$, such that

$$\mathbf{L} \cap [\mu, \infty) = \mathbf{M} \cap [\mu, \infty) = [\mu, \infty).$$

But the parts of the Markov and Lagrange spectra in the interval $[3, \mu]$ have a more complex structure. Namely, they are closed sets with an infinite number of adjoining intervals. That is, they exhibit gaps; for example in $(\sqrt{12}, \sqrt{13})$ there are no points of either the Lagrange or Markov spectrum. For a more detailed survey of results over the real numbers see [25]. Analogously to the case over the real numbers, we define binary quadratic forms $Q$, with coefficients in $\mathbb{Q}((1/t))$. They are homogeneous expressions of degree 2 of the form

$$Q = Q(X,Y) = AX^2 + BXY + CY^2,$$

with $A, B, C \in \mathbb{Q}((1/t))$, of discriminant $D(Q) = B^2 - 4AC$, and with corresponding minima

$$m(Q) = \inf_{\substack{X,Y \in \mathbb{Q}((1/t)) \\ (X,Y) \neq (0,0)}} \partial eg\ Q(X,Y).$$

Moreover, the square root $\sqrt{D}$ is well-defined in $\mathbb{Q}((1/t))$, see Lemma 2.2.2. Thus the Markov spectrum over $\mathbb{Q}((1/t))$ is given by

$$\mathscr{M} := \left\{ \partial eg\ \sqrt{D(Q)} - m(Q)\ :\ Q \text{ binary quadratic form} \right\}.$$

In order to describe $\mathscr{M}$, we take an analogous approach to the one used by Markov [26], first showing that both Markov and Lagrange spectra are equal to sets of quantities attached to doubly infinite sequences of non-constant polynomials. For the appropriate analogue, in the definition of $A = \ldots, a_{-1},\ a_0,\ a_1, \ldots$ and $\lambda_n(A)$, we replace positive integers $a_i$, by positive degree polynomials $a_i(t) \in \mathbb{Q}[t]$. We thus prove

**Theorem 1.1.8.**

1. *The Lagrange spectrum $\mathscr{L}$ is equal to the set*

$$\mathbb{L} := \{L(A) : A \textit{ is a doubly infinite sequence of } a_i \in \mathbb{Q}[t],\ \deg a_i > 0\},$$

*where* $L(A) := \limsup_{n\in\mathbb{Z}} \partial eg\ \lambda_n(A)$.

2. *The Markov spectrum $\mathscr{M}$ is equal to the set*

$$\mathbb{M} := \{M(A) : A \textit{ is a doubly infinite sequence of } a_i \in \mathbb{Q}[t],\ \deg a_i > 0\},$$

*where* $M(A) := \sup_{n\in\mathbb{Z}} \partial eg\ \lambda_n(A)$.

We then use this result to explicitly compute the Markov spectrum, showing that the two spectra coincide and exhibit no gaps.

**Theorem 1.1.9.** *The Markov spectrum for $\mathbb{Q}((1/t))$ is equal to the Lagrange spectrum for $\mathbb{Q}((1/t))$ and they are both equal to $\mathbb{N} \cup \{\infty\}$.*

## 1.2 Organisation of the thesis

In chapter 2 we introduce the setting of this thesis, $\mathbb{Q}((1/t))$, the field of formal Laurent series in $1/t$ with coefficients in the rational numbers. We then discuss the theory of continued fractions of irrational elements $\alpha \in \mathbb{Q}((1/t))$, stating and proving important properties of the convergents. Then we present the theory of rational approximations in function fields, and survey the results necessary to define and compute Lagrange spectrum, discussed in chapter 4. Finally, we highlight the connection between 'good' rational approximations to quadratic irrational elements $\sqrt{D(t)} \in \mathbb{Q}((1/t))$ given by the convergents, and solutions to the polynomial Pell's equation for $D(t) \in \mathbb{Q}[t]$.

In chapter 3, we focus completely on the polynomial Pell's equation and its solutions $(u_n(t), v_n(t))_{n\in\mathbb{Z}}$. For $D(t)$, $u(t)$ and $v(t) \in \mathbb{C}[t]$ we investigate the possibility of $v_n(t) \in \mathbb{C}[t]$ having repeated factors, and give estimates on their number. Restricting the polynomials $D(t)$, $u(t)$ and $v(t) \in \mathbb{Q}[t]$ we prove an upper bound on the number of polynomials in $\mathbb{Q}[t]$, of degree at most $N \in \mathbb{N}$, that divide $v_n(t)$. We conclude with Galois theoretic results on the degree of real algebraic numbers that arise as factors of high multiplicity in the factorisation of $v_n(t) \in \mathbb{Q}[t]$.

Chapter 4 is dedicated to the Lagrange spectrum of formal Laurent series in $1/t$. We survey results in the literature, concerned with the accuracy of the approximation of irrational elements $\alpha \in \mathbb{Q}((1/t))$ by rational functions of polynomials with coefficients in $\mathbb{Q}$. This leads to the definition of the Lagrange (approximation) constant $l(\alpha)$. We prove that for a Pellian polynomial $D(t)$ of degree $2d$, $l(\sqrt{D(t)}) = d$ and also investigate $l(\sqrt{D(t)})$ when $D(t)$ is non-Pellian. The chapter culminates in the computation of the Lagrange spectrum over $\mathbb{Q}((1/t))$, and the proof that its elements are in one-to-one correspondence with $\limsup_{n\in\mathbb{Z}} \lambda_n(A)$, attached to doubly infinite sequences of non-constant polynomials $A$.

In the final chapter, we lay down the theory of binary quadratic forms with coefficients in $\mathbb{Q}((1/t))$, which we have been unable to find in the necessary detail in the literature. We study the equivalence and representation of binary quadratic forms, tools which we use to define the Markov spectrum $\mathscr{M}$ over $\mathbb{Q}((1/t))$. As part of the process of computing the spectrum, we prove that it is equal to a set obtained from doubly infinite sequences of non-constant polynomials. Finally, we prove $\mathscr{M} = \mathbb{N} \cup \{\infty\}$.

In the Appendix we give a short Mathematica code, written by the author in order to compute the continued fraction expansion for rational functions and square roots of polynomials with coefficients in the rational numbers.

Chapter 2

# Preliminary definitions and results

In this chapter we will describe the setting of our investigations, covering all of the preliminary notions and results needed for the remainder of the thesis. Firstly, we will set the scene by defining the set of formal Laurent series in $1/t$. Even though our main object of study – continued fractions – can be defined over any normed field, we will concentrate on the set up of formal series with coefficients in the rational numbers. Secondly, we will describe the continued fraction algorithm in this function field setting and any relevant results. Finally, we will outline the connection with the study of solutions to Pell's equation, which is the other prominent player in this thesis. Throughout we will draw parallels between the results in the function field case and the well-known classical setting.

## 2.1 The field of formal Laurent series in $1/t$

Let $\mathbb{Q}[t]$ be the ring of polynomials with coefficients in the rational numbers, and $\mathbb{Q}(t) = \{A/B : A,B \in \mathbb{Q}[t],\ B \neq 0\}$ be its field of fractions. These will, respectively, play the roles of the integers and rational numbers in the classical case. Furthermore, the analogue of the real numbers is given by the set of formal Laurent series in $1/t$ with coefficients in $\mathbb{Q}$, denoted by

$$\mathbb{Q}((1/t)) = \left\{ \sum_{i=-\infty}^{m} a_i t^i : m \in \mathbb{Z}, a_i \in \mathbb{Q}, \forall i,\ a_m \neq 0 \right\}.$$

It is easy to see that $\mathbb{Q}((1/t))$ forms a ring, where the sum and product are defined as expected:

$$\sum_{i=-\infty}^{m} a_i t^i + \sum_{i=-\infty}^{n} b_i t^i = \sum_{i=-\infty}^{\max(n,m)} (a_i + b_i) t^i,$$
$$\left(\sum_{i=-\infty}^{m} a_i t^i\right)\left(\sum_{j=-\infty}^{n} b_j t^j\right) = \sum_{k=-\infty}^{m+n} \left(\sum_{l \leq m} a_l b_{k-l}\right) t^k,$$

where for $i > m$ or for $j > n$, we set $a_i = 0$ or $b_j = 0$, respectively. Notice that this implies that $\mathbb{Q}[t]$ is a subring of $\mathbb{Q}((1/t))$.

Furthermore, this formal set of Laurent series is also a field, where for a non-zero $\alpha = \sum_{i=-\infty}^{m} a_i t^i$, its inverse is given by $\beta = \sum_{j=-\infty}^{-m} b_j t^j$, for which we can explicitly describe the coefficients, by examining

$$\left(\sum_{i=-\infty}^{m} a_i t^i\right)\left(\sum_{j=-\infty}^{-m} b_j t^j\right) = \sum_{k=-\infty}^{0} \left(\sum_{l=m+k}^{m} a_l b_{k-l}\right) t^k = 1.$$

Hence the coefficient for $k = 0$ must be equal to 1, yielding $b_{-m} = 1/a_m$; and for $k < 0$, the coefficients must satisfy $\sum_{l=m+k}^{m} a_l b_{k-l} = 0$. This final expression gives us the equations $a_m b_{k-m} = -\sum_{l=m+k}^{m-1} a_l b_{k-l}$, or upon multiplying through by $a_m^{-1} = b_{-m}$:

$$b_{k-m} = -\frac{1}{a_m} \sum_{l=m+k}^{m-1} a_l b_{k-l}, \text{ for each } k < 0.$$

After solving these equations inductively, we obtain an explicit expression for the multiplicative inverse $\beta$. As a consequence, $\mathbb{Q}(t)$ is a subfield of $\mathbb{Q}((1/t))$.

**Lemma 2.1.1.** *The formal Laurent series $\alpha = \sum_{i=-\infty}^{m} a_i t^i \in \mathbb{Q}((1/t))$, represents a rational function if and only if there exist a finite sequence of rational numbers $b_0, \ldots, b_n$ not all $0$, and an integer $m_0 \leq m$, such that for all $k \leq m_0$,* *we have*

$$a_k b_0 + \cdots + a_{k-n} b_n = 0.$$

*Proof.* The idea is that $\alpha \in \mathbb{Q}(t)$ if and only if there exists a polynomial $b \in \mathbb{Q}[t]$ such that $\alpha b \in \mathbb{Q}[t]$. So if we take the $b_i$, to be the coefficients of the polynomial $b$, the result follows. □

We can extend the usual definition of degree to $\mathbb{Q}((1/t))$ in the following way:

**Definition 2.1.1.** For $\alpha = \sum_{-\infty}^{m} a_i t^i$, $a_m \neq 0$, define

$$\begin{aligned} \partial eg\ &: \mathbb{Q}((1/t)) \to \mathbb{Z} \\ &\alpha \mapsto m, \end{aligned}$$

with the convention $\partial eg\ 0 = -\infty$.

This map is well defined on rational functions and it agrees with the usual definition of degree on polynomials, i.e.

**Lemma 2.1.2.** *For $A, B \in \mathbb{Q}[t]$, with $B \neq 0$, of degrees $m$ and $n$, respectively*

1. $\partial eg\ \frac{A}{B} = \deg A - \deg B$.

2. $\partial eg\ A = \deg A$.

*Proof.* Observe that the first implies the second, so it suffices to prove 1. Consider $A, B \in \mathbb{Q}[t]$, with $B \neq 0$. Then

$$A = \sum_{i=0}^{m} a_i t^i = a_m t^m \left(1 + \sum_{i=0}^{m-1} A_i t^{i-m}\right),$$
$$B = \sum_{i=0}^{n} b_i t^i = b_n t^n \left(1 + \sum_{i=0}^{n-1} B_i t^{i-n}\right)$$

and $a_m, b_n \neq 0$. Furthermore,

$$\begin{aligned}\frac{A}{B} &= \frac{a_m}{b_n} t^{m-n} \left(1 + O(t^{-1})\right) \left(1 + O(t^{-1})\right)^{-1} \\ &= \frac{a_m}{b_n} t^{m-n} \left(1 + O(t^{-1})\right).\end{aligned}$$

*Here by $O(t^{-1})$ we mean lower order terms in $t^{-1}$.* Hence, $\partial eg\ \frac{A}{B} = m - n = \deg A - \deg B$, as required. □

*Remark* 2.1.1. For $\alpha \in \mathbb{Q}((1/t))$, we have that $ord(\alpha) := -\partial eg\ \alpha$ is a valuation. We can further regard $\mathbb{Q}((1/t))$ as the completion of $\mathbb{Q}(t)$ under it. We can also associate a norm $\|\cdot\|$, given by $\|\alpha\| = c^{\partial eg\ \alpha}$, where $c \in \mathbb{R}$ and $c > 1$. One of the major differences in the study of continued fractions in this setting arises precisely from the fact that this norm is non-Archimedean, namely $\|\alpha + \beta\| \leq \max(\|\alpha\|, \|\beta\|)$, with equality when $\|\alpha\| \neq \|\beta\|$.

Over the real numbers, we use the continued fraction algorithm as an easy method to check if a real number is rational. Specifically, given a real number $r$, we subtract its integral part $\lfloor r \rfloor$, take the reciprocal and repeat the process. If this algorithm terminates in a finite number of steps then $r$ must be rational. Since $\mathbb{Q}((1/t))$ is a normed field, an analogous continued fraction expansion can be defined; but as we have shown above, taking the integral part of a real number is an essential part of the computation. To be able to define the process over $\mathbb{Q}((1/t))$, we should define an equivalent notion as follows.

**Definition 2.1.2.** The *polynomial part* of $\alpha = \sum_{-\infty}^{m} a_i t^i \in \mathbb{Q}((1/t))$ is given by

$$\lfloor \alpha \rfloor := \begin{cases} 0, & \text{if } \partial eg\ \alpha < 0 \\ \sum_{i=0}^{m} a_i t^i, & \text{if } \partial eg\ \alpha = m > 0. \end{cases}$$

The *fractional part* of $\alpha \in \mathbb{Q}((1/t))$ is defined as $\{\alpha\} := \alpha - \lfloor \alpha \rfloor$.

Observe that we can think of the polynomial part as the unique polynomial $a \in \mathbb{Q}[t]$, such that $\partial eg\ (\alpha - a) < 0$.

Furthermore, the polynomial part satisfies the following properties $\lfloor \alpha \rfloor + \lfloor \beta \rfloor = \lfloor \alpha + \beta \rfloor$ and $\lfloor r\alpha \rfloor = r\lfloor \alpha \rfloor$, where $\alpha, \beta \in \mathbb{Q}((1/t))$ and $r \in \mathbb{Q}$. However, $\lfloor \alpha \rfloor \lfloor \beta \rfloor = \lfloor \alpha\beta \rfloor$ does not always hold.

Moreover, this notion of polynomial part will have a central role in the reduction algorithm of indefinite binary quadratic forms defined later in the thesis.

## 2.2 Continued fraction algorithm over $\mathbb{Q}((1/t))$

The continued fraction algorithm over function fields works in a completely analogous way to the one over the real numbers. Nonetheless, for completeness, we will describe it below.

Let $\alpha \in \mathbb{Q}((1/t))$. First let $\alpha_0(t) = \alpha(t) \in \mathbb{Q}((1/t))$ and set $a_0(t) := \lfloor \alpha_0(t) \rfloor$. Hence $\alpha_0(t) = a_0(t) + \{\alpha_0(t)\}$, with $\{\alpha_0(t)\} \in \mathbb{Q}((1/t))$ of finite negative degree. Here, we are using $\{.\}$ and $\lfloor . \rfloor$, with a non-traditional meaning given in Definition 2.1.2. Therefore $\{\alpha_0(t)\}^{-1}$, also an element of $\mathbb{Q}((1/t))$, is well defined and of positive degree. Next, set $\alpha_1(t) := \{\alpha_0(t)\}^{-1}$, then $\alpha_0 = a_0 + 1/\alpha_1$. We proceed by recursion. Define

$$\begin{aligned} a_i(t) &:= \lfloor \alpha_i(t) \rfloor, \\ \alpha_{i+1}(t) &:= \{\alpha_i(t)\}^{-1} \\ \Rightarrow \alpha_i &= a_i + \frac{1}{\alpha_{i+1}}. \end{aligned}$$

Hence

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots \cfrac{1}{\alpha_{i+1}}}},$$

equivalently,

$$\alpha = [a_0,\ a_1,\ \ldots,\ a_i,\ \alpha_{i+1}].$$

The algorithm terminates if the fractional part $\{\alpha_i(t)\}$ is ever 0. We will refer to the $\alpha_i$ as the *complete quotients* and to the polynomials $a_i \in \mathbb{Q}[t]$ as the *partial quotients* of $\alpha$.

*Remark* 2.2.1. The polynomials $a_i(t)$, defined for $i$ up to the point of termination, are all of positive degree, except perhaps for $i = 0$. In particular, $a_0(t)$ can be a constant, however the others must have at least a linear term, since $\partial eg\ a_i(t) = \partial eg\ \lfloor \alpha_i(t) \rfloor = -\partial eg\ \{\alpha_i(t)\} > 0$.

The continued fraction of $\alpha$ will be infinite for most $\alpha \in \mathbb{Q}((1/t))$. In fact, we have the same correspondence between the finiteness of the algorithm and $\alpha$ being rational.

**Proposition 2.2.1.** *The continued fraction of $\alpha \in \mathbb{Q}((1/t))$ has a finite number of terms if and only if $\alpha \in \mathbb{Q}(t)$.*

*Proof.* If $\alpha$ has a finite continued fraction, then it is easy to see that the resulting expression will be a rational function.

For the converse, suppose that $\alpha_0 = p(t)/q(t) \in \mathbb{Q}(t) \backslash \mathbb{Q}[t]$, with $q(t) \neq 0$. Running the continued fraction algorithm we let $a_0 = \lfloor \alpha_0 \rfloor = \lfloor p/q \rfloor$, a polynomial with coefficients in $\mathbb{Q}$, and therefore

$$\alpha_1 = \frac{1}{\alpha_0 - a_0} = \frac{q}{p - a_0 q} \in \mathbb{Q}(t).$$

So set $q = r_0$ and define $r_1 := r_0/\alpha_1$. Hence, the polynomial $r_1 = p - a_0 r_0$ is such that $\deg r_1 < \deg r_0$, since $\partial eg\ \alpha_1 > 0$. This is equivalent to the first step in the Euclidean division algorithm, where $a_0$ is the quotient and $r_1$ is the remainder, in the division of $p$ by $q$.

To show that this is not a coincidence, let's look at the $i$ th step in the continued fraction algorithm in more detail. Let $r_i$ be defined recursively by

$i := r_{i-1}/\alpha_i$, $a_i = \lfloor \alpha_i \rfloor$ and $r_{i+1} = r_i/\alpha_{i+1}$. Then

$$\alpha_i = a_i + \frac{1}{\alpha_{i+1}} \;\Leftrightarrow\; \frac{r_{i-1}}{r_i} = a_i + \frac{r_{i+1}}{r_i} \;\Leftrightarrow\; r_{i-1} = a_i r_i + r_{i+1}.$$

Hence, $r_{i+1} \in \mathbb{Q}[t]$, and since $\partial eg\ \alpha_{i+1} > 0$, we have $\deg r_{i+1} < \deg r_i$. Therefore the continued fraction algorithm for $\alpha \in \mathbb{Q}(t)$, is in correspondence with the Euclidean division algorithm. Moreover, the latter is well-known to be finite, i.e. eventually $r_i = 0$. This corresponds to $\alpha_{i-1} \in \mathbb{Q}[t]$ and consequently $\{\alpha_{i-1}\} = 0$, terminating the continued fraction algorithm for $p/q$ in a finite number of steps. □

**Example 2.2.1.** Consider $\alpha = (t^7 + t^4 + t^2)/(t^5 + t + 1)$, then this has a continued fraction expansion

$$\left[t^2,\ t+1,\ t-1,\ -t,\ -\frac{t}{2}+\frac{1}{4},\ \frac{8t}{3}+\frac{4}{3}\right].$$

Another central object in our investigation will be quadratic irrationals, in particular, square roots of polynomials with coefficients in $\mathbb{Q}$. To see when they are well-defined elements of the field of formal Laurent series, consider the following result.

**Lemma 2.2.2.** *Let $D(t) \in \mathbb{Q}[t]$ be a monic polynomial of even degree. Then the square root of $D(t)$ is a well-defined element of $\mathbb{Q}((1/t))$, i.e., $\sqrt{\alpha}$ has a unique Laurent series expansion in $1/t$ with rational coefficients.*

*Proof.* Suppose we have $D(t)$ as above,

$$\begin{aligned} D(t) &= t^{2d} + \sum_{i=0}^{2d-1} a_i t^i \\ &= t^{2d}\left(1 + \sum_{i=0}^{2d-1} a_i t^{i-2d}\right). \end{aligned}$$

Since $\partial eg\left(\sum_{i=0}^{2d-1} a_i t^{i-2d}\right) < 0$, then

$$\left(1+\sum_{i=0}^{2d-1} a_i t^{i-2d}\right)^{1/2} = \sum_{n=0}^{\infty} \binom{1/2}{n} \left(\sum_{i=0}^{2d-1} a_i t^{i-2d}\right)^n$$

converges in $\mathbb{Q}((1/t))$. Thus, we define

$$\sqrt{D(t)} = t^d \left(1+\sum_{i=0}^{2d-1} a_i t^{i-2d}\right)^{1/2},$$

which is indeed an element of $\mathbb{Q}((1/t))$. □

*Remark* 2.2.2. Notice that we do not necessarily need $D(t)$ to be monic. As long as the leading coefficient of $D(t)$ is a square in $\mathbb{Q}$, $lc(D(t)) = a^2$, the above lemma still holds. Moreover, $\left(1+\sum_{i=0}^{2d-1} a_i t^{i-2d}\right)^{1/2}$ is unique up to the choice of sign, that is up to the choice of the square root of $lc(D(t))$, $\sqrt{a^2}$. We will accept the convention that $\sqrt{D} = at^d\left(1+\sum_{i=0}^{2d-1} a_i t^{i-2d}\right)^{1/2}$ and $-\sqrt{D} = -at^d\left(1+\sum_{i=0}^{2d-1} a_i t^{i-2d}\right)^{1/2}$.

Hence for $D(t) \in \mathbb{Q}[t]$ that are not square, but are of even degree, with leading coefficient a rational square, we have $\sqrt{D(t)} \in \mathbb{Q}((1/t))$. Therefore we can compute the continued fraction expansion of $\sqrt{D(t)}$ using the algorithm described in this section. Furthermore, since $D(t)$ is not a perfect square, $\sqrt{D(t)} \notin \mathbb{Q}(t)$ and its continued fraction is infinite.

**Example 2.2.2.** For $D(t) = 9t^8 + 7t$,

$$\begin{aligned}\sqrt{D(t)} &= \left[3t^4,\ 6t^3/7,\ 6t^4,\ 6t^3/7,\ 6t^4, \ldots\right] \\ &= \left[3t^4,\ \overline{6t^3/7,\ 6t^4}\right].\end{aligned}$$

That is, the continued fraction expansion is periodic with period 2.

Furthermore, if $D(t)$ is a quadratic polynomial we have an explicit expression for the continued fraction expansion.

**Example 2.2.3.** Suppose $D(t) \in \mathbb{Q}[t]$ is a quadratic polynomial, not a perfect square. Say, $D(t) = (at+b)^2 + c$, with $a, b, c \in \mathbb{Q}$ and $ac \neq 0$, then

$$\sqrt{D(t)} = \sqrt{(at+b)^2+c} = \left[at+b,\ \overline{\frac{2}{c}(at+b),\ 2(at+b)}\right].$$

However, and here lies the first major difference with the case over the real numbers, not every square root of a polynomial has a periodic continued fraction expansion.

**Example 2.2.4.** For $D(t) = t^4 + t^3$, we have

$$\sqrt{D(t)} = \left[t^2 + \frac{t}{2} - \frac{1}{8},\ 16t+10,\ -\frac{4t}{3} - \frac{13}{18},\ \frac{27t}{2} + \frac{225}{32},\ -\frac{512t}{405} - \frac{1312}{2025}, \dots\right].$$

It certainly does not look like the terms in the expansion will start repeating, but in general it is quite hard to determine if $\sqrt{D}$ is periodic or not. To justify why this particular continued fraction is not periodic, we invoke two theorems:

**Theorem.** (Dubickas & Steuding [12]) *The equation $x^2 - D(t)y^2 = 1$, for $D(t) \in \mathbb{C}[t]$, has no non-trivial solutions over the complex polynomials if the number of distinct roots $n(D(t)) \leq \deg D(t)/2$.*

And

**Theorem.** (Abel [1]) *The continued fraction for $\sqrt{D(t)}$ is periodic if and only if the equation $x^2 - D(t)y^2 = 1$ has non-trivial polynomial solutions in $\mathbb{C}((1/t))$.*

Therefore, $\sqrt{t^4+t^3}$ has a non-periodic continued fraction. The theorem of Dubickas and Steuding is an immediate consequence of the abc theorem for polynomials and will be discussed further in section 3.4. We will also pay closer attention to both periodic and non-periodic continued fractions for square roots of polynomials in section 4.2.1.

## 2.3 Convergents

Given an infinite continued fraction expansion, we can truncate at any point, say $[a_0, a_1, \dots, a_h]$, and since this is a finite expansion, the resulting expression will be a rational function of the form $p_h/q_h(t)$. Similarly to the integers case, we have the recursive relations

$$\begin{aligned} p_h &= a_h p_{h-1} + p_{h-2}, \\ q_h &= a_h q_{h-1} + q_{h-2}, \end{aligned}$$

with the convention $p_{-1} = 1,\ q_{-1} = 0$. This provides a sequence of *continuants* $(p_h)_{h\geq 0}$ and $(q_h)_{h\geq 0}$, and their quotient $p_h/q_h$, called *convergents.* A direct computation using these recurrence relations gives the following identities.

**Proposition 2.3.1.** *Given* $p_h/q_h = [a_0, a_1, \dots, a_h]$ *and* $p_{h-1}/q_{h-1} = [a_0, a_1, \dots, a_{h-1}]$, *we have*

$$\frac{p_h}{p_{h-1}} = [a_h, a_{h-1}, \dots, a_0] \quad \textit{and} \quad \frac{q_h}{q_{h-1}} = [a_h, a_{h-1}, \dots, a_1].$$

*Proof.* For $p_h$ we have

$$\begin{aligned} \frac{p_h}{p_{h-1}} &= a_h + \frac{p_{h-2}}{p_{h-1}} \\ &= a_h + \frac{1}{a_{h-1} + \frac{p_{h-3}}{p_{h-2}}} \\ &\dots \end{aligned}$$

ending at $a_0 = p_0/p_{-1}$.

The computation for $q$ is almost identical to that for $p$, as the same recurrence relation holds. The only difference comes from the final term, since $q_0 = 0$. This means that the continued fraction terminates at $a_1 = q_1/q_2$. □

An alternative representation of the continuants was given by Van der Poorten and Shallit [37]. They showed that you can also compute the numerator and denominator of the convergents using matrices. Observe that

$$\frac{p_1}{q_1} = [a_0,\ a_1] \leftrightarrow \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 \\ 1 \end{pmatrix} = \begin{pmatrix} p_1 \\ q_1 \end{pmatrix}.$$

Similarly we have

$$\frac{p_2}{q_2} = [a_0,\ a_1,\ a_2] \leftrightarrow \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_2 \\ 1 \end{pmatrix} = \begin{pmatrix} p_2 \\ q_2 \end{pmatrix}.$$

Furthermore, we can iterate this process and obtain the following matrix identity

$$\begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_h & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} p_h & p_{h-1} \\ q_h & q_{h-1} \end{pmatrix}.$$

Moreover, since we can write $\alpha = [a_0,\ a_1, \ldots,\ a_h,\ \alpha_{h+1}]$ we have the *convergents correspondence*

$$\alpha \leftrightarrow \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_h & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha_{h+1} \\ 1 \end{pmatrix} = \begin{pmatrix} p_h & p_{h-1} \\ q_h & q_{h-1} \end{pmatrix} \begin{pmatrix} \alpha_{h+1} \\ 1 \end{pmatrix}$$

$$\leftrightarrow \frac{p_h \alpha_{h+1} + p_{h-1}}{q_h \alpha_{h+1} + q_{h-1}}.$$

This leads to the identity

$$\alpha = \frac{p_h \alpha_{h+1} + p_{h-1}}{q_h \alpha_{h+1} + q_{h-1}}. \tag{2.1}$$

Furthermore, if we take the determinants of the matrices above, we obtain the following proposition.

**Proposition 2.3.2.** *Given a continued fraction expansion of a formal Laurent* *series* $\alpha = [a_0,\ a_1, \ldots]$*, its continuants* $p_h$ *and* $q_h$ *satisfy*

$$(-1)^{h-1} = p_h q_{h-1} - p_{h-1} q_h.$$

**Proposition 2.3.3.** *The continuants satisfy* $\partial eg\ p_h < \partial eg\ p_{h+1}$ *and* $\partial eg\ q_h < \partial eg\ q_{h+1}$ *for* $h \geq 0$*.*

*Proof.* We prove the result by induction. First suppose $a_0 \neq 0$. Then, since $\partial eg\ a_i > 0$ for all $i > 0$, we have

$$\partial eg\ p_1 = \partial eg\ (a_1 a_0 + 1) = \partial eg\ a_1 + \partial eg\ a_0 > \partial eg\ a_0 = \partial eg\ p_0,$$
$$\partial eg\ q_1 = \partial eg\ (a_1) > 0 = \partial eg\ q_0.$$

If $a_0 = 0$, then $\partial eg\ p_1 = \partial eg\ 1 = 0 > -\infty = \partial eg\ 0 = \partial eg\ p_0$ and $\partial eg\ q_1 = \partial eg\ a_1 > 0 = \partial eg\ q_0$.

Next, we suppose $\partial eg\ p_{h-1} < \partial eg\ p_h$ and $\partial eg\ q_{h-1} < \partial eg\ q_h$, then

$$\partial eg\ p_{h+1} = \partial eg\ (a_{h+1} p_h + p_{h-1}) = \partial eg\ a_{h+1} + \partial eg\ p_h > \partial eg\ p_h,$$
$$\partial eg\ q_{h+1} = \partial eg\ (a_{h+1} q_h + q_{h-1}) = \partial eg\ a_{h+1} + \partial eg\ q_h > \partial eg\ q_h.$$

Here the latter inequality in the expressions for both degree of $p_{h+1}$ and $q_{h+1}$ are consequence of $\partial eg\ a_{h+1} > 0$. □

We now showcase a property of the convergents as solutions to Diophantine equations, which will be employed in chapter 5.

**Proposition 2.3.4.** *The pair of continuants* $(q_{h-1}, p_{h-1})$ *gives the unique solution to* $p_h x - q_h y = 1$*, such that* $\partial eg\ x < \partial eg\ q_h$ *and* $\partial eg\ y < \partial eg\ p_h$*, provided* $h$ *is an odd integer. And if* $h$ *is even then* $(-q_{h-1}, -p_{h-1})$ *gives the unique solution to* $p_h x - q_h y = 1$*, such that* $\partial eg\ x < \partial eg\ q_h$ *and* $\partial eg\ y < \partial eg\ p_h$*.*

*Proof.* If $h$ is even, then from Proposition 2.3.2 $(q_{h-1}, p_{h-1})$ certainly satisfies

$p_h x - q_h y = 1$. For the uniqueness observe that

$$\begin{aligned} p_h x - q_h y &= p_h q_{h-1} - p_{h-1} q_h, \\ p_h(x - q_{h-1}) &= q_h(y - p_{h-1}). \end{aligned}$$

Since $p_h$ and $q_h$ have no common factors, we must have some polynomial $f \in \mathbb{Q}[t]$, such that

$$\begin{aligned} x - q_{h-1} &= f q_h, \\ y - p_{h-1} &= f p_h. \end{aligned}$$

From Proposition 2.3.3 we know $\partial eg\ p_{h-1} < \partial eg\ p_h$ and $\partial eg\ q_{h-1} < \partial eg\ q_h$, then $f = 0$ and $(q_{h-1}, p_{h-1})$ is the unique solution to the Diophantine equation $p_h x - q_h y = 1$ such that $\partial eg\ x < \partial eg\ q_h$ and $\partial eg\ y < \partial eg\ p_h$. The proof for $h$ even is analogous. □

All the results up until now are well-known and analogous to those over the real numbers and can be found in [32], for example. However, in the setting of formal Laurent series, we can go further and give an exact expression for the degree of $q_h$.

**Lemma 2.3.5.** *For $\alpha \in \mathbb{Q}((1/t))$ with continued fraction $[a_0,\ a_1, \ldots]$, $a_i \neq 0$ for $i \geq 1$, and $n^{th}$ convergent $p_h/q_h$, $h \geq 1$, we have that*

$$\deg q_h = \sum_{i=1}^{h} \deg a_i.$$

*Proof.* The proof is by induction on $h$. Since $q_1 = a_1$ and $q_2 = a_1 a_2 + 1$, the statement follows easily for $h = 1, 2$. Then suppose $\deg q_h = \sum_{i=1}^{h} \deg a_i$. Consider the recurrence relation

$$q_{h+1} = q_h a_{h+1} + q_{h-1}.$$

Since $\deg q_{h-1} < \deg q_h$, and $\deg a_{h+1} \geq 1$, the result follows. □

**Proposition 2.3.6.** *Suppose $\alpha \in \mathbb{Q}((1/t))$ has a continued fraction expansion $[a_0,\ a_1, \cdots]$ and convergents $p_h/q_h$. Then $\partial eg\ \alpha = \partial eg\ \frac{p_h}{q_h}$, and in particular*

$$\partial eg\ \alpha = \begin{cases} \deg a_0, & \text{if } \partial eg\ \alpha \geq 0 \\ -\deg a_1, & \text{otherwise.} \end{cases}$$

*Proof.* We prove the result by induction once again, and we will just show the case $\partial eg\ \alpha \geq 0$, the other case follows in a similar way. Suppose $a_0 \neq 0$, then $\partial eg\ p_0 = \deg a_0$, and $\partial eg\ q_0 = 0$, hence $\partial eg\ (p_0/q_0) = \deg a_0$. Moreover, $\partial eg\ \alpha = \partial eg\ \lfloor \alpha \rfloor = \deg a_0$.

If $a_0 = 0$, then $\deg p_1 = 0$ and $\deg q_1 = \deg a_1$, hence $\partial eg\ (p_1/q_1) = -\deg a_1$. Furthermore, observe that since $a_0 = 0$, $\alpha = \{\alpha\}$ and $a_1 = \lfloor 1/\{\alpha\} \rfloor$, and hence $\partial eg\ a_1 = -\partial eg\ \alpha$.

From the recurrence relations for $h > 1$, $\deg p_h = \deg a_h + \deg p_{h-1}$ and $\deg q_h = \deg a_h + \deg q_{h-1}$, we have

$$\partial eg\ \frac{p_h}{q_h} = \deg p_h - \deg q_h = \deg p_{h-1} - \deg q_{h-1} = \deg a_0.$$

The last equality follows from the induction hypothesis. □

Since the degree of $\alpha$ and its convergents are the same, it is interesting to see what happens to their difference. We can give an explicit result on what the degree of this difference is for any $\alpha \in \mathbb{Q}((1/t))$ and all $h$. The following theorem does not have an equivalent over the real numbers, and it will be instrumental in the computation of the Lagrange spectrum in chapter 4.

**Theorem 2.3.7.** *Suppose $\alpha \in \mathbb{Q}((1/t))$ and $p_h/q_h$ is its $h^{th}$ convergent. Then*

$$\partial eg\ \left(\alpha - \frac{p_h}{q_h}\right) = -2\deg q_h - \deg a_{h+1}.$$

*Proof.* Let $p_h/q_h$ be the $h^{\text{th}}$ convergent of $\alpha$, then by (2.1) and Proposition

2.3.2

$$\alpha - \frac{p_h}{q_h} = \frac{(-1)^h}{q_h(\alpha_{h+1}q_h + q_{h-1})}.$$

Considering degree of both sides and using that $\partial eg\ \alpha_{h+1} = \deg a_{h+1}$, by definition, we get

$$\partial eg\ \left(\alpha - \frac{p_h}{q_h}\right) = -2\deg q_h - \deg a_{h+1}.$$

□

**Corollary 2.3.8.** *For $\alpha \in \mathbb{Q}((1/t))$ with convergents $p_h/q_h$,*

1. $\partial eg\ \left(\alpha - \frac{p_h}{q_h}\right) = -\deg q_h - \deg q_{h+1}$,
2. $\partial eg\ \left(\alpha - \frac{p_{h-1}}{q_{h-1}}\right) > \partial eg\ \left(\alpha - \frac{p_h}{q_h}\right)$.

*Proof.* For 1, we use the fact that $\deg q_{h+1} = \deg a_{h+1} + \deg q_h$ in the equality in Theorem 2.3.7. To show the second result we employ the equality in 1, combined with the inequalities in Proposition 2.3.3. □

Looking at the degree of this difference tells us how far down the formal Laurent expansion we need to go until the terms no longer agree. Equivalently, it judges how close $\alpha \in \mathbb{Q}((1/t))$ is to a rational function.

## 2.4 Rational approximation

For a real number $r$ its convergents $p_h/q_h$ satisfy $|r - p_h/q_h| < 1/q_h^2$. On the other hand, if $|r - p/q| < 1/2q^2$, then $p/q$ must be a convergent for $r$. As the size of the continuants grow, the convergents get closer and closer to $r$, meaning that they are a good rational approximation for a real number. We can translate this result in the setting of the thesis, and show a slightly simplified result.

**Proposition 2.4.1.** *Suppose* $\alpha \in \mathbb{Q}((1/t))$ *and* $p, q \in \mathbb{Q}[t]$*, with* $q \neq 0$*. Then*

$$\partial eg \left(\alpha - \frac{p}{q}\right) < -2\deg q$$

*if and only if* $p/q$ *is a convergent for* $\alpha$*.*

Notice that $p/q$ is a convergent of $\alpha = [a_0,\ a_1 \ldots]$ if and only if $p/q = [a_0,\ a_1, \ldots,\ a_i]$, for some $i \geq 0$. Then the proposition is a direct corollary of the following.

**Proposition 2.4.2.** *Suppose we have* $\alpha, \beta \in \mathbb{Q}((1/t))$*, distinct. Then*

$$\partial eg\ (\alpha - \beta) < -2\deg q_i,$$

*where* $q_i$ *is the denominator of the* $i^{th}$ *convergent of* $\alpha$*, if and only if the first* $i+1$ *partial quotients of their continued fraction expansions are the same.*

*Proof.* Suppose $\alpha = [a_0,\ a_1, \ldots,\ a_i,\ \alpha_{i+1}]$, and $\beta = [a_0,\ a_1, \ldots,\ a_i,\ \beta_{i+1}]$, with $\alpha_{i+1} \neq \beta_{i+1}$. Without loss of generality, we can take $\partial eg\ \alpha_{i+1} \leq \partial eg\ \beta_{i+1}$. Then the first $i$ convergents must be the same for both $\alpha$ and $\beta$. From the convergents correspondence (2.1),

$$\alpha = \frac{\alpha_{i+1} p_i + p_{i-1}}{\alpha_{i+1} q_i + q_{i-1}} \quad \text{and} \quad \beta = \frac{\beta_{i+1} p_i + p_{i-1}}{\beta_{i+1} q_i + q_{i-1}}.$$

Taking the difference and applying Proposition 2.3.2 yields

$$\alpha - \beta = \frac{(-1)^{i+1}(\alpha_{i+1} - \beta_{i+1})}{(\alpha_{i+1} q_i + q_{i-1})(\beta_{i+1} q_i + q_{i-1})}. \tag{2.2}$$

Considering the degree of both sides of the equality, and using that by definition $\partial eg\ \alpha_{i+1} = \deg a_{i+1}$ and $\partial eg\ \beta_{i+1} = \deg b_{i+1}$, we get

$$\begin{aligned}
\partial eg\ (\alpha - \beta) &= -\left(\deg a_{i+1} + \deg b_{i+1} + 2\deg q_i - \deg(a_{i+1} - b_{i+1})\right) \\
&\leq -\deg a_{i+1} - 2\deg q_i \\
&< -2\deg q_i.
\end{aligned}$$

For the inequalities we use that $\deg(a_{i+1}-b_{i+1}) \leq \deg b_{i+1}$, by assumption; and $\deg a_{i+1} \geq 1$, by definition. This completes the proof in one direction. For the converse, suppose that $\partial eg\ (\alpha - \beta) < -2\deg q_i$, and $a_0 = b_0, \dots, a_{h-1} = b_{h-1}$, but $a_h \neq b_h$ for some $h < i$. Without loss of generality, we will assume that $\deg a_h \leq \deg b_h$. If we do the computation (2.2) for $h-1$ and consider the degree of both sides of the equality, we get

$$\begin{aligned}\partial eg\ (\alpha - \beta) &= -(\deg a_h + \deg b_h + 2\deg q_{h-1} - \deg(a_h - b_h)) \\ &< -2\deg q_i.\end{aligned}$$

After rearranging and applying the result from Lemma 2.3.5, we have

$$\deg a_h + \deg b_h - \deg(a_h - b_h) > 2\sum_{j=h}^{i} \deg a_j.$$

Furthermore, by assumption, $\deg a_h \leq \deg b_h$, hence

$$2\deg a_h \geq \deg a_h + \deg b_h - \deg(a_h - b_h).$$

Therefore, $\deg a_h > \sum_{j=h}^{i} \deg a_j$, yielding a contradiction. □

It is a well-known property of the convergents $p/q$ of a real number $r$ that they provide the 'best rational approximation'. The notion of 'best' refers to the distance between $r$ and its convergent $p/q$ being smaller for any other fraction of denominator smaller than $q$. This motivates the following definition.

**Definition 2.4.1.** We call $p/q \in \mathbb{Q}(t)$ a *best rational approximation for* $\alpha \in \mathbb{Q}((1/t))$, if for every other pair of polynomials $P, Q \in \mathbb{Q}[t]$, such that $\deg P \leq \deg p$, $\deg Q \leq \deg q$ and $p/q \neq P/Q$, we have

$$\partial eg\ \left(\alpha - \frac{p}{q}\right) < \partial eg\ \left(\alpha - \frac{P}{Q}\right).$$

In the classical case the best approximation theorem states:

**Theorem.** *For a real number $r$, all of its convergents $p_n/q_n$, $n \geq 2$ are best* *rational approximations, but not every best rational approximation is a convergent. Instead, if a reduced fraction $P/Q$ satisfies $Q|r-P/Q| < q|r-p/q|$, for any other integers $p$ and $q$ such that $q \leq Q$, then $P/Q$ is a convergent of $r$.*

Unsurprisingly, an analogous result holds in the function fields setting as well, but in a much simpler form.

**Proposition 2.4.3.** *For $\alpha \in \mathbb{Q}((1/t))$, and a pair of relatively prime polynomials $p$ and $q \in \mathbb{Q}[t]$, with $q \neq 0$, we have $p/q$ is the best rational approximation to $\alpha$ if and only if $p/q$ is amongst the convergents of $\alpha$.*

*Proof.* First, we show that the convergents indeed provide best rational approximations to $\alpha$. In order to do so, we will show that for any polynomial $q$ such that $\deg q \leq \deg q_n$, and any $p$, we have the inequality

$$\partial eg\left(\alpha - \frac{p}{q}\right) \geq \partial eg\left(\alpha - \frac{p_{n-1}}{q_{n-1}}\right). \tag{2.3}$$

Given this, we use Corollary 2.3.8(2), namely $\partial eg\ (\alpha - p_n/q_n) < \partial eg\ (\alpha - p_{n-1}/q_{n-1})$, to prove that the convergents are best approximations to $\alpha$.

To show (2.3), first observe that from Corollary 2.3.8(2) the convergents $p_h/q_h$, with $h \leq n-1$, satisfy $\partial eg\ (\alpha - p_h/q_h) \geq \partial eg\ (\alpha - p_{n-1}/q_{n-1})$. So suppose that $p/q$ is not a convergent, and is given by $p/q = [a_0, a_1, \dots, a_{i-1}, \beta_i]$, where $\alpha = [a_0, a_1, \dots, a_{i-1}, \alpha_i]$, and $i \leq n-1$ with $\alpha_i \neq \beta_i$. Using (2.2), we get

$$\alpha - \frac{p}{q} = \frac{(-1)^i(\alpha_i - \beta_i)}{(\alpha_i q_{i-1} - q_{i-2})q}.$$

Taking degrees of both sides, we use the fact that $\alpha_i \neq \beta_i$ both of which have non-negative degree, together with $\partial eg\ (\alpha_i q_{i-1} - q_{i-2}) = \partial eg\ q_i$ which we can deduce from Lemma 2.3.5, which yields

$$\begin{aligned}\partial eg\left(\alpha-\frac{p}{q}\right) &\geq -\deg q-\deg q_i\\ &\geq -\deg q_n-\deg q_{n-1}\\ &= \partial eg\left(\alpha-\frac{p_{n-1}}{q_{n-1}}\right).\end{aligned}$$

The final equality is simply Corollary 2.3.8(1). For the converse, suppose $p/q$ is a best approximation to $\alpha$, but is not a convergent. Furthermore, we can assume there exists an $n$ such that $\deg q_{n-1} < \deg q \leq \deg q_n$. Then from the best approximation property for $p/q$ we have $\partial eg\ (\alpha - p/q) < \partial eg\ (\alpha - p_{n-1}/q_{n-1})$. But from (2.3) the converse inequality holds, yielding the desired contradiction. □

We will study rational approximations of formal Laurent series further in chapter 4.

Let us now restrict out attention to quadratic irrationals. In particular, let $D \in \mathbb{Q}[t]$ be of degree $2d$, but not a square, and with leading coefficient a rational square, then Lemma 2.2.2 and Remark 2.2.2 imply $\sqrt{D} \in \mathbb{Q}((1/t))$. For $\alpha = \sqrt{D}$, the approximation theorems take the following form:

**Proposition 2.4.4.** *Suppose $D \in \mathbb{Q}[t]$ has a leading coefficient a rational square and of degree $2d$, but which is not a perfect square, and let $p, q \in \mathbb{Q}[t]$ be coprime. Then, up to a sign, $p/q$ is a convergent of $\sqrt{D}$ if and only if*

$$\deg\left(p^2 - Dq^2\right) \leq d-1. \tag{2.4}$$

*Proof.* By Proposition 2.4.1, $p/q$ is a convergent for $\sqrt{D}$ if and only if $\partial eg\ \left(\sqrt{D}-p/q\right) \leq -2\deg q - 1$. Moreover, we can assume that $\partial eg\ \left(\sqrt{D}+p/q\right) \neq \partial eg\ \left(\sqrt{D}-p/q\right)$. This is because if $\partial eg\ \left(\sqrt{D}+p/q\right) = \partial eg\ \left(\sqrt{D}-p/q\right)$, then it must be at least $d$, but this yields a contradictions in both directions. Firstly, if $p/q$ is a convergent then Proposition 2.4.1 is contradicted, and secondly if (2.4) holds,

$$\begin{aligned} d-1 \geq \deg\left(p^2-Dq^2\right) &= \partial eg\left(\sqrt{D}-\frac{p}{q}\right)+\partial eg\left(\sqrt{D}+\frac{p}{q}\right)+2\deg q \\ &\geq 2d+2\deg q \\ \Rightarrow -1 \geq d+\deg q \end{aligned}$$

Hence we can assume wlog that $\partial eg\ \left(\sqrt{D}+p/q\right) > \partial eg\ \left(\sqrt{D}-p/q\right)$, because for the reverse inequality the argument below will hold for $-p/q$.

This inequality also implies that $\partial eg\ \left(\sqrt{D}+p/q\right) = \partial eg\ \sqrt{D} = \partial eg\ p/q = d$. Then

$$\begin{aligned} \deg\left(p^2-Dq^2\right) &= \partial eg\left(\sqrt{D}-\frac{p}{q}\right)+\partial eg\left(\sqrt{D}+\frac{p}{q}\right)+2\deg q \\ &\leq d-1. \end{aligned}$$

□

Moreover, observe that if $p_h/q_h$ is a convergent of $\sqrt{D}$, we can use the result of Theorem 2.3.7 to show that $\deg\left(p_h^2-Dq_h^2\right) = d-\deg a_{h+1}$. Now, since $p_h$, $q_h$ and $D$ are all polynomials with coefficients in $\mathbb{Q}$, we must have $\deg a_{h+1} \leq d$. Moreover, $\deg a_{h+1} = d$ if and only if $p_h^2-Dq_h^2 = c \in \mathbb{Q}^\times$. In that case, $\left((p_h^2+Dq_h^2)^2/c, 2p_hq_h/c\right)$ solves the Diophantine equation $x^2-Dy^2=1$, better known as Pell's equation.

Suppose $\sqrt{D} = [a_0,\ a_1, \ldots,\ \alpha_{h+1}]$ has a periodic continued fraction with period starting at $a_1$ of length $h+1$. It can be shown, using methods analogous to those of Olds [32], that if $\sqrt{D}$ has a periodic continued fraction, then $\sqrt{D} = [a_0,\ \overline{a_1, \ldots,\ 2a_0}]$. In particular, this implies $h$ is the smallest positive integers, such that $a_{h+1} = 2a_0$ and $\deg a_{h+1} = d$ and consequently $\alpha_{h+1} = a_0+\sqrt{D}$. We then use the convergents correspondence (2.1) to obtain

$$\sqrt{D} = \frac{(a_0+\sqrt{D})p_h+p_{h-1}}{(a_0+\sqrt{D})q_h+q_{h-1}}.$$

After simplifying the fraction and equating coefficients of $\sqrt{D(t)}$ from the resulting equality, we get the simultaneous equations:

$$a_0 q_h + q_{h-1} = p_h$$
$$a_0 p_h + p_{h-1} = q_h D.$$

Eliminating $a_0$ gives $p_h^2 - Dq_h^2 = (-1)^h$, and if $h$ is even then $(p_h,\ q_h)$ solves Pell's equation. Therefore the discussion presented above yields a special case of Abel's theorem in one direction. Additionally, observe that if $h \mid n$, then the same argument yields that any pair $(p_n,\ q_n)$ is a solution to $x^2 - Dy^2 = (-1)^n$. These multiple solutions and their properties will be the focus of the next chapter.

## Chapter 3

# Solutions to the polynomial Pell's equation

For a polynomial $D(t) \in \mathbb{C}[t]$, the quadratic Diophantine equation in indeterminants $x$ and $y$, given by

$$x^2 - Dy^2 = 1, \tag{3.1}$$

is called Pell's equation. Observe that $(\pm 1, 0)$ always satisfies (3.1), and is called the *trivial solution.* In this chapter we study the *non-trivial solutions*, pairs $(u(t), v(t))$, with $v(t) \neq 0$, satisfying (3.1). If we are satisfied with solutions in $\mathbb{C}((1/t))$, then for any $D \in \mathbb{C}[t]$, there exists $v \in \mathbb{C}((1/t))$ such that $\sqrt{1+Dv^2} \in \mathbb{C}((1/t))$, and the pair $\left(\sqrt{1+Dv^2}, v\right)$ satisfies (3.1). However, we restrict our interest to solutions in polynomials with coefficients in $\mathbb{C}$ or $\mathbb{Q}$ – in analogy to the thoroughly studied theory of integer solutions to Pell's equation, for a non-negative integer $D$.

Observe that (3.1) does not have non-trivial polynomial solutions for every polynomial $D(t)$. This is obvious when $D(t)$ is of an odd degree (if $D(t) \in \mathbb{Q}[t]$ we must also impose that its leading coefficient is a square in $\mathbb{Q}$), since the term of highest degree cannot be cancelled. Therefore, we fix $D(t)$ to be a polynomial of degree $2d$. However, this is not a sufficient condition for (3.1) to have a solution. We have seen in section 2.2 that (3.1), Pell's equation for

$D(t)=t^4+t^3$, has no non-trivial solutions over $\mathbb{C}[t]$.

**Definition 3.0.1.** A polynomial $D(t)\in\mathbb{C}[t]$ is called *Pellian* if its corresponding Pell's equation (3.1) has a non-trivial solution $(u(t),v(t))\in\mathbb{C}[t]^2$.

If, however, a non-trivial solution exists, infinitely many more can be obtained by taking powers of the solution with smallest degree $(u(t),v(t))$. We denote the $n^{\text{th}}$ generated solution by $(u_n(t),v_n(t))$, and we study the factors of $v_n(t)$ as $n$ ranges in the integers. We prove that $v(t)\mid v_n(t)$ for all $n$, and write $v_n(t)/v(t)$ as a product of expressions written in $u(t)$, which turn out to be polynomials with integer coefficients, denoted by $v_n^{\text{new}}(t)$, and which become the focus of our investigation.

Firstly, if $D(t)$, $v(t)$ and $u(t)\in\mathbb{C}[t]$, we show that there are finitely many repeated factors of $v_n^{\text{new}}(t)$ for some $n$, giving an explicit upper bound on their number. Moreover if we restrict the polynomials $D(t),v(t),u(t)$ to have coefficients in the rational numbers, then $v_n^{\text{new}}(t)$ has at most $2\deg u(t)$ factors. Moreover, in this setting $v_n^{\text{new}}(t)$ has repeated roots only for "small" (relative to $\deg u(t)$) values of $n$, which we quantify further. This will be followed by an extensive discussion on which algebraic complex numbers $\alpha$ can be repeated roots of $v_n^{\text{new}}(t)$.

Finally, we show how the grasp of the factorisation of the solutions to (3.1) for a Pellian polynomial $D(t)$ can be used to obtain more Pellian polynomials.

## 3.1 Factorisation properties of $v_n(t)$

Let $D\in\mathbb{C}[t]$ be a Pellian polynomial with *fundamental solution* $(u,v)$, with $v\neq 0$ of smallest degree. Then, for each integer $n$ greater than 1, we obtain a new pair of polynomials $(u_n,v_n)$ satisfying the same Pell's equation, by

$$u_n+v_n\sqrt{D}=(u+v\sqrt{D})^n.$$

Furthermore, we can extend this definition to the negative integers by applying the identity $(u+v\sqrt{D})^{-1} = u - v\sqrt{D}$. This equivalence also gives

$$u_n - v_n\sqrt{D} = (u - v\sqrt{D})^n,$$

so that

$$v_n = \frac{(u+v\sqrt{D})^n - (u-v\sqrt{D})^n}{2\sqrt{D}}.$$

By definition, $v_1 = v$ and, as $a^n - b^n = \prod_{\xi:\ \xi^n=1}(a - b\xi)$, we have

$$v_n = v_1 \prod_{\substack{\xi:\ \xi^n=1,\\ \xi\neq 1}} \Big((u+v\sqrt{D}) - \xi(u-v\sqrt{D})\Big).$$

Note that $\xi$ is a root of $t^n - 1$, which can be written as a product of irreducible factors as $\prod_{d|n}\phi_d(t)$, where $\phi_d(t)$ denotes the cyclotomic polynomials. Therefore

$$v_n = v_1 \prod_{m|n, m>1} \psi_m, \tag{3.2}$$

where

$$\psi_m := \prod_{\xi:\ \phi_m(\xi)=0} \Big((u+v\sqrt{D}) - \xi(u-v\sqrt{D})\Big). \tag{3.3}$$

We can exploit the fact that the product in (3.3) is taken over the roots of the cyclotomic polynomials to show that $\psi_m$ does not depend on $v$ or $\sqrt{D}$.

**Lemma 3.1.1.** *For all integers $m$ greater than $1$, $\psi_m \in \mathbb{Z}[2u]$.*

*Proof.* Firstly, note that $\phi_2(t) = t+1$ and so $\psi_2 = 2u$. Now assume that $m > 2$, then $\phi_m$ is always of even degree and the $\xi$'s come in conjugate pairs. We will study $\psi_m$ by pairing up the terms for $\xi$ and $\overline{\xi}$. Together we have

$$\Big((u+v\sqrt{D}) - \xi(u-v\sqrt{D})\Big)\Big((u+v\sqrt{D}) - \overline{\xi}(u-v\sqrt{D})\Big) = (2u)^2 - (\xi + 2 + \overline{\xi}).$$

This implies that the product in $\psi_m$ is a product over conjugates and therefore belongs to $\mathbb{Z}[2u]$. □

To better understand the factors of $v_n$ it suffices to factorise $\psi_m$ over $\mathbb{C}[u]$.

**Lemma 3.1.2.** *The polynomials $\psi_m(u)$ have roots $\cos\frac{r\pi}{m}$, for $1 \leq r < m$ and $(r,m) = 1$. Namely,*

$$\psi_m(u) = 2^{\varphi(m)} \prod_{\substack{1\leq r<m \\ (r,m)=1}} \left(u - \cos\frac{r\pi}{m}\right).$$

*Proof.* Let $e(a) := e^{2a\pi i}$. Then, the roots of $\phi_m$ are $e(\frac{r}{m})$ for $1 \leq r < m$ with $(r,m) = 1$, and for each conjugate pair we take $\xi = e(\frac{r}{m})$ with $1 \leq r < m/2$. Using Euler's formula $e(a) = \cos 2a + i \sin 2a$, we have

$$\xi + 2 + \overline{\xi} = e\left(\frac{r}{m}\right) + 2 + e\left(-\frac{r}{m}\right) = 2\cos\frac{2r\pi}{m} + 2 = 4\cos^2\frac{r\pi}{m}.$$

The final equality comes from the double angle formula. Consequently,

$$\psi_m = \prod_{\substack{1\leq r<m/2 \\ (r,m)=1}} \left((2u)^2 - \left(2\cos\frac{r\pi}{m}\right)^2\right).$$

Now $\cos\frac{r\pi}{m} = -\cos\frac{(m-r)\pi}{m}$, thus

$$\psi_m = \prod_{\substack{1\leq r<m/2 \\ (r,m)=1}} \left(2u - 2\cos\frac{r\pi}{m}\right)\left(2u - 2\cos\frac{(m-r)\pi}{m}\right).$$

Observe that $m/2 < s < m$, with $(s,m) = 1$, if and only if $s = m - r$, where $0 < r \leq m/2$, with $(r,m) = 1$. Thus the above becomes

$$\psi_m = \prod_{\substack{1\leq r<m \\ (r,m)=1}} \left(2u - 2\cos\frac{r\pi}{m}\right) = 2^{\varphi(m)} \prod_{\substack{1\leq r<m \\ (r,m)=1}} \left(u - \cos\frac{r\pi}{m}\right).$$

□

Furthermore, since the cosines are distinct, as $m$ ranges in the natural numbers and $r$ in the given interval, we get the following.

**Lemma 3.1.3.** *The polynomials $\psi_m$ for $m > 1$, have no common roots.*

If now we restrict ourselves to working over polynomials in $u$, with coefficients in $\mathbb{Q}$, we obtain:

**Theorem 3.1.4.** *The polynomials $\psi_m$ are irreducible over $\mathbb{Q}[u]$ for $m$ even; and split into two irreducible factors of degree $\varphi(m)/2$, if $m$ is odd. Namely, for odd integers $m > 1$*

$$\psi_m(u) = (-1)^{\varphi(m)/2}\psi_m^*(u)\psi_m^*(-u),$$

*where*

$$\psi_m^*(u) = 2^{\varphi(m)} \prod_{\substack{1 \le q < m/2 \\ (q,m)=1}} \left(u - \cos\frac{2q\pi}{m}\right).$$

*Proof.* To see this, recall from Lemma 3.1.2 that $\psi_m(u)$ have roots $\alpha_r = e(\frac{r}{2m}) + e(\frac{-r}{2m})$, where $1 < r < m$ and $(r,m) = 1$. The field $\mathbb{Q}(\alpha_r)$ is the real subfield of $\mathbb{Q}\left(e(\frac{r}{2m})\right)$ of relative degree 2. Then we have the following tower of extensions.

$$\begin{tikzcd}
\mathbb{Q}\left(e(\frac{r}{2m})\right) \arrow[d, dash, "2"] \arrow[dd, dash, bend right=60, "\varphi(2m)"'] \\
\mathbb{Q}(\alpha_r) \arrow[d, dash] \\
\mathbb{Q}
\end{tikzcd}$$

Therefore $\mathbb{Q}(\alpha_r)$ has degree $\varphi(2m)/2$ over the rational numbers, and if $m$ is even, this equals $\varphi(m)$, implying that $\psi_m$ is irreducible. However, if $m$ is odd, then $\mathbb{Q}(\alpha_r)$ has degree $\varphi(m)/2$ over the rational numbers. Hence $\psi_m$ must be a product of two irreducible polynomials of degree $\varphi(m)/2$. In particular, if $r = 2q$, then $e(\frac{r}{2m}) = e(\frac{q}{m})$; and if $r$ is odd, then write $r = m - 2q$ and so

$e(\frac{r}{2m}) = e(\frac{m-2q}{2m}) = -e(\frac{-q}{m})$. We deduce that

$$\psi_m = \prod_{\substack{1\le q<m/2\\(q,m)=1}} \left(2u - \left(e\left(\frac{q}{m}\right) + e\left(\frac{-q}{m}\right)\right)\right)\left(2u + \left(e\left(\frac{q}{m}\right) + e\left(\frac{-q}{m}\right)\right)\right).$$

That is, $\psi_m(u) = (-1)^{\varphi(m)/2}\psi_m^*(u)\psi_m^*(-u)$, where

$$\begin{aligned}\psi_m^*(u) &:= \prod_{\substack{1\le q\le m/2\\(q,m)=1}} \left(2u - \left(e\left(\frac{q}{m}\right) + e\left(\frac{-q}{m}\right)\right)\right)\\ &= 2^{\varphi(m)} \prod_{\substack{1\le q\le m/2\\(q,m)=1}} \left(u - \cos\left(\frac{2q\pi}{m}\right)\right)\end{aligned}$$

is irreducible. □

In summary, we have $v_n = v\prod_{\substack{m|n\\m>1}} \psi_m(u)$, with $\psi_m$ integral polynomials only depending on $u$. Observe further that, if $\alpha = \cos(r\pi/n)$ with $(r,n) = 1$, then $\psi_n(\alpha) = 0$, but $\psi_m(\alpha) \ne 0$ for all integers $m$ smaller than $n$. That is $\psi_n$ picks out the *"new roots"* of $v_n$. Therefore, over $\mathbb{C}[t]$, we can write $v_n(t) = v_n^{\text{new}}(t)v_n^{\text{old}}(t)$, where $v_n^{\text{new}}(t) = \psi_n(u(t))$.

## 3.2 Bounding the number of factors of $v_n^{\text{new}}(t)$

We use the observation that $v_n^{\text{new}}(t) = \psi_n(u(t))$, together with the factorisation results in section 3.1, to study the factors and repeated factors of $v_n^{\text{new}}(t)$ as polynomials in $t$. Whenever necessary, we will adopt the notation $\deg_x(f)$ to indicate the degree of $f$ as a polynomial in $x$.

### 3.2.1 Bounds on the number of factors

**Lemma 3.2.1.** *Let $\pi(u) \in \mathbb{Q}[u]$ be a product of $k$ irreducible factors in $\mathbb{Q}[u]$. Then $P(t) := \pi(u(t)) \in \mathbb{Q}[t]$ has no more than $k\deg u$ irreducible factors over $\mathbb{Q}[t]$.*

*Proof.* We prove this when $\pi(u)$ is irreducible over $\mathbb{Q}[u]$, and whenever it is reducible, we multiply the result by the number of irreducible factors of $\pi$.

Suppose $\pi(u)$ is irreducible over $\mathbb{Q}[u]$. Let $A$ be a root of $\pi(u)$ over $\mathbb{C}$. Then $\pi(A) = 0$, so there exists $\alpha \in \mathbb{C}$, such that $P(\alpha) = \pi(A) = 0$. In particular, $\alpha$ is a root of $u(t) - A$ and we have the tower of extensions

$$\begin{tikzcd}
\mathbb{Q}(\alpha) \arrow[d, dash, "1\leq"'] \arrow[dd, dash, bend left, "\geq \deg_u \pi"] \\
\mathbb{Q}(A) \arrow[d, dash, "\deg_u \pi"'] \\
\mathbb{Q}
\end{tikzcd}$$

yielding that the minimal polynomial of $\alpha$ over the rationals must be of degree at least $\deg_u \pi$. Now all roots of $P(t)$ arise as described above, and $\deg_t P = \deg_u \pi \deg u$, therefore $P(t)$ has at most $\deg u$ irreducible factors over $\mathbb{Q}[t]$. □

**Proposition 3.2.2.**

*Proof.* In the introduction to this chapter, we observed that $v_n^{\mathrm{new}}(t) = \psi_n(u(t))$. Furthermore, from Theorem 3.1.4, the polynomials $\psi_n(u)$ split into two irreducible factors over $\mathbb{Q}[u]$ if $n$ is odd and are irreducible if $n$ is even. The result is then a consequence of Lemma 3.2.1, for $\psi_n(u)$ and $u = u(t) \in \mathbb{Q}[t]$. □

We now turn our attention to the repeated factors of $v_n(t)$.

### 3.2.2 Bounds on the number of repeated factors

Suppose $\alpha \in \mathbb{C}$ is a repeated root of some $v_n(t)$. That is $(t-\alpha)^2 \mid v_n(t)$, and since the $v_n^{\mathrm{new}}$ have no common roots, we must have $(t-\alpha)^2 \mid v_m^{\mathrm{new}}(t)$, for some $m \mid n$. Hence, to understand the repeated factors of $v_n(t)$, it suffices to consider the repeated factors of $v_n^{\mathrm{new}}(t)$. In this section we study their existence and its dependence on $n$.

**Theorem 3.2.3.** *For any Pellian polynomial $D(t) \in \mathbb{C}[t]$, with fundamental solution $(u(t), v(t))$, we define*

$$R(D) := \{\alpha \in \mathbb{C} : (t-\alpha)^2 \mid v_n(t) \textit{ for some } n\}.$$

*Then* $\#R(D) \leq \deg u - 1$.

*Proof.* By the discussion in the introduction to subsection 3.2.2, it suffices to consider repeated factors of $v_n^{\mathrm{new}}(t)$. We first study $v_1^{\mathrm{new}}(t) = v(t)$, as it cannot be expressed as a polynomial in $u$. Suppose $(t-\alpha)^2 \mid v(t)$, then $(t-\alpha)^4 \mid D(t)v^2(t)$. Since $(u(t), v(t))$ is a solution to Pell's equation, we must have

$$\begin{aligned} &(t-\alpha)^4 \mid u^2(t) - 1 \\ \Rightarrow\ &(t-\alpha)^3 \mid u(t)u'(t). \end{aligned}$$

Observe that this implies that $(t-\alpha)^3$ is a factor of $u'(t)$, since $u(\alpha) = \pm 1$. Next suppose that $(t-\alpha)$ is a repeated factor of $v_n^{\mathrm{new}}(t)$, for $n > 1$. Therefore we must have $(t-\alpha)^2 \mid u(t) - \cos \pi r/n$, for some positive integer $r < n$, co-prime to $n$. Then $(t-\alpha)$ must be a factor of $u'(t)$. In both cases, the repeated factors of $v_n^{\mathrm{new}}(t)$ over $\mathbb{C}[t]$ arise from roots of $u'(t)$, and there are at most $\deg u - 1$ of them. □

**Corollary 3.2.4.** *For any Pellian $D(t) \in \mathbb{C}[t]$, there are only finitely many $n$, for which $v_n^{new}(t)$ has repeated factors.*

*Proof.* In the proof of Theorem 3.2.3 we showed that if $\alpha$ is a repeated root of $v_n^{\mathrm{new}}(t)$ for any $n$, then $(t-\alpha) \mid u'(t)$. Since $u(t)$ is a polynomial, it has finitely many roots over $\mathbb{C}$. Since the polynomials $v_n^{\mathrm{new}}(t)$ have no common factors, there are only finitely many $n$ for which $v_n^{\mathrm{new}}(t)$ has repeated factors. □

The proof of Theorem 3.2.3 gives us a method of explicitly finding all repeated roots of $v_n^{\mathrm{new}}(t)$. Namely, suppose $(t-\alpha)^k \parallel u'(t)$, and if further $u(\alpha) = \cos(\pi r/n)$, for some $r < n$, co-prime to $n$, then $(t-\alpha)^{k+1} \parallel v_n^{\mathrm{new}}(t)$. To see why this works, recall $v_n^{\mathrm{new}}(t) = \prod_r (u(t) - \cos(\pi r/n))$, where the product ranges over positive integers $r < n$, co-prime to $n$. Then the repeated factors of $v_n^{\mathrm{new}}(t)$ must arise from repeated roots $\alpha \in \mathbb{C}$ of $u(t) - \cos(\pi r/n)$.

We now focus our attention to repeated factors of $v_n^{\mathrm{new}}(t)$ over the rational numbers. Restricting the factors to $\mathbb{Q}[t]$ implies that the repeated root $\alpha$ must come from a field extension of degree $d_\alpha$, satisfying:

$$\begin{tikzcd}
\mathbb{Q}(\alpha) \arrow[d, dash] \arrow[dd, dash, bend right=60, "d_\alpha"'] \\
\mathbb{Q}\left(\cos\left(\frac{\pi r}{n}\right)\right) \arrow[d, dash, "\varphi(2n)/2"] \\
\mathbb{Q}
\end{tikzcd}$$

**Theorem 3.2.5.** *For any Pellian $D(t) \in \mathbb{Q}[t]$, with fundamental solution $(u(t), v(t))$, if $v_n^{new}(t)$ has a repeated root, then $n \ll d \log\log d$, with $d = \deg u$.*

*Proof.* Let $\alpha \in \mathbb{C}$ algebraic of degree $d_\alpha$ be a repeated root of multiplicity $k > 1$ of $v_n^{\mathrm{new}}(t)$. Then from the discussion preceding the statement of the theorem we have that $d = \deg u > d_\alpha$, because $u \in \mathbb{Q}[t]$ and $(t-\alpha)^{k-1} \parallel u'(t)$. Moreover, from the Tower Law extension above $d_\alpha > \varphi(2n)/2$. Combining the two inequalities yields $\varphi(2n) < 2d$. Furthermore, the Euler totient function satisfies the bound $\varphi(n) \gg n/\log\log n$, see [40]. Taking logs of the right hand side $\log(n/\log\log n) = \log n - \log\log\log n \gg \log n$, since for $n$ large enough, $\log\log\log n < (\log n)/2$. Then $\log\log d \gg \log\log n$ and multiplying through by $n/\log\log n$, yields $n \ll d \log\log d$. □

## 3.3 The degrees of the factors of $v_n^{\mathrm{new}}(t)$

In this section we let $D(t) \in \mathbb{Q}[t]$ be a Pellian polynomial with fundamental solution $(u, v)$ and we study the degrees of the rational irreducible factors of $v_n^{\mathrm{new}}(t)$.

### 3.3.1 Factors of given degree

We once again exploit the fact that $v_n^{\mathrm{new}}(t)$ can also be written as the composition of two polynomials. This time we invoke the following technical lemma.

**Lemma 3.3.1.** *Let $P, Q \in \mathbb{Q}[X]$. Any rational factor of $P(Q(X))$ is of degree at least that of the degree of the smallest rational factor of $P(X)$.*

*Proof.* Let $\alpha \in \mathbb{C}$ be a root of $P(X)$ of smallest degree and let $\beta \in \mathbb{C}$ be an arbitrary root of $P(Q(X))$. Therefore $Q(\beta)$ will be a root of $P(X)$, and by the minimality of $\alpha$, we will have $\deg Q(\beta) \geq \deg \alpha$. A final observation that $\deg \beta \geq \deg Q(\beta)$ completes the proof. □

Recall that $v_n^{\text{new}}(t) = \psi_n(u(t))$, where $\psi_n$ is polynomial with coefficients in $\mathbb{Q}$ and of degree $\varphi(2n)/2$. We use Lemma 3.3.1, together with an asymptotic bound on the number of solutions to the equation $\varphi(n) = m$, to get the following.

**Theorem 3.3.2.** *Let $N$ be a positive integer and define*

$$I(N) := \{P(t) \in \mathbb{Q}[t],\ \textit{irreducible}: \deg P(t) \leq N,\ P(t) \mid v_n^{new}(t)\ \textit{for some}\ n\}.$$

*For $N$ sufficiently large, $\#I(N) \leq 10N \deg u$.*

*Proof.* Suppose that $P(t)$ is a factor of $v_n^{\text{new}}(t)$. By Lemma 3.3.1, $\varphi(2n)/2 \leq \deg P$, since any rational factor of $v_n^{\text{new}}(t) = \psi_n(u(t))$ must be at least the degree of the smallest rational factor of $\psi_n(t)$. Fix the degree of $P$ to be at most some positive integer $N$. To estimate the number of elements of $I(N)$ it suffices to compute the number of integers $n$ that satisfy the inequality $\varphi(2n)/2 \leq N$ and multiply it by $\deg u$ or $2\deg u$ depending on the parity of $n$. Observe that

$$\#\{n : \varphi(2n) \leq 2N\} = \#\{n \text{ even} : \varphi(n) \leq N\} + \#\{n \text{ odd} : \varphi(n) \leq 2N\}.$$

From [40] p.22 we have that $\#\{m : \varphi(m) \leq x\} = \zeta(2)\zeta(3)/\zeta(6)x + R(x)$, with $R(x)$ of order at most $x/(\log x)^l$, for any positive $l$. Thus the number of elements in the set id at most $2x$ for $x$ sufficiently large. Hence $\#I(N) \leq 2N \deg u + 8N \deg u$ for $N$ sufficiently large. □

If we wish to find an inequality that holds for all positive integers of $N$, we simply use a bound on the Euler totient function. However that makes our bound much worse for large values of $N$.

**Proposition 3.3.3.** *With the definition as in Theorem 3.3.2 we have that for all positive values of $N$, $\#I(N) \leq 4N^2 \deg u$.*

*Proof.* Similar to the proof of Theorem 3.3.2, if $P(t)$ is a factor of $v_n^{\mathrm{new}}(t)$, then $\varphi(2n)/2 \leq \deg P$, since the smallest factor of $v_n^{\mathrm{new}}(t)$ is of degree $\varphi(2n)/2$. Hence any irreducible rational factor of $v_n^{\mathrm{new}}(t)$, of degree up to $N$, satisfies $\varphi(2n) < 2N$. Using the lower bound of the Euler totient function, $\varphi(n) \geq \sqrt{n}$, and simplifying we obtain $n \leq 2N^2$. Now from Lemma 3.3.1, $v_n^{\mathrm{new}}$ has at most $\deg u$ irreducible factors for each $n$ even, and $2\deg u$ irreducible factors for each $n$ odd. Hence $\#I(N) \leq 4N^2 \deg u$. □

**Corollary 3.3.4.** *Let $D(t) \in \mathbb{Q}[t]$ be a square-free Pellian polynomial and N a positive integer. We define*

$$J(N) := \{P(t) \in \mathbb{Q}[t],\ \textit{irreducible}: \deg P(t) = N,\ P(t) \mid v_n^{new}(t) \textit{ for some } n\}.$$

*Then $\#J(N) < \infty$.*

Observe that $J(N) = I(N) - I(N-1)$, both of which are bounded quantities. Furthermore, we can obtain more explicit results, by considering factors of specific degree.

**Theorem 3.3.5.** *Suppose $D(t) \in \mathbb{Q}[t]$ is a Pellian polynomial with fundamental solution $(u, v)$. Then:*

1. *There are no linear polynomials with coefficients in $\mathbb{Q}$ that divide $v_n^{new}(t)$, for $n \geq 4$.*
2. *There are no quadratic polynomials with coefficients in $\mathbb{Q}$ that divide $v_n^{new}(t)$, for $n \geq 7$.*

*Proof.* We once again use the fact that the smallest factor of $v_n^{\mathrm{new}}(t)$ is of degree $\varphi(2n)/2$.

1. Therefore if $\varphi(2n)/2 > 1$, there cannot be a rational factor of $v_n^{\mathrm{new}}(t)$. This corresponds to $\varphi(n) > 1$ and $n$ even, or $\varphi(n) > 2$ and $n$ odd. For $n \geq 4$, both of those inequalities are satisfied.

2. For no quadratic rational factors of $v_n^{\mathrm{new}}(t)$, we need $n$ to satisfy $\varphi(2n)/2 > 2$. In particular, we must have $\varphi(n) > 2$ and $n$ even and $\varphi(n) > 4$ and $n$ odd. For $n \geq 7$ both inequalities hold.

□

Both of these results are the best possible. To see this, consider the following example.

**Example 3.3.1.** Let $D(t) = t^2 - 1$, then $(t, 1)$ is the smallest solution to the corresponding Pell's equation and thus it generates all the others. The only linear factors of $v_n(t)$ are $v_2^{\mathrm{new}} = 2t$ and the factors of $v_3^{\mathrm{new}}$, i.e. $2t \pm 1$. Furthermore, the only quadratic irreducible factors are $v_4^{\mathrm{new}} = 2t^2 - 1$, $v_6^{\mathrm{new}} = 4t^2 - 3$ and the factors of $v_5^{\mathrm{new}}$, namely $4t^2 \pm 2t - 1$. For $D(t) = t^4 + t^2$, with fundamental solution $(2t^2 + 1,\ 2)$, we have $v_2^{\mathrm{new}} = 2(2t^2 + 1)$ and $v_3^{\mathrm{new}} = (4t^2 + 1)(4t^2 + 3)$, having quadratic irreducible factors. Suppose $D(t) = t^8 + 4t^6 + 6t^4 + 5t^2 + 2$, this has fundamental solution $\left(2t^6 + 6t^4 + 6t^2 + 3,\ 2(t^2 + 1)\right)$, then $v_1^{\mathrm{new}} = 2(t^2 + 1)$ is a quadratic irreducible.

### 3.3.2 Repeated factors of given degree

Suppose that $\alpha \in \mathbb{C}$ is algebraic with minimal polynomial $p_\alpha(t)$ of degree $d_\alpha$ over the rational numbers. As discussed in subsection 3.2.2, if $\alpha$ is a repeated root of $v_n^{\mathrm{new}}(t)$, then $(t - \alpha)^k \parallel u(t) - \cos(\pi r/n)$, for some $r < n$, coprime to $n$ and $k \geq 2$. We restrict $D, u, v \in \mathbb{Q}[t]$, and define $w(t) \in \mathbb{Q}[t]$ to be the remainder when dividing $u(t)$ by $p_\alpha^k(t)$. That is, $w(t) = u(t) - p_\alpha^k(t)q(t) \in \mathbb{Q}[t]$, with $\deg w(t) < kd_\alpha$. If $\deg w(t) \neq 0$, we can reduce the problem to looking at repeated factors $(t - \alpha)^k \parallel w(t) - \cos(\pi r/n)$, instead. Differentiating this divisibility condition gives $(t - \alpha)^{k-1} \parallel w'(t)$, and since $w(t) \in \mathbb{Q}[t]$ we deduce that $p_\alpha^{k-1} \parallel w'(t)$. This yields a lower bound on the degree of $w(t)$, $\deg w(t) \geq (k-1)d_\alpha + 1$.

But let us first examine the case when $w(t)$ is a constant.

**Lemma 3.3.6.** *Let $D(t) \in \mathbb{Q}[t]$ be a Pellian polynomial, with fundamental solution $(u, v)$. Suppose $\alpha \in \mathbb{C}$, algebraic of degree $d_\alpha$ with minimal polynomial*

*$p_\alpha(t)$, is a repeated root of $v_n^{new}(t)$ of multiplicity $k > 1$. Then the remainder, when dividing $u(t)$ by $p_\alpha^k(t)$, is a constant if and only if $n = 1,\ 2,$ or $3$.*

*Proof.* Since $\alpha$ is a repeated root of $v_n^{\text{new}}(t)$, of multiplicity $k > 1$, we have $(t-\alpha)^k \parallel u(t) - \cos(\pi r/n)$, for some $r < n$, $(r,n) = 1$. From the division algorithm, there exists a polynomial $w(t) \in \mathbb{Q}[t]$, given by $w(t) = u(t) - p_\alpha^k(t)q(t)$ of degree less than $kd_\alpha$. Suppose $\deg w(t) = 0$, then we must have $w(t) = w \in \mathbb{Q}$. Furthermore, $\cos(\pi r/n) = u(\alpha) = w$ must be a rational number, which is only true for $n = 1,\ 2,$ or $3$. Conversely, suppose that $n = 1$, then $v_1^{\text{new}}(t) = v(t)$. For a repeated root $\alpha$ of $v(t)$, we must have $p_\alpha^k \parallel v(t)$. Hence $p_\alpha^{2k} \parallel u^2(t) - 1$, and therefore $p_\alpha^{2k} \parallel u(t) \pm 1$, and $w(t) = \pm 1$ for all $t$. For $n = 2,\ 3$, $v_2^{\text{new}}(t) = u(t)$ and $v_3^{\text{new}}(t) = 1 \pm 2u(t)$ are both polynomials with coefficients in $\mathbb{Q}$, and therefore $p_\alpha^k \parallel u(t)$ or $p_\alpha^k \parallel 1 \pm 2u(t)$. Hence $w(t) = 0$ or $w(t) = \pm 1/2$, respectively, for all $t$. □

**Corollary 3.3.7.** *The polynomials $v_2^{new}(t)$, $v_3^{new}(t)$ have a repeated complex root $\alpha$ if and only if $u(t) = q(t)p_\alpha^k(t)$ or $u(t) = q(t)p_\alpha^k(t) \pm 1/2$, respectively.*

We can use this corollary to construct, for any $\delta \geq 1$ and $k > 1$, a rational Pellian polynomial $D(t)$, such that $v_2(t)$ has a repeated factor $p(t) \in \mathbb{Q}[t]$ of degree $\delta$ and multiplicity $k$. Pick $\alpha \in \mathbb{C}$, algebraic with minimal polynomial $p(t)$ of degree $\delta \geq 1$ over the rational numbers, and an integer $k > 1$. Let $u(t) = p^k(t)$, then $D(t) = u^2 - 1 \in \mathbb{Q}[t]$ is Pellian, with fundamental solution $(p^k(t), 1)$. Furthermore, $v_2^{\text{new}}(t) = 2p^k(t)$, and it clearly has a repeated factor of degree $\delta$ and multiplicity $k$. We can do the same for $v_3^{\text{new}}(t)$, but instead $D(t) = u^2 - 1 \in \mathbb{Q}[t]$, where $u(t) = q^k(t) + 1/2$, and $q(t)$ is the minimal polynomial of some $\beta \in \mathbb{C}$ of degree 3.

We have dealt with the case when $w(t)$ is a constant, and simultaneously understood the repeated factors of $v_n^{\text{new}}(t)$ for small values of $n$. Therefore, for our investigation into the degree of repeated roots $\alpha \in \mathbb{C}$ of $v_n^{\text{new}}(t)$, we assume $n > 3$, equivalently $\deg w(t) > 0$, and proceed by case analysis.

### 3.3.2.1 The case of an odd degree $\alpha$

Suppose $\alpha \in \mathbb{C}$ is an algebraic number of degree $d_\alpha > 1$, an odd „integer. Furthermore, let $\alpha$ be a repeated root of $v_n^{\text{new}}(t)$ for $n > 3$, then $(t-\alpha)^k \parallel u(t) - \cos(\pi r/n)$, for some $r < n$, co-prime to $n$ and $k \geq 2$. Then we have the following tower of extensions:

$$\begin{tikzcd} \mathbb{Q}(\alpha) \arrow[d, dash] \arrow[dd, dash, bend right=60, "d_\alpha"'] \\ \mathbb{Q}\left(\cos\left(\frac{\pi r}{n}\right)\right) \arrow[d, dash, "\frac{\varphi(2n)}{2}>1"] \\ \mathbb{Q} \end{tikzcd}$$

From the Tower Law, $d_\alpha$ must be divisible by $\varphi(2n)/2$. Furthermore,

$$\frac{\varphi(2n)}{2} = \begin{cases} \varphi(n), & \text{if } n \text{ is even} \\ \varphi(n)/2, & \text{if } n \text{ is odd.} \end{cases}$$

Since $d_\alpha$ is odd and $\varphi(n)$ is even for all integers $n > 3$, the only possibility is for $\varphi(n)/2$ with $n$ odd, to divide $d_\alpha$.

**Theorem 3.3.8.** *Let $D(t) \in \mathbb{Q}[t]$ be Pellian with fundamental solution $(u,v)$. Suppose that for $n > 3$, the polynomial $v_n^{new}(t)$ has a repeated root $\alpha$ of odd degree $d_\alpha$, then $n = q^s$, where $q \equiv 3 \mod 4$ is prime and $s$ is a positive integer. Moreover, $d_\alpha$ must be a multiple of $\varphi(n)/2$.*

*Proof.* From the introduction to this section, we know that since $d_\alpha$ is odd, we must have $n$ and $\varphi(n)/2$ both odd. Lemma 3.3.10, to follow, states that $\varphi(n)$ is twice an odd number, if and only if $n = q^s$ for a prime $q \equiv 3 \mod 4$, and in that case $\varphi(n)/2 = (q-1)q^{s-1}/2$, which must divide $d_\alpha$. □

Furthermore, if we only consider odd prime degree, we can say more.

**Theorem 3.3.9.** *Suppose $D(t) \in \mathbb{Q}[t]$ is Pellian with fundamental solution $(u,v)$. If for any $n > 3$, the polynomial $v_n^{new}(t)$ has a repeated root $\alpha$ of a prime* *odd degree $d_\alpha$, then $n = 2d_\alpha + 1$ is also prime or $n = 9$, in which case $\alpha$ is cubic.*

*Proof.* Suppose $d_\alpha$ is an odd prime and $n > 3$, then we must have $[\mathbb{Q}(\cos\frac{r\pi}{n}) : \mathbb{Q}] > 1$ and thus $d_\alpha = \varphi(n)/2$, with $n$ odd. We employ the property of the Euler totient function described in Lemma 3.3.11, showing that a prime $d_\alpha = \varphi(n)/2$ if and only if $n = 2d_\alpha + 1$ or $n = 9$ and $d_\alpha = 3$. □

We now state and prove the technical lemmas on the properties of the Euler totient function needed in the proofs of Theorem 3.3.8 and Theorem 3.3.9.

**Lemma 3.3.10.** *Suppose $m > 3$ is an odd integer. Then $\varphi(m)/2$ is odd if and only if $m = q^s$ with $q \equiv 3 \mod 4$ prime and $s \geq 1$ an integer.*

*Proof.* Since $m$ is an odd integer, it can be represented as $\prod_{i=1}^{k} q_i^{s_i}$, where $q_i$ are distinct odd primes and $s_i$ are positive integers. For each $i$, we have $q_i - 1 \mid \varphi(m)$. Now if $q_i \equiv 1 \mod 4$, for some $i$, then $\varphi(m)/2$ is even. Hence $q_i \equiv 3 \mod 4$ for all $i$. Furthermore, if we have two distinct primes $q_i$ and $q_j$, both dividing $m$, then $(q_i - 1)(q_j - 1) \mid \varphi(m)$, and once again $\varphi(m)/2$ is even. Therefore, the only possibility is that $m$ is a power of a prime $q \equiv 3 \mod 4$. □

**Lemma 3.3.11.** *Suppose $m$ is an odd integer greater than 3, and $p$ is an odd prime. Then $\varphi(m)/2 = p$ if and only if $m = 2p+1$ is prime or $m = 9$ and $p = 3$.*

*Proof.* From Lemma 3.3.10, since $p$ is odd we must have $m = q^s$, where $q \equiv 3 \mod 4$ prime, and $s$ a positive integer. Therefore $\varphi(m)/2 = (q - 1)q^{s-1}/2$. For this expression to be equal to the prime $p$, we have two possibilities. Either $q = 2p+1$ and $s = 1$, yielding $m = 2p+1$, or $q = p = 3$, $s = 2$, giving $m = 9$ and $2p+1 = 7$. In both cases, $2p+1$ is prime.

Conversely, if $2p + 1$ is prime, then $\varphi(2p + 1) = 2p$ and $\varphi(9) = 2 \times 3$. Hence, for both $m = 2p+1$ and $m = 9$, $\varphi(m)/2$ is prime. □

*Remark* 3.3.1. We can use Theorem 3.3.9 to discount complex numbers $\alpha$ of odd prime degree $d_\alpha$, as repeated roots of $v_n^{\text{new}}(t)$ for $n > 3$. Namely, if $2d_\alpha + 1$

is not a prime, then $v_n^{\text{new}}(t)$ for $n > 3$ has no repeated root of degree $d_\alpha$. For example, we cannot have $\alpha$ of degree 7, 13, 17, 19, etc. Furthermore prime numbers $p$, such that $2p+1$ is prime are called Sophie Germain primes and are quite rare. In particular, they are a density 0 subset of the primes. Therefore, for most primes $p$, there are never repeated roots of $v_n^{\text{new}}(t)$ of degree $p$.

#### 3.3.2.2 The case of $\alpha$ quadratic

**Proposition 3.3.12.** *Suppose $D(t) \in \mathbb{Q}[t]$ is Pellian with fundamental solution $(u,v)$. Let $\alpha \in \mathbb{C}$ lie in a quadratic extension over the rational numbers. If $\alpha$ is a repeated root of $v_n^{new}(t)$ for $n > 3$, then $n = 4,\ 5$ or $6$ and $\alpha \in \mathbb{Q}(\sqrt{l})$, for $l = 2,\ 5$ or $3$, respectively.*

*Proof.* Since $n$ is greater than 3, $1 < [\mathbb{Q}\left(\cos\left(\frac{r\pi}{n}\right)\right) : \mathbb{Q}]$, and, by the Tower Law, is a factor of $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$. In particular, $\mathbb{Q}(\alpha) = \mathbb{Q}\left(\cos\left(\frac{\pi r}{n}\right)\right)$ and we have the following tower of extensions:

$$\begin{tikzcd} \mathbb{Q}(\sqrt{l}) = \mathbb{Q}\left(\cos\left(\frac{\pi r}{n}\right)\right) \arrow[d, dash, "\frac{\varphi(2n)}{2}>1"] \arrow[d, dash, bend right=60, "2"'] \\ \mathbb{Q} \end{tikzcd}$$

Therefore, $\varphi(n) = 2$ with $n$ even, i.e. $n = 4,\ 6$ or $\varphi(n) = 4$ with $n$ odd, i.e. $n = 5$. Consequently, $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2})$ or $\mathbb{Q}(\sqrt{3})$, in the former case since the cosines are either $\pm\sqrt{2}/2$ or $\pm\sqrt{3}/2$, respectively. In the latter case, $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{5})$, since $\cos\frac{\pi r}{5} = \pm(1 \pm \sqrt{5})/4$. □

**Proposition 3.3.13.** *Suppose $D(t) \in \mathbb{Q}[t]$ is Pellian with fundamental solution $(u,v)$. Let $\alpha \in \mathbb{C}$ be an algebraic integer with minimal polynomial $p_\alpha$, lying in a quadratic extension over the rational numbers. If $\alpha$ is a repeated root of $v_n^{new}(t)$ for $n > 3$, of multiplicity $k > 1$, then $u(t) = g(t)p_\alpha^k(t) + w(t)$, where*

$$w(t) = \int_\alpha^t a_k p_\alpha^{k-1}(x)dx + \cos\frac{\pi r}{n},$$

*and*

$$a_k = \frac{(2k-1)!g}{(-4l)^{k-1}s^{2k-1}((k-1)!)^2},$$

*with $g = \pm 1/2$, when $l = 2,\ 3$ and $g = \pm 1/4$, when $l = 5$. And $s$ is a quantity which can be determined from the computation in the proof.*

*Proof.* Let $\alpha$ be as in the statement of the theorem, with minimal polynomial $p_\alpha(t)$ of degree $d_\alpha = 2$. From the discussion at the beginning of subsection 3.3.2, we know $(k-1)d_\alpha + 1 \leq \deg w(t) < kd_\alpha$. Therefore, for $\alpha$ a quadratic irrational, $\deg w(t) = 2k-1$. In addition, since $w'(t) \in \mathbb{Q}[t]$ and $(t-\alpha)^k$ is a factor of $w(t) - \cos(\pi r/n)$, we must have $p_\alpha^{k-1} \parallel w'(t)$, and thus $\deg p_\alpha^{k-1}(t) = 2k-2 = \deg w'(t)$. Hence

$$\begin{aligned} &w'(t) = a_k p_\alpha^{k-1}(t), \text{ for } a_k \in \mathbb{Q}^*, \text{ and} \\ &w(\alpha) = \cos\frac{\pi r}{n}. \end{aligned}$$

Equivalently,

$$w(t) = \int_\alpha^t a_k p_\alpha^{k-1}(t)dx + \cos\frac{\pi r}{n}.$$

To completely determine $w(t)$, it remains to compute the coefficient $a_k$.

Suppose that $\alpha$ has minimal polynomial $p_\alpha(t) = t^2 + 2bt + c \in \mathbb{Q}[t]$. Then using $T = t + b$, we can rewrite it as $P_\alpha(T) = T^2 - A$, where $A = b^2 - c$. From Proposition 3.3.12 we know that $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{l})$, for $l = 2,\ 3$ or $5$. Hence

$A = s^2 l$, for some rational number $s$, and

$$\begin{aligned}
w(t) &= \int_\alpha^t a_k p_\alpha^{k-1}(x)dx + \cos\frac{r\pi}{n} \\
&= \int_{\alpha+b}^{t+b} a_k(X^2 - A)^{k-1} dX + \cos\frac{\pi r}{n} \\
&= a_k \int_{\sqrt{A}}^{t+b} \sum_{j=0}^{k-1} \binom{k-1}{j} X^{2j}(-A)^{k-1-j} dX + \cos\frac{r\pi}{n} \\
&= a_k \int_{s\sqrt{l}}^{t+b} \sum_{j=0}^{k-1} \binom{k-1}{j} X^{2j}(-s^2 l)^{k-1-j} dX + \cos\frac{\pi r}{n} \\
&= a_k \sum_{j=0}^{k-1} \binom{k-1}{j} (-s^2 l)^{k-1-j} \left[\frac{X^{2j+1}}{2j+1}\right]_{s\sqrt{l}}^{t+b} + \cos\frac{r\pi}{n} \\
&= a_k \sum_{j=0}^{k-1} \binom{k-1}{j} (-s^2 l)^{k-1-j} \left[\frac{(t+b)^{2j+1}}{2j+1} - \frac{s^{2j+1} l^j \sqrt{l}}{2j+1}\right] + \cos\frac{\pi r}{n}.
\end{aligned}$$

Furthermore, $\cos\frac{\pi r}{n}$ is also in a quadratic extension of the rational numbers, so let it be of the form $h + g\sqrt{l}$, with $h, g \in \mathbb{Q}$. Now, $w(t)$ is a polynomial with coefficients in the rational numbers, and thus the value of $g$ will be such that it cancels the coefficient of $\sqrt{l}$ in the sum above. Namely,

$$\begin{aligned}
g &= a_k \sum_{j=0}^{k-1} \binom{k-1}{j} (-s^2 l)^{k-1-j} \frac{s^{2j+1} l^j}{2j+1} \\
\Rightarrow g &= a_k s^{2k-1} l^{k-1} \sum_{j=0}^{k-1} \binom{k-1}{j} \frac{(-1)^{k-1-j}}{2j+1}.
\end{aligned}$$

In a lemma given after the proof, we show that the sum in the expression for $g$ evaluates to

$$\frac{(-4)^{k-1}(k-1)!}{(2k-1)!}.$$

After rearranging appropriately, we obtain the required form for $a_k$. □

**Lemma 3.3.14.** *For a positive integer $n$, we have the following combinatorial identity*

$$\sum_{j=0}^{n} \binom{n}{j} \frac{(-1)^{n-j}}{2j+1} = \frac{(-4)^n (n!)^2}{(2n+1)!}.$$

*Proof.* Let $f(n) = \int_0^1 (x^2-1)^n dx$. After expanding, we get

$$f(n) = \int_0^1 (x^2-1)^n dx = \int_0^1 \sum_{j=0}^{n} \binom{n}{j} (-1)^{n-j} x^{2j} dx$$
$$= \sum_{j=0}^{n} \binom{n}{j} \frac{(-1)^{n-j}}{2j+1}.$$

Integrating $f(n)$ by parts, we obtain a recursive relation

$$\begin{aligned} f(n) &= [x(x^2-1)^n]_0^1 - \int_0^1 2nx^2(x^2-1)^{n-1} dx \\ &= -2n \int_0^1 x^2(x^2-1)^{n-1} dx \\ &= -2n\,(f(n)+f(n-1))\,. \end{aligned}$$

Therefore

$$f(n) = \frac{-2n}{2n+1} f(n-1) = f(0) \prod_{i=1}^{n} \frac{(-1)^i 2i}{2i+1} = \frac{(-4)^n (n!)^2}{(2n+1)!}.$$

The final equality follows since $f(0) = 1$. □

**Corollary 3.3.15.** *The polynomials $v_n^{new}(t)$ for $n > 3$ and $u(t) \in \mathbb{Z}[t]$ have no quadratic irrationals as repeated roots of multiplicity $k > 1$.*

*Proof.* If $\alpha$ is as in the statement and $u(t) \in \mathbb{Z}[t]$, then $w(t) \in \mathbb{Z}[t]$, since it is the remainder in the division of $u(t)$ by the minimal polynomial $p_\alpha(t) \in \mathbb{Z}[t]$. This implies that $a_k \in \mathbb{Z}$. However, for $k > 1$, the power of 2 dividing

$$\frac{(2k-1)!}{4^{k-1}((k-1)!)^2}$$

is smaller than $0$. To see this, we rearrange the expression to get

$$\frac{2k-1}{2^{2k-2}} \binom{2k-2}{k-1}.$$

We apply Kummer's theorem [18], which says that for a prime $p$, $p^l \mid \binom{n}{m}$ only if $p^l \leq n$. And $2^{2k-2} > 2k-2$ for $k > 1$, hence $a_k$ is not an integer for any integer $k$ greater than 1. □

## 3.4 Non square-free Pellian polynomials

It is well-known that for every positive integer $D$, $x^2 - Dy^2 = 1$ has non-trivial solutions, but this no longer holds true for every polynomial $D(t) \in \mathbb{C}[t]$. In general, it is fairly difficult to determine whether a given complex polynomial is Pellian or not. However, for a polynomial with roots of high multiplicity, as a consequence of the ABC theorem [27][42], there is an easy criterion that we can check. To see this, recall that the ABC theorem for complex polynomials says that if $a+b=c$ has a non-trivial solution with $a,b,c \in \mathbb{C}[t]$ having no common roots, then the number of distinct roots of $abc$, denoted by $n(abc)$, is greater than the maximum of their degrees. We apply this result to Pell's equation for $D(t) \in \mathbb{C}[t]$ with non-trivial solution $(u(t), v(t))$ to obtain

$$n(u^2Dv^2) = n(uDv) > \max\{\deg u^2, \deg Dv^2\}.$$

Furthermore

$$n(uDv) \leq \deg u + n(D) + \deg v.$$

Hence

$$\begin{aligned} n(D) &> \deg D + \deg v - \deg u \\ n(D) &> \frac{1}{2}\deg D. \end{aligned}$$

This is precisely what Dubickas and Steuding [12] showed.

**Theorem 3.4.1.** (Dubickas & Steuding) *If the number $n(D)$ of distinct zeros of $D \in \mathbb{C}[t]$ is less than or equal to $\frac{1}{2}\deg D$, then the polynomial Pell equation has no non-trivial solutions in $\mathbb{C}[t]$.*

Observe that given a separable polynomial $F(t) \in \mathbb{C}[t]$, and a square-free polynomial $D(t) \in \mathbb{C}[t]$, both of positive degree, and relatively prime, then

$n(F^2D(t)) = \deg F(t) + \deg D(t) > \frac{1}{2}\deg F^2D(t)$. Hence, for polynomials with coefficients in $\mathbb{C}$, and a single square factor, Theorem 3.4.1 cannot be used to determine whether they are Pellian or not. We thus focus our attention on polynomials of that form.

Suppose that $F^2D(t)$ is a Pellian with complex coefficients. Then there exist polynomials $X(t), Y(t) \in \mathbb{C}[t]$ solving the corresponding Pell's equation. Moreover, $(X(t), FY(t))$ solves Pell's equation for $D(t)$. On the other hand we have the following.

**Lemma 3.4.2.** *If $D(t) \in \mathbb{C}[t]$ is Pellian with solutions $(u_n(t), v_n(t))$ then $\Delta(t) = F^2D(t)$ is also Pellian, whenever $F(t) \mid v_n(t)$ for some $n$.*

*Proof.* If $v_n(t) = FV(t)$ for some $n$, then $(u_n(t), V(t))$ is a solution to Pell for $\Delta(t)$, and thus $\Delta(t)$ is Pellian. □

Therefore, all Pellian polynomials of the form $F^2D(t)$ arise from square-free Pellian polynomials $D(t)$ and a factor $F$ of $v_n^{\text{new}}(t)$. This lemma gives a simple method for checking whether a polynomial $F^2D \in \mathbb{Q}[t]$ is Pellian or not. Restricting our investigation to polynomials $D(t)$ with rational coefficients, yields the following result.

**Proposition 3.4.3.** *Let $D(t) \in \mathbb{Q}[t]$ be square-free and Pellian. Then for a given positive integer $f$, there exist only finitely many irreducible $F \in \mathbb{Q}[t]$, of degree $f$, such that $F^2D$ is also Pellian.*

*Proof.* From Lemma 3.4.2, $F$ must be a factor of $v_n(t)$. Furthermore, any such factor arises from a factor of $v_m^{\text{new}}(t)$, for $m$ a factor of $n$. By corollary 3.3.4, there are only finitely many such factors of a fixed degree. □

This proposition comes in contrast to the classical case, where for any positive integer $d$, Pell's equation for $g^2d$ has non-trivial solutions for infinitely many $g$. For details, see chapter 8 of [22].

**Example 3.4.1.** Consider $D(t) = t^2 - 1$. We wish to find all quadratic polynomials $F \in \mathbb{Q}[t]$ such that $F^2(t^2 - 1)$ is Pellian. These polynomials must be factors of $v_n^{\mathrm{new}}(t)$ for some $n$. By Theorem 3.3.5, we should only look at factors of $v_n^{\mathrm{new}}(t)$ for $n \leq 6$. Therefore, the only quadratic polynomials $F$ for which $F^2(t^2-1)$ is Pellian are $v_4^{\mathrm{new}}(t)$, $v_6^{\mathrm{new}}(t)$, and the factors of $v_5^{\mathrm{new}}(t)$. Respectively, these are given by

$$2t^2-1,\ 4t^2-3,\ \text{and}\ 4t^2 \pm 2t - 1.$$

Even though not all polynomials $D \in \mathbb{Q}[t]$ are Pellian, we have seen that the connection with the continued fraction expansion of $\sqrt{D(t)}$ is preserved in the polynomial setting. We next turn our attention to studying the continued fraction expansion for quadratic irrationals of polynomials and other algebraic functions over the field of formal Laurent series.

## Chapter 4

# Diophantine approximation and the Lagrange spectrum

For an irrational number $r \in \mathbb{R}$, we know that its convergents $p/q$ satisfy $|r - p/q| < 1/q^2$. Moreover, as discussed in section 2.4, the best rational approximations to $\alpha \in \mathbb{Q}((1/t))$ are also given by its convergents $p(t)/q(t)$, and an analogous inequality is satisfied, where we replace the absolute values by $\partial eg\ (\cdot)$. We then measure the accuracy of the approximation by studying $\partial eg\ (\alpha - p(t)/q(t))$ as a function of the degree of the denominator $q$. For real numbers, these questions are part of Diophantine approximation, and their power series analogue will be the topic of this chapter. The first section consists of a brief discussion of the results of Mahler [23] and Uchiyama [43], the function field equivalents to Liouville's theorem and Roth's theorem, respectively. For these, the accuracy is studied in terms of multiples of $\deg q$, and is related to the analogue of the problem of approximation exponents over the real numbers. For Laurent series with coefficients in $\mathbb{Q}$ the approximation exponent is known; however for coefficients in finite fields it is still an ongoing area of research, see [19] and [41].

We dedicate the remainder of the chapter to studying a different quantity, measuring the accuracy of the approximation of $\alpha$ by its convergents, the Lagrange constant, $l(\alpha)$. We use the connection with the periodicity of $\sqrt{D(t)}$ to show that for Pellian polynomials $D(t)$ of degree $2d$, $l(\sqrt{D(t)}) = d$. Moreover, we give some insight into the value of $l(\sqrt{\Delta(t)})$, for a class of non-Pellian polynomials $\Delta(t)$. Finally, we define the Lagrange spectrum and show that it is equal to a different set related to doubly infinite sequences of non-constant polynomials.

## 4.1 Diophantine approximation

Recall from Proposition 2.4.1 that for $\alpha \in \mathbb{Q}((1/t))$ and $p(t)$ and $q(t) \in \mathbb{Q}[t]$ with $q \neq 0$, we have that

$$\partial eg \left(\alpha - \frac{p(t)}{q(t)}\right) < -2\deg q(t)$$

if and only if $p(t)/q(t)$ is a convergent for $\alpha$.

**Proposition 4.1.1.** *Given $\alpha \in \mathbb{Q}((1/t))$, not a rational function, there exist infinitely many pairs of polynomials $p(t), q(t) \in \mathbb{Q}[t]$, with $q(t) \neq 0$ such that*

$$\partial eg \left(\alpha - \frac{p(t)}{q(t)}\right) < -2\deg q(t).$$

*Proof.* We know that the convergents of $\alpha$ satisfy the inequality of the proposition. Furthermore, since $\alpha$ is not a rational function, it has an infinite continued fraction, resulting in infinitely many convergents. □

The first quantity that we will discuss, measuring the accuracy of the approximation to $\alpha$ by its convergents, is given by Schmidt in [41].

**Definition 4.1.1.** Let $c_h := c(p_h(t)/q_h(t))$, be such that

$$\partial eg \left(\alpha - \frac{p_h(t)}{q_h(t)}\right) = -(1+c_h)\deg q_h(t).$$

We define the *approximation spectrum* of $\alpha$, denoted by $S(\alpha)$, to be the set of limit points of $c_h$ as $h$ runs through the non-negative integers.

From Proposition 4.1.1, $S(\alpha)$ is a closed subset of $[1,\infty]$.

*Remark* 4.1.1. Moreover, the maximum $r(\alpha)$ (possibly $\infty$) of $S(\alpha)$ is called the *approximation exponent.* In particular, when $r(\alpha) < \infty$, given $\varepsilon > 0$, there are infinitely many rational elements $p(t)/q(t) \in \mathbb{Q}(t)$ satisfying

$$\partial eg\ \left(\sqrt{D(t)} - \frac{p(t)}{q(t)}\right) < (-1 - r(\alpha) + \varepsilon) \deg q(t),$$

but only finitely many satisfying

$$\partial eg\ \left(\sqrt{D(t)} - \frac{p(t)}{q(t)}\right) < (-1 - r(\alpha) - \varepsilon) \deg q(t).$$

For a quadratic irrational $\alpha = \sqrt{D(t)} \in \mathbb{Q}((1/t))$, where $D(t)$ is a polynomial of degree $2d$ with rational coefficients, we have:

**Proposition 4.1.2.** *Any polynomial $D(t) \in \mathbb{Q}[t]$ of even degree $2d$ and with leading coefficient a square in $\mathbb{Q}$, and any $p$ and $q \in \mathbb{Q}[t]$, satisfy the following inequality*

$$\partial eg\ \left(\sqrt{D(t)} - \frac{p(t)}{q(t)}\right) \geq -2 \deg q(t) - d. \tag{4.1}$$

*Proof.* Recall from Proposition 2.4.3 that the convergents of $\alpha$ give the best rational approximation of it. Hence it suffices to show the inequality holds when $p(t)/q(t)$ is a convergent of $\alpha$. Further recall Theorem 2.3.7, which states that

$$\partial eg\ \left(\alpha - \frac{p_h(t)}{q_h(t)}\right) = -2 \deg q_h(t) - \deg a_{h+1}(t),$$

where $a_{h+1}$ is a partial quotient of $\sqrt{D(t)}$ and $p_h(t)/q_h(t)$ its convergent. The proof is then an immediate consequence of the fact that $1 \leq \deg a_h(t) \leq d$. □

Hence, we have that $S(\sqrt{D(t)}) = 1$.

A direct generalisation of this proposition to algebraic power series of any degree and the function field equivalent of Liouville's theorem is given by Mahler in [23]. We say $\alpha \in \mathbb{Q}((1/t))$ is algebraic if it is algebraic over the field of rational functions $\mathbb{Q}(t)$. Furthermore, the degree of an algebraic element $\alpha \in \mathbb{Q}((1/t))$ is defined to be $[\mathbb{Q}(t)(\alpha):\mathbb{Q}(t)]$, the degree of the field extension generated by $\alpha$. We now state and prove a slightly different form of Mahler's result, giving an explicit form for the right-hand side of the inequality for the degree of $\alpha - p(t)/q(t)$.

**Theorem 4.1.3.** *Suppose $\alpha \in \mathbb{Q}((1/t))$ is algebraic of degree $M \geq 2$ over $\mathbb{Q}[t]$. Then all polynomials $p(t), q(t) \in \mathbb{Q}[t]$ satisfy*

$$\partial eg \ \left(\alpha - \frac{p(t)}{q(t)}\right) \geq -M \deg q(t) - (M-1)\partial eg \ \alpha - F,$$

*where $F$ denotes the maximum degree of the coefficients of the minimal polynomial of $\alpha$ over $\mathbb{Q}[t]$.*

*Proof.* Suppose for a contradiction, that there exists some $\alpha \in \mathbb{Q}((1/t))$ with minimal polynomial $f = \sum_{i=0}^{M} f_i X^i \in \mathbb{Q}[t][X]$ over $\mathbb{Q}[t]$, such that there exists a pair of polynomials $p, q \in \mathbb{Q}[t]$, satisfying

$$\partial eg \ \left(\alpha - \frac{p(t)}{q(t)}\right) < -M \deg q(t) - (M-1)\partial eg \ \alpha - F,$$

where $F = \max_{i \in [0,M]} \deg f_i$. Then, there exists $B = B(\alpha)$ of degree less than $-(M-1)\partial eg \ \alpha - F$ such that

$$\alpha - \frac{p(t)}{q(t)} = \frac{B}{q^M(t)}. \tag{4.2}$$

Then

$$q^M(t)\left(f\left(\alpha - \frac{B}{q^M(t)}\right) - f(\alpha)\right) = q^M(t) f\left(\frac{p(t)}{q(t)}\right).$$

Observe that $\partial eg$ RHS $\geq 0$. The degree of the LHS requires some further computation:

$$\begin{aligned}
\text{LHS} &= q^M(t)\sum_{i=0}^{M} f_i\left(\left(\alpha-\frac{B}{q^M(t)}\right)^i-\alpha^i\right)\\
&= q^m\sum_{i=0}^{M}\sum_{j=1}^{i} f_i\binom{i}{j}\left(-\frac{B}{q^M(t)}\right)^j\alpha^{i-j}\\
&= q^M\sum_{k=0}^{M-1}\left(\sum_{j=1}^{M-k} f_{k+j}\binom{k+j}{j}\left(-\frac{B}{q^M(t)}\right)^j\right)\alpha^k.
\end{aligned}$$

We can then bound the degree of the LHS, by maximising the degree of the above expression. That is

$$\begin{aligned}
\partial eg\ \text{LHS} &\leq \max_{\substack{0\leq k\leq M-1\\ 1\leq j\leq M-k}} M\deg q(t)+\deg(f_{k+j})+j\partial eg\ B-Mj\deg q(t)+k\partial eg\ \alpha\\
&\leq \partial eg\ B+(M-1)\partial eg\ \alpha+F<0.
\end{aligned}$$

To get from the first to the second line we use the fact that $\partial eg\ B \leq M\partial eg\ q(t)$, which is a consequence of (4.2), together with $\partial eg\ (\alpha - p(t)/q(t)) \leq 0$. And the final inequality follows from the definition of $B$ and yields the desired contradiction. □

As a consequence, we have that for $\alpha\in\mathbb{Q}((1/t))$ algebraic of degree $M$, $S(\alpha)\subset[1,\ M-1]$.

Furthermore, we have $S(\alpha)=1$, precisely when an equivalent of Roth's theorem holds. For fields of power series with coefficients in $\mathbb{Q}$, Uchiyama [43] proved the following.

**Theorem.** (Uchiyama) *For $\alpha\in\mathbb{Q}((1/t))$ algebraic of finite degree, there exist only finitely many polynomials $p,q\in\mathbb{Q}[t]$ satisfying*

$$\partial eg\ \left(\alpha-\frac{p}{q}\right)<-(2+\varepsilon)\deg q,$$

*for a given $\varepsilon>0$.*

The proof, given by Uchiyama, uses methods analogous to those over number fields, and is in a sense ineffective. Both Wang in [45] and Ru in [39] provide an effective Roth's theorem.

Moreover, the approximation exponent problem for $\alpha \in \mathbb{Q}((1/t))$ is therefore resolved. For fields of formal Laurent series with coefficients in finite fields, it is ongoing, studied by Lasjaunias in [19] and Schmidt in [41].

We now proceed with our investigation into the accuracy of the rational approximations of $\alpha \in \mathbb{Q}((1/t))$, by studying the analogue of the approximation constant and its corresponding spectrum.

## 4.2 Lagrange constant and its spectrum

If we consider all non-rational $\alpha \in \mathbb{Q}((1/t))$ collectively, then the inequality

$$\partial eg \left(\alpha - \frac{p}{q}\right) \leq -2\deg q - 1,$$

satisfied by infinitely many polynomials $p$ and $q \in \mathbb{Q}[t]$, cannot be improved. However, given a specific non-rational Laurent series $\alpha$, we can sometimes sharpen the bound. This motivates the following definition.

### 4.2.1 Lagrange constant

**Definition 4.2.1.** Given $\alpha \in \mathbb{Q}((1/t))$, we define the *approximation (Lagrange) constant*, $l(\alpha)$ to be the supremum over all integers $k$ such that

$$\partial eg \left(\alpha - \frac{p}{q}\right) \leq -2\deg q - k$$

is satisfied by infinitely many polynomials $p$ and $q$ with coefficients in $\mathbb{Q}$.

*Remark* 4.2.1. From corollary 2.4.1, the inequality $\partial eg\ (\alpha - p/q) < -2\partial eg\ q$ is satisfied only by the convergents of $\alpha$, say $p_h/q_h$. By Theorem 2.3.7, the left hand-side is simply equal to $-2\partial eg\ q_h - \partial eg\ a_{h+1}$, where $a_{h+1}$ is a partial quotient of $\alpha$. Thus we can substantially simplify the calculation of the Lagrange constant, by using the formula

$$l(\alpha) = \limsup_{h\to\infty} \partial eg\ a_h.$$

**Example 4.2.1.** Recall example 2.2.3. For $D = (at+b)^2 + c$, with $a, b, c \in \mathbb{Q}$ and $ac \neq 0$

$$\sqrt{D} = \sqrt{(at+b)^2 + c} = \left[at+b,\ \overline{\frac{2}{c}(at+b),\ 2(at+b)}\right].$$

Notice that all partial quotients have degree 1. Therefore $l(\sqrt{D}) = 1$ for $D$ a square-free quadratic polynomial with rational coefficients.

For more interesting examples of Lagrange constants we need to find $\alpha \in \mathbb{Q}((1/t))$, such that $\deg a_h = d > 1$, for infinitely many $h$.

**Theorem 4.2.1.** *For $a, b, c \in \mathbb{Q}[t]$, we have*

1. $\sqrt{a^2+1} = [a,\ \overline{2a}]$*;*

2. $\sqrt{a^2+c} = [a,\ \overline{2b,\ 2a}]$*, if* $a = bc$*.*

*Proof.* Observe that 1. is a consequence of 2., if we take $b = a$. Hence it suffices to prove the second result. Suppose we are given the continued fraction expansion $[a,\ \overline{2b,\ 2a}] = \alpha \in \mathbb{Q}((1/t))$. This is equivalent to the expression

$$\alpha = a + \frac{1}{\beta}, \text{ where}$$

$$\beta = 2b + \cfrac{1}{2a + \cfrac{1}{\beta}}.$$

After rearranging and simplifying the above, we get the following quadratic equation in $\beta$:

$$a\beta^2 - 2ab\beta - b = 0,$$

therefore

$$\beta = \frac{ab + \sqrt{a^2b^2 + ab}}{a}.$$

Observe that here we pick $\beta$ to be the solution which has the highest degree, by convention, mimicking what happens in the number fields case where we always pick the positive root. Therefore

$$\begin{aligned}\alpha &= a + \frac{a}{ab + \sqrt{a^2b^2 + ab}} \times \frac{ab - \sqrt{a^2b^2 + ab}}{ab - \sqrt{a^2b^2 + ab}} \\ &= \sqrt{a^2 + \frac{a}{b}} \\ &= \sqrt{a^2 + c}, \text{ where } a = bc.\end{aligned}$$

Moreover, if we had picked the other root of the equation then $\alpha = -\sqrt{a^2 + c}$.

□

**Example 4.2.2.** Let $d$ be a positive integer. Then Theorem 4.2.1 gives us the following examples

1. $\sqrt{t^{2d} + t^l} = [t^d, \overline{2t^{d-k}, 2t^d}]$, for $0 \leq k < d$;
2. $\sqrt{t^{2d} + t^d} = [t^d, \overline{2t^d}]$.

**Theorem 4.2.2.** *Let $d$ be a positive integer, then*

1. *for $D = t^{2d} + t^k$, where $0 \leq k < d$, the continued fraction expansion of $\sqrt{D}$ has partial quotients $a_h$ with*

$$\deg a_h = \begin{cases} d, & \text{if } h \text{ is even} \\ d - k, & \text{if } h \text{ is odd.} \end{cases}$$

2. *for $D = t^{2d} + t^d$, the continued fraction expansion of $\sqrt{D}$ has partial quotients $a_h$ of degree $d$ for all $h \geq 0$.*

*Furthermore, $l(\sqrt{D}) = d$ for any of the polynomials $D$ described in the statement of the theorem.*

*Proof.* Since $D \in \mathbb{Q}[t]$ has even degree, $\sqrt{D} \in \mathbb{Q}((1/t))$, and hence it has an infinite continued fraction expansion. From part *2* of example 4.2.2, we see that $\deg a_h = d$, for all $h$, and part *1* of example 4.2.2 gives

$$\deg a_h = \begin{cases} d, & \text{if } h \text{ is even} \\ d-k, & \text{if } h \text{ is odd.} \end{cases}$$

Finally, remark 4.2.1 says $l(\alpha) = \limsup_{h\to\infty} \partial eg\ a_h$, and since $d-k < d$, we conclude $l(\sqrt{D}) = d$ for both parts. □

We have seen that for periodic continued fractions, computing Lagrange constants is quite easy. However, most non-rational $\alpha \in \mathbb{Q}((1/t))$ have non-periodic continued fraction expansions. As a matter of fact, Zannier and Masser showed in [28] that for most 1-dimensional families of polynomials $D(t)$ of degree $2d > 6$, there are only finitely many such that $\sqrt{D(t)}$ has a periodic continued fraction expansion. So it is of interest to us to compute $l(\sqrt{D})$, for $\sqrt{D}$ with non-periodic continued fraction. Equivalently, it suffices to understand the degrees of the partial quotients $a_n$ for all $n$. For a general algebraic function, not much is known, since this question is closely related to a strong version of Roth's theorem over function fields. However, if we restrict $\alpha$ to be a quadratic irrational, we have results of Zannier and his students. Below we present a short survey of what is known, together with what the implications for the Lagrange constant are.

**Proposition 4.2.3.** (Zannier) *If $D(t)$ is a rational non-Pellian polynomial (not necessarily square-free) of even degree $2d$, with $d \leq 3$, or such that $y^2 = D(t)$ has genus $0$, then either $\sqrt{D(t)}$ has a periodic continued fraction or there are only finitely many partial quotients with $\deg a_n > 1$.*

However, already for $d = 4$ there is an example due to Merkert [29] for which we have infinitely many partial quotients of degree 2.

**Example 4.2.3.** The polynomial

$$D(t) = t^8 - t^7 - \frac{3}{4}t^6 + \frac{7}{2}t^5 - \frac{21}{4}t^4 + \frac{7}{2}t^3 - \frac{3}{4}t^2 - t + 1$$

is such that $\sqrt{D}$ has a non-periodic continued fraction expansion, with infinitely many partial quotients of degree 2. In particular, the degrees of the quotients follow the pattern $4,1,1,2,\overline{1,1,1,1,1,1,1,1,2}$. Hence $l(\sqrt{D}) = 2$.

Furthermore, the fact that Merkert's example exhibits a periodic pattern is not a coincidence. In fact Zannier [47] proved:

**Theorem 4.2.4.** (Zannier) *For a polynomial $D(t) \in \mathbb{C}[t]$, non-square and of even degree, the sequence of the degrees of the partial quotients of $\sqrt{D(t)}$ is eventually periodic.*

The most common case is for all degrees to be eventually 1 (or eventually constant). For example, if we concentrate on polynomials that have a square factor, say of the form $\Delta(t) = F^2 D(t)$, where $D(t)$ is not a square and of even degree, then Theorem 5 of Malagoli in [24] states the following:

**Theorem 4.2.5.** (Malagoli) *For a non-square polynomial $D(t) \in k[t]$ of even degree, with leading coefficient a square in $k$, there exist $F(t) \in k[t]$ such that all but finitely many of the partial quotients of $F\sqrt{D}(t)$ have degree $1$.*

Furthermore, it is a theorem of Zannier in [47], that for $D(t) \in \mathbb{C}[t]$, square-free and non-Pellian of degree $2d$, then all partial quotients of $\sqrt{D(t)}$ are of degree bounded above by $d/2$.

However, for non-Pellian polynomials with a square factor, this is no longer true. Using a remark of Zannier in [47], together with the result in section 3.4, we showcase a method of constructing polynomials of the form $\Delta(t) = F^2 D(t)$ with $l(\sqrt{\Delta(t)})$ being at least $\deg \Delta(t)/4$.

**Theorem 4.2.6.** *Suppose $D(t) \in \mathbb{Q}[t]$ is of degree $2d$, and its corresponding Pell's equation has non-trivial polynomial solutions $(u_n(t), v_n(t))_{n \in \mathbb{Z}}$. Moreover,* *let $F(t) \in \mathbb{Q}[t]$ of degree $f < d/3$, such that $F(t) \nmid v_n(t)$ for any $n \in \mathbb{Z}$. Then $l(F\sqrt{D}) > (f+d)/2$.*

*Remark* 4.2.2. It is worth noting that for a fixed $D(t) \in \mathbb{Q}[t]$, a square in $\mathbb{Q}((1/t))$, there are only finitely many polynomials of fixed degree, that divide $v_n(t)$, for some $n$, therefore such polynomials $F$ exist.

*Proof.* Suppose $D$ is a Pellian polynomial of degree $2d$, with $(u_n(t), v_n(t))_{n\in\mathbb{Z}}$ solving its corresponding Pell's equation. We have seen that there are only finitely many polynomials $F$ of a fixed degree $f$, that divide $v_n(t)$ for some $n$. Furthermore, if we can pick $F$, not a factor of $v_n(t)$, then the polynomial $\Delta(t) = F^2D(t) \in \mathbb{Q}[t]$ of degree $2\delta$ is not Pellian, and therefore by Lemma 3.4.2 and Abel's theorem $F\sqrt{D}(t)$ has a non-periodic continued fraction. We further impose the condition $d > 3f$ on the degrees of $D(t)$ and $F(t)$. Since $D(t)$ is Pellian, its continued fraction is periodic, and it has infinitely many convergents $p/q$ with corresponding partial quotient of degree $d$. That is

$$\partial eg\ (p^2 - Dq^2) = d - \deg a_n = 0.$$

Moreover, observe that

$$\deg\left((Fp)^2 - F^2Dq^2\right) = \deg F^2 + \deg\left(p^2 - Dq^2\right) = 2f < d \leq \delta - 1.$$

Therefore, by Proposition 2.4.4 $Fp(t)/q(t)$ is a convergent for $\sqrt{\Delta(t)}$. Thus its corresponding partial quotient, $a_i(t)$, satisfies:

$$\deg a_i(t) = \delta - \deg\left((Fp)^2 - F^2Dq^2\right) = \delta - 2f = d - f > \frac{\delta}{2}.$$

Observe that there are infinitely many convergents $p/q$ of $\sqrt{D(t)}$, with corresponding partial quotients of degree $d$, hence there will be infinitely many convergents $Fp/q$ of $\sqrt{\Delta(t)}$, with corresponding partial quotients of degree bigger than $\delta/2$. Consequently for these examples $l(\sqrt{\Delta(t)}) > \delta/2$. □

### 4.2.2 The Lagrange spectrum and its realisations

Over the real numbers, the collection of Lagrange constants for all real but not rational numbers describes the so-called Lagrange spectrum. Analogously, in the setting of formal Laurent series we make the following definition.

**Definition 4.2.2.** The *Lagrange spectrum* over $\mathbb{Q}((1/t))$ is defined to be

$$\mathscr{L} := \{l(\alpha) : \alpha \in \mathbb{Q}((1/t)),\ \text{not rational}\}.$$

As an easy consequence of Theorem 2.3.7 we can compute the spectrum, and the polynomials described in theorem 4.2.2 provide an example for each $l \in \mathscr{L}$.

**Corollary 4.2.7.** *The Lagrange spectrum of* $\mathbb{Q}((1/t))$ *is equal to* $\mathbb{N} \cup \{\infty\}$.

*Remark* 4.2.3. For us, the natural numbers $\mathbb{N}$ do not include $0$.

*Proof.* For each positive integer $n$, there exists $\alpha \in \mathbb{Q}((1/t))$ such that $l(\alpha) = n$. Just take $\alpha$ to be one of the square roots described in Theorem 4.2.2. □

Observe that $\alpha \in \mathbb{Q}((1/t))$, not a rational function, with a continued fraction expansion $[a_0,\ a_1, \cdots,\ \alpha_{h+1}]$, then from (2.1) and Proposition 2.3.2 it follows the identity

$$\alpha - \frac{p_h}{q_h} = \frac{(-1)^h}{q_h^2\left(\alpha_{h+1} + \frac{q_{h-1}}{q_h}\right)}.$$

Hence $\partial eg\ (\alpha - p_h/q_h) + 2\partial eg\ q_h = -\partial eg\ (\alpha_{h+1} + q_{h-1}/q_h)$, and Lagrange constant is given by $l(\alpha) = \limsup_{h\to\infty} \partial eg\ (\alpha_{h+1} + q_{h-1}/q_h)$. Furthermore

$$\alpha_{h+1} = [a_{h+1},\ a_{h+2}, \cdots] \ \text{ and } \ \frac{q_{h-1}}{q_h} = [0,\ a_h,\ a_{h-1}, \cdots,\ a_1],$$

where each $a_i \in \mathbb{Q}[t]$ has positive degree. This observation, in a similar fashion to what happens over the real numbers, prompts an alternative realisation of Lagrange constant:

**Definition 4.2.3.** Given a doubly infinite sequence of polynomials with coefficients in $\mathbb{Q}$ of positive degree $G = \cdots,\ g_{-1},\ g_0,\ g_1, \cdots$, we define

$$\lambda_i(G) := [g_i,\ g_{i+1}, \cdots] + [0,\ g_{i-1},\ g_{i-2}, \cdots].$$

Furthermore, let

$$L(G) := \limsup_{i \in \mathbb{Z}} \partial eg\ \lambda_i(G).$$

We now show that the two definitions indeed coincide.

**Theorem 4.2.8.** *The Lagrange spectrum $\mathscr{L}$ is equal to*

$$\mathbb{L} := \{L(G) : G \textit{ is a doubly infinite sequence of non-constant polynomials}\}.$$

*Proof.* For $\alpha \in \mathbb{Q}((1/t))/\mathbb{Q}(t)$, with a continued fraction expansion $[a_0,\ a_1, \cdots]$, let

$$G = \cdots, a_1,\ a_0,\ a_1, \cdots$$

then $L(G) = \limsup_{i \to \infty} \partial eg\ \ \lambda_i(G) = \limsup_{i \to \infty} \deg a_i$. Furthermore, from Theorem 2.3.7, we know that $l(\alpha) = \limsup_{i \to \infty} \deg a_i$. Therefore, $l(\alpha) \in \{L(G) : G \text{ as above}\}$.

For the converse, let $G$ be a doubly infinite sequence as in the definition. Then $L(G)$ is either $\limsup_{i \to +\infty} \partial eg\ \lambda_i(G)$ or $\limsup_{i \to -\infty} \partial eg\ \lambda_i(G)$. In the first case we take $\alpha = [g_0,\ g_1, \cdots]$ and in the latter case we take $\alpha = [g_0,\ g_{-1}, \cdots]$. Then $L(G) \in \mathbb{L}$. □

Over the real numbers, the role of $G$ is played by doubly infinite sequences of positive integers, which were first introduced by Markov in [26]. He defined these objects to show that the Lagrange spectrum is contained in another famous spectrum, called the Markov spectrum, consisting of numbers represented by binary quadratic forms. Furthermore, using techniques of Markov it has been shown that for numbers below 3 the two spectra coincide. We therefore proceed by investigating the analogy of Markov spectrum in the setting of formal Laurent series.

# Chapter 5

# Binary quadratic forms and the Markov spectrum

Binary quadratic forms are homogeneous polynomials of degree 2, in two variables whose general theory, for coefficients in the real numbers, was developed by Lagrange, Legendre, and Gauss. A famous example is $q(x,y) = x^2 - Dy^2$, where asking whether 1 is representable by $q$, is equivalent to looking for integer solutions of Pell's equation for $D$. The question of representations by binary quadratic forms is thus of great importance, and, is fundamental for the definition of the Markov spectrum.

In the first part of this chapter, we lay down the general theory of indefinite binary quadratic forms with coefficients in $\mathbb{Q}((1/t))$. Since we could not find them in the literature, we spend some time proving relevant properties. We discuss the equivalence of binary quadratic forms, in particular showing that every such form is equivalent to a reduced one, and that equivalent forms can be put in a chain.

The latter part concentrates on the representation of elements of $\mathbb{Q}((1/t))$ by binary quadratic forms. We obtain results analogous to those over the real numbers, for example that two equivalent forms represent the same elements. This leads us to the classical definition of the Markov spectrum, $\mathscr{M}$. In order to describe $\mathscr{M}$ fully, we prove it is equivalent to a different set connected to doubly infinite sequences of non-constant polynomials. The pay off comes in the form of $\mathscr{M} = \mathbb{N} \cup \{\infty\}$, and is in complete contrast to the complicated structure of the Markov spectrum for real numbers.

## 5.1 Binary quadratic forms over $\mathbb{Q}((1/t))$

To set the scene for the definition of the Markov spectrum we need to first develop the theory of binary quadratic forms in the setting of formal Laurent series in $1/t$.

**Definition 5.1.1.** A binary quadratic form over $\mathbb{Q}((1/t))$ is defined to be an expression

$$Q = Q(X,Y) = (A,B,C) := AX^2 + BXY + CY^2,$$

where $A,B,C \in \mathbb{Q}((1/t))$, not all rational functions in $t$. We define the discriminant to be $D = B^2 - 4AC$, which is also an element of $\mathbb{Q}((1/t))$.

**Definition 5.1.2.** We call a binary quadratic form $(A,B,C)$ *indefinite*, if the discriminant $D$ is a square in $\mathbb{Q}((1/t))$. From Lemma 2.2.2, this is precisely when $D$ is a polynomial of even degree and with leading coefficient a rational square.

For an indefinite binary quadratic form $Q(X,Y)$, $X - \omega Y$ is a factor, where $\omega$ is a root of

$$A\omega^2 + B\omega + C = 0.$$

We define the *first* and *second* roots to be

$$f := \frac{\sqrt{D} - B}{2A} \qquad s := \frac{-\sqrt{D} - B}{2A}, \tag{5.1}$$

respectively. Furthermore, assuming $A \neq 0$ and $f, s \notin \mathbb{Q}(t)$, the Laurent series for $f, s$ and $\sqrt{D}$ uniquely determine $A, B, C$. Observe that $f$ and $s$ are both in $\mathbb{Q}(t)$ if and only if $A, B$ and $C$ are all rational functions in $t$ and $D$ is a perfect square.

Suppose we substitute

$$x = \alpha X + \beta Y \qquad y = \gamma X + \delta Y, \tag{5.2}$$

with $\alpha,\ \beta,\ \gamma,\ \delta \in \mathbb{Q}[t]$ not all 0, into $q(x,y)$. This takes the binary quadratic form $q(x,y)$ to the binary quadratic form $Q(X,Y)$. We can also use the matrix form

$$H = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix},$$

with the convention that applying the matrix to a binary quadratic form is the same as applying the linear transformation (5.2) to it.

**Definition 5.1.3.** We say that two forms $q$ and $Q$ are *equivalent* if such a matrix $H$ exists and $\det(H) = \pm 1$.

Furthermore, we say that $q$ and $Q$ are *properly equivalent* if $\det H = 1$, and *improperly equivalent* if $\det H = -1$.

*Remark* 5.1.1. Observe that equivalence (proper equivalence) is an equivalence relation. However improper equivalence fails the transitive property.

**Proposition 5.1.1.** *The form $q = (a,b,c)$ is transformed into the form $Q = (A,B,C)$ via $H = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in GL_2(\mathbb{Q}[t])$, if and only if their first roots $f$ and $F$ and their second roots $s$ and $S$, are connected by the relations*

$$f = \frac{\alpha F + \beta}{\gamma F + \delta} \quad \textit{and} \quad s = \frac{\alpha S + \beta}{\gamma S + \delta}.$$

The proof consists of a computation analogous to the one over the real numbers, see [11].

### 5.1.1 Reduced indefinite binary quadratic forms

**Definition 5.1.4.** The indefinite binary quadratic form $Q = (A,B,C)$ is called *reduced* if

$$\partial eg\ f < 0 < \partial eg\ s, \text{ and } f \neq 0.$$

From (5.1), this is equivalent to

$$\partial eg\ (\sqrt{D} - B) < \partial eg\ (A) < \partial eg\ (\sqrt{D} + B), \text{ and } \sqrt{D} \neq B.$$

**Proposition 5.1.2.** *If $q = (A,B,C)$ is reduced, then so is $Q = (C,B,A)$.*

*Proof.* Consider the transformation $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ taking $q$ to $Q$, and in particular the roots $(f,s)$ to $(F,S) = \left(\frac{1}{s}, \frac{1}{f}\right)$. Since $q$ is reduced, then $\partial eg\ f < 0 < \partial eg\ s$. Hence $\partial eg\ F = -\partial eg\ s < 0$, and $\partial eg\ S = -\partial eg\ f > 0$. □

Analogously to the real case, every binary quadratic form $q$ is equivalent to a reduced one. However the reduction algorithm for $q$ with coefficients in $\mathbb{Q}((1/t))$ is different.

**Theorem 5.1.3.** *An indefinite binary quadratic form is properly equivalent to a reduced one.*

*Proof.* Let $q = (a,b,c) = ax^2 + bxy + cy^2$, with $a,b,c \in \mathbb{Q}((1/t))$, be an indefinite binary quadratic form of discriminant $D \neq 0$. It has first and second root $f = (\sqrt{D} - b)/2a$ and $s = (-\sqrt{D} - b)/2a$, respectively. We will first show that $q$ is either a reduced form or is properly equivalent to a binary quadratic form with a first root of non-negative degree. Suppose that the degree of $f$ is negative, then either $q$ is already reduced or $\partial eg\ s \leq 0$. If we are in the latter case, apply the transformation $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Then, $q$ is properly equivalent to an indefinite binary quadratic form with roots $-1/f$ and $-1/s$, both of positive degree. Hence $q$ is properly equivalent to a binary quadratic form with roots $(\varphi, \sigma)$, such that $\partial eg\ \varphi \geq 0$.

We next apply the transformation $\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}$ with $h = \lfloor \varphi \rfloor \in \mathbb{Q}[t]$. This takes the roots $(\varphi, \sigma)$ to $(F, S)$, where $F = \{\varphi\}$ and $S = \sigma - h$.

Now if $\lfloor \varphi \rfloor \neq \lfloor \sigma \rfloor$, then $\partial eg\ F < 0$ and $\partial eg\ S > 0$, and hence $q$ is properly equivalent to a reduced form.

If $\lfloor \varphi \rfloor = \lfloor \sigma \rfloor$, then consider the continued fraction expansion $\varphi = [a_0,\ a_1, \cdots]$ and $\sigma = [b_0,\ b_1, \cdots]$. Pick the smallest $m$ such that $a_m \neq b_m$, $m > 0$, then we have

$$\varphi = [a_0,\ a_1, \cdots,\ a_{m-1},\ f_m] \ \text{ and } \ \sigma = [a_0,\ a_1, \cdots,\ a_{m-1},\ s_m].$$

Since $a_m \neq b_m$, then $f_m \neq s_m$, and in particular $\lfloor f_m \rfloor \neq \lfloor s_m \rfloor$. Observe that the convergents for $\varphi$ and $\sigma$ are the same up to and including the $(m-1)^{\text{st}}$ term. Then the transformation $\begin{pmatrix} p_{m-1} & p_{m-2} \\ q_{m-1} & q_{m-2} \end{pmatrix}$ takes $(\varphi, \sigma)$ to $(f_m, s_m)$. Furthermore, this matrix has polynomial entries and is of determinant $(-1)^{m-2}$, i.e. 1 or $-1$ depending on the parity of $m$. Apply

$$\begin{pmatrix} (-1)^m & h \\ 0 & 1 \end{pmatrix} \quad \text{with } h = \lfloor f_m \rfloor.$$

This takes $(f_m, s_m)$ to $(F, S)$, where $F = (-1)^m \{f_m\}$ has negative degree and $S = (-1)^m (s_m - h)$ has non-negative degree. Since $\lfloor s_m \rfloor \neq \lfloor f_m \rfloor$, $\partial eg\ S$ is positive, and the new quadratic form is reduced and properly equivalent to $q$. □

## 5.1.2 Chain of reduced forms

All of the results in this section are the direct analogue to the case over the real numbers and can be found in [11]. We follow the same approach as Dickson, however the proofs differ in some details - in particular in the need of lemma 5.1.7.

**Definition 5.1.5.** Two reduced binary quadratic forms with coefficients in

$\mathbb{Q}((1/t))$, $Q=(A,B,C)$ and $q=(C,b,c)$, are called *neighbours* if they are properly equivalent and $B+b=2PA$, for some polynomial $P\in\mathbb{Q}[t]$. Further, we call the form $q$ *right neighbouring form* for $Q$; and $Q$ a *left neighbouring form* for $q$.

**Theorem 5.1.4.** *Every reduced indefinite binary quadratic form has a unique right neighbouring form.*

*Proof.* Let $Q=(A,B,A_1)$ be an indefinite reduced binary quadratic form of discriminant $D$. The transformation $\Delta=\begin{pmatrix}0&1\\-1&\delta\end{pmatrix}$, with $\delta\in\mathbb{Q}[t]$ to be determined later, takes $Q$ to the equivalent form $Q_1=(A_1,B_1,A_2)$, such that $B_1=-B-2\delta A_1$ and $A_2$ is such that $D=B_1^2-4A_1A_2$. Furthermore,

$$f\overset{\Delta}{\rightarrow}F=\delta-\frac{1}{f}$$
$$s\overset{\Delta}{\rightarrow}S=\delta-\frac{1}{s}.$$

Since $Q$ is reduced, $\partial eg\, f<0<\partial eg\, s$. Take $\delta=\lfloor 1/f\rfloor\in\mathbb{Q}[t]$, which has positive degree. Then $\partial eg\ F=\partial eg\ \{1/f\}<0$ and $\partial eg\ S=\partial eg\ \delta-1/s=\partial eg\ \delta>0$, i.e. $Q_1$ is reduced. Observe that if $\delta\neq\lfloor 1/f\rfloor$, then $\partial eg\ F>0$. Hence $Q_1$ is reduced only if $\delta$ is chosen to be $\lfloor 1/f\rfloor$. □

**Corollary 5.1.5.** *Every reduced form has one and only one reduced left neighbouring form.*

*Proof.* If $(A,B,A_1)$ is reduced, then $(A_1,B,A)$ is reduced as well by Proposition 5.1.2. From the theorem above, there is a unique reduced right neighbouring form $(A,B_1,A_2)$. Then by Proposition 5.1.2, $(A_2,B_1,A)$ is also reduced. Moreover, it has $(A,B,A_1)$ as its unique right neighbouring form. □

Therefore, given a reduced indefinite binary quadratic form $Q$ of discriminant $D\neq 0$, we can construct a chain of equivalent reduced indefinite binary quadratic forms of the same discriminant, say

$$\cdots, \Phi_{-1}, \Phi_0, \Phi_1, \cdots,$$

where $\Phi_i = \big((-1)^i A_i,\ B_i,\ (-1)^{i+1} A_{i+1}\big)$ and $\Phi_0 = Q$. The transformation $\Delta_i = \begin{pmatrix} 0 & 1 \\ -1 & \delta_i \end{pmatrix}$ takes $\Phi_i$ to $\Phi_{i+1}$. Furthermore, we have the relation $B_i + B_{i+1} = 2g_i A_{i+1}$, where $g_i = (-1)^i \delta_i$.

Let

$$f_i = \frac{\sqrt{D} - B_i}{(-1)^i 2A_i} \quad \text{and} \quad s_i = \frac{\sqrt{D} + B_i}{(-1)^{i+1} 2A_i}$$

be the first and second roots of $\Phi_i$, and define $F_i := (-1)^i / f_i$ and $S_i := (-1)^{i+1}/s_i$. Then

$$F_i = \frac{\sqrt{D} + B_i}{2A_{i+1}} \quad \text{and} \quad S_i = \frac{\sqrt{D} - B_i}{2A_{i+1}},$$

with $\partial eg\ F_i > 0 > \partial eg\ S_i$, since the $\Phi_i$ are reduced. From the fact that $\Delta_i$ takes $\Phi_i$ to $\Phi_{i+1}$, we know that their roots are related by

$$f_{i+1} = \delta_i - \frac{1}{f_i} \quad \text{and} \quad s_{i+1} = \delta_i - \frac{1}{s_i}. \tag{5.3}$$

Multiplying both by $(-1)^{i+1}$ and using the definition of $F_i$, $S_i$ and $g_i$, we get

$$F_i = g_i + \frac{1}{F_{i+1}} \quad \text{and} \quad S_{i+1} = \frac{1}{g_i + S_i}.$$

Hence

$$F_i = [g_i,\ g_{i+1}, \cdots] \quad \text{and} \quad S_i = [0,\ g_{i-1},\ g_{i-2}, \cdots].$$

Using properties of continued fractions, we obtain

$$\frac{1}{f_0} = F_0 = [g_0,\ g_1, \ldots,\ g_i,\ F_{i+1}] \tag{5.4}$$

$$(-1)^{i+1} s_i = \frac{1}{S_i} = \left[g_{i-1},\ g_{i-2}, \cdots,\ g_0,\ \frac{1}{S_0}\right]. \tag{5.5}$$

Observe that

$$F_i + S_i = \frac{\sqrt{D}}{A_{i+1}} = [g_i,\ g_{i+1}, \cdots] + [0,\ g_{i-1},\ g_{i-2}, \cdots]. \tag{5.6}$$

**Theorem 5.1.6.** *Two properly equivalent reduced indefinite binary quadratic forms belong to the same chain.*

*Proof.* Let $q$ and $Q$ be reduced indefinite binary quadratic forms with coefficients in $\mathbb{Q}((1/t))$ and discriminant $D \neq 0$. Suppose the transformation $H = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL_2(\mathbb{Q}[t])$ makes them properly equivalent. Furthermore, the entries of the transformation $H$ satisfy $\deg\alpha < \deg\beta$, $\deg\gamma < \deg\delta$ and $\deg\beta < \deg\delta$ which will be shown in Lemma 5.1.7, after the proof.

Now consider the continued fraction expansion of $\delta/\beta = [a_0,\ a_1, \cdots,\ a_i]$, and its $(i-1)^{\text{st}}$ convergent $p_{i-1}/q_{i-1} = [a_0,\ a_1, \cdots,\ a_{i-1}]$. Since $\deg\beta < \deg\delta$, the polynomials $a_i$ have positive degree for all $i$. Moreover if $i$ is odd, Proposition 2.3.4 implies that the pair $(q_{i-1}, p_{i-1})$ is the unique non-zero solution over $\mathbb{Q}[t]$ to $\delta x - \beta y = 1$, such that $\partial eg\ x < \partial eg\ \beta$ and $\partial eg\ y < \partial eg\ \delta$. However, from the determinant of $H$, $\alpha\delta - \beta\gamma = 1$, and from Lemma 5.1.7 we have $\deg\alpha < \deg\beta$, $\deg\gamma < \deg\delta$. Hence $(\alpha, \gamma)$ is also a solution and thus $\gamma/\alpha = [a_0,\ a_1, \cdots,\ a_{i-1}]$.

Let $F \in \mathbb{Q}((1/t))$ be the first root of $Q$, and consider the continued fraction expansion

$$\left[a_0,\ a_1, \cdots,\ a_i, \frac{1}{F}\right].$$

Using the convergents correspondence (2.1), together with the fact that $\delta/\beta =$

$[a_0,\ a_1, \cdots,\ a_i]$, we get

$$\left[a_0,\ a_1, \cdots,\ a_i, \frac{1}{F}\right] = \frac{\frac{\delta}{F}+\gamma}{\frac{\beta}{F}+\alpha}.$$

Furthermore, since $H$ sends $q$ to $Q$, by Proposition 5.1.1 it also connects their corresponding first roots $f$ and $F$ in the following way

$$\frac{1}{f} = \frac{\frac{\delta}{F}+\gamma}{\frac{\beta}{F}+\alpha} = \left[a_0,\ a_1, \cdots,\ a_i, \frac{1}{F}\right]. \tag{5.7}$$

Observe that since $Q$ is reduced, we know that $\partial eg\ F < 0$, and in particular $\partial eg\ 1/F > 0$, and all other partial quotients $a_j$ are of positive degree. Thus (5.7) uniquely describes $1/f$ up to the $i^{\text{th}}$ partial quotient in its continued fraction expansion.

On the other hand for any chain of reduced forms $(\Phi_j)_{j\in\mathbb{Z}}$, we have shown (5.4):

$$1/f_0 = F_0 = [g_0,\ g_1, \cdots,\ g_i,\ F_{i+1}],$$

where $f_0$ is the first root of the form $\Phi_0$, and $F_i = (-1)^{i+1}/f_{i+1}$, where $f_{i+1}$ is the first root of the form $\Phi_{i+1}$. So consider the chain of forms, where $q$ is $\Phi_0$. This implies that $f = f_0$, and from the uniqueness of the expansion of $1/f$, we must have $g_j = a_j$ for all $0 \le j \le i$ and $F = 1/F_{i+1} = (-1)^{i+1} f_{i+1} = f_{i+1}$, since $i$ is odd. In particular this proves that $F$, the first root of $Q$, is also the first root of the form $\Phi_{i+1}$ in the chain where $\Phi_0 = q$.

It remains to show that the second root $s_{i+1}$ of $\Phi_{i+1}$ is equal to $S$ (the second root of $Q$), given the second root $s_0$ of $\Phi_0$ is equal to $s$ (the second root of $q$). The relations for the second roots $s_{i+1}$ of the chain forms given in (5.12) state

$$(-1)^{i+2} s_{i+1} = \frac{1}{S_{i+1}} = \left[g_i,\ g_{i-1}, \cdots,\ g_0, \frac{1}{S_0}\right]$$
$$\Rightarrow -s_{i+1} = [a_i,\ a_{i-1}, \cdots,\ a_0, -s],$$

since $i$ is odd, $s = s_0$ and $g_j = a_j$ for all $0 \leq j \leq i$. Now, $\partial eg\ s$ is positive, so this expansion is unique up to the term $a_0$. Furthermore, from Proposition 2.3.1 applied to the continued fraction of $\delta/\beta$, we know that

$$\frac{\delta}{\gamma} = [a_i,\ a_{i-1}, \cdots,\ a_0] \text{ and } \frac{\beta}{\alpha} = [a_i,\ a_{i-1}, \cdots,\ a_1].$$

Hence from the convergents correspondence, we have

$$-s_{i+1} = [a_i,\ a_{i-1}, \cdots,\ a_0, -s] = \frac{-s\delta + \beta}{-s\gamma + \alpha} = -S.$$

The final equality follows from $s$ and $S$ being connected via $H$. Therefore, $S$ is equal to the second root of the form $\Phi_{i+1}$ in the chain with $\Phi_0 = q$. Namely, $q$ and $Q$ are in the same chain. The case when $i$ is even is identical, but instead we use the fact that $(-q_{i-1}, -p_{i-1}) = (\alpha, \gamma)$ provides the unique solution to the equation $\delta x - \beta y = 1$.

□

**Lemma 5.1.7.** *If two distinct reduced indefinite binary quadratic forms of the same discriminant $D \neq 0$ are properly equivalent via the transformation $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, then*

$$\deg \alpha \leq \deg \beta,\ \deg \gamma < \deg \delta,\ \textit{and}\ \deg \beta < \deg \delta. \tag{5.8}$$

*Proof.* Since $q$ and $Q$ are properly equivalent, $\alpha\delta = \beta\gamma + 1$. We proceed by case analysis:

Case i. Suppose $\deg \alpha\delta < 0$. Since $\alpha,\ \delta \in \mathbb{Q}[t]$, $H$ is one of the following

$$\begin{pmatrix} 0 & \pm 1 \\ \mp 1 & \delta \end{pmatrix} \text{ or } \begin{pmatrix} \alpha & \pm 1 \\ \mp 1 & 0 \end{pmatrix}.$$

If we are in the latter case, consider $H^{-1} = \begin{pmatrix} 0 & \pm 1 \\ \mp 1 & \alpha \end{pmatrix}$, taking $Q$ to $q$. The matrix $H$ connects the roots by $-\delta = \frac{1}{f} + F$, hence $\deg \delta = \partial eg\ 1/f > 0$; and since $\deg \alpha < 0$ and $\deg \beta = \deg \gamma = 0$, the conditions are satisfied. If $H = \begin{pmatrix} \alpha & \pm 1 \\ \mp 1 & 0 \end{pmatrix}$, the conditions are thus satisfied for $H^{-1}$.

If $\beta\gamma = 0$, then $H$ is one of the following

$$\begin{pmatrix} \pm 1 & \beta \\ 0 & \pm 1 \end{pmatrix} \text{ or } \begin{pmatrix} \pm 1 & 0 \\ \gamma & \pm 1 \end{pmatrix}.$$

The first transformation connects the first roots $f$ and $F$, by $f - F = \beta$, and since the degrees of both $f$ and $F$ are negative, $\beta = 0$, i.e. $H$ is the identity. For the latter matrix, consider the second roots $s$ and $S$. Then $\frac{1}{s} = \gamma + \frac{1}{S}$, and since $s$ and $S$ are of positive degree, we must have $\gamma = 0$, and $H$ is the identity matrix. However, $q \neq Q$, so we can assume that $\beta\gamma \neq 0$.

Case ii. If $\deg \alpha\delta \geq 0$ and $\beta\gamma \neq \pm 1$. Then $\deg(\beta\gamma + 1) = \deg \beta\gamma \geq 0$. Hence

$$\deg \beta + \deg \gamma = \deg \alpha + \deg \delta \tag{5.9}$$

and

$$\deg \alpha < \deg \beta \Leftrightarrow \deg \gamma < \deg \delta \tag{5.10}$$

(a) Suppose $\deg \alpha < \deg \delta$, then (5.9) implies $\deg \beta + \deg \gamma < 2 \deg \delta$.

- if $\deg \beta = \deg \gamma$, then $\deg \beta < \deg \delta$ and $\deg \gamma < \deg \delta$. Then from (5.10) $\deg \alpha < \deg \beta$.
- if $\deg \gamma < \deg \beta$, then (5.10) implies that $\deg \gamma < \deg \delta$ and

$\deg\alpha < \deg\beta$. Furthermore, under $H$, the first roots satisfy

$$\frac{1}{f} = \frac{\gamma+\delta/F}{\alpha+\beta/F}$$

and since $\partial eg\, f < 0$, we must have $\partial eg\ (\gamma+\delta/F) > \partial eg\ (\alpha+\beta/F)$. Moreover, $\deg\gamma < \deg\delta + \partial eg\ 1/F$, since $\partial eg\ 1/F > 0$. Hence

$$\partial eg\ (\gamma+\delta/F) = \deg\delta + \partial eg\ \frac{1}{F} > \partial eg\ (\alpha+\beta/F) \geq \partial eg\ \frac{\beta}{F}.$$

The latter inequality follows from $\partial eg\ \frac{\beta}{F} > \deg\beta > \deg\alpha$. Therefore $\deg\delta > \deg\beta$.

- if $\deg\beta < \deg\gamma$, then (5.9) implies $\deg\beta < \deg\delta$ and $\deg\alpha < \deg\gamma$. We use the relation of the second roots under the transformation $H$, namely

$$\begin{aligned}\frac{1}{s} &= \frac{\gamma+\delta/S}{\alpha+\beta/S}\\ \Rightarrow 1 &= \left(\frac{\alpha}{s}-\gamma\right)(\alpha S+\beta).\end{aligned}$$

Hence $\partial eg\ \left(\frac{\alpha}{s}-\gamma\right) = -\partial eg\ (\alpha S+\beta)$. In addition, $\partial eg\ 1/s < 0$ so

$$\partial eg\ \left(\frac{\alpha}{s}-\gamma\right) = \deg\gamma = -\partial eg\ (\alpha S+\beta).$$

Furthermore, $\deg\gamma > \deg\alpha \geq 0$, i.e. $\partial eg\ (\alpha S+\beta) < 0$. Since $\alpha,\beta \in \mathbb{Q}[t]$ and $\partial eg\ S > 0$, this can only happen if $\partial eg\ \alpha S = \deg\beta$. Hence $\deg\alpha < \deg\beta$.

(b) if $\deg\delta < \deg\alpha$. Consider $H^{-1}$, taking $Q$ to $q$. Then

$$H^{-1} = \begin{pmatrix} A & B \\ \Gamma & \Delta \end{pmatrix} = \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix}$$

hence $\deg A < \deg\Delta$, and the same analysis as in the above cases works.

(c) if $\deg\alpha = \deg\delta$, then $2\deg\alpha = 2\deg\delta = \deg\beta + \deg\gamma$.

- if $\deg\beta = \deg\gamma$, then $\deg\alpha = \deg\beta = \deg\gamma = \deg\delta$. Moreover, consider

$$1 = \left(\frac{\alpha}{f} - \gamma\right)(\alpha F + \beta). \tag{5.11}$$

Since $\partial eg\ 1/f > 0$ and $\partial eg\ F < 0$, we have that

$$-\deg\beta = -\partial eg\ (\alpha F + \beta) = \partial eg\ \left(\frac{\alpha}{f} - \gamma\right) > \deg\alpha$$

a contradiction.

- if $\deg\beta > \deg\gamma$, then $\deg\alpha < \deg\beta$ and $\deg\delta < \deg\beta$. From (5.10), we have $\deg\gamma < \deg\delta$ and $\deg\gamma < \deg\alpha$. Furthermore, taking the degree of (5.11) we get

$$\partial eg\ (\alpha F + \beta) = -\partial eg\ \left(\frac{\alpha}{f} - \gamma\right)$$

and since $\partial eg\ 1/f > 0$ and $\partial eg\ F < 0$ we have

$$-\deg\beta = -\partial eg\ (\alpha F + \beta) = \partial eg\ \left(\frac{\alpha}{f} - \gamma\right) > \deg\alpha.$$

But also, $\deg\beta > \deg\alpha$, hence $\deg\alpha < 0$, i.e, $\alpha = 0 = \delta$, and $\beta = \pm 1 = \gamma$, but by assumption $\deg\beta > \deg\gamma$, a contradiction.

- if $\deg\beta < \deg\gamma$, then $\deg\beta < \deg\alpha < \deg\gamma$ and $\deg\beta < \deg\delta < \deg\gamma$. We next consider

$$1 = \left(\frac{\alpha}{s} - \gamma\right)(\alpha S + \beta). \tag{5.12}$$

Taking degree and using $\partial eg\ 1/s < 0 < \partial eg\ S$, we have

$$\deg\alpha < \deg\gamma = -\partial eg\ \left(\frac{\alpha}{s} - \gamma\right) = -\deg\alpha - \partial eg\ S,$$

i.e $\partial eg\ S < -2\deg\alpha$ and $\deg\alpha < 0$. Thus $\alpha = 0$, and the same analysis as above, gives us a contradiction.

□

### 5.1.3 Representation by indefinite binary quadratic forms

**Definition 5.1.6.** We say that $A \in \mathbb{Q}((1/t))$ is *represented by an indefinite binary quadratic form $Q$ with coefficients in* $\mathbb{Q}((1/t))$, if there exist polynomials $X$ and $Y \in \mathbb{Q}[t]$, not both zero, such that $A = Q(X,Y)$. We say $A$ is *properly represented by $Q$*, if there exist co-prime polynomials $X$ and $Y \in \mathbb{Q}[t]$ such that $A = Q(X,Y)$.

**Proposition 5.1.8.** *Properly equivalent binary quadratic forms represent the same elements of* $\mathbb{Q}((1/t))$.

*Proof.* Let $q$ and $Q$ be two binary quadratic forms which are properly equivalent via the transformation $H = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL(\mathbb{Q}[t])$, and let $M \in \mathbb{Q}((1/t))$ be represented by $q$. That is, there are some polynomials with coefficients in $\mathbb{Q}$, $x$ and $y$, not both 0, such that $q(x,y) = M$. Then $X = \delta x - \beta y$ and $Y = -\gamma x + \alpha y$ are both in $\mathbb{Q}[t]$, and $Q(X,Y) = M$. Finally, $X$ and $Y$ cannot both be zero, since $x$ and $y$ are not both zero and the determinant of $H$ is equal to 1. Therefore $M$ is also represented by $Q$. □

**Theorem 5.1.9.** *If the forms $\left((-1)^i A_i, B_i, (-1)^{i+1} A_{i+1}\right)$, for $i$ ranging over the integers, are a chain of reduced forms of discriminant $D \neq 0$, a square in $\mathbb{Q}((1/t))$, then the $A_i$'s include all elements of $\mathbb{Q}((1/t))$ of degree less than the degree of $\sqrt{D}$ which are properly represented by a form in the chain.*

*Proof.* Let $M \in \mathbb{Q}((1/t))$ with $\partial eg\ M < \partial eg\ \sqrt{D}$ be represented by such a reduced form $Q = \big((-1)^i A_i, B_i, (-1)^{i+1} A_{i+1}\big)$ of discriminant $D$ in a chain. That is, there exist polynomials $x$ and $y \in \mathbb{Q}[t]$ not both zero, such that $(-1)^i A_i x^2 + B_i xy + (-1)^{i+1} A_{i+1} y^2 = M$. If we take $\alpha = x$ and $\gamma = y$, where $x$ and $y$ are co-prime, then there exist $\beta, \delta \in \mathbb{Q}[t]$, such that $\alpha\delta - \gamma\beta = 1$. Then the transformation $H = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ takes $Q$ to a properly equivalent form $(M, B, C)$ of the same discriminant $D$, which also represents $M$. However, this form is not necessarily reduced. Consider its first and second roots $f = (\sqrt{D} - B)/2M$ and $s = (-\sqrt{D} - B)/2M$. Observe that $\partial eg\ (f - s) = \partial eg\ \sqrt{D} - \partial eg\ M > 0$. Therefore, we cannot have both the degrees of $f$ and $s$ being negative, and we can assume that $\partial eg\ f \geq 0$, otherwise $Q$ is reduced. Furthermore, $\lfloor f \rfloor \neq \lfloor s \rfloor$, so we apply $\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}$, with $h = \lfloor f \rfloor$. This transformation sends $(M, B, C)$ to $(M, N, L)$, which is reduced and represents $M$. From Theorem 5.1.6, $(M, N, L)$ must be one of the forms in the chain, i.e $M$ must appear amongst the $A_i$'s. □

**Theorem 5.1.10.** *Suppose $Q$ is an indefinite binary quadratic form which forms a chain of equivalent reduced forms $\Phi_i = \big((-1)^i A_i, B_i, (-1)^{i+1} A_{i+1}\big)$, for $i \in \mathbb{Z}$. Then*

$$\inf_{\substack{X,Y \in \mathbb{Q}[t] \\ (X,Y) \neq (0,0)}} \partial eg\ Q(X,Y) = \inf_{i \in \mathbb{Z}} \partial eg\ A_i.$$

*Proof.* If $Q$ is not a reduced form, then we can use the algorithm in Theorem 5.1.3 to find a properly equivalent form $\hat{Q}$ that is reduced, and moreover, since they are properly equivalent, they will represent the same elements by Proposition 5.1.8. Thus we can assume that $Q = (A, B, C)$ is a reduced form of discriminant $D$. Then

$$\partial eg\ \left(\frac{\sqrt{D}}{A}\right) = \partial eg\ \left(\frac{\sqrt{D}+B}{2A} + \frac{\sqrt{D}-B}{2A}\right) > 0.$$

In particular, $A \in \mathbb{Q}((1/t))$ is such that $\partial eg\, A < \partial eg\, \sqrt{D}$. Additionally observe that when investigating $\inf_{\substack{X,Y \in \mathbb{Q}[t] \\ (X,Y) \neq (0,0)}} \partial eg\, Q(X,Y)$, it suffices to focus our attention on $\inf\ \partial eg\, M$, where the infimum is taken over $M \in \mathbb{Q}((1/t))$, properly represented by $Q$. Hence, in order to study $\inf_{\substack{X,Y \in \mathbb{Q}[t] \\ (X,Y) \neq (0,0)}} \partial eg\, Q(X,Y)$ we need to only look at Laurent series $M$, properly represented by $Q$ and which are of degree less than $\partial eg\, \sqrt{D}$. By Theorem 5.1.9, these are given precisely by the $A_i$'s, i.e. the first coefficients in the chain of reduced forms, where $Q = \Phi_0$. Therefore running over $i \in \mathbb{Z}$, yields

$$\inf_{\substack{X,Y \in \mathbb{Q}[t] \\ (X,Y) \neq (0,0)}} \partial eg\, Q(X,Y) = \inf_{i \in \mathbb{Z}} \partial eg\, A_i.$$

□

## 5.2 The Markov spectrum over $\mathbb{Q}((1/t))$

### 5.2.1 The classical definition

**Definition 5.2.1.** Let $Q$ be an indefinite binary quadratic form of discriminant $D \neq 0$. Let $m(Q) := \inf_{\substack{X,Y \in \mathbb{Q}[t] \\ (X,Y) \neq (0,0)}} \partial eg\, Q(X,Y)$. Then the *Markov spectrum* is defined to be

$$\mathscr{M} := \left\{ \partial eg\, \sqrt{D(Q)} - m(Q)\ :\ Q \text{ indefinite binary quadratic form} \right\}.$$

From Theorem 5.1.10 we can conclude that

$$\mathscr{M} = \left\{ \partial eg\, \sqrt{D(\Phi_i)} - \inf_{i \in \mathbb{Z}} \partial eg\, A_i\ :\ \Phi_i = \left((-1)^i A_i, B_i, (-1)^{i+1} A_{i+1}\right) \text{ chain} \right\}.$$

Similarly to the Lagrange spectrum, we can alternatively define the Markov spectrum via doubly infinite sequences of polynomials of positive degree, $G = \ldots, g_{-1}, g_0, g_1, \ldots$. We will use this new form of the spectrum to completely determine $\mathscr{M}$.

### 5.2.2 Alternative realisation

To give some intuition on how the Markov spectrum is realised via doubly infinite sequences, we re-examine a few identities from section 5.1. Suppose we are given an indefinite binary quadratic form $Q$ of discriminant $D$, which forms a chain of equivalent forms

$$\Phi_i = \left((-1)^i A_i, B_i, (-1)^{i+1} A_{i+1}\right).$$

Just as in the discussion after corollary 5.1.5, we can define $F_i := (-1)^i/f_i$ and $S_i := (-1)^{i+1}/s_i$, where $f_i$ and $s_i$ are the first and second roots of $\Phi_i$. Then from (5.6), we have

$$F_i + S_i = \frac{\sqrt{D}}{A_{i+1}} = [g_i,\ g_{i+1},\ldots] + [0,\ g_{i-1},\ g_{i-2},\ldots],$$

where $g_i \in \mathbb{Q}[t]$ have positive degree. Furthermore, by Theorem 5.1.10, the elements of the Markov spectrum are given by $\partial eg\ \sqrt{D} - \inf_{i\in\mathbb{Z}} \partial eg\ A_i$. Recall that given a doubly infinite sequence of polynomials with coefficients in $\mathbb{Q}$, of positive degree $G = \ldots,\ g_{-1},\ g_0,\ g_1,\ldots$, we have defined

$$\lambda_i(G) = [g_i,\ g_{i+1},\ldots] + [0,\ g_{i-1},\ g_{i-2},\ldots].$$

**Theorem 5.2.1.** *The Markov spectrum $\mathscr{M}$ can be realised as the set*

$$\mathbb{M} = \{M(G) : G \textit{ doubly infinite sequence of } g_i \in \mathbb{Q}[t],\ \deg g_i > 0\},$$

*where* $M(G) := \sup_{i\in\mathbb{Z}} \partial eg\ \lambda_i(G)$.

*Proof.* From the discussion above and (5.6), given an indefinite binary quadratic form $Q$ of discriminant $D \neq 0$ we obtain a doubly infinite sequence of non constant polynomials $G$, such that $M(G) = \partial eg\ \sqrt{D} - m(Q)$. Hence $\mathscr{M} \subseteq \mathbb{M}$.

On the other hand, given a doubly infinite sequence of polynomials with coefficients in $\mathbb{Q}$, of positive degree $G = \ldots,\ g_{-1},\ g_0,\ g_1, \ldots$, we consider

$$\lambda_i(G) = [g_i,\ g_{i+1}, \ldots] + [0,\ g_{i-1},\ g_{i-2}, \ldots] \in \mathbb{Q}((1/t))\,.$$

Thus we can find an element of $\mathbb{Q}((1/t))$, say $A_{i+1}$, of degree $-\deg g_i < 0$, such that $\lambda_i(G) = 1/A_{i+1}$. Let $F_i = [g_i,\ g_{i+1}, \ldots]$ and $S_i = [0,\ g_{i-1},\ g_{i-2}, \ldots]$, then $F_i + S_i = 1/A_{i+1}$. Define $B_i := 2F_iA_{i+1} - 1 \in \mathbb{Q}((1/t))$ then

$$F_i = \frac{1+B_i}{2A_{i+1}} \quad \text{and} \quad S_i = \frac{1-B_i}{2A_{i+1}}.$$

Then we consider $f_i := (-1)^i/F_i$ and $s_i := (-1)^i/S_i$, i.e

$$f_i = \frac{1-B_i}{2(-1)^i a_i} \quad \text{and} \quad s_i = \frac{1+B_i}{2(-1)^i a_i},$$

where $4A_{i+1}a_i = 1 - B_i^2$. Furthermore, $\partial eg\ S_i < 0 < \partial eg\ F_i$ and thus $\partial eg\ f_i < 0 < \partial eg\ s_i$. Therefore, $f_i$ and $s_i$ are the roots of the reduced indefinite binary quadratic form $Q_i = \big((-1)^i a_i, B_i, (-1)^{i+1}A_{i+1}\big)$ of discriminant 1. From the continued fraction expansion of $F_i$ and $S_i$ we have

$$\begin{aligned} F_i = g_i + \frac{1}{F_{i+1}} \quad &\text{and} \quad \frac{1}{S_i} = g_{i-1} + S_{i-1} \\ \Rightarrow f_{i+1} = \delta_i - \frac{1}{f_i} \quad &\text{and} \quad s_{i+1} = \delta_i - \frac{1}{s_i}, \end{aligned}$$

where $\delta_i = (-1)^i g_i$. Then the transformation $\Delta_i = \begin{pmatrix} 0 & 1 \\ -1 & \delta_i \end{pmatrix}$ sends $Q_i$ to $Q_{i+1}$, and in particular $a_i = A_i$. Hence the forms $Q_i = \big((-1)^i A_i, B_i, (-1)^{i+1}A_{i+1}\big)$ are reduced, of discriminant 1 and in a chain. From Theorem 5.1.10, we know that $\inf_{i\in\mathbb{Z}} \partial eg\ A_i = m(Q)$, where $Q$ is an indefinite quadratic form of discriminant

1 properly equivalent to $Q_i$. Then

$$\begin{aligned} M(G) = \sup_{i\in\mathbb{Z}} \partial eg\ \lambda_i(G) = \sup_{i\in\mathbb{Z}} \partial eg\ &\left(\frac{1}{A_{i+1}}\right) \\ &= -\inf_{i\in\mathbb{Z}} \partial eg\ A_{i+1} \\ &= -m(Q). \end{aligned}$$

Since $\partial eg\ 1 = 0$, we can conclude $\mathbb{M} \subseteq \mathscr{M}$. □

**Theorem 5.2.2.** *The Markov spectrum* $\mathscr{M} = \mathbb{N} \cup \{\infty\}$.

*Proof.* From the above theorem

$$\mathscr{M} = \mathbb{M} = \{M(G) : G \text{ doubly periodic sequence of } g_i \in \mathbb{Q}[t],\ \deg g_i > 0\}.$$

Furthermore, $M(G) = \sup_{i\in\mathbb{Z}} \partial eg\ \lambda_i(G)$, and $\partial eg\ \lambda_i(G) = \partial eg\ g_i$, where $g_i \in \mathbb{Q}[t]$ have positive degree. The result follows. □

**Corollary 5.2.3.** *The Lagrange and Markov spectra coincide.*

# Appendix A

# Mathematica code for computing continued fractions of formal Laurent series

Here we will present two small Mathematica programmes, written by the author, implementing the continued fraction algorithm for certain $\alpha \in \mathbb{Q}((1/t))$. Firstly, we display below the code for computing the continued fraction expansion of $p/q \in \mathbb{Q}(t)$.

```
PolyPart[s_] := Module[{r = 0, i = 0},
                 While[i < Exponent[s, x] + 1,
                        r = r + Coefficient[s, x, i]*x^i ;
                        i++];
                 r]

    (* computes the polynomial part of a Laurent series, ⌊α⌋ *)

RatPart[s_] := s - PolyPart[s]

    (* computes the fractional part of a Laurent series, {α} *)

Invert[s_, precision_] := (x^(-Exponent[s, x])/
                          Coefficient[s, x^{Exponent[s, x]}]*
                          Series[(s*x^(-Exponent[s, x])/
                                 Coefficient[s, x^{Exponent[s, x]}])^{-1},
                                 {x, Infinity, precision}])[[1]]

    (* computes the multiplicative inverse of a series α ∈ ℚ((1/t)) *)

CF[p_, q_, n_, precision_] := Module[{A = {PolyPart[Series[p*q^{-1},
                                                    {x, Infinity, precision}][[1]]]},
                                      s = RatPart[Series[p*q^{-1},
                                                  {x, Infinity, precision}][[1]]],
                                      i = 0},
                               While[i < n,
                                      A = Append[A, PolyPart[Invert[s, precision]]];
                                      s = RatPart[Invert[s, precision]];
                                      i++];
                               A]

    (* gives the continued fraction expansion of p/q ∈ ℚ(t) in
       the form [a_0, a_1, a_2,...., a_n] *)
```

Secondly, we display the Mathematica programme for computing the continued fraction expansion of $\sqrt{D(t)}$, whenever $D(t) \in \mathbb{Q}[t]$ is of even degree and with leading coefficient a square in $\mathbb{Q}$.

```
FactorOut[D_] := {x^{Exponent[D, x]}, Apart[D/(x^{Exponent[D, x]})]}

   (* it factors out the highest order term, so it can be
      expanded to the power -1/2 *)

SquareRoot[D_, precision_] := (Sqrt[FactorOut[D][[1]]]*
                               Series[FactorOut[D][[2]]^{1/2},
                                      {x, Infinity, precision}])[[1]]

   (* expands the above to the power -1/2, up to the precision'ed
      degree term*)

PolyPart[s_] := Module[{r = 0, i = 0},
                 While[i < Exponent[s, x] + 1,
                        r = r + Coefficient[s, x, i]*x^i ;
                        i++];
                 r]

   (* computes the polynomial part of a Laurent series, ⌊α⌋ *)

RatPart[s_] := s - PolyPart[s]

   (* computes the fractional part of a Laurent series, {α} *)

Invert[s_, precision_] := (x^(-Exponent[s, x])/
                           Coefficient[s, x^{Exponent[s, x]}]*
                           Series[(s*x^(-Exponent[s, x])/
                                  Coefficient[s, x^{Exponent[s, x]}])^{-1},
                                  {x, Infinity, precision}])[[1]]

    (* computes the multiplicative inverse of a series α ∈ ℚ((1/t)) *)

CF[D_, n_, precision_] := Module[{A = {PolyPart[SquareRoot[D, precision]]},
                                  s = RatPart[SquareRoot[D, precision]],
                                  i = 0},
                           While[i < n, A = Append[A, PolyPart[Invert[s, precision]]];
                                  s = RatPart[Invert[s, precision]];
                                  i++];
                           A]
    (* gives the continued fraction expansion of $\sqrt{D}$ in
       the form [a_0, a_1, a_2,...., a_n] *)

PolyCF[D_, n_, precision_ ] := Module[{i = 1, b },
                                      b = CF[D, n, precision][[n]];
                                While[i < n,
                                      b = CF[D, n, precision][[n - i]] + 1/b;
                                      i++];
                                b];

    (* gives the continued fraction of $\sqrt{D}$ in the fractional
       form up to the  $n^{th}$ iteration *)

PolyConvergent[D_, n_, precision_ ] := Module[{i = 0, b },
                                               b = CF[D, n, precision][[n]];
                                        While[i < n,
                                               b = Together[CF[D, n, precision]
                                                               [[n - i]] + 1/b];
                                               i++];
                                        b];

    (* gives the  $n^{th}$ convergent of $\sqrt{D}$ *)

PolyApprox[D_, n_, precision_] := SquareRoot[D, precision] -
                                  Series[PolyConvergent[D, n, precision],
                                         {x, Infinity, precision}];

    (* gives the difference between $\sqrt{D}$ and its $n^{th}$
      convergent *)

DegreePolyApprox[D_, n_, precision_] := Exponent[PolyApprox[D, n, precision],  x ];

    (* gives the degree of the difference between $\sqrt{D}$ and
       its $n^{th}$ convergent *)
```

# Bibliography

[1] N H Abel. “Über die Integration der Differential-Formel $\rho$dx/√r, wenn r und $\rho$ ganze Functionen sind”. In: *Journal für die reine und angewandte Mathematik* 1 (1826), pp. 185–221.

[2] W W Adams and M J Razar. “Multiples of Points on Elliptic Curves and Continued Fractions”. In: *Proceedings of the London Mathematical Society* s3-41.3 (Nov. 1980), pp. 481–498. ISSN: 00246115. DOI: 10.1112/plms/s3-41.3.481.

[3] T G Berry. “On periodicity of continued fractions in hyperelliptic function fields”. In: *Archiv der Mathematik* 55.3 (Sept. 1990), pp. 259–266. ISSN: 0003889X. DOI: 10.1007/BF01191166.

[4] J Bourgain. “A remark on solutions of the pell equation”. In: *International Mathematics Research Notices* (2015). ISSN: 16870247. DOI: 10.1093/imrn/rnu023. arXiv: 1311.5911.

[5] J Brillhart et al. *Factorizations of bn±1, b= 2, 3, 5, 6, 7, 10, 11, 12 Up to High Powers. Contemporary Mathematics.* Vol. 22. 2nd. American Mathematical Society (Providence, RI), 1988. ISBN: 0821850784.

[6] Y Bugeaud. “Nonarchimedean quadratic Lagrange spectra and continued fractions in power series fields”. In: *Fundamenta Mathematicae* 247.2 (2019), pp. 171–189. ISSN: 00162736. DOI: 10.4064/fm622-2-2019.

[7] J W S Cassels. *Introduction to diophantine approximation.* Cambridge University Press, 1972. ISBN: 9780028426501.

[8] P L Chebyshev. “Sur l’intégration des différentielles qui contiennent une racine carrée d’un polynôme du troisième ou du quatrième degré”. In: *J. Math. Pures Appl.* 2 (1857), pp. 1–42.

[9] T W Cusick and M E Flahive. *The Markoff and Lagrange spectra.* American Mathematical Society, 1989, p. 97. ISBN: 9780821815311.

[10] B Delone and A Vinogradov. “Über den Zusammenhang zwischen den Lagrangeschen Klassen der Irrationalitaten mit begrenzten Teilnennern und den Markoffschen Klassen der extremen Formen”. In: *Leonard Euler zum 250 Geburstag.* Berlin: Leonard Euler zum 250 Geburstag, 1959, pp. 100–108.

[11] L E Dickson. *Introduction to the theory of numbers.* Dover, 1957. ISBN: 9780486603421.

[12] A Dubickas and J Steuding. “The polynomial Pell equation”. In: *Elemente der Mathematik* 59.4 (Nov. 2004), pp. 133–143. ISSN: 0013-6018. DOI: 10.1007/s00017-004-0214-7.

[13] G A Freiman. “On the coincidence of the Markov and Lagrange spectra”. In: *Mat. Zametki* 3 (1968).

[14] A Hurwitz. “Ueber die angenäherte Darstellung der Irrationalzahlen durch rationale Brüche”. In: *Mathematische Annalen* 39.2 (June 1891), pp. 279–284. ISSN: 00255831. DOI: 10.1007/BF01206656.

[15] A Khintchine. *Kettenbrüche.* Leipzig: B. G. Teubner Verlagsgesellschaft, 1956, p. 96.

[16] P G Kogoniya. “On the set of Markov numbers”. In: *Dokl. Akad. Nauk SSSR* 78 (1951).

[17] P G Kogoniya. “On the structure of the set of Markov numbers”. In: *Tr. Tbilissk. Mat. Inst.* 19 (1953).

[18] E E Kummer. “10. Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen”. In: *Journal fur die Reine und Angewandte Mathematik* 1852.44 (1852), pp. 93–146. ISSN: 14355345. DOI: 10.1515/crll.1852.44.93. URL: https://zenodo.org/record/1448864.

[19] A Lasjaunias. *A survey of diophantine approximation in fields of power series.* 2000. DOI: 10.1007/s006050070036.

[20] D H Lehmer. “On the Multiple Solutions of the Pell Equation”. In: *The Annals of Mathematics* 30.1/4 (1928), p. 66. ISSN: 0003486X. DOI: 10.2307/1968268.

[21] H W Lenstra. *Solving the Pell equation.* Tech. rep. 2008.

[22] WJ LeVeque. *Topics in Number Theory, volumes I and II.* Courier Corporation, 2012. ISBN: 0486152081.

[23] K Mahler. “On a Theorem of Liouville in Fields of Positive Characteristic”. In: *Can. J. Math.* 1 (1949), pp. 397–400.

[24] F Malagoli and U Zannier. “Continued fractions in function fields: polynomial analogues of McMullen’s and Zaremba’s conjectures”. PhD thesis. 2017. arXiv: 1704.02640v2.

[25] A V Malyshev. “Markov and Lagrange spectra (survey of the literature)”. In: *Journal of Soviet Mathematics* 16.1 (May 1981), pp. 767–788. ISSN: 00904104. DOI: 10.1007/BF01213889.

[26] A Markoff. “Sur les formes quadratiques binaires indéfinies”. In: *Mathematische Annalen* 15.3-4 (Sept. 1879), pp. 381–406. ISSN: 00255831. DOI: 10.1007/BF02086269.

[27] R C Mason. *Diophantine Equations over Function Fields.* London Mathematical Society Lecture Note Series. Cambridge, England: Cambridge University Press, 1984.

[28] D Masser and U Zannier. “Torsion points on families of simple abelian surfaces and Pell’s equation over polynomial rings”. In: *Math. Soc* 17 (2013), pp. 2379–2416. DOI: 10.4171/JEMS/560.

[29] O Merkert. “Reduction and specialization of hyperelliptic continued fractions”. PhD thesis. 2015. arXiv: 1706.04801v1.

[30] S Müller, B Kirchheim, and E Kopecká. “Monotone curves”. In: *Mathematische Annalen* (2010), pp. 1–14. ISSN: 1432-1807.

[31] M B Nathanson. “Polynomial Pell’s Equations”. In: *Proceedings of the American Mathematical Society* 56.1 (Apr. 1976), p. 89. ISSN: 00029939. DOI: 10.2307/2041581.

[32] C D Olds. *Continued Fractions*. Washington DC: The Mathematical Association of America, 2011. ISBN: 9780883859261. DOI: 10.5948/UPO9780883859261.

[33] J Parkkonen and F Paulin. “On the nonarchimedean quadratic Lagrange spectra”. In: *Mathematische Zeitschrift* 294.3 (Apr. 2019), pp. 1065–1084. ISSN: 14321823. DOI: 10.1007/s00209-019-02300-1.

[34] O Perron. *Die Lehre von den Kettenbrüchen. Bd I. Elementare Kettenbrüche.* 1954.

[35] O Perron. “Uber die Approximation irrationaler Zahlen durch rationale, 2”. In: *S.-B. Heidelberg Akad. Wiss.* (1921).

[36] A J van der Poorten. “Non-periodic continued fractions in hyperelliptic function fields”. In: *Bulletin of the Australian Mathematical Society* 64.02 (Oct. 2001), p. 331. ISSN: 0004-9727. DOI: 10.1017/S000497270003999X.

[37] A J van der Poorten and J Shallit. “Folded continued fractions”. In: *Journal of Number Theory* 40.2 (Feb. 1992), pp. 237–250. ISSN: 0022314X. DOI: 10.1016/0022-314X(92)90042-N.

[38] A J van der Poorten and X C Tran. "Quasi-Elliptic Integrals and Periodic Continued Fractions". In: *Monatshefte für Mathematik* 131.2 (Nov. 2000), pp. 155–169. ISSN: 0026-9255. DOI: 10.1007/s006050070018.

[39] M Ru. "A weak effective roth's theorem over function fields". In: *Rocky Mountain Journal of Mathematics* 30.2 (2000), pp. 723–734. ISSN: 00357596. DOI: 10.1216/rmjm/1022009292.

[40] J Sándor et al. *Handbook of number theory I.* Kluwer Academic, 2006, p. 622. ISBN: 9781402042157.

[41] W M Schmidt. "On continued fractions and diophantine approximation in power series fields". In: *Acta Arithmetica* 95.2 (2000), pp. 139–166. ISSN: 00651036. DOI: 10.4064/aa-95-2-139-166.

[42] W W Stothers. "Polynomial identities and hauptmoduln". In: *Quarterly Journal of Mathematics* 32.3 (Sept. 1981), pp. 349–370. ISSN: 00335606. DOI: 10.1093/qmath/32.3.349.

[43] S Uchiyama. "Rational approximations to algebraic functions". In: *Journal of Faculty of Science, Hokkaido University. Series I. Mathematics* 15.3-4 (1961), pp. 173–192. ISSN: 2189-3187. DOI: 10.14492/hokmj/1530756192.

[44] A Vinogradov, B Delone, and D Fuks. "On rational approximations to irrational numbers with bounded incomplete quotients". In: *Dokl. Akad. Nauk SSSR* 118 (1958).

[45] J T Y Wang. "An effective roth's theorem for function fields". In: *Rocky Mountain Journal of Mathematics* 26.3 (1996), pp. 1225–1234. ISSN: 00357596. DOI: 10.1216/rmjm/1181072046.

[46] A C Woods. "The markoff spectrum of an algebraic number field". In: *Journal of the Australian Mathematical Society* 25.4 (1978), pp. 486–488. ISSN: 14468107. DOI: 10.1017/S1446788700021467.

[47] U Zannier. “Hyperelliptic continued fractions and generalized Jacobians”. In: *American Journal of Mathematics* 141.1 (2019), pp. 1–40. DOI: 10.1353/ajm.2019.0000.

[48] U Zannier. “Unlikely intersections and Pell’s equations in polynomials”. In: *Springer INdAM Series*. Vol. 8. Springer International Publishing, 2014, pp. 151–169. DOI: 10.1007/978-3-319-05254-0_12.