BAR-ILAN UNIVERSITY

Fibonacci numbers as special values of polynomials

Adi Ostrov

Submitted in partial fulfillment of the requirements for the Master's Degree in the

Department of Mathematics, Bar-Ilan University

Ramat-Gan, Israel October 13, 2025

This work was carried out under the supervision of

Dr. Eyal Subag

Department of Mathematics, Bar-Ilan University

and

Prof. Danny Neftin

Department of Mathematics, Technion

I would like to express my deep gratitude to Professor Danny Neftin, who has been my mentor and guide in the world of mathematics over the past few years. Thank you for the countless hours of conversation and guidance, which have contributed immensely to my mathematical development in general, and to this thesis in particular. Thank you as well for introducing me to so many fascinating ideas and topics, which I hope to continue exploring in the future.

I am also grateful to Dr. Eyal Subag for his invaluable support behind the scenes.

I would like to thank Professor Avi Berman, who sparked my initial interest in mathematics and suggested the problem that eventually became the basis of this thesis.

Finally, I wish to thank the many friends who supported me along the way and patiently listened to me speak endlessly about this work.

Contents

Abstract

The Fibonacci sequence is the well-known recurrence sequence with initial values $F_0 = 0$ and $F_1 = 1$, ansatisfying the recurrence relation $F_{n+2} = F_{n+1} + F_n$.

A long standing question, answered affirmatively by Cohn in 1964, is whether the only perfect squares in the Fibonacci sequence are $0, 1$ and 144. His elementary proof also identified all the elements in the sequence which are twice a square, and solved the same problems for the related Lucas sequence, defined by $L_0 = 2$, $L_1 = 1$ and $L_n = L_{n-1} + L_{n-2}$. The higher degree equations $F_n = x^p$ and $F_n = x^p \pm 1$ in the Fibonacci numbers were solved by Bugeaud, Mignotte and Siksek. All these equations turned out to have only finitely many solutions. Recent work by Voutier bounded the number of perfect squares in various other rank-two recurrence sequences[1]. All these questions fall within the subject of *Diophantine equations in recurrence sequences.*

In the first part of this work, we continue the study of Diophantine equations involving the rank-two recurrence sequences. Given a recurrence sequence r_n with a Fibonacci-like recurrence relation, we describe all the rational functions $\phi(x) \in \mathbb{Q}(x)$ for which there are infinitely many solutions $(n, x) \in \mathbb{Z} \times \mathbb{Q}$ to the equation $r_n = \phi(x)$. A particular example of interest is the Fibonacci sequence, for which, despite the aforementioned finiteness results, there exist such $\phi(x)$ whose image contains infinitely many Fibonacci numbers.

In the second part of this work, we consider the problem of *reducibility at elements from a rank-two recurrence sequence.* Given an polynomial $P(t, x) \in \mathbb{Q}(t)[x]$ with $\deg_x P \geq 2$ and a rational number $t_0 \in \mathbb{Q}$, we consider the specialization of P at t_0, namely the polynomial $P(t_0, x) \in \mathbb{Q}[x]$. If $P(t, x)$ is irreducible over $\mathbb{Q}(t)$, then the spe-

[1] Recall that the rank of a recurrence sequence is the number of previous elements involved in its recurrence relation.

cializations $P(t_0, x) \in \mathbb{Q}[x]$ may or may not remain irreducible over $\mathbb{Q}$. For instance, if $P(t_0, x) \in \mathbb{Q}[x]$ has a rational root $x \in \mathbb{Q}$, it must factor as a product of a linear term and another polynomial. We can thus regard the reducibility of a specialization $P(t_0, x)$ (i.e., reducibility of P at t_0) as a weaker version of solvability. Accordingly, for a given Fibonacci-like recurrence sequence r_n, we are also interested in identifying the irreducible polynomials $P(t, x) \in \mathbb{Q}(t)[x]$ for which $P(r_n, x) \in \mathbb{Q}[x]$ is reducible for infinitely many elements from r_n. In the second part of the work we address precisely this problem.

A more basic question was answered by Pierre Dèbes in the case of the geometric sequence $G_n = \alpha^n$, which is a rank-one recurrence sequence. In this case, the exceptional polynomials – i.e., those with infinitely many reducible values in the sequence – were characterized geometrically: They are exactly those which pull back to a reducible polynomial when pulled back along $x \mapsto x^p$ or $x \mapsto -4x^4$.

An enlightening persepective on this question comes from the study of universal Hilbert sets. These are sets $U \subset \mathbb{Q}$ which satisfy the property that any irreducible polynomial $P(t, x) \in \mathbb{Q}(t)[x]$ has finitely many reducible specialization $P(u, x) \in \mathbb{Q}[x]$ for $u \in U$. Many recurrence sequences are known to form universal Hilbert sets. However, the elements of various rank-two recurrence sequences – and in particular, the elements of the Fibonacci sequence – do *not* form a universal Hilbert set. Despite this, we show that this failure of universality is limited and occurs only for polynomials satisfying a geometric condition unique to rank-two sequences. Specifically, whenever $P(t, x)$ pulls back to a reducible polynomial along certain rational functions.

Chapter 1: Introduction

The Fibonacci numbers are the quintessential example of a recurrence sequence, defined by the initial values $F_0 = 0, F_1 = 1$ and the recurrence relation $F_{n+2} = F_{n+1} + F_n$.

In this M.Sc. thesis, we study the intersection of the Fibonacci numbers (and similar recurrence sequences) with two arithmetically defined sets:

1. the set of values $\phi(K)$ attained on elements of K, and
2. the set of reducible values $\mathrm{Red}_P(K)$ of an irreducible polynomial $P(t,x) \in K(t)[x]$, that are those values $t_0 \in K$ such that $P(t_0, x) \in K[x]$ is a reducible polynomial,

where K is some number field. We address each problem separately in the following two sections.

Before discussing these two problems, let us recall the principle of unlikely intersections. We begin with a central example. Set $\mathcal{Y} = \{(\zeta, \eta) : \zeta, \eta \in \mu_\infty\}$ the set of points in $\mathbb{A}^2_{\mathbb{C}}$ with coordinates which are roots of unity. Looking for curves $X = \{f(x,y) = 0\} \subset \mathbb{A}^2$ which intersect (i.e., contain) infinitely many points from $\mathcal{Y}$, Lang shows [1] that such X must be special: X must have the form $x^a y^b = \rho$ or $x^a = y^b \rho$ for some positive integers a, b and ρ a root of unity. These curves are precisely the cosets (shifted by a root of unity) of algebraic subgroups of $\mathbb{G}_m^2(\mathbb{C}) = \{(x,y) \mid x, y \in \mathbb{C}^\times\}$. For such special $f(x,y)$, the curve $X = \{f(x,y) = 0\}$ always contains infinitely many points from $\mathcal{Y}$.

More generally, for a fixed $r < n$, let $\mathcal{Y}$ be a set of "special" algebraic varieties $Y \subset \mathbb{A}^n$ of low dimension $\dim(Y) \leq r$. Here, "special" conveys that the collection $\mathcal{Y}$ has some arithmetic (but not algebraic) nature. In such cases, one should expect for a generic $X \subset \mathbb{A}^n$ of low dimension $s < n - r$, that very few, if any, $Y \in \mathcal{Y}$ will intersect X. Thus, X's which intersect "a lot" of Y's must be special, in some sense, with respect to the family $\mathcal{Y}$. Such unlikely intersections typically arise for "special" varieties X that reflect some geometric property intrinsic to the family $\mathcal{Y}$. This is the aforementioned principle of unlikely intersections.

Both of the sets we are interested in, $\phi(\mathbb{Q})$ and $\mathrm{Red}_P(\mathbb{Q})$, are quite sparse sets of arithemtic nature. Following the principle of unlikely intersections, we suspect that except for some special ϕ's and P's, the intersection of these sets with a given recurrence sequence should be very small, i.e., finite. We follow this suspicion for both cases and for various recurrence sequences, and determine when is it correct.

1.1 Recurrence sequences as values of rational functions

Results on the subject of Diophantine equations involving Fibonacci numbers have started with the work of Cohn [2] in 1964, which proved the long-standing conjecture that the only integer solutions (n, x) to the equation $F_n = x^2$ have $F_n = 0, 1$ or 144. He likewise described all the finitely many solutions to the equation $F_n = 2x^2$ and the equations $L_n = x^2$ and $L_n = 2x^2$ involving the Lucas sequence, which is given by $L_0 = 2, L_1 = 1$, and $L_{n+2} = L_{n+1} + L_n$. Further works [3] [4] continued this line of research, and managed to describe all the – again, finitely many – Fibonacci numbers which are either perfect powers or are one away from a perfect power. More recent results [5] have managed to bound the number of perfect squares which appear in various other rank-two recurrence sequences (i.e., those sequences in which each element depends on the previous two elements).

Questions of this nature are part of the subject of *polynomial exponential Diophantine equations*, which is concerned with equations of the form

$$P(x_1, x_2, \ldots, x_r, \alpha_1^{x_1}, \alpha_2^{x_2}, \ldots, \alpha_r^{x_r}) = 0$$

for a fixed $P \in \mathbb{Q}[x_1, \ldots, x_r, y_1, \ldots, y_r]$ and fixed complex numbers $\alpha_1, \ldots, \alpha_r$, and whose solutions $x_1 = a_1, \ldots, x_r = a_r$ are required to be integers or rational numbers. Particular interest exists for such equations – which we may call *separated* – in which the dependence on each of the variables x_i is either entirely algebraic or entirely exponential. More precisely, those equations in which at least one of the x_i's or the y_i's does not appear in $P(x_1, \ldots, x_r, y_1, \ldots, y_r)$ for each $1 \leq i \leq r$.

Recall that a linear recurrence sequence over a field K is a sequence $(r_n)_{n\in\mathbb{Z}}$ satisfying a recurrence relation of the form $r_n = \sum_{i=1}^{r} a_i r_{n-i}$ for fixed $a_1, \ldots, a_r \in K$. In this work we shall consider sequences which extend infinitely in both the positive and the negative direction. We call r the *rank* of the recurrence, and the polynomial $p(x) = x^r - \sum_{i=1}^{r} a_i x^{r-i}$ the characteristic polynomial of the recurrence. Assuming the recurrence is simple (that is, that the characteristic polynomial has only roots of multiplicity one), it is well known that the vector space of sequences $(r_n)_{n\in\mathbb{Z}}$ satisfying a fixed recurrence relation is spanned by the sequences $(\alpha^n)_{n\in\mathbb{Z}}$, where α is a root of the characteristic polynomial. Indeed, our central example, the Fibonacci sequence, satisfies a simple recurrence relation of rank-two and can be written as $F_n = \frac{1}{\sqrt{5}}(\varphi^n - (-\varphi)^{-n})$, where $\varphi = \frac{1+\sqrt{5}}{2}$ is the golden ratio. In this case, the roots are φ and $-\varphi^{-1}$. When the roots have larger multiplicity, we may have a polynomial dependence on n, as well as an exponential one. (For example, $a_n = n$ is a solution to the recurrence equation $a_{n+1} = 2a_n - a_{n-1}$).

A problem of interest in the subject of polynomial exponential Diophantine equations is that of *polynomial values in a (simple) recurrence sequence*, which deals with solutions $(n, x) \in \mathbb{Z} \times \mathbb{Q}$ to equations of the form $r_n = g(x)$, for some fixed $g(x) \in \mathbb{Q}[x]$, and some fixed (simple) recurrence sequence $r_n = \sum_{i=1}^{r} A_i \alpha_i^n$ with *roots* $\alpha_i \in \mathbb{C}$, and coefficients $A_i \in \mathbb{C}$. Such equations are examples of (separated) polynomial exponential Diophantine equations. For example, [6] treats polynomial equations in recurrence squences with integral roots.

If we take r_n to be any recurrence sequence, then for any polynomial $g(x)$, the sequence $S_n = g(r_n)$ will also be a recurrence sequence, usually of a much higher rank. For this sequence, the equation $S_n = g(x)$ will clearly have infinitely many solutions. However, we can see that even for some low rank sequences, there may be infinitely many solutions to such equations. The Fibonacci numbers, to name an example, satisfy the following identity: $F_{3n} = 5F_n^3 + (-1)^n 3F_n$, and hence, in particular, they contain infinitely many rational values of the polynomials $g(x) = 5x^3 + 3x$ and $g(x) = 5x^3 - 3x$.

Nemes–Pethö [7] described all the polynomials $f(x) \in \mathbb{Z}[x]$ which attain infinitely many elements of a given rank-two recurrence sequence in their set of integer values $f(\mathbb{Z})$, and Ostrov–Neftin–Berman–Elrazik [8] have extended the description to functions taking values in $\mathbb{Q}$.

In the first part of this thesis work we are interested in describing all the *rational functions* $\phi(x) \in K(x)$ that attain infinitely many elements from a given recurrence sequence in their image $\phi(K)$. This both continues the line of work described above, and resolves the unlikely intersections suspicion we opened with.

To present our results, recall that the Dickson polynomial $D_{\alpha,d}(x) \in \mathbb{Q}(\alpha)$ of degree $d \in \mathbb{N}$ with parameter α is the unique degree-d polynomials that satisfies $D_{\alpha,d}(x+\alpha/x) = x^d + \alpha^d/x^d$, and the Rédei function of degree $d \in \mathbb{N}$ and parameter δ is $R_{\delta,d}(x) = \mu_\delta^{-1}(\mu_\delta(x)^d) \in \mathbb{Q}(\delta^2))(x)$, where $\mu_\delta(x) = (x+\delta)/(x-\delta)$. We denote by $\eta^{\circ k}(x) = \eta(\eta(\ldots(\eta(x))\ldots))$ is the k-fold composition. Our results in the special case of the Fibonacci sequence are given in the following theorem:

Theorem 1.1. *Suppose that $\phi(x) \in \mathbb{Q}(x)$ is a rational function of degree $d \geq 2$ that attains infinitely many Fibonacci numbers in its image, that is, $\#(\phi(\mathbb{Q}) \cap \{F_n\}) = \infty$. Then either*

- *d is odd and $\phi(x) = (\pm 5)^{-(d+1)/2} D_{\pm 5,d}(\ell(x))$ for some degree one rational map $\ell(x) \in \mathbb{Q}(x)$, or*
- *d is even and $\phi(x) = q_{\pm 1}(\eta^{\circ k}(R_{\sqrt{5},d/2}(\ell(x))))$ for some $0 \leq k < d/2$ and some degree one rational map $\ell(x) \in \mathbb{Q}(x)$,*

where $\eta(x) = 5(x+1)/(x+5)$, $q_{-1}(x) = (x^2 - 2x + 5)/(x^2 - 5)$ and $q_1(x) = -4x/(x^2 - 5)$, and where we take the signs to be -1 if $\phi(\mathbb{Q})$ meets infinitely many even-indexed Fibonacci numbers, and to be $+1$ if it meets infinitely many odd-indexed Fibonacci numbers.

Our examples from earlier, with $g(x) = 5x^3 \pm 3x$ are instances of the first case given in the theorem. Each of the functions mentioned in the theorem indeed attains infinitely many Fibonacci numbers in its image. For example, for the even Fiboancci numbers, we have the identities

$$F_{2nd} = (-5)^{-(d+1)/2} D_{-5,d}(5F_{2n})$$

for any odd d, and

$$F_{2nd+2k} = q_1(\eta^{\circ k}(R_{\sqrt{5},d}(\frac{L_{2n}+2}{F_{2n}})))$$

for any $d \in \mathbb{N}$. Similar identities exist for the odd-indexed Fibonacci numbers.

We prove a version of this result for rank-two recurrence sequences which satisfy a recurrence relation of the form $r_{n+2} = ar_{n+1} - \zeta r_n$ for some m-th root of unity ζ. We begin by finding a family of curves $V_0, \ldots, V_{m-1}$ such that every element in the sequence appears as the x-coordinate of a rational point on one of these curves. If a rational map ϕ attains infinitely many elements from the sequence, the pullback of one of these curves along ϕ must have infinitely many integral points. We then apply Siegel's theorem on integral points on curves to narrow down the range of possibilities for ϕ, and then study the ramification of ϕ until we reach the explicit description given in the theorem. The proof appears in Chapter 3.

1.2 Recurrence sequences as reducible values of polynomials

Let $P(t,x) \in \mathbb{Q}(t)[x]$ be an irreducible polynomial. Hilbert studied how often the specializations of such $P(t,x)$, namely the polynomials $P(t_0,x) \in \mathbb{Q}[x]$ for various $t_0 \in \mathbb{Q}$, remain irreducible. Let

$$\mathrm{Red}_P(\mathbb{Q}) = \{t_0 \in \mathbb{Q} \mid P(t_0,x) \in \mathbb{Q}[x] \text{ is undefined or reducible}\}$$

denote the set of reducible values of the polynomial, sometimes called the set of special values of $P(t,x)$. We remark that this definition also includes the finite set of undefined values, consisting of t_0's which appear in the denominators of the coefficients of $P(t,x)$.

However, this is not an issue for our purposes, as our interest lies in infinite subsets of this set which would surely contain infinitely many reducible and defined values.

Hilbert's celebrated irreducibility theorem states this set is a *thin set*, as per the following definition due to Serre. Recall the a covering map of curves is a non-constant morphism.

Definition 1.2. *A set $S \subset \mathbb{P}^1(\mathbb{Q})$ is a thin set if we can write it as a union*

$$S = \bigcup_i \phi_i(V_i(\mathbb{Q})) \cup F,$$

for some finite set F and for some finite list of (smooth, geometrically irreducible projective) curves V_i with covering maps $\phi_i : V_i \to \mathbb{P}^1$ of degree ≥ 2.

The name "thin" is not misleading: There are $O(\sqrt{H})$ rational numbers of height at most H in a given thin set, where we define the height $H(p/q)$ of a rational number in reduced form to be $\max(|p|, |q|)$.

We now flip the script on Hilbert's irreducibility theorem. Fix some "sparse" and "special"[1] set $U \subset \mathbb{Q}$ of rational numbers, and consider the sets $\mathrm{Red}_P(U) = \mathrm{Red}_P(\mathbb{Q}) \cap U$ as the irreducible polynomial $P(t, x)$ varies. For example, fix U to be the set of elements in a particular recurrence sequence. In the spirit of unlikely intersections, Hilbert's theorem suggests that these sets should be quite small, as they are the intersection of a thin set with an unrelated sparse set.

In many cases this claim turns out to be very much true! For example, if $U = \{2^n + 5^n \mid n \in \mathbb{N}\}$, then $\mathrm{Red}_P(U)$ is finite for every irreducible polynomial $P(t, x)$ [9]. More generally, such sets U for which $\mathrm{Red}_P(U)$ is finite for all the irreducible polynomials $P(t, x) \in \mathbb{Q}(t)[x]$ are known as *universal Hilbert sets*[2], and have been studied from various angles [6] [10] [11] [12]. However, not all recurrence sequences give rise to universal Hilbert sets. For instance, the elements of the geometric sequence $G_n = \alpha^n$ fail to form a universal Hilbert set, as we can see by the fact that $\mathrm{Red}_{x^2-t}(\{G_n\}) \supset \{G_{2n}\}$ is an infinite set.

[1] The quoted words should be taken to have an intuitive, informal meaning.

[2] The name originates from the fact that these sets serve as proofs of a weaker form of Hilbert's irreducibility theorem, which simply states that for every irreducible polynomial there are infinitely many irreducibe values.

A theorem by Dèbes [13] provides a full description of the failures to universality for the geometric sequence. For an irreducible polynomial $P(t,x) \in \mathbb{Q}(t)[x]$ let X_P be the (projective) curve defined by $P(t,x) = 0$ (by which we mean a projective model for the variety defined by the roots of $P(t,x)$), and let $\pi_x : X_P \to \mathbb{P}^1$ be the projection to the x-coordinate. Fix $\alpha \in \mathbb{Q}\backslash\{0,1,-1\}$. Then the irreducible polynomials $P(t,x) \in \mathbb{Q}(t)[x]$ that are reducible at infinitely many elements from the sequence $\{\alpha^n\}$ are only those for which π_x factors either as $\pi_x = \alpha^j x^p \circ \pi'$ for some prime p, some $j < p$ and some map $\pi' : X_P \to \mathbb{P}^1$, or $\pi_x = -4\alpha^j x^4 \circ \pi'$ for some $j < 4$ and for some $\pi' : X_P \to \mathbb{P}^1$. Here, the first factors of each map are given in affine coordinates. More recent work by L. Bary-Soroker et. al. [14] provided density 0 results (conditional on the Generalized Riemann Hypothesis) in the multivariate case $f(t_1, \dots, t_r, x) \in \mathbb{Q}[t_1, \dots, t_r, x]$, barring some exceptional polynomials. More precisely, they showed that for fixed $a_1, \dots, a_r \in \mathbb{Z} \setminus \{0,1,-1\}$, the polynomial $f(a_1^{n_1}, \dots, a_r^{n_r}, x)$ remains irreducible in $\mathbb{Q}[x]$ for almost all[3] $n_1, \dots, n_r$, unless X_f pulls back to a reducible cover along a map of the form $(t_1, \dots, t_r) \mapsto (t_1^{n_1}, \dots, t_r^{n_r})$. We can see that in both of these results the exceptional polynomials can be described in a geometric fashion. This aligns with the principle of unlikely intersections discussed earlier.

As with the geometric sequence, the Fibonacci sequence and other rank-two recurrence sequences do not always give rise to universal Hilbert sets. We already saw a counterexample to universality of the Fibonacci sequence in the previous section: the identity $F_{6n} = 5F_{2n}^3 + 3F_{2n}$ shows that the polynomial $P(t,x) = 5x^3 + 3x - t$ will have infinitely many reducible specializations with t in the Fibonacci sequence.

In the second part of this work we show that – just as is the case for the geometric sequence – the counterexamples to universality of rank-two recurrence sequences can be described geometrically, as in the following theorem for the special case of the Fibonacci sequence. As in the previous theorem, we denote $\eta(x) = 5(x+1)/(x+5)$, $q_1(x) = (x^2 - 2x + 5)/(x^2 - 5)$ and $q_{-1}(x) = -4x/(x^2 - 5)$, and let $R_{\sqrt{5},n}(x)$ stand for the Rédei functions with parameter $\sqrt{5}$. Moreover, for a pair of maps $\phi : V \to \mathbb{P}^1$ and $\psi : W \to \mathbb{P}^1$, we let $\phi^*\psi$ stand for the pullback map $V \times_{\mathbb{P}^1} W \to V$.

[3] Here, almost all is taken to mean that the proportion of such tuples in $[-N, N]^r$ approaches 1 as N goes to infinity

Theorem 1.3. *Suppose that $P(t,x) \in \mathbb{Q}(t)[x]$ is an irreducible polynomial of odd x-degree $d = \deg_x P \geq 3$, such that the specializations $P(F_n, x) \in \mathbb{Q}[x]$ are reducible for infinitely many Fibonacci numbers F_n. Let X_P be a projective model of variety defined by $P(t,x) = 0$, and denote by $\pi_x = \pi_{P,x} : X_P \to \mathbb{P}^1$ the projection to the x-coordinate. Then either*

- *π_x factors as $(\pm 5)^{-(p+1)/2} D_{\pm 5,p} \circ \pi'$ for some prime $p \,|\, d$ and some $\pi' : X_P \to \mathbb{P}^1$, or*
- *$q_{\pm 1}^* \pi_x$ factors as $\eta^{\circ j} \circ R_{\sqrt{5},p} \circ \pi'$ for some prime $p \,|\, d$, some $0 \leq j < p$ and some $\pi' : X_P \to \mathbb{P}^1$,*

where we take the signs to be -1 if $P(t,x)$ is reducible at infinitely many even-indexed Fibonacci numbers, and $+1$ if it is reducible at infinitely many odd-indexed Fibonacci numbers.

If $P(t,x)$ is a counterexample to universality (i.e., $P(F_n,x)$ is reducible for infinitely many n's), then so must $\tilde{P}(t,x) = P(t, A(t,x))$ be, for any $A(t,x) \in \mathbb{Q}(t)[x]$. When considering the projections $\pi_{P,x}$ and $\pi_{\tilde{P},x}$ to the x-coordinate, as in the theorem, we can see that $\pi_{\tilde{P},x} = \pi_{P,x} \circ \tilde{A}$, where $\tilde{A} : (t,x) \mapsto (t, A(t,x)) \in X_P$. Thus, our theorem must allow for the arbitrary factor π' (here seen explicitly as $\tilde{A}$) to appear in the result.

For each of the possibilities for the factorization of π_x mentioned in the theorem there is a polynomial $P(t,x)$ that satisfies the conditions of the theorem and for which π_x factorizes in the prescribed fashion. This can be seen from the fact that all the functions stated in Theorem 1.1 indeed attain infinitely many Fibonacci numbers in their image. More precisely, we take $P(t,x) = f(x) - tg(x)$, where $\phi(x) = f(x)/g(x)$ is one of the functions mentioned in Theorem 1.1.

We prove the theorem for the more general case of binary recurrence sequences satisfying a recurrence relation of the form $r_{n+2} = ar_{n+1} - \zeta r_n$, where ζ is an m-th root of unity. We begin by applying Hilbert's irreducibility theorem to show that there exists some map $\phi(z)$ that attains infinitely many elements from the sequence, and for which $P(\phi(z), x)$ is reducible over $\mathbb{Q}(z)$. We then use the classification obtained in Chapter 3, along with variants of the Grunwald-Wang theorem proven in Chapter 4 to show that the projection must factor through a Dickson polynomial, or that the pullback by some q_j must factor through a Rédei function. This is done in Chapter 5.

Besides the proofs of the two theorems hereby presented, which occur in Chapters 3 and 5, respectively, Chapter 2 cites and proves the necessary algebraic and number theoretic preliminaries needed for the proofs, and Chapter 4 discusses reducibility results for the Dickson polynomials and the Rédei functions which are useful in the proof of Theorem 1.3.

Chapter 2: Preliminaries

2.1 Group theory

Let $\mathbb{Z}_n$ denote the cyclic group of order n, and $\mathrm{AGL}_1(\mathbb{Z}_n) = \mathbb{Z}_n \rtimes \mathbb{Z}_n^\times$ the group of one-dimensional affine linear transformations over $\mathbb{Z}_n$, also known as the *holomorph* of $\mathbb{Z}_n$. Since $\mathrm{AGL}_1(\mathbb{Z}_n)$ consists of affine linear transformations over $\mathbb{Z}_n$, we use the notation $x \mapsto ax + b$ or simply $ax + b$ to denote the element $(b, a) \in \mathrm{AGL}_1(\mathbb{Z}_n)$. In this notation, the group multiplication corresponds to functional composition. Moreover, $\mathbb{Z}_n \rtimes 1$ is the subgroup of elements of the form $x + b$ and $0 \rtimes \mathbb{Z}_n^\times$ is the subgroup of elements of the form ax. We have a natural action of $\mathrm{AGL}_1(\mathbb{Z}_n)$ on $\{0, \dots, n-1\}$ given via $(b, a) \cdot k = (ax + b) \cdot k = ak + b \mod n$. We will often implicitly think of this action when considering subgroups of $\mathrm{AGL}_1(\mathbb{Z}_n)$, and thus call $H \subset \mathrm{AGL}_1(\mathbb{Z}_n)$ an (in)transitive subgroup if H acts (in)transitively on $\{0, \dots, n-1\}$. For example, the subgroup $\mathbb{Z}_n \rtimes 1$ is transitive.

Proposition 2.1. *Write $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, where $p_1, \dots, p_k$ are distinct primes. Then $\mathrm{AGL}_1(\mathbb{Z}_n) \cong \prod_{i=1}^k \mathrm{AGL}_1(\mathbb{Z}_{p_i^{a_i}})$. Moreover, the action of $\mathrm{AGL}_1(\mathbb{Z}_n)$ on $\mathbb{Z}_n$ commutes with the action of the product on $\prod \mathbb{Z}_{{p_i}^{a_i}} \cong \mathbb{Z}_n$ along this isomorphism.*

Proof. Indeed, every element $ax + b = (b, a) \in \mathrm{AGL}_1(\mathbb{Z}_n)$ determines an element in the product $\big((b \mod p_i^{a_i}, a \mod p_i^{a_i})\big)_{i=1,\dots,r}$. By the Chinese Remainder Theorem, every such tuple comes from a unique element modulo n. Since the isomorphism consists only of taking remainders, it clearly commutes with the action which is defined by modular multiplication and addition. □

Lemma 2.2. *Let p be a prime. A non-identity element $ax + b \in \mathrm{AGL}_1(\mathbb{Z}_p)$ satisfies exactly one of the following:*

- *$a \neq 1$, and $ax + b$ has a single fixed point, or*
- *$ax + b = x + b$ has no fixed points, acts transitively, and generates all of $\mathbb{Z}_p \rtimes 1$.*

Proof. Suppose $a \neq 1$, then $1 - a \in \mathbb{Z}_p^\times$ is invertible, and the unique solution to the equation $aX + b = X$ is $X = (1 - a)^{-1} b$. If $a = 1$, for a non-identity element we must have $b \neq 0$ in which case $x \mapsto x + b$ has no fixed points. Since $\mathbb{Z}_p \rtimes 1$ is of prime order, $x + b$ generates all of it. □

Lemma 2.3. *The only subgroup of* $\mathrm{AGL}_1(\mathbb{Z}_p)$ *of order* p *is* $\mathbb{Z}_p$*.*

Proof. We first note that p divides $\# \mathrm{AGL}_1(\mathbb{Z}_p) = p(p-1)$ exactly once. All p-Sylow groups are conjugate. However, $\mathbb{Z}_p$ is normal in $\mathrm{AGL}_1(\mathbb{Z}_p)$, hence it is preserved under conjugation. □

Lemma 2.4. *A subgroup* $H \subset \mathrm{AGL}_1(\mathbb{Z}_p)$ *is transitive if and only if* $\mathbb{Z}_p \rtimes 1 \subset H$*.*

Proof. Since $\mathbb{Z}_p \rtimes 1$ is transitive, the "if" direction is obvious. Let us prove the "only if": Since H has a single orbit of size p, by the orbit-stabilizer theorem $p \mid \#H$. It's p-Sylow subgroup will be a p-Sylow subgroup of $\mathrm{AGL}_1(\mathbb{Z}_p)$, and the only subgroup of $\mathrm{AGL}_1(\mathbb{Z}_p)$ of order p is $\mathbb{Z}_p$ □

Lemma 2.5. *Let* p *be a prime, and suppose* $H < \mathrm{AGL}_1(\mathbb{Z}_p)$ *is intransitive, then* H *is conjugate to a subgroup of* $0 \rtimes \mathbb{Z}_p^\times$*.*

Proof. The order of H must not be divisible by p, since if it was, its p-Sylow subgroup would be $\mathbb{Z}_p \rtimes 1$, but this is a transitive subgroup. Now, consider the representation $H \to \mathrm{End}(\mathbb{F}_p^2)$ given by $ax + b \mapsto \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$. This representation has a one dimensional subrepresentation $\mathbb{F}_p \times 0$. Since $p \nmid \#H$, this subrepresentation must have a direct complement $U = \mathrm{span} \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$, where $\beta \neq 0$. Therefore, for any element $ax + b \in H$ there exists some c such that $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} c\alpha \\ c\beta \end{pmatrix}$. Since in the second component we have that $\beta = c\beta$, we must have $c = 1$. Thus, $a\alpha + b\beta = \alpha$. Since $\beta \neq 0$, we can rewrite that as $a\frac{\alpha}{\beta} + b = \frac{\alpha}{\beta}$. Therefore, $\frac{\alpha}{\beta}$ is a shared fixed point of all the elements of H. Conjugating by $g = x + \frac{\alpha}{\beta}$, we can see that $g^{-1}Hg \subset \mathrm{stab}(0) = 0 \rtimes \mathbb{Z}_p^\times$. □

Given $m \mid n$, let $q_{n,m} : \mathrm{AGL}_1(\mathbb{Z}_n) \to \mathrm{AGL}_1(\mathbb{Z}_m)$ denote the mod m projection. We will also (sometimes implicitly) consider the action of $\mathrm{AGL}_1(\mathbb{Z}_n)$ on $\{0, \ldots, m-1\}$ that factors through $q_{n,m}$ and the usual action of $\mathrm{AGL}_1(\mathbb{Z}_m)$. In the same fashion as earlier, we shall call a subgroup $H \leq \mathrm{AGL}_1(\mathbb{Z}_n)$ (in)transitive modulo m if $q_{n,m}(H)$ is (in)transitive, i.e., acts (in)transitively on $\{0, \dots, m-1\}$.

Lemma 2.6. *Let p be an odd prime, $k \geq 1$, and $H \subset \mathrm{AGL}_1(\mathbb{Z}_{p^k})$ be a subgroup of G. Then the following are equivalent:*

1. *H acts transitively on $\{0, \dots, p^k - 1\}$,*
2. *$q_{p^k,p}(H) \subset \mathrm{AGL}_1(\mathbb{Z}_p)$ acts transitively on $\{0, \dots, p-1\}$, and*
3. *there exists an element of the form $ax + b \in H$ where $a = 1 \mod p$ and $b \neq 0 \mod p$.*

Proof. Lemmas 2.4 and 2.2 show that (2) is true if and only if (3) is, and clearly, (1) implies (2). We shall prove that (3) implies (1) by induction on k. For $k = 1$ this is trivial. Suppose $k > 1$, and that the implication is true for $k-1$. By our assumption there exists an element $h = ax + b \in H$ such that $a = 1 \mod p$ and $b \neq 0 \mod p$. We claim that h generates a transitive subgroup of $\mathrm{AGL}_1(\mathbb{Z}_{p^k})$. To see this, we consider the orbit of 0. First, we show that $g = h^p$ acts transitively on the set $\{0, p, \dots, p^k - p\}$ of multiples of p. Write $g = a^p x + (1 + a + \cdots + a^{p-1})b = Ax + B$. Since $B = 1 + 1 + \cdots + 1 = 0 \mod p$, it's clear that g sends the set of multiples of p to itself. More generally we can see that g preserves residue modulo p. Further, observe that the action of g on the multiples of p is isomorphic to the action of $Ax + \frac{B}{p} \in \mathrm{AGL}_1(\mathbb{Z}_{p^{k-1}})$ on $\{0, \dots, p^{k-1}\}$: $A(kp)+B = p(Ak+\frac{B}{p})$. Now, by our induction hypothesis, to show that g acts transitively it suffices to show that $A = 1 \mod p$ and $\frac{B}{p} \neq 0 \mod p$. Thus, we compute $A \mod p$ and $B \mod p^2$. Clearly, $A = a^p = 1 \mod p$. Now, write $a = 1 + p\alpha$. Then $a^i = 1 + ip\alpha \mod p^2$. Hence $B = (1 + 1 + p\alpha + 1 + 2p\alpha + \cdots + 1 + (p-1)p\alpha) = p + \binom{p}{2}p\alpha \mod p^2$. Since for any odd p, we have $p \,|\, \binom{p}{2} = p \cdot \frac{p-1}{2}$, we can see that $B \mod p^2 = p$. Thus, $g = h^p$ is transitive on the set of multiples of p.

Lastly, observe that $h^i \cdot 0 = i \mod p$. Since g commutes with h^i, the orbit of $h^i 0$ under g must be of size p^{k-1} as well, and since g preserves the residue modulo p, the orbit must be the entire class. Recalling that $g = h^p$, and running through $i = 0, \ldots, p-1$ we can see that the orbit of 0 under h must be all of $\mathbb{Z}_{p^k}$, as desired. □

Remark 2.7. The dihedral group $D_4 = \langle r, s \mid r^4 = s^2 = rsrs = 1 \rangle$ is isomorphic to $\mathrm{AGL}_1(\mathbb{Z}_4)$ via the isomorphism $r \mapsto x + 1$ and $s \mapsto -x$.

Proposition 2.8. *The only transitive proper subgroups of* $\mathrm{AGL}_1(\mathbb{Z}_4)$ *are* $\mathbb{Z}_4 \rtimes 1$ *and* $\langle x + 2, -x + 1 \rangle$.

Proof. Any such subgroup must be of order at least 4 (and smaller than $\# D_4 = 8$). These subgroups are clearly transitive. The only other subgroup of order 4 is $\langle x + 2, -x \rangle$, for which the orbit of 0 is $\{0, 2\}$. □

Proposition 2.9. *Any subgroup of* $\mathrm{AGL}_1(\mathbb{Z}_4)$ *is either transitive, intransitive modulo 2, or is conjugate to* $\langle -x + 1 \rangle$*, and these options are mutually exclusive.*

Proof. Among the subgroups of order 4, the subgroups $\langle x + 1 \rangle$ and $\langle x + 2, -x + 1 \rangle$ act transitively, while $\langle x + 2, -x \rangle$ acts intransitively modulo 2. Among the subgroups of order 2, the subgroups $\langle x + 2 \rangle$, and $\langle -x \rangle$ are intransitive modulo 2, while the subgroups $\langle -x \pm 1 \rangle$ are both intransitive, transitive modulo 2, and conjugate among themselves (via $-x$). □

Proposition 2.10. *Let* $k \geq 2$*, and let* $H \subset \mathrm{AGL}_1(\mathbb{Z}_{2^k})$*. Then the following are equivalent:*

1. *H acts transitively on* $\{0, \ldots, 2^k - 1\}$,
2. $q_{2^k,4}(H) \subset \mathrm{AGL}_1(\mathbb{Z}_4)$ *acts transitively on* $\{0, 1, 2, 3\}$*, and*
3. *H contains either*
   - *an element of the form $ax + b$ where $a = 1 \mod 4$ and $2 \nmid b$, or*
   - *two elements of the form $ax + b, cx + d \in H$ such that $-a = b = c = 1 \mod 4$ and $d = 2 \mod 4$.*

Proof. Again, the equivalence between (2) and (3) is clear from Proposition 2.8, and the implication (1) implies (2) is clear.

We will prove that (3) implies (1) by induction, similar to the odd prime case. For $k = 2$, this follows from Proposition 2.8. Let $k > 2$, and assume that the implication holds for $k - 1$.

We start by treating the first case, for which there is an element $h = ax + b \in H$ with $a = 1 \mod 4$ and $2 \not| b$. As in the odd prime case, we claim that this element generates a transitive subgroup. We first show that $g = h^4$ acts transitively on the multiples of 4. Write $g = a^4 x + (1 + a + a^2 + a^3)b = Ax + B$. Then $B = (1 + 1 + 1 + 1)b = 0 \mod 4$, and thus g preserves the set of multiples of 4. As in the odd prime case, we can see that g acts on $\left\{0, 4, \ldots, 2^k - 4\right\}$ isomorphic to how $Ax + \frac{B}{4}$ acts on $\left\{0, \ldots, 2^{k-2}\right\}$. Thus, to use the induction hypothesis it suffices to show that $2 \not| (B/4)$. Write $a = 1 + 4\alpha$, then $a^i = 1 + 4i\alpha \mod 8$. Now compute $B = (1 + (1 + 4\alpha) + (1 + 8\alpha) + (1 + 12\alpha))b = 4b + 32\alpha b = 4b \mod 8$. As $2 \not| b$, we find that $2 \not| (B/4)$ as desired. We finish the argument similarly to the odd prime case by observing that h acts transitively modulo 4.

Now, for the second case, suppose that $h_1 = ax + b$ and $h_2 = cx + d$ are as in the theorem. Since $2 \mid d$, we have that h_2 acts on the set $\{0, 2, \ldots, 2^k - 2\}$. By a similar fashion to the previous arguments, this action is isomorphic to the action of $cx + \frac{d}{2}$ on $\left\{0, \ldots, 2^{k-1} - 1\right\}$. Since $c = 1 \mod 4$ and $2 \not| (d/2)$, using the induction hypothesis on the first case with $k - 1$, the subgroup generated by h_2 acts transitively on the multiples of 2. All that is left in order to finish is to observe, again, that $ax + b$ is transitive mod 2. □

Lemma 2.11. *Let H be a group acting on two finite sets A and B such that $(\#A, \#B) = 1$. Then H acts transitively on $A \times B$ if and only if it acts transitively on both A and B.*

Proof. The only if part is obvious. Now, let $(a, b) \in A \times B$ be any element in the product. Observe that $\operatorname{stab}(a, b) = \operatorname{stab} a \cap \operatorname{stab} b$. Since H acts transitively on both A and B, we have that $\operatorname{stab} a$ and $\operatorname{stab} b$ are of indices $\#A$ and $\#B$ in H respectively. Their intersection must have index divisible by $\operatorname{lcm}(\#A, \#B) = \#A \cdot \#B$. However, by the orbit stabilizer theorem, this index can be at most the size of the orbit of (a, b), i.e., at most $\#A \cdot \#B$, thus we have equality. □

Lemma 2.12. *Suppose $H \subset \mathrm{AGL}_1(\mathbb{Z}_n)$ acts intransitively on $\mathbb{Z}_n$, then either $q_{n,p}(H)$ acts intransitively on $\mathbb{Z}_p$ for some $p \,|\, n$ (and is thus conjugate to a subgroup of $0 \rtimes \mathbb{Z}_p^\times$), or $4 \,|\, n$ and $q_{n,4}(H)$ is conjugate to $\langle -x + 1 \rangle$.*

Proof. Indeed, apply the previous lemma inductively to the Chinese remainder decomposition given in Proposition 2.1, and conclude using the results of Lemmas 2.6, 2.10 and Proposition 2.9, which treat the odd prime components, the 2-component, and the special case of 4, respectively. □

2.2 Field Theory

We provide some preliminary background material from field theory. For a more in depth overview of this matrial, see [15]. Throughout this section, we let K be a characteristic-zero field.

A general degree-one function $\ell(x) \in K(x)$ has the form $\frac{ax+b}{cx+d}$. Given a 2×2 invertible matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ we can map it to a corresponding degree one function $\frac{ax+b}{cx+d}$. We may sometimes call the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ a matrix form of the function $\frac{ax+b}{cx+d}$. This mapping sends invertible matrices up to scalar multiplication to a unique degree one function. Moreover, this map satisfies the property that the product of two matrices is mapped to the composition of the corresponding functions. Phrased differently, this map factors through the group isomorphism $\mathrm{PGL}_2(K) \xrightarrow{\sim} \{\text{degree-one functions over } K \text{ with composition}\}$.

Proposition 2.13. *Let L be a Galois extension of K. Suppose a rational function $\phi(x) \in L(x)$ is fixed under the action of* $\mathrm{Gal}\left({}^{L}\!/\!_{K}\right)$*. Then $\phi(x) \in K(x)$.*

Proof. Write $\phi(x) = cp(x)/q(x)$, where $p(x)$ and $q(x)$ are relatively prime monic polynomials with coeffiecents in L. The roots of $\phi(x)$ are the same as the roots of $p(x)$, which are, by the hypothesis, the same as the roots of $\sigma\phi(x)$ which are the roots of $\sigma p(x)$ for any $\sigma \in \mathrm{Gal}\left({}^{L}\!/\!_{K}\right)$. Since $p(x)$ is monic, this implies $p(x) = \sigma p(x)$. By the same logic applied to the poles of $\phi(x)$, we find that $q(x) = \sigma q(x)$. Lastly, the equalities $\phi(x) = \sigma\phi(x)$ and $p(x)/q(x) = \sigma(p(x)/q(x))$ imply that $c = \sigma c$ for any $\sigma \in \mathrm{Gal}\left({}^{L}\!/\!_{K}\right)$, i.e., that $c \in K$. □

A rational function $f(x) \in K(x)$ induces a map $\mathbb{P}^1(K) \to \mathbb{P}^1(K)$, in which the poles of f are sent to infinity, and the value at infinity is the same as the value of 0 under $f(1/x)$. Henceforth we identify this map with f itself.

Definition 2.14. *Given a rational function $f(x) \in K(x)$, the set of finite* ramification points *of f is the set of points in $\bar{K}$ where $f'(x) = 0$. We say that f is ramified at infinity (and consider infinity as a ramification point) if $f(1/x)$ is ramified at zero. The* *set of* branch points *is the image of the set of ramification points under f. If α is a ramification point of f, we may sometimes say that f is ramified at α, and that $f(\alpha)$ is a branch point. We also say that f is ramified over the branch point $f(\alpha)$. The* ramification index $e_f(\alpha)$ *of a point $\alpha \in \bar{K}$ is the smallest positive integer n such that the derivative $f^{(n)}(\alpha) \neq 0$. We may refer to $e_f(\alpha)$ as the multiplicity of α in the preimage or fiber $f^{-1}(f(\alpha))$. The ramification index at infinity is defined as the ramification index of zero for the function $f(1/x)$. If the ramification index $e_f(\alpha)$ equals the degree of f, we say that f* totally ramifies *at α.*

Definition 2.15. *The* ramification type *or* ramification data *of a rational function $f \in K(x)$ is a list of tuples describing the ramification indices over each branch point. Note that the elements of each tuple in the list must sum to the degree of the function. In the tuple notation, exponents denote multiplicity, i.e., the notation $2^{n/2-2}1^2$ signifies the tuple in which 2 appears $n/2 - 2$ times and 1 appears twice. For our purposes, we consider the following ramification types:*

- (n, n),
- $(n, 2^{n/2}, 2^{n/2-2}1^2)$ *for even n, and*
- $(n, 2^{(n-1)/2}1, 2^{(n-1)/2}1)$ *for odd n.*

The first ramification type is the ramification type of a degree-n function totally ramified at exactly two points, for example $f(x) = x^n$. The last two are the ramification types of a degree-n function which has 3 branch points, totally ramified over one of them, and with ramification index 2 at every other ramification point. These are the ramification types of the Chebyshev polynomials of even and odd degree respectively [16, Lemma 3.2]. For brevity, we will denote both these ramification types by $(n, 2, 2)$.

Definition 2.16. *Given a function $f(x) \in K(x)$, its monodromy group over K is defined as the Galois group of $f(X) - t \in K(t)(X)$, by which we mean the Galois group of the splitting field of $p(X) - tq(X) \in K(t)[X]$, where $f(x) = p(x)/q(x)$ with relatively prime polynomials $p(x)$ and $q(x)$.*

Definition 2.17. *Two rational functions $f(x), g(x) \in K(x)$ are called* linearly related *if there exist degree-1 functions $\eta, \eta' \in \bar{K}(x)$ such that*

$$f(x) = \eta'(g(\eta(x))).$$

Moreover, we say that f and g are linearly related over K, or K-linearly related, if there exists such $\eta, \eta' \in K(x)$. If we can take $\eta' = \eta^{-1}$, we say that f is a (K-rational) twist *of g.*

We say that the linear relation preserves (respectively, stabilizes) the point α (respectively, the set S) if $\eta(\alpha) = \eta'(\alpha) = \alpha$ (respectively, $\eta(S) = \eta'(S) = S$).

Remark 2.18. Linearly related rational functions have the same ramification type.

Definition 2.19. *Let M be a field, and let $L, K \subseteq M$ be subfields both containing a common subfield $F \subseteq L \cap K$. We say that L and K are* linearly disjoint *over F if $[LK : L] = [K : F]$.*

Proposition 2.20. *Let Ω be a field, let $L, K \subseteq \Omega$ be subfields both containing a common subfield $F \subset L \cap K$ such that Ω is a finite Galois extension of F. Let G be the subgroup stabilising the compositum LK, and denote by H_1 and H_2 the subgroups of G stabilising L and K, respectively. Then L and K are linearly disjoint over F if and only if*

$$G = H_1 H_2 = \{h_1 h_2 \mid h_i \in H_i\}.$$

Proof. Suppose first that $G = H_1 H_2$. Then

$$[LK : F] = [LK : L][L : F] = \#G \leq \#H_1 \#H_2 = [LK : L][LK : K].$$

In particular, $[L : F] \leq [LK : K]$. However, it is always the case that $[LK : K] \leq [L : F]$ (because an F-basis for L will span LK over K), and thus equality is established. Now suppose that L and K are linearly disjoint. Clearly the stabilizer of the compositum LK

is the intersection $H_1 \cap H_2$. Now,

$$\#H_1 = [\Omega : L] = [\Omega : LK][LK : L] = \#(H_1 \cap H_2)[K : F] = \#(H_1 \cap H_2)\#G/\#H_2.$$

Lastly,

$$\#(H_1H_2) = \frac{\#H_1\#H_2}{\#(H_1 \cap H_2)} = \#G$$

proves the result. □

Proposition 2.21. *Suppose K and L are not linearly disjoint over F, and suppose that K is Galois over F. Then K intersects L non-trivially. That is, $F \subsetneq K \cap L$.*

Proof. Indeed, let Ω be a Galois extension of F which contains both L and K. Using the notation of the previous proposition, since the fields are not linearly disjoint $H_1H_2 \neq G$. Since K is Galois over F, the subgroup H_2 of G is normal, and thus H_1H_2 is a subgroup of G. By the previous proposition, it must be a non-trivial subgroup, since the fields are not linearly disjoint. Thus, $\Omega^{H_1H_2}$ is a subfield of $L \cap K$ which is a non-trivial extension of F. □

We say that a rational function $f(x) \in K(x)$ is reducible (over K) if when written in reduced form as $f(x) = g(x)/h(x)$, the numerator $g(x)$ is reducible as a polynomial (over K). This is equivalent to the statement that for any (or, equivalently, for some) extension $K(x)$ of K in which $f(x) = 0$ is of degree strictly smaller than the degree of $f(x)$. If G is the Galois group of $f(x)$, which naturally acts on the roots of $f(x)$, then $f(x)$ is reducible if and only if this action is intransitive.

Let L be an algebraic function field over K of transendence degree 1, i.e., a finite extension of $K(t)$. Assume further that it is Galois. Henceforth, all places considered will be assumed to be trivial on K. Let $\nu : t \to a$ be a place of $K(t)$ and ν' a place of L which lies over ν. We say that ν is unramified in the extension if $\nu(K(t)) = \nu'(L)$ for any ν' which lies over ν. Otherwise, we say that the (unique) positive e for which $\nu(K(t)) = e \cdot \nu'(L)$ is the ramification index of ν' over ν. We denote this value by $e_{\nu}^{\nu'}$.

Lemma 2.22 (Abyhanker's Lemma). *Let L, L' be linearly disjoint algebraic extensions of $K(t)$, for some characteristic-zero field K. Let ν be a place of the compositum, and let $\nu_L, \nu_{L'}$ and $\nu_{K(t)}$ be the places lying under ν in L, L' and $K(t)$ correspondingly. Then the ramification index $e^{\nu}_{\nu_{K(t)}} = \operatorname{lcm}(e^{\nu_L}_{\nu_{K(t)}}, e^{\nu_{L'}}_{\nu_{K(t)}})$.*

Proof of this lemma can be found in [15, Theorem 3.9.1].

We will denote by $t \to a$ the place $\nu_a(f) = \operatorname{ord}_{t-a}(f)$ of $K(t)$. These, together with the place at infinity $t \to \infty$ given by $\nu_\infty(f) = \deg f$ give rise to all places of $K(t)$. We let $\mathcal{O}_L$ be the ring of non-negatively valued elements, and let $\mathfrak{m}_L$ be the unique maximal ideal of $\mathcal{O}_L$ consisting of all positively valued elements of $\mathcal{O}_L$. The specialization of ${}^{L}/_{K(t)}$ at the place $t \to a$ is $L_a = {}^{\mathcal{O}_L}/_{\mathfrak{m}_L}$. It is a Galois extension of K. Notice that L_a depends on a choice of ν' lying over $t \to a$. However, since L is Galois over $K(t)$, all such ν' give rise to isomorphic fields. The degree $[L_a : K]$ is called the *residue degree* of ν_a, and is denoted by $f = f(\nu_a)$, where ν_a is the place $t \to a$.

When $L = K(z)$ with $f(z) = t$ for some rational function $f(x) \in K(x)$, then the ramification index of the place $z \to z_0$ over $t \to f(z_0)$ is the same as the ramification index of z_0 over $f(z_0)$ as defined earlier.

The decomposition group $D \leq \operatorname{Gal}({}^{L}/_{K(t)})$ of a place ν' of L is the subgroup of all elements $\sigma \in \operatorname{Gal}({}^{L}/_{K(t)})$ for which $\nu'(\sigma x) > 0$ if and only if $\nu'(x) > 0$, for all $x \in \mathcal{O}_L$. The inertia group $I \leq D$ is the subgroup of all $\sigma \in \operatorname{Gal}({}^{L}/_{K(t)})$ for which $\nu'(x - \sigma(x)) > 0$ for all $x \in \mathcal{O}_L$. Both of these groups depend on a choice of ν', however different choices of ν' give rise to conjugate subgroups. Thus, for a specific place ν of K we may refer to the decomposition group of some ν' extending ν as *a decomposition group* of ν, which is defined up to conjugation. If D, e and, f are, respectively, a decomposition group, the ramification index, and residue degree of $t \to a$, then $\#D = ef$.

We have that $I = 1$ if and only ν' is unramified, in which case D is the Galois group of the specialization $\operatorname{Gal}({}^{L_a}/_{K})$.

Any element $z \in \mathcal{O}_L$ has a corresponding specialization $\bar{z} \in L_a$ given by the quotient map. Being a quotient, this operation is a ring homomorphism. In the unramified case the action of D on L_a factors through this quotient, hence specialization preserves algebraic relations in the Galois action: If $\sigma \in D$ and $z \in \mathcal{O}_L$ such that $P(z, \sigma z) = 0$ for some polynomial $P(x, y) \in K[x, y]$, then $P(\bar{z}, \sigma\bar{z}) = 0$. In particular, in the unramified case fixed points of D in $\mathcal{O}_L$ specialize to elements of K.

Let $f(x) \in K(x)$ be a rational function, and let L be the splitting field of $f(x) - t \in K(t)$. The following well known lemma (see, for example, [17, Lemma 3.1]) shows that the place $t \to a$ is ramified in the extension ${}^{L}/_{K(t)}$ if and only if $f(x)$ is ramified at a.

Lemma 2.23. *Let $m_1, m_2, \ldots, m_r$ be the multiplicies of the elements of $\mathbb{P}^1(\bar{K})$ in the fiber of $f^{-1}(a)$ for $a \in \bar{K} \cup \{\infty\}$. Let I be the inertia group of a place of L lying above the place $t \to a$ of $K(t)$. Then I is cyclic and generated by an element which has cycle lengths $m_1, m_2, \ldots m_r$ in the action on the roots of $f(x) - t$.*

Indeed, $I = 1$ if and only if $m_1 = m_2 = \cdots = 1$ if and only if $f(x)$ isn't ramified at a.

2.3 Siegel's Theorem

Let K be a number field, $R \subset K$ a finitely generated subring, and $\phi : V \to \mathbb{P}^1$ be a cover of the projective line. Siegel's theorem provides necessary conditions on ϕ for the image $\phi(K)$ to contain infinitely many elements from $\mathbb{P}^1_R \subset \mathbb{P}^1_K$.

Theorem 2.24 (Siegel)**.** *Let $\phi : V \to \mathbb{P}^1_K$ be a cover of the projective line. Suppose that $\phi(K) \cap \mathcal{O}_K$ is infinite. Then V is of genus 0, and ϕ has at most two poles, i.e., $\#\phi^{-1}(\infty) \leq 2$. We may therefore regard $\phi(z) \in K(z)$ as a rational function.*

Moreover, in the special case where $K = \mathbb{Q}$ and $R = \mathbb{Z}$, and $\#\phi^{-1}(\infty) = 2$, the two poles must be real and algebraically conjugate.

The result can be found in [17, Proposition 2.3]. Functions which satisfy the condition of the theorem are typically called *Siegel functions*.

2.4 Hilbert's Irreducibility Theorem

Definition 2.25. *Let $P(t,x) \in K(t)[x]$ be an irreducible polynomial over number field K and let $S \subset K$ be a set of numbers. The* set of reducible values *of $P(t,x)$ in S is*

$$\mathrm{Red}_P(S) = \{s \in S \mid P(s,x) \in K[x] \textit{ is either undefined or reducible}\},$$

where by saying that $P(s,x)$ is "undefined" we mean that s is a pole of some coefficient of $P(t,x)$.

Theorem 2.26 (Hilbert's Irreducibility Theorem)**.** *The set of reducible values* $\mathrm{Red}_P(K)$ *can be written as the union of finitely many rational value sets of morphisms $\phi_i : V_i \to \mathbb{P}^1_K$ of degree ≥ 2 together with a finite set:*

$$\mathrm{Red}_P(K) = \bigcup \phi_i(V_i(K)) \cup F,$$

where $F \subset K$ is a finite set of values. Moreover, for each i the pullback of $P(t,x)$ along ϕ_i, namely, $P(\phi_i(t,z),x) \in K(V_i)[x]$, is reducible. Here (t,z) denote coordinates on V_i.

2.5 Rédei functions

Throughout this section, let K be a field of characteristic zero, let $\delta \in \overline{K}^{\times}$ be such that $\delta^2 \in K$, and let $n \in \mathbb{N}$. The Rédei function of degree n with parameter δ is defined by the composition

$$R_{\delta,n}(x) = \mu_{\delta}^{-1}(\mu_{\delta}(x)^n) \in K[\delta](x)$$

where $\mu_{\delta}(x) = \frac{x+\delta}{x-\delta} \in K[\delta](x)$, and $\mu_{\delta}^{-1}(x) = \delta\frac{x+1}{x-1}$. This is a $K[\delta]$-twist of the function x^n. Fix some δ throughout this section, and denote $\mu = \mu_{\delta}$ and $R_n(x) = R_{\delta,n}(x)$.

Note that μ maps δ to infinity and $-\delta$ to zero. Note further that whenever $\delta \notin K$, there exists an automorphism σ of $K[\delta]$ fixing K and exchanging δ with $-\delta$.

As an example, let us compute

$$\begin{aligned} R_2(x) &= \delta\frac{\left(\frac{x+\delta}{x-\delta}\right)^2+1}{\left(\frac{x+\delta}{x-\delta}\right)^2-1} \\ &= \delta\frac{(x+\delta)^2+(x-\delta)^2}{(x+\delta)^2-(x-\delta)^2} \\ &= \delta\frac{2x^2+2\delta^2}{4x\delta} \\ &= \frac{x^2+\delta^2}{2x}. \end{aligned}$$

In this section, we will define and prove “twisted” versions of facts regarding the family of functions x^n. The corresponding definitions and results are summarized in the following table:

x^n	$R_n(x)$
$x \mapsto cx$	$x \mapsto \eta_c(x)$
$x^n \circ x^m = x^{nm}$	$R_n \circ R_m = R_{nm}$
x^n is totally ramified at 2 points	R_n is totally ramified at 2 points
$(cx)^n = c^n x^n$	$R_n \circ \eta_c = \eta_{c^n} \circ R_n$
Roots of unity	Poles of $R_n(x)$
Monodromy group of x^n is $\leq \mathrm{AGL}_1(\mathbb{Z}_n)$	Monodromy group of $R_n(x)$ is $\leq \mathrm{AGL}_1(\mathbb{Z}_n)$

Proposition 2.27. *The Rédei function $R_{\delta,n}(x)$ is a rational function defined over K. Moreover, it is totally ramified at δ and $-\delta$, with branch points δ and $-\delta$, respectively.*

We will show that the Rédei function is unique with respect to this property, up to a K-linear relation preserving $\{\delta, -\delta\}$. The proof of this proposition will appear after Lemma 2.38.

Lemma 2.28. *Suppose $\delta \notin K$, and let σ be the automorphism swapping $\pm\delta$. Then we have that $\sigma\mu(x) = 1/\mu(x)$, and $\sigma\mu^{-1}(x) = -\mu^{-1}(x)$.*

Proof. Indeed,

$$\sigma\mu(x) = \sigma\frac{x+\delta}{x-\delta} = \frac{x-\delta}{x+\delta} = 1/\mu(x).$$

Likewise,

$$\begin{aligned}\sigma\mu^{-1}(x) &= \sigma\delta\frac{x+1}{x-1}\\ &= -\delta\frac{x+1}{x-1}\\ &= -\mu^{-1}(x).\end{aligned}$$

□

Lemma 2.29. *The following identities hold:*

1. $\mu^{-1}(1/x) = -\mu^{-1}(x)$,
2. $\mu^{-1}(-x) = \delta^2/\mu^{-1}(x)$.

Proof. We compute,

$$\mu(1/x) = \delta\frac{1/x+1}{1/x-1} = \delta\frac{1+x}{1-x} = -\delta\frac{x+1}{x-1} = -\mu^{-1}(x).$$

Similarly,

$$\begin{aligned}\mu^{-1}(-x) &= \delta\frac{-x+1}{-x-1}\\ &= \frac{\delta^2}{\delta\frac{-x-1}{-x+1}}\\ &= \frac{\delta^2}{\delta\frac{x+1}{x-1}}\\ &= \delta^2/\mu^{-1}(x).\end{aligned}$$

□

Lemma 2.30. *Suppose $\delta \notin K$, and let σ be the automorphism swapping $\pm\delta$. Then $c \in K[\delta]^\times$ satisfies $c \in \mu K$ if and only if $\sigma c = c^{-1}$.*

Proof. The first direction follows from Lemma 2.28. In the other direction, we can see that for such c we have that $\sigma(\mu^{-1}c) = -\mu^{-1}(c^{-1})$, again by Lemma 2.28. Lastly, $-\mu^{-1}(c^{-1})$ is equal to $\mu^{-1}c$ by the previous lemma, showing that $\mu^{-1}c \in K$. □

Lemma 2.31. *The following identities hold:*

1. $\mu(a)\mu(b) = \mu(\frac{ab+\delta^2}{a+b})$.

2. $\mu(a)^{-1} = \mu(-a)$.

3. $\mu(a) + \mu(b) = \mu(\delta\frac{3ab-\delta(a+b)-\delta^2}{ab+\delta(a+b)-3\delta^2})$

Proof. 1. Indeed,

$$\begin{aligned}\mu(a)\mu(b) &= \frac{a+\delta}{a-\delta}\cdot\frac{b+\delta}{b-\delta}\\ &= \frac{ab+(a+b)\delta+\delta^2}{ab-(a+b)\delta+\delta^2}\\ &= \frac{\frac{ab+\delta^2}{a+b}+\delta}{\frac{ab+\delta^2}{a+b}-\delta}\\ &= \mu(\frac{ab+\delta^2}{a+b}).\end{aligned}$$

2. Indeed,

$$\mu(a)^{-1} = \left(\frac{a+\delta}{a-\delta}\right)^{-1} = \frac{a-\delta}{a+\delta} = \frac{(-a)+\delta}{(-a)-\delta} = \mu(-a).$$

3. This also follows from an explicit calculation. Indeed

$$\mu(a) + \mu(b) = \frac{a+\delta}{a-\delta} + \frac{b+\delta}{b-\delta} = 2\frac{ab-\delta^2}{ab-\delta(a+b)+\delta^2}.$$

Likewise,

$$\begin{aligned}\mu(\delta\frac{3ab-\delta(a+b)-\delta^2}{ab+\delta(a+b)-3\delta^2}) &= \frac{\delta\frac{3ab-\delta(a+b)-\delta^2}{ab+\delta(a+b)-3\delta^2}+\delta}{\delta\frac{3ab-\delta(a+b)-\delta^2}{ab+\delta(a+b)-3\delta^2}-\delta} \\ &= \frac{3ab-\delta(a+b)-\delta^2+ab+\delta(a+b)-3\delta^2}{3ab-\delta(a+b)-\delta^2-ab-\delta(a+b)+3\delta^2} \\ &= \frac{4ab-4\delta^2}{2ab-2\delta(a+b)+2\delta^2},\end{aligned}$$

where in between the first and second lines we cancel the δ and multiply by the inner denominator.

□

Remark 2.32. The first and second points of the previous lemma show that μK is closed under multiplication and division.

Definition 2.33. *For $c \in \bar{K} \cup \infty$, define $\eta_c(x) = \eta_{\delta,c}(x) := \mu^{-1}(c\mu(x))$. Likewise, $\eta'_c(x) = \eta'_{\delta,c}(x) := \mu^{-1}(c/\mu(x))$. These are, respectively, twists of the linear maps $x \mapsto cx$ and $x \mapsto c/x$.*

Lemma 2.31, (1) shows that $\eta_c(x) = \frac{\mu^{-1}(c)x+\delta^2}{x+\mu^{-1}(c)}$.

Remark 2.34. For $c = 0$ or $c = \infty$, we find that $\eta_c(x)$ and $\eta'_c(x)$ are both the constant function $\mu^{-1}(c)$.

Since compositions of the form $\eta_c \circ R_n(x)$ will appear frequently in this thesis, we will often omit the composition operator and just write $\eta_c R_n(x)$.

We lay out some properties of η_c that will be useful later:

Lemma 2.35. *The following are true:*

1. *The map η is multiplicative in its parameter, that is, $\eta_{cc'} = \eta_c \circ \eta_{c'}$. Similarly, $\eta'_{cc'} = \eta'_c \circ \eta_{1/c'}$.*

2. *$\eta_{-1}(x) = \delta^2/x$.*

3. *$R_2(x) = \frac{1}{2}(x + \eta_{-1}(x))$.*

Proof. 1. Indeed, $\eta_c \circ \eta_{c'}(x) = \mu^{-1}(c\mu(\mu^{-1}(c'\mu(x)))) = \mu^{-1}(cc'\mu(x))$. Likewise, $\eta'_c \circ \eta_{1/c'}(x) = \mu^{-1}(c/\mu(\mu^{-1}(\mu(x)/c'))) = \mu^{-1}(cc'/\mu(x))$.

2. By Lemma 2.29, we have that $\mu^{-1}(-y) = \delta^2/\mu^{-1}(y)$. By setting $y = \mu(x)$ we get

$$\delta^2/x = \mu^{-1}(-\mu(x)) = \eta_{-1}(x).$$

3. As we have computed at the start of the Chapter, $R_2(x) = \frac{x^2+\delta^2}{2x}$. Indeed, this is equal to $\frac{1}{2}(x + \delta^2/x)$.

□

Lemma 2.36. *For every $c \in \bar{K}$ we have that $R_n \circ \eta_c = \eta_{c^n} \circ R_n$.*

Proof. Indeed,

$$R_n \circ \eta_c(x) = \mu^{-1}(\mu(\mu^{-1}(c\mu(x)))^n) = \mu^{-1}(c^n\mu(x)^n) = \eta_{c^n} \circ R_n(x).$$

□

Lemma 2.37. *For every $c \in \bar{K}^\times$ we have $\eta_c(\pm\delta) = \eta'_c(\mp\delta) = \pm\delta$. Moreover, if a degree-one function $\ell(x) \in \bar{K}(x)$ stabilizes the set $\{\delta, -\delta\}$, i.e., $\ell(\{\delta, -\delta\}) = \{\delta, -\delta\}$, then $\ell(x) = \eta_c(x)$ or $\eta'_c(x)$ for some $c \in \bar{K}^\times$.*

Proof. The first part follows from the fact that $\mu_\delta(\{\delta, -\delta\}) = \{0, \infty\}$, and that this set is preserved under multiplication by (non-zero) $c \in \bar{K}$.

Now, suppose $\ell(\{\delta, -\delta\}) = \{\delta, -\delta\}$. Then $\mu \circ \ell \circ \mu^{-1}$ is a degree-one map sending $\{0, \infty\}$ to itself and therefore must be either $x \mapsto cx$ or $x \mapsto c/x$. This proves the claim. □

Lemma 2.38. *For $c \in \bar{K} \cup \{\infty\}$, the function $\eta_c(x) \in K(x)$ if and only if $\eta'_c(x) \in K(x)$, if and only if $\mu^{-1}(c) \in K \cup \{\infty\}$.*

Proof. Let us first of all treat the case $\mu^{-1}(c) = \infty$. This holds only for $c = 1$, in which case $\eta_c(x)$ is the identity function which is clearly in $K(x)$, and by Lemma 2.29 we have $\eta'_c(x) = -x \in K(x)$.

From now on we may assume $\mu^{-1}c \neq \infty$. Now, if either $\eta_c(x)$ or $\eta'_c(x) \in K(x)$, then $\eta_c(0) = \eta'_c(0) = \mu^{-1}(-c) \in K \cup \{\infty\}$. Thus by Lemma 2.29, we have $\mu^{-1}(c) = \delta^2/\mu^{-1}(-c) \in K$.

Assume conversely that $\mu^{-1}(c) \in K$. In the case where $\delta \in K$, we have that $\mu(x) \in K(x)$. Therefore, $c = \mu(\mu^{-1}(c)) \in K$ and thus $\eta_c(x) \in K(x)$, being the composition of functions with coefficients in K. Otherwise, let σ be the automorphism swapping $\pm\delta$. Since $\mu^{-1}(c) \in K$, we have that $\sigma\mu^{-1}(c) = \mu^{-1}(c)$. This implies (by Lemma 2.28) that $\sigma c = \sigma(\mu(\mu^{-1}(c))) = 1/(\mu(\mu^{-1}(c))) = 1/c$. Now,

$$\begin{aligned}
\sigma\eta_c(x) &= (\sigma\mu^{-1})(\sigma(c)\sigma(\mu(x))) \\
&= -\mu^{-1}(\sigma(c)/\mu(x)) && \text{(Lemma 2.28, twice)} \\
&= \mu^{-1}(\mu(x)/\sigma(c)) && \text{(Lemma 2.29)} \\
&= \mu^{-1}(c\mu(x)) \\
&= \eta_c(x).
\end{aligned}$$

Likewise,

$$\begin{aligned} \sigma\eta_c'(x) &= (\sigma\mu^{-1})(\sigma(c)/\sigma(\mu(x))) \\ &= -\mu^{-1}(\sigma(c)\mu(x)) && \text{(Lemma 2.28, twice)} \\ &= \mu^{-1}(1/(\mu(x)\sigma(c))) && \text{(Lemma 2.29)} \\ &= \mu^{-1}(c/\mu(x)) \\ &= \eta_c'(x). \end{aligned}$$

All that remains to show is that if σ fixes a degree-one function, then this function can be defined over K. This follows from Proposition 2.13, but let us also show it more explicitly. Suppose that $\sigma\ell(x) = \ell(x)$ for some degree-one map $\ell(x) \in K[\delta](x)$. This implies that the values of ℓ at zero, one, and infinity belong to $K \cup \{\infty\}$. By composition with an appropriate invertible function in $K(x)$ we may assume that these values all belong to K. Now, it is well known that

$$\ell(x) = \frac{(x - \ell(0))(\ell(1) - \ell(\infty))}{(x - \ell(\infty))(\ell(1) - \ell(0))},$$

in which all the coefficients belong to K. □

Proof of Proposition 2.27. We can now deduce that $R_{\delta,n}(x)$ is indeed defined over K. A-priori, since $\mu = \mu_\delta \in K[\delta](x)$, we have that $R_n(x) = R_{\delta,n}(x) = \mu^{-1}(\mu(x)^n)$ is defined over $K[\delta]$. If $\delta \in K$, we are done. Otherwise $\delta \notin K$ but by definition $\delta^2 \in K$. Thus, let σ be the automorphism of $K[\delta]$ swapping $\pm\delta$. We shall show that $\sigma R_n(x) = R_n(x)$.

Indeed,

$$\begin{aligned}\sigma R_n(x) &= \sigma(\mu^{-1}(\mu(x)^n)) \\ &= -\mu^{-1}(\sigma\mu(x)^n) && \text{(Lemma 2.28)} \\ &= -\mu^{-1}(1/\mu(x)^n) && \text{(Lemma 2.28)} \\ &= \mu^{-1}(\mu(x)^n) && \text{(Lemma 2.29)} \\ &= R_n(x).\end{aligned}$$

Per Proposition 2.13, this implies that $R_n(x) \in K(x)$.

Now, the ramification points of $R_n(x)$ are δ and $-\delta$, for μ maps $\{\delta, -\delta\}$ to the ramification points of x^n, which are $\{0, \infty\}$. Lastly, a direct computation shows that $R_{\delta,n}(\pm\delta) = \pm\delta$. □

Theorem 2.39. *Let $f(x) \in K(x)$ be a rational function which has ramification type (n, n). Then $f(x)$ is linearly related to $R_{\delta,n}(x)$ over K for some $\delta \in \bar{K}^\times$ for which $\delta^2 \in K$. Further, $\delta \in K$ if and only if at least one of the ramification points of f is in K, if and only if $f(x)$ is linearly related to x^n over K.*

Proof. First of all, x^n is clearly linearly related to $R_{\delta,n}(x)$ for any $\delta \in K^\times$. Denote the ramification points of $f(x)$ by δ and δ'. If $\{\delta, \delta'\} = \{0, \infty\}$, we can assume (via precomposing f with an appropriate degree-one map) that $f(0) = 0$ and $f(\infty) = \infty$, and then clearly $f(x) = cx^n$ for some $c \in K$ and we are done. From now on assume that $\{\delta, \delta'\} \neq \{0, \infty\}$. Thus, we can assume without loss of generality that both δ and δ' are not ∞: If one of them is equal to ∞, we shall consider $f(1/x)$ instead.

The ramification points are obtained as the roots of $f'(x)$, whose numerator must factor to irreducibles over K as either $(x - \delta)^{n-1}(x - \delta')^{n-1}$ with δ and $\delta' \in K$, or as $q(x)^{n-1}$, where $q(x) = x^2 - (\delta + \delta')x + \delta\delta' \in K[x]$ is irreducible. Thus, either both ramification points belong to K, or they are algebraically conjugate.

In particular, if one of the ramification points is in K then they are both in K, and composing f with the degree-one map sending δ and δ' to 0 and ∞ reduces to the case we considered first, showing the further statement, that in this case f is K-linearly related to x^n.

If both ramification points are not in K, they must be conjugate. That is, they must be of the form $d \pm \tilde{\delta}$ for some $d \in K$ and some $\tilde{\delta} \in \bar{K}$ such that $\tilde{\delta} \notin K$ and $\tilde{\delta}^2 \in K$. Precomposing f with the map $x \mapsto x + d$ lets us assume that $d = 0$ and the ramification points of f are $\{\delta, -\delta\}$.

Now, the branch points of $f(x)$, being $f(\pm\delta)$, are both in $K[\delta]$. Since f is defined over K, these values are also conjugate, and we may again assume that they differ only by a sign, that is, $f(\pm\delta) = \pm f(\delta)$. Since σ swaps $\pm\delta$, we can also write this fact as $\sigma f(\delta) = -f(\delta)$. This shows that $\delta/f(\delta) \in K$. Thus, postcomposing f with the map $x \mapsto \delta x/f(\delta)$ we may assume $f(\pm\delta) = \pm\delta$.

We may now observe that $\mu_\delta \circ f \circ \mu_\delta^{-1}$ fixes both 0 and ∞, and is totally ramified over them. Thus, it is equal to cx^n for some $c \in \bar{K}$. Note that this linear relation is not defined over K. However, $f(0) = \mu^{-1}((-1)^n c) \in K$. Lemma 2.29 shows that this is equivalent to $\mu^{-1}(c) \in K$, and by Lemma 2.38 we have that $\eta_c(x) \in K(x)$. Direct calculation verifies that indeed $f(x) = \eta_c(R_n(x))$, and this also demonstrates the linear relation. □

Throughout the section, we may use the fact that x^n is linearly related to $R_{1,n}(x)$, so that we may assume δ as in the theorem is always non-zero.

Lemma 2.40. *For every $c \in \bar{K}$ and $n \in \mathbb{N}$ we have that $\eta'_c \circ R_n = \eta_c \circ R_n \circ \eta'_1$.*

Proof. This follows from a direct calculation:

$$\begin{aligned}
\eta'_c \circ R_n(x) &= \mu^{-1}(c/\mu(R_n(x))) \\
&= \mu^{-1}(c/\mu(x)^n) \\
&= \mu^{-1}(c\mu(\mu^{-1}((1/\mu(x))^n))) \\
&= \eta_c(R_n(\eta'_1(x))).
\end{aligned}$$

□

Proposition 2.41. *Let $\delta, \delta' \in \bar{K}^\times$ be two elements such that $\delta^2, \delta'^2 \in K$. Then $R_{\delta,n}$ and $R_{\delta',n}$ are linearly related over K if and only if $\delta/\delta' \in K$. Moreover, in this case they* *are K-rational twists of eachother.*

Proof. Indeed, if $\delta/\delta' \in K$, then the map $\ell(x) = \delta x/\delta'$ satisfies $\mu_\delta \circ \ell = \mu_{\delta'}$, and thus $\ell^{-1} \circ R_{\delta,n} \circ \ell = R_{\delta',\ell}$.

On the other hand, if $R_{\delta,n}(x)$ and $R_{\delta',n}(x)$ are linearly related over K, then there is some K-rational degree one map $\ell(x)$ which sends $\{\pm\delta\}$ to $\{\pm\delta'\}$. In particular, $\delta' \in K[\delta]$. Since $\delta'^2 \in K$, this implies $\delta/\delta' \in K$. □

Proposition 2.42. *Suppose $\phi(x) \in K(x)$ is totally ramified over $\{\delta, -\delta\}$. Then $\phi(x) = \eta_c \circ R_{\delta,n} \circ \ell(x)$ for some $c \in \mu(K) \cup \{\infty\}$ and some degree-one map $\ell(x) \in K(x)$.*

Proof. Indeed, by Theorem 2.39, such function must be equal to $\ell' \circ R_{\delta',n} \circ \ell$ for some $\delta' \in \bar{K}^\times$ such that $\delta'^2 \in K$ and some degree-one functions $\ell(x), \ell'(x) \in K(x)$. Now, in a similar fashion to that of the previous proposition, $\ell'(x)$ must map the branch points $\{\delta', -\delta'\}$ of $R_{\delta',n}(x)$ to the branch points $\{\delta, -\delta\}$ of $f(x)$, which implies $\delta/\delta' \in K$. Thus, by applying the previous proposition, we may assume without loss of generality that $\delta = \delta'$.

Now, by Lemma 2.37, since ℓ' preserves the set $\{\delta, -\delta\}$, we must have $\ell' = \eta_c$ or η'_c for some $c \in \bar{K}$. By Lemma 2.38, the fact that $\ell'(x) \in K(x)$ implies that $c \in \mu(K) \cup \{\infty\}$. We finish the argument by noticing that we may insert η'_1 “into” the Rédei function as per Lemma 2.40. □

2.6 The monodromy group of the Rédei function

Throughout this section we fix $\delta \in \bar{K}^\times$ satisfying $\delta^2 \in K$, and denote $R_n(x) = R_{\delta,n}(x)$. In this section we show that the monodromy group of $R_n(x)$ over the field K can be naturally identified with a subgroup of $\mathrm{AGL}_1(\mathbb{Z}_n) = \mathbb{Z}_n \rtimes \mathbb{Z}_n^\times$ containing $\mathbb{Z}_n \rtimes 1$.

Unless states otherwise, we denote by ζ's n-roots of unity, and by ξ's "twists of roots of unity", i.e., poles of $R_n(x) = R_{\delta,n}(x)$, or equivalently numbers of the form $\mu^{-1}\zeta$, as in the following lemma. .

Lemma 2.43. *A number $\xi \in \bar{K}$ is a pole of $R_n(x)$ if and only if $\zeta = \mu(\xi)$ is an n-th root of unity.*

Proof. Since $\mu^{-1}(x) = \delta\frac{x+1}{x-1}$, we have that $\mu(\xi)^n = 1$ if and only if $\mu^{-1}(\mu(\zeta)^n) = \infty$. □

Lemma 2.44. *If ξ is a pole of $R_n(x)$, then for any $a \in \mathbb{N}$, we have that $R_a(\xi)$ is also a pole of $R_n(x)$.*

Proof. Since $\zeta = \mu(\xi)$ is an n-th root of unity, $\mu(R_a(\xi)) = \mu(\xi)^a = \zeta^a$ is also an n-th root of unity. □

Definition 2.45. *We say that a pole ξ of $R_n(x)$ is a* primitive pole *if it is not a pole of $R_m(x)$ for any $m < n$ (equivalently, for any $m \mid n$).*

Lemma 2.46. *A pole ξ of $R_n(x)$ is a primitive pole if and only if $\mu(\xi)$ is a primitive n-th root of unity.*

Proof. By Lemma 2.43, a pole ξ of $R_n(x)$ is a pole of $R_m(x)$ for some $m < n$ if and only if $\mu(\xi)$ is an m-th root of unity for that same m. Negating both sides of the equivalence proves the lemma. □

Lemma 2.47. *If ξ is a primitive pole of $R_n(x)$, then all other poles of $R_n(x)$ are obtained as $R_a(\xi)$ for some $a \in \mathbb{N}$.*

Proof. By the previous lemma, $\zeta = \mu(\xi)$ is a primitive n-th root of unity. Thus, all n-th roots of unity are obtained as ζ^a for $a \in \mathbb{N}$. Now, by Lemma 2.43, all finite poles of $R_n(x)$ are obtained as $\mu^{-1}(\zeta^a) = \mu^{-1}(\mu(\xi)^a) = R_a(\xi)$. □

Lemma 2.48. *If ξ is a primitive pole of $R_n(x)$, and $(n, a) = 1$, then $R_a(\xi)$ is a primitive pole of $R_n(x)$. Further, all primitive poles are obtained as such.*

Proof. We need to show that $\mu(R_a(\xi)) = \mu(\xi)^a$ is a primitive root of unity. However, $\mu(\xi)$ is a primitive root of unity. Indeed, all primitive roots of unity can be obtained in this way. □

Lemma 2.49. *For a given primitive pole ξ of $R_n(x)$ we have that $R_a(\xi) = R_b(\xi)$ if and only if $a = b \mod n$.*

Proof. Write $\zeta = \mu(\xi)$. We have $\mu(R_a(\xi)) = \zeta^a$ and $\mu(R_b(x)) = \zeta^b$. Now, since ζ is an n-th root of unity, we have $R_a(\xi) = R_b(\xi)$ if and only if $a = b \mod n$. □

Let F_n denote the extension of K obtained via adjoining all the finite poles of $R_n(x)$.

Lemma 2.50. *The extension F_n/K is Galois, and has Galois group which is a subgroup of $\mathbb{Z}_n^\times$.*

Proof. Let $Q_n(x)$ denote the denominator of $R_n(x)$. Then F_n is the splitting field of $Q_n(x)$, hence Galois over K. Fix a primitive pole ξ of $R_n(x)$. Lemma 2.48 shows that all other poles are obtained as rational functions $R_a(\xi)$ in that pole, hence the action of $\sigma \in \mathrm{Gal}\left({}^{F_n}/_{K}\right)$ is determined by where σ sends ξ. The primitive pole ξ must map to a primitive pole $R_{a_\sigma}(\xi)$, and we must have $\gcd(n, a_\sigma) = 1$. The map $\sigma \mapsto a_\sigma$ from $\mathrm{Gal}\left({}^{F_n}/_{K}\right) \to \mathbb{Z}_n^\times$ is a homomorphism, since $R_{a_\sigma}(R_{a_{\sigma'}}(\xi)) = R_{a_\sigma a_{\sigma'}}(\xi)$. Since the action of σ is determined only by its value on ξ, this homomorphism is also injective by Lemma 2.49.

□

Proposition 2.51. *Let ζ be an n-th root of unity, and recall $\eta_c(x) = \mu^{-1}(c\mu(x))$, and let L be some field containing K. Then for any $z \in L$ we have that $R_n(z) = R_n(\eta_\zeta(z))$. Furthermore, all preimages of $R_n(z)$ under $R_n(x)$ are of this form.*

Proof. By Lemma 2.36, we have $R_n(\eta_\zeta(z)) = \eta_1 R_n(z) = R_n(z)$, where the last equality follows from the fact that $\eta_1(x)$ is the identity. Observe that $\eta_\zeta(x) = \frac{\xi x + \delta^2}{\xi + x}$ where $\xi =$

$\mu^{-1}\zeta$. Now, all the points $\eta_\zeta(z)$ for various roots of unity ζ are the images of various poles ξ of $R_n(x)$ under the degree-one map $\xi \mapsto \frac{\xi z+\delta^2}{\xi+z}$. Since they are the images of n distinct points under a degree-one map, they must be distinct themselves. Now, since $R_n(x)$ is a degree-n map, these must be all the preimages. □

Lemma 2.52. *The Galois closure of the extension ${}^{K(z)}/_{K(t)}$ which is defined by $R_n(z) - t = 0$ is $F_n(z)$.*

Proof. We claim F_n is contained in the Galois closure. Indeed, for any pole $\xi = \mu(\zeta)$ of $R_n(x)$, the element $z' = \eta_\zeta(z) = \frac{z\xi+\delta^2}{\xi+z}$ is also a root of $R_n(x) - t$, and thus belongs to the Galois closure. Thus $\xi = \frac{zz'-\delta^2}{-z'+z}$ also belongs to the Galois closure. Hence, all of F_n is contained in the Galois closure. By the previous lemma, all the solutions to $R_n(x) = t$ are of the obtained as $\eta_\zeta(z) \in F_n(z)$, showing that $F_n(z)$ is indeed the splitting field of $R_n(x) - t$. □

From now on let t be a transcendental variable, and let the extension $K(z)/K(t)$ be defined via $R_n(z) = t$. For $a \in \mathbb{Z}_n^\times$, extend the definition of $\sigma_a \in \mathrm{Gal}\left({}^{F_n}/_K\right)$ given in the proof of Lemma 2.50 to $F_n(z)$ by acting trivially on z. This is possible because $K(z)$ is linearly disjoint from F_n, as the former is purely transcendental while the latter is algebraic. Moreover, define $\tau_\zeta \in \mathrm{Gal}\left({}^{F_n(z)}/_{F_n(t)}\right)$ to be the automorphism sending z to $\eta_\zeta(z)$.

Lemma 2.53. *Let ζ, ζ' be n-th roots of unity. Then $\eta_\zeta(z) = \eta_{\zeta'}(z)$ if and only if $\zeta = \zeta'$.*

Proof. Recall that if $\xi = \mu\zeta$, then $\eta_\zeta(z) = \frac{z\xi+\delta^2}{\xi+z}$. Apply the following degree one map to both sides of the equation: $x \mapsto \frac{xz-\delta^2}{z-x}$ and find that $\xi = \mu(\zeta) = \mu(\zeta') = \xi'$. □

Proposition 2.54. *The monodromy group of $R_n(x) \in K(x)$ is isomorphic to a subgroup of $\mathrm{AGL}_1(\mathbb{Z}_n)$ containing a copy of $\mathbb{Z}_n \rtimes 1$. Further, its action on the roots of $R_n(x) - t$ is isomorphic to that induced by the action of $\mathrm{AGL}_1(\mathbb{Z}_n)$ on $\{0, \dots, n-1\}$.*

Proof. We know from Lemma 2.52 that the Galois closure of $K(z)/K(t)$, where $R_n(z) - t = 0$ is $F_n(z)$. Consider first the extension $F_n(t)/K(t)$. By Lemma 2.50 we know that this extension is Galois with Galois group which is a subgroup H of $\mathbb{Z}_n^\times$. Fixing a particular primitive pole $\xi \in F_n$ of $R_n(x)$, the action of $\sigma \in \operatorname{Gal}\left({}^{F_n(t)}/_{K(t)}\right)$ is given by $\sigma(\xi) = R_a(\xi)$ for some $a \in H$. Let $\sigma_a = \sigma$ denote this element. Now, this is a normal subextension of $F_n(z)/K(t)$. Observe that as before we can extend the action of H to all of $KF_n(z)$ by letting it act trivially on z. The extension $F_n(z)/F_n(t)$ is thus also Galois. Note that this extension is of degree n. We can see that the Galois group of this extension is $\mathbb{Z}_n \cong \{\zeta \mid \zeta^n = 1\}$, where ζ acts via τ_ζ. Thus, over all $\operatorname{Gal}\left({}^{F_n(z)}/_{K(t)}\right) = \mathbb{Z}_n \rtimes H$.

Indeed, letting $k \in \{0, \dots, n-1\}$ correspond to $\tau_{\zeta^k} z$ we can see that the action of τ_{ζ^b} is additive while the action of σ_a is multiplicative, showing the isomorphism of the action. □

Proposition 2.55. *Let $n' \,|\, n$ be integers. Recall that $q_{n,n'} : \mathrm{AGL}_1(\mathbb{Z}_n) \to \mathrm{AGL}_1(\mathbb{Z}_{n'})$ is the mod n' map. Let $H \subset \mathrm{AGL}_1(\mathbb{Z}_n)$ be the Galois group of $R_n(x) - t$, i.e., the monodromy group of $R_n(x)$. Then the field fixed by $\ker q_{n,n'} \cap H$ is the splitting field of $R_{n'}(x) - t$.*

Proof. Indeed, consider the extension $F_n(z)$ where $R_n(z) = t$, and let ζ be a primitive n-th root of unity. We see that all the roots of $R_{n'}(x) - t = 0$ can be obtained as

$$\left\{\eta_{\zeta^{nk/n'}} R_{n/n'}(z) \mid k = 0, \dots, \frac{n}{n'} - 1\right\}.$$

Indeed,

$$R_{n'}(\eta_{\zeta^{nk/n'}} R_{n/n'}(z)) = R_{n'} R_{n/n'}(z) = R_n(z) = t.$$

Now, the action of $ax + b \in H$ on $\eta_{\zeta^{nk/n'}} R_{n/n'}(z)$ yields

$$\eta_{\zeta^{ank/n'}} R_{n/n'}(\eta_{\zeta^b z}) = \eta_{\zeta^{(ak+b)n/n'}} R_{n/n'}(z).$$

All these roots are fixed if and only if for every k we have that $k = ak + b \mod n'$. In particular, $k = 0$ and $k = 1$ show that $b = 0 \mod n'$ and $a = 1 \mod n'$, correspondingly. Moreover these conditions really ensure that $k = ak + b \mod n'$ for all k. □

2.7 Dickson and Chebyshev polynomials

Let K be a number field, let $\alpha \in K^\times$ and $n \in \mathbb{N}$. The Dickson polynomial of degree n with parameter α is the unique degree-n polynomial over K satisfying

$$D_{\alpha,n}(x + \frac{\alpha}{x}) = x^n + \frac{\alpha^n}{x^n}.$$

They can be defined recursively via the recurrence relation $D_{\alpha,n}(x) = xD_{\alpha,n-1}(x) - \alpha D_{\alpha,n-2}(x)$ for $n \geq 2$, and with initial values $D_{\alpha,0} = 2$ and $D_{\alpha,1}(x) = x$. The Chebyshev polynomials appear as the special case $T_n(z) = D_{1,n}(z)$.

The Dickson polynomials are all linearly related over $\bar{K}$ to the Chebyshev polynomials (and hence to each other): $D_{\alpha,n}(z) = \alpha^{n/2}T_n(\frac{z}{\sqrt{\alpha}})$, although they may not be linearly related over K. The Dickson polynomial $D_{\alpha,n}(x)$ has ramification type $(n, 2, 2)$, with branch points at $\pm 2\alpha^{n/2}$ and infinity. In the case where n is even the ramification indices are $2^{n/2-2}1^2$ over $2\alpha^{n/2}$, with $\pm 2\sqrt{\alpha}$ being the non-ramified preimages, and $2^{n/2}$ over $-2\alpha^{n/2}$.

Up to linear relation, the Dickson polynomails are the only degree-n rational functions which have these ramification types.

As with the Rédei functions, two Dickson polynomials $D_{\alpha,n}(x)$ and $D_{\beta,n}(x)$ are linearly related over K if and only if $\alpha/\beta \in K^{\times 2}$, that is α and β differ by a square. More precisely, in this case

$$\alpha^{-n/2}D_{\alpha,n}(\sqrt{\alpha/\beta}x) = \beta^{-n/2}D_{\beta,n}(x).$$

Conversely, suppose $D_{\alpha,n}(x) = \ell'(D_{\beta,n}(\ell(x)))$. If n is odd then ℓ' must map the branch point $2\beta^{n/2}$ to one of the branch points $\pm 2\alpha^{n/2}$, which implies α/β is a square. On the other hand, if n is even, ℓ must map the non-ramified preimages $\pm\sqrt{\alpha}$ of $2\alpha^{n/2}$ to the non-ramified preimages $\pm\sqrt{\beta}$ of $2\beta^{n/2}$, which again implies α/β is a square.

Proposition 2.56. *Let $f(z) \in K(z)$ be a degree-n rational function with ramification type $(n, 2, 2)$. Then there exists $\alpha \in K$ such that $f(z)$ is K-linearly related to $D_{\alpha,n}(z)$.*

A proof of this fact can be found in [16, Lemma 3.2].

Remark 2.57. Let n, m be integers. The Dickson polynomials satisfy

$$D_{\alpha,nm}(x) = D_{\alpha^m,n} \circ D_{\alpha,m}(x),$$

since they both map $x + \alpha/x$ to $x^{nm} + \alpha^{nm}/x^{nm}$.

Proposition 2.58. *The monodromy group of $D_{\alpha,n}(x)$ is a subgroup of $\mathrm{AGL}_1(\mathbb{Z}_n)$ which contains $\mathbb{Z}_n \rtimes C_2$. Moreover, the action of this monodromy group on the roots of $D_{\alpha,n}(x)-t$ is isomorphic to the natural action of $\mathrm{AGL}_1(\mathbb{Z}_n)$ on $\{0, \dots, n-1\}$.*

Proof. We compute the Galois closure Ω of the polynomial $D_{\alpha,n}(x) - t$ over $K(t)$. First, consider the quadratic extension $K(u)/K(t)$ defined by the relation $t = u + \frac{\alpha^n}{u}$. This extension has a unique non-trivial automorphism $\tau : u \mapsto \alpha^n/u$. The Galois closure of $x^n - u$ over $K(u)$ is $\Omega_u = K(v, \zeta)$, where $v^n = u$ and ζ is a primitive n-th root of unity. Moreover, the Galois group $G = \mathrm{Gal}\left({}^{\Omega_u}/_{K(u)}\right)$ is the monodromy group of x^n, and hence is isomorphic to a subgroup of $\mathrm{AGL}_1(\mathbb{Z}_n)$ which contains $\mathbb{Z}_n \rtimes 1$. Note that the Galois closure of $D_{\alpha,n}(x) - t$ over $K(t)$ is contained in Ω_u, since all the roots

$$\left\{\zeta^k v + \frac{\alpha}{\zeta^k v} \mid k = 0, \dots, n-1\right\}$$

lie in Ω_u.

$$\begin{tikzcd}
 & \Omega_u = K(v,\zeta) \arrow[dl, dash] \arrow[dr, dash, "G"] & \\
\Omega \arrow[dr, dash] & & K(u) \arrow[dl, dash, "C_2"] \\
 & K(t) &
\end{tikzcd}$$

First, suppose that $\zeta \in K$. Then $G = \mathbb{Z}_n \rtimes 1$, and the element $x \mapsto x + b$ acts via $v \mapsto \zeta^b v$. We observe that in this case, the Galois closure of $D_{\alpha,n}(x) - t$ must be all of Ω_u. Indeed, both the roots $z = v + \alpha/v$ and $z' = \zeta v + \alpha/(\zeta v)$ are in Ω, and therefore so is $v = (z - \zeta z')/(1 - \zeta^2) \in \Omega$. Extend τ to Ω_u by letting $\tau v = \alpha/v$. We can see that the overall Galois group is $\mathbb{Z}_n \rtimes C_2$. In this semidirect product, $\tau \in C_2$ acts on $\mathbb{Z}_n$ by negation, so we can consider this group as a subgroup of $\mathrm{AGL}_1(\mathbb{Z}_n)$.

Now, suppose $\zeta \notin K$. In this case, we have that G moreover conatins $\mathbb{Z}_n \rtimes C_2$, where the element of order two fixes v and maps ζ to ζ^{-1}. Moreover, we have that $K(v)$ and $K(\zeta)$ are linearly disjoint (v is transcendental). We can thus extend τ to Ω_u via $v \mapsto \alpha/v$ and $\zeta \mapsto \zeta^{-1}$. This extension of τ remains of order 2. Further, we show that this extension commutes with all the members of G. Indeed:

$$(ax+b)\tau v = (ax+b)\frac{\alpha}{v} = \frac{\alpha}{\zeta^b v} = \tau(\zeta^b v) = \tau(ax+b)v,$$

and

$$(ax+b)\tau\zeta = (ax+b)\frac{1}{\zeta} = \frac{1}{\zeta^a} = \tau(\zeta^a) = \tau(ax+b)\zeta.$$

Thus, the Galois group $\mathrm{Gal}\left({}^{\Omega_u}/_{K(t)}\right) = C_2 \times G$.

We observe that τ fixes all the roots of $D_{\alpha,n}(x) - t$, as can be seen by the computation

$$\tau(\zeta^k v + \alpha(\zeta^k v)^{-1}) = \alpha(\zeta^k v)^{-1} + \zeta^k v.$$

We now show that the Galois closure $\Omega = \Omega_u^{C_2}$. Since τ fixed all the roots of $D_n(x) - t$, we have that $\Omega_u^{C_2} \subset \Omega$. Now note that $u \notin \Omega$, since τ does not fix u (but does fix all the roots of $D_n(x) - t$). Hence the quadratic extension $\Omega[u]$ is the compositum $K(u)\Omega$ of two Galois extensions of $K(t)$, and must therefore be Galois over $K(t)$. Since it is Galois over $K(t)$ and contains $K(u)$, it must contain Ω_u. However, it is the compositum of two fields contained in Ω_u, and we must have equality. This shows that Ω is a subfield of index 2 in Ω_u. Furthermore, since we showed that Ω contains $\Omega_u^{C_2}$, we must have equality.

Computing the action

$$(ax+b) \cdot (\zeta^k v + \alpha/\zeta^k v) = \zeta^{ak+b} v + \alpha/\zeta^{ak+b} v)$$

we can see the action isomorphism. □

Proposition 2.59. *Let $n' \,|\, n$ be integers. Recall that $q_{n,n'} : \mathrm{AGL}_1(\mathbb{Z}_n) \to \mathrm{AGL}_1(\mathbb{Z}_{n'})$ is the mod n' map. Let $H \subset \mathrm{AGL}_1(\mathbb{Z}_n)$ be the Galois group of $D_{\alpha,n}(x) - t$ over $K(t)$. Then the field fixed by $\ker q_{n,n'} \cap H$ is the splitting field of $D_{\alpha^{n/n'},n'}(x) - t \in K(t)[x]$.*

Proof. Recall that $D_{\alpha,n}(x) = D_{\alpha^{n/n'},n'} \circ D_{\alpha,n/n'}(x)$. As before, write $t = u + \alpha^n/u$ and $v^n = u$, and fix some primitive n-th root of unity ζ. All the roots of $D_{\alpha,n}(x) - t$ are given as $\zeta^k v + \alpha(\zeta^k v)^{-1}$, for any k. Then direct computation shows that all the solutions to $D_{\alpha^{n/n'},n'}(x) = t$ are obtained as

$$D_{\alpha,n/n'}(\zeta^k v + \alpha(\zeta^k v)^{-1}) = \zeta^{nk/n'} v^{n/n'} + \alpha^{n/n'} \zeta^{-nk/n'} v^{-n/n'}.$$

Let $ax + b \in H$. This element fixes a root $\zeta^{nk/n'} v^{n/n'} + \alpha^{n/n'} \zeta^{-nk/n'} v^{-n/n'}$ if and only if

$$(ax+b)(\zeta^{nk/n'} v^{n/n'} + \alpha^{n/n'} \zeta^{-nk/n'} v^{-n/n'}) = \zeta^{nka/n'+bn/n'} v^{n/n'} + \alpha^{n/n'} \zeta^{-(nka/n'+bn/n')} v^{-n/n'}$$

equals

$$\zeta^{nk/n'} v^{n/n'} + \alpha^{n/n'} \zeta^{-nk/n'} v^{-n/n'}.$$

This holds if and only if $(ank)/n' = nk/n'$ and $(bn)/n' = 0 \bmod n$. As in the proof of the analogous statement for the Rédei functions, this is true exactly when $a = 1$ and $b = 0$ modulo n', which means that $ax + b \in \ker q_{n,n'}$. This completes the proof. □

Chapter 3: Rational functions attaining values in a recurrence sequence

Let K be a number field, and let $(r_n)_{n\in\mathbb{Z}}$ be a rank-2 linear recurrence sequence satisfying $r_{n+2} = a_1 r_{n+1} + a_2 r_n$, where $a_1 \in K$ and $a_2 = -\zeta \in K$ for some m-th root of unity ζ. Let φ and $\zeta\varphi^{-1}$ be the roots $\frac{a_1\pm\sqrt{\Delta}}{2}$ of the recurrence relation, where $\Delta = a_1^2 + 4a_2$. These are the roots of the characteristic polynomial $x^2 - a_1 x - a_2$. Assume that $\Delta \neq 0$. Then we can write $r_n = A\varphi^n + B(\zeta\varphi^{-1})^n$ for some $A, B \in K[\varphi]$. Assume that r_n is not the constant zero sequence. This implies that at least one of A or B is not 0.

Define $\tilde{\Delta} = D_{\zeta,m}(a_1) - 4$, where $D_{\zeta,m}(x)$ is the m-th Dickson polynomial. Also define

$$N = N_r = a_2 r_0^2 + a_1 r_0 r_1 - r_1^2 = r_0 r_2 - r_1^2,$$

and for each $0 \leq j \leq m-1$, define

$$\tilde{N}_j = r_{2m+j} r_j - r_{m+j}^2.$$

We note that the subsequences

$$\tilde{r}_{j,n} = r_{nm+j} = A\varphi^j(\varphi^m)^n + B\varphi^{-j}\zeta^j(\varphi^{-m})^n$$

for $j = 0, \ldots, m-1$ are themselves rank-2 recurrence sequences, with roots φ^m and φ^{-m}.

The characteristic polynomial for their recurrence relation must be

$$(x-\varphi^m)(x-\varphi^{-m}) = x^2 - (\varphi^m + \varphi^{-m})x + 1 = x^2 - \tilde{a}_1 x - \tilde{a}_2.$$

Since $a_1 = \varphi + \zeta\varphi^{-1}$, we have that $\tilde{a}_1 = \varphi^m + \varphi^{-m} = D_{\zeta,m}(a_1)$. We can see that the discriminants of these subsequences are all equal to $\tilde{\Delta}$, and that $\tilde{N}_j = N_{\tilde{r}_j}$. Note that this implies that $\varphi^m = \frac{\tilde{a}_1+\delta}{2}$ or $\frac{\tilde{a}_1-\delta}{2}$. For notational convenience we pick the root $\delta = \sqrt{\tilde{\Delta}}$ such that $\varphi^m = \frac{\tilde{a}_1+\delta}{2}$. We may sometimes refer to N_r as the norm of the sequence r_n, and to $\tilde{N}_j$ the norms of the subsequences (with the implication of referring to the subsequences $\tilde{r}_{j,n}$). We additionally assume that $\tilde{\Delta} \neq 0$ and $\tilde{N}_j \neq 0$ for all $0 \leq j < m$.

In this chapter we prove the following theorem:

Theorem 3.1. *Let K be a number field, and let $(r_n)_{n\in\mathbb{Z}}$ be a rank-two recurrence sequence satisfying $r_{n+2} = a_1 r_{n+1} + a_2 r_n$ where $a_1 \in K$ and $a_2 = -\zeta \in K$ for some ζ such that ζ is a root of unity of order m. Further, denote $\tilde{\Delta} := D_{\zeta,m}(a_1)^2 - 4$, and $\delta := \sqrt{\tilde{\Delta}}$, and $\tilde{N}_j := r_{2m+j}r_j - r_{m+j}^2$. Suppose additionally that $\tilde{\Delta} \neq 0$ and that $\tilde{N}_j \neq 0$ for all $j < m$.*

If the value set $\phi(K)$ of a rational function $\phi(x) \in K(x)$ of degree $d \geq 2$ contains infinitely many elements from the sequence $\{r_n\}_{n\in\mathbb{Z}}$, that is, if $\#(\phi(K) \cap \{r_n \mid n \in \mathbb{Z}\}) = \infty$, then $\phi(x)$ is of one of the following forms

1. *$\pm\sqrt{\frac{\tilde{N}_j}{\tilde{\Delta}\alpha^d}} D_{\alpha,d}(\ell(x))$ for some $0 \leq j < m$, a degree-one map $\ell(x) \in K(x)$ and some $\alpha \in K$ such that $\frac{\tilde{N}_j}{\tilde{\Delta}\alpha^d}$ is a square in K, or*

2. *$q_j(\eta_{\delta,\varphi^{mk}}(R_{\delta,d/2}(\ell(x))))$ for some $0 \leq k < d/2$ and $0 \leq j < m$ and for some degree-one map $\ell(x) \in K(x)$, where d is even and*

$$q_j(x) = \frac{r_j(x^2+\tilde{\Delta}) - (4r_{m+j} - 2\tilde{a}_1 r_j)x}{x^2 - \tilde{\Delta}} \in K(x),$$

$$\mu_\delta(x) = \frac{x+\delta}{x-\delta}, \quad R_{\delta,n}(x) = \mu_\delta^{-1}(\mu_\delta(x)^n) \in K(x),$$

and where $\eta_{\delta,c}(x) = \mu_\delta^{-1}(c\mu_\delta(x))$. We note that for the particular $c = \varphi^{mk}$ we have $\eta_{\delta,c}(x) \in K(x)$.

Moreover, when the value set contains infinitely many elements from the sequence in either case above, for the corresponding j there are infinitely many elements from the subsequence $\{r_{mn+j}\}_{n\in\mathbb{Z}}$ in the value set $\phi(K)$.

In Remark 3.8 below we comment on the converse of the theorem.

Remark 3.2. Note that because

$$\alpha^{-d/2}D_{\alpha,d}(\sqrt{\alpha/\alpha'}x) = \alpha'^{d/2}D_{\alpha',d}(x),$$

one may freely vary α up to a square in 1. In particular, when d is odd, since $N_j/\tilde{\Delta}\alpha^d$ must be a square, one can take $\alpha = \frac{\tilde{\Delta}}{\tilde{N}_j}$. Additionally, in this case we have that $-D_{\alpha,d}(x) = D_{\alpha,d}(-x)$, and we can drop the ± sign.

Remark 3.3.

1. $N_r = 0$ if and only if r_n is a geometric sequence, either $A\varphi^n$ or $B(\zeta\varphi^{-1})^n$. In this case the problem is treated by a work of Dèbes [13] on geometric seuquences.
2. When $\Delta = 0$, the characteristic polynomial has a single root of multiplicity two, and the sequence r_n has the form $A\alpha^n + Bn\alpha^n$.

Remark 3.4. By studying the ramification of the functions mentioned in the theorem, we can see that (over $\bar{K}$) the functions $q_j \circ \eta_{\delta,c} \circ R_{\delta,n}(x)$ are linearly related to the composition of a Dickson polynomial $D_{\alpha,n}$ with an appropriate quadratic function. Therefore, the two possibilities which appear in the theorem are closely related, arising in such different forms only because we chose to write them as the composition of functions defined over K.

The only function in the theorem which is not obviously defined over K is $\eta_{\delta,\varphi^{mk}}(x)$.

Claim 3.5. *The function $\eta_{\delta,\varphi^{mk}}(x)$ is defined over K for every k.*

Proof. We know by Lemma 2.35 that $\eta_{cc'}(x) = \eta_c \circ \eta_{c'}(x)$, and so $\eta_{\delta,\varphi^{mk}}(x)$ is the k-fold composition of the map $\eta_{\delta,\varphi^m}(x)$ with itself. Thus, it suffices to show that $\eta_{\delta,\varphi^m}(x)$ is defined over K.

Whenever $\delta \in K$, we also have that $\varphi^m = \frac{\tilde{a}_1+\delta}{2} \in K$. Thus, the entire composition $\mu_\delta^{-1}(\varphi^m \mu_\delta(x))$ is defined over K. Otherwise, let σ be the unique automorphism of $K[\delta]$. Since $\varphi\sigma\varphi = \zeta$, we have that $\sigma\varphi^m = \varphi^{-m}$. The fact that the function is defined over K follows from the fact that $\eta_c(x)$ is defined over K if and only if $c \in \mu K$, and that $c \in \mu K$ if and only if $\sigma c = c^{-1}$, as seen in Lemmas 2.38 and 2.30. □

Remark 3.6. The last line of the proof shows that $\varphi^m \in \mu(K)$.

Recall the subsequences $\tilde{r}_{j,n} = r_{mn+j}$, for $0 \leq j < m$. Clearly, if a rational map attains infinitely many values from the sequence r_n, then for some j, it must attain infinitely many values from $\tilde{r}_{j,n}$. Let us now restate the theorem for the case where $a_2 = -1$, from which the main theorem follows precisely by considering this decomposition into complementary subsequences.

Theorem 3.7. *Let K be a number field, and let $(r_n)_{n\in\mathbb{Z}}$ be a rank-2 recurrence sequence satisfying $r_{n+2} = a_1 r_{n+1} - r_n$ where $a_1 \in K$. Denote $\Delta = a_1^2 - 4$, and $N = r_0 r_2 - r_1^2$ as above, and set $\delta = \sqrt{\Delta}$. Suppose additionally that both $\Delta \neq 0$ and $N \neq 0$. If a rational map $\phi(x) \in K(x)$ of degree $d \geq 2$ has infinitely many elements from r_n in its image, that is, if $\#(\phi(K) \cap \{r_n \mid n \in \mathbb{Z}\}) = \infty$, then ϕ must equal one of the following:*

1. $\pm\sqrt{\frac{N}{\Delta\alpha^d}} D_{\alpha,d}(\ell(x))$ *for some degree-one map $\ell(x) \in K(x)$ and some $\alpha \in K$ such that $\frac{N}{\Delta\alpha^d}$ is a square in K, or*

2. $q(\eta_{\delta,\varphi^k}(R_{\delta,d/2}(\ell(x))))$, *where d is even, and as in Theorem 3.1*

$$q(x) = \frac{r_0(x^2+\Delta) - (4r_1 - 2a_1 r_0)x}{x^2 - \Delta} \in K(x),$$

$$\mu_\delta(x) = \frac{x+\delta}{x-\delta}, \quad R_{\delta,n}(x) = \mu_\delta^{-1}(\mu_\delta(x)^n), \quad \eta_{\delta,\varphi^k}(x) = \mu^{-1}(\varphi^k \mu(x)) \in K(x),$$

for some $0 \leq k < d/2$ and some degree-one map $\ell(x) \in K(x)$.

Remark 3.8. One can show that all the functions having the form given in 2 do indeed attain infinitely many elements from the given sequence (this can be infered, for example, from the last part of Proposition 3.12 given below).

As for the functions given in 1, we do not know whether the converse statement is true but we are able to give two illuminating examples:

- For the sequences $r_n = A\varphi^n + A\varphi^{-n} \in K$ where $A \in K$, we find that $N = A^2\Delta$, and therefore, for any d and n we have that
$$r_{dn} = \sqrt{\frac{N}{\Delta}} D_{1,d}(\varphi^n + \varphi^{-n}).$$
- For the sequences $r_n = \delta A\varphi^n - \delta A\varphi^{-n} \in K$ where $A \in K$, we find that $N = -A^2\Delta^2$, and therefore, for any n and for any odd d we have
$$r_{dn} = \sqrt{\frac{N}{\Delta(-\Delta)^d}} D_{-\Delta,d}(\delta\varphi^n - \frac{\Delta}{\delta\varphi^{-n}}).$$

  In further work we intend to precisely nail down the possible values of α for which the converse holds.

We can now use this theorem to prove the main theorem of this chapter.

Proof of Theorem 3.1. Recall that the subsequences $\tilde{r}_{j,n} = r_{nm+j}$ satisfy a recurrence relation with characteristic polynomial $(x - \varphi^m)(x + \varphi^m) = x^2 - \tilde{a}_1 x + 1$, whose roots are $\varphi^{\pm m}$. The assumptions of our theorem precisely imply that the assumptions of Theorem 3.7 hold for each sequence $\tilde{r}_{j,n}$, except maybe for the assumption of infinite intersection with the value set $\phi(K)$. However, if $\phi(x)$ attains infinitely many values from r_n, it must attain infinitely many values from $\tilde{r}_{j,n}$ for some j, showing the result. □

To prove Theorem 3.7, we set S to be the set of primes that divide any one of the denominators of a_1, r_0 or r_1. Then all the elements from $\{r_n \mid n \in \mathbb{Z}\}$ are S-integral. Therefore, $\phi(x)$ as in Theorem 3.7 must be a Siegel function, and so we are to classify the Siegel functions which attain infinitely many elements from $\{r_n \mid n \in \mathbb{Z}\}$. Recall that a Siegel function may have either one or two poles. Proposition 3.15 below treats the case of one pole, and Proposition 3.18 below treats the case of two poles.

We now turn to making prepareations towards a proof of Theorem 3.7.

Lemma 3.9. *Denote by* $r_n^{+1} = r_{n+1}$ *the sequence* r_n *with an index shift of* 1. *Then* $N_{r^{+1}} = -a_2 N_r$. *In particular, whenever* $a_2 = -1$ *we have that* $N_{r^+} = N_r$.

Proof. We observe that N_r can be written as a determinant, and find that

$$N_{r^+} = r_1 r_3 - r_2^2 = \det \begin{pmatrix} r_1 & r_2 \\ r_2 & r_3 \end{pmatrix} = \det \begin{pmatrix} a_1 & a_2 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_0 & r_1 \\ r_1 & r_2 \end{pmatrix} = -a_2 N_r.$$

□

Proposition 3.10. *Suppose that* $a_2 = -1$. *Let* V *be a smooth projective model of the affine curve* $y^2 = \Delta x^2 - 4N$. *Then for any* $n \in \mathbb{Z}$, *we have that* $(r_n, 2r_{n+1} - a_1 r_n) \in V \cap \mathbb{A}^2$. *In particular, if* S *is the set of primes dividing the denominators of* a_1, r_0 *and* r_2, *then there are infinitely many* S*-integral points on* V.

Proof. Applying Lemma 3.9 repeatedly n times we find that $N = r_{n+2} r_n - r_{n+1}^2$ for any $n \in \mathbb{N}$. Likewise, applying the Lemma to the sequence given by shifting r_n *back* by one or more elements shows that the relation holds for any $n \in \mathbb{Z}$. Rewriting using $r_{n+2} = a_1 r_{n+1} - r_n$, we find that

$$r_{n+1}^2 - a_1 r_n r_{n+1} + r_n^2 + N = 0.$$

By multiplying by 4 and completing the square with respect to $4r_{n+1}^2$ we find that

$$(2r_{n+1} - a_1 r_n)^2 - a_1^2 r_n^2 + 4r_n^2 + N = 0,$$

that is, that $(2r_{n+1} - a_1 r_n)^2 = \Delta r_n^2 - 4N$. □

Remark 3.11. Observe that infinity has two preimages (over $\bar{K}$) under the projection $\pi_x : V \to \mathbb{P}^1_{\bar{K}}$, which in affine coordinates is given by $\pi_x : (x, y) \to x$.

Lemma 3.12. *The following provides a parameterization of the curve* V*:*

$$(x(w), y(w)) = \left(\frac{r_0(w^2 + \Delta) - (4r_1 - 2a_1 r_0)w}{w^2 - \Delta}, \frac{(a_1 r_0 - 2r_1)w^2 + 2\Delta r_0 w + (a_1 r_0 - 2r_1)\Delta}{w^2 - \Delta} \right).$$

Denote $q(w) = x(w)$ and set $\delta = \sqrt{\Delta}$. Recall that $\mu_\delta(x) = (x+\delta)/(x-\delta)$. Then we have that

$$r_n = q(\mu_\delta^{-1}(\varphi^n)) = q(\mu_\delta^{-1}((B/A)\varphi^{-n})).$$

Proof. To verify this, we substitute the parameterization into the curve equation. We refer the reader to Appendix A.1 for a symbolic calculation that shows the parameterization satisfies the defining equation of V. In fact, the appendix gives a parameterization for the curve $y^2 = \Delta x^2 - 4N$ for any value of a_2.

To prove the last part of the lemma, recall the notation $r_n = A\varphi^n + B\varphi^{-n}$. We claim that $q \circ \mu_\delta^{-1}(x) = Ax + Bx^{-1}$. This composition yields a degree-two function with poles at zero and infinity, since $q(\mu_\delta^{-1}(\{0, \infty\})) = q(\{\delta, -\delta\}) = \infty$. Therefore, $q \circ \mu_\delta^{-1}(x)$ has the form $ax + bx^{-1}$ for some $a, b \in \bar{K}$. Thus, to show the result we simply need to verify that $a = A$ and $b = B$. First, plug in $x = 1$:

$$a + b = q \circ \mu_\delta^{-1}(1) = q(\infty) = r_0 = A + B.$$

Next, plug in $x = -i$:

$$-ai + bi = q \circ \mu_\delta^{-1}(-i) = q(i\delta) = -(2r_1 - a_1 r_0)/(i\delta).$$

Now, since, $\frac{\delta(A-B)}{i\delta} = -iA + iB$,

$$2r_1 - a_1 r_0 = A(a_1 + \delta) + B(a_1 - \delta) - a_1 A - a_1 B = \delta(A - B).$$

Putting the last two equations together, we find that $-ai + bi = -Ai + Bi$. Overall, we find $A = a$ and $B = b$, as desired. Lastly, if $y = (B/A)x^{-1}$, then the equality $Ay + B/y = Ax + B/x$ demonstrates the truth of the last equality presented in the lemma. □

Henceforth we shall denote $q(w) = x(w)$ for the quadratic given in the parameterization.

Remark 3.13. The last line of the proof shows that, in general, $q \circ \eta'_{\delta,B/A}(x) = q(x)$.

The following lemma presents a twisted version of the claim that if $cx_0^n = \varphi^t$ for some rational x_0 and integer t, then c must be a (small) power of φ times an n-th power.

Lemma 3.14. *Let $c \in \bar{K}^\times$ be such that $\mu_\delta^{-1}c \in K$, and let $n > 1$. Suppose that the image of K under the map $\eta_c R_{\delta,n}(x) \in K(x)$ contains an element of the form $\mu_\delta^{-1}(\varphi^t)$, for some $t \in \mathbb{Z}$. Then $c = d^n\varphi^k$ for some $d \in \mu_\delta K$ and some $0 \leq k < n$.*

Proof. Suppose that $\eta_c R_{\delta,n}(x_0) = \mu_\delta^{-1}\varphi^t$ for some $x_0 \in K$. Write $t = qn+k$ for $0 \leq k < n$. Apply $\eta_{\varphi^{-k}}(x)$ to both sides of the equation, then

$$\begin{aligned}\eta_{\varphi^{-k}}\eta_c R_n(x_0) &= \eta_{\varphi^{-k}}(\mu^{-1}(\varphi^{qn+k}))\\ &= \mu_\delta^{-1}\varphi^{nq}\\ &= R_{\delta,n}(\mu_\delta^{-1}(\varphi^q)).\end{aligned}$$

Applying μ_δ to both sides, we find that $\varphi^{-k}c\mu_\delta(x_0)^n = \varphi^{qn}$. Thus $c = \varphi^k d^n$ where $d = \varphi^q/\mu_\delta(x_0)$. We know that both $\mu_\delta(x_0)$ and $\varphi^q \in \mu_\delta K$ (by Remark 3.6), and again by Remark 2.32 we find that their quotient $d \in \mu_\delta K$. □

Proposition 3.15. *Let the recurrence sequence $r_{n+2} = a_1 r_{n+1} - r_n \in K$ be as in Theorem 3.7 (i.e., with $N \neq 0$ and $\Delta \neq 0$). Suppose $\phi \in K(x)$ is a function of degree $d \geq 2$, having only one pole, and suppose that the image $\phi(K)$ attains infinitely many values from $\{r_n \mid n \in \mathbb{Z}\}$. Then $\phi(z) = \pm\sqrt{\frac{N}{\Delta\alpha^d}}D_{\alpha,d}(\ell(z))$ for some $\alpha \in K$, and a degree one map $\ell \in K(z)$, and where $d = \deg\phi$.*

To show this, we apply the contrapositive of a previous result of the authors. We use the following updated version of the notation, in which G_n, B, u and χ_G are replaced with r_n, a_1, a_2 and N_r respectivaly.

Theorem 3.16 ([8, Theorem 7])**.** *Let r_n be as in the proposition, and let $g(x) \in K[x]$ be a polynomial of degree ≥ 2, such that $g(x)$ is not of the form $\pm\sqrt{\frac{\epsilon N}{\Delta m^d}}D_{d,m}(\ell(x))$ for all* *linear $\ell(x) \in K[x]$, for all $m \in K$, and for $\epsilon = \pm 1$ when $a_2 = 1$, or $\epsilon = 1$ when $a_2 = -1$. Then $\#(g(K) \cap \{r_n \mid n \in \mathbb{Z}\}) < \infty$*

Remark 3.17. We fixed a typo from the original statement, so that in the leading coefficent m^d appears in the denominator, and not in the numerator.

Proof of Proposition 3.15. If the single pole of $\phi(x)$ is at infinity, then $\phi(x)$ is a polynomial. Otherwise, denote the pole of $\phi(z)$ by $p \in K$. Note that this pole belongs to K since it is the only pole. Then $\tilde{\phi}(z) = \phi(\frac{pz+1}{z})$ is a polynomial over K, as it has a single pole at ∞. Recall the we restrict to the case $a_2 = -1$. Clearly, this polynomial also attains infinitely many elements from r_n as values, hence by the theorem $\tilde{\phi}(z) = \pm\sqrt{\frac{N}{\Delta m^d}} D_{d,m}(\ell(z))$ for some degree-one function $\ell(x) \in K(x)$ and $m \in K$ such that $N/\Delta m^d$ is a square. Thus, $\phi(z) = \pm\sqrt{\frac{N}{\Delta m^d}} D_{d,m}(\ell'(z))$ where $\ell'(z) = \ell(\frac{pz+1}{z})$. We of course take $\alpha = m$. □

Proposition 3.18. *Restrict to the case $a_2 = -1$, and let N, Δ and δ be as in Theorem 3.7. Suppose $\phi(x)$ is a Siegel function with two poles, and that the image $\phi(K)$ contains infinitely many elements from $\{r_n \mid n \in \mathbb{Z}\}$. Then $\phi(x) = q(\eta_{\delta,\varphi^k}(R_{\delta,n}(\ell(x)))$, for some $0 \leq k < n$ and some degree-one map $\ell(x) \in K(x)$, and for*

$$q(x) = \frac{r_0(x^2 + \Delta) - (4r_1 - 2a_1 r_0)x}{x^2 - \Delta} \in K(x),$$

is as in Lemma 3.12.

Proof. Recall the curve V defined in Proposition 3.10. Let $\tilde{V} = \phi^* V$ be the pullback of the projection $\pi_x : V \to \mathbb{P}^1$ to the x-coordinate by the map $\phi : \mathbb{P}^1 \to \mathbb{P}^1$. We remark that the projection π_x has been computed in affine coordinates in Lemma 3.12 to be the quadratic map $q(x)$ given in the proposition. For clarity, we shall refer to it as π_x.

Consider the following field diagram, and the graph depicting the corresponding preimages of ∞ along the various maps shown in the diagram:

$$\begin{tikzcd}
 & K(\tilde{V}) = K(z,y) \arrow[dl, dash] \arrow[dr, dash] & \\
K(\phi(z),y) = K(w) \arrow[dr, dash] & & K(z) \arrow[dl, dash] \\
 & K(\phi(z)) &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & v_1, v_2 \arrow[dl, mapsto, "\pi_x^*\phi"'] \arrow[dr, mapsto, "\phi^*\pi_x"] & \\
w_1, w_2 \arrow[dr, mapsto, "\pi_x"'] & & z_1, z_2 \arrow[dl, mapsto, "\phi"] \\
 & \infty &
\end{tikzcd}$$

Let z_1, z_2 denote the preimages of ∞ under ϕ. Due to the parameterization given in Lemma 3.12, we can write $K(\phi(z), y) = K(w)$. Moreover, as mentioned in Remark 3.11, infinity has two preimages under the map π_x, which we shall denote by w_1, w_2.

The image of $\phi(x)$ contains infinitely many elements from $\{r_n\}_{n\in\mathbb{Z}}$. Again, let S be the set of primes dividing the denominators of a_1, r_0 and r_1, such that all the elements in the sequence are S-integers.

Then, in light of Proposition 3.10, there are infinitely many K-rational points on $\tilde{V}$ whose images under the composite map $\phi \circ \phi^*\pi_x : (z, y) \mapsto \phi(z)$ are S-integral . Then by Siegel's Theorem this curve is of genus 0 and the composite map is a Siegel function. Moreover, this composite map must have at most 2 poles. However, since ϕ has exactly two poles the composite function must also have exactly two poles. Let us denote them by v_1 and v_2, and let us fix the notation such that these map respectively to w_1 and w_2 under $\pi_x^*\phi$, and to z_1, z_2 under $\phi^*\pi_x$.

Both w_1 and w_2 each have only one preimage (in $\bar{K}$) under $\pi_x^*\phi$. Thus, $\pi_x^*\phi$ must be totally ramified over these points, with ramification indices $e_{w_i}(v_i)$ equal to the index $[K(\tilde{V}) : K(w)]$. Since both w_1 and w_2 are unramified under ϕ, this implies that the ramification index of v_i over ∞ is likewise equal to $[K(\tilde{V}) : K(w)]$.

Since V is a curve of degree two, the index $[K(\tilde{V}) : K(z)] \leq 2$. If the in the field diagram above $K(z)$ and $K(w)$ are linearly disjoint over $K(\phi(z))$, i.e., $[K(\tilde{V}) : K(z)] = 2$, then ∞ should have $4 = 2 \cdot 2$ preimages over $\bar{K}$ in $\tilde{V}$, by Lemma 2.22 (Abyhanker's Lemma). As we say, there are only two such preimages, hence the diagram is reducible and $K(\tilde{V}) = K(z)$.

In particular $w = w(z) \in K(z)$ is a rational function in z, which is totally ramified at

z_1 and z_2.

Observe that $\phi = \pi_x \circ w$, and thus that the branch points of w are the preimages of ∞ under the projection, which are $\pm\delta$. Thus, from Proposition 2.42, $w(z) = \eta_{\delta,c}(R_{\delta,n}(\ell(z)))$, for some $c \in \mu_\delta(K)$, and some degree-one map $\ell(x) \in K(x)$.

If $n = 1$ we find that $\phi(x) = q(\ell'(x))$, where $\ell' = \eta_c \circ \ell$, and we're done.

From now on suppose that $n \geq 2$. We would like to show that, up to changing $\ell(x)$ we can choose c to be a (small) power of φ. By the latter part of Lemma 3.12, we know that there are infinitely many elements from the set $\left\{\mu_\delta^{-1}(\varphi^t), \mu_\delta^{-1}((B/A)\varphi^{-t})\right\}$ in the image of $w(z)$. By Lemma 3.14 (applied twice) we must have $c = d^n\varphi^k$ or $c = B/Ad^n\varphi^k$ for some $0 \leq k < n$.

For the case $c = d^n\varphi^k$, we use the fact that $\eta_{\delta,d^n}R_{\delta,n} = R_n\eta_d$ to get the required form $\phi(x) = q(\eta_{\delta,\varphi^k}R_{\delta,n}(\ell(x)))$ for some appropriate $\ell(x)$. For the case $c = B/Ad^n\varphi^k$, we first recall that $q \circ \eta'_{\delta,B/A}(x) = q(x)$ (Remark 3.13). Moreover, by Lemma 2.40, we can see that $\eta_{\delta,(B/A)c}R_{\delta,n}(x) = \eta'_{\delta,B/A}\eta_{\delta,1/c}R_{\delta,n}\eta'_{\delta,1}(x)$. Therefore, we can write $\phi(x) = q(\eta_{\delta,1/c}R_{\delta,n}(\ell(x))$ for some appropriate $\ell(x)$. Now note that $1/c = d'^n\varphi^{k'}$, with $d' \in \mu^{-1}(K)$ and $0 \leq k' < n$, for $d' = \varphi/d$ and $k' = n - k$ if $k \neq 0$ and $d' = 1/d, k' = 0$ otherwise. Thus, in the same we as before we can see that $\eta_{\delta,1/c}R_{\delta,n}(x) = \eta_{\delta,\varphi^{k'}}R_n(\eta_{\delta,d'}(x))$ yields the required form.

Overall, we find that $\phi(x) = q(\eta_{\delta,\varphi^k}(R_{\delta,n}(\ell(x))))$ for an appropriate $\ell(x) \in K(x)$. □

Finally, we can prove Theorem 3.7.

Proof of Theorem 3.7. Let S be the set of primes dividing any one of the denominators of a_1, r_0 or r_1. Then all the elements of $\{r_n \mid n \in \mathbb{Z}\}$ are S-integers, and thus $\phi(x)$ as in the thoerem must be Siegel function, and by Theorem 2.24 (Siegel's theorem), $\phi(x)$ has either one or two poles. Proposition 3.15 treats the case of one pole and yields that $\phi(x)$ must have the form given in 1, and Proposition 3.18 treats the case of two poles and yields that $\phi(x)$ must have the form given in 2. □

We now turn to the proof of the special case of the Fibonacci sequence given in the introduction:

Proof of Theorem 1.1. For the Fibonacci sequence, we have that $\zeta = -1$ is a second root of unity. The roots of the Fibonacci sequence are the golden ratio $\varphi = (1+\sqrt{5})/2$ and its conjugate $-\varphi^{-1} = (1-\sqrt{5})/2$. Thus, when applying Theorem 3.1, we need to consider the cases $j = 0$ and $j = 1$. The recurrence relation satisfied by the even-index and odd-index Fibonacci subsequences is $F_{2n+4+\epsilon} = 3F_{2n+2+\epsilon} - F_{2n+\epsilon}$, where $\epsilon \in \{0, 1\}$. Thus, we set $\tilde{a}_1 = 3$. Using the notation of the theorem, we also have that $\tilde{\Delta} = \tilde{a}_1^2 - 4 = 9 - 4 = 5$, and thus $\delta = \sqrt{5}$, and lastly $\tilde{N}_0 = F_4F_0 - F_2^2 = -1$, and $\tilde{N}_1 = F_5F_1 - F_3^2 = 1$.

Likewise, we calculate $\eta_{\sqrt{5},\varphi^2}(x)$: We represent degree-one functions in a matrix form, relying on the well-known fact that the product of these matrices corresponds to the composition of the functions. We have that $\mu_{\sqrt{5}}(x) = \frac{x+\sqrt{5}}{x-\sqrt{5}}$ and $\mu_{\sqrt{5}}^{-1}(x) = \sqrt{5}\frac{x+1}{x-1}$. Thus, corresponding to the composition $\mu_{\sqrt{5}}^{-1} \circ (\varphi^2 x) \circ \mu_{\sqrt{5}}$ is the product:

$$\begin{pmatrix} \sqrt{5} & \sqrt{5} \\ 1 & -1 \end{pmatrix} \begin{pmatrix} \varphi^2 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \sqrt{5} \\ 1 & -\sqrt{5} \end{pmatrix} = \begin{pmatrix} \varphi^2\sqrt{5} & \sqrt{5} \\ \varphi^2 & -1 \end{pmatrix} \begin{pmatrix} 1 & \sqrt{5} \\ 1 & -\sqrt{5} \end{pmatrix} = \begin{pmatrix} (\varphi^2+1)\sqrt{5} & 5(\varphi^2-1) \\ \varphi^2-1 & (\varphi^2+1)\sqrt{5} \end{pmatrix}.$$

We finish the calculation by noting that this matrix defines the composition up to a scalar multiple. Thus, dividing the entire matrix by $\varphi = \varphi^2 - 1$, and noting that $(\varphi^2+1)/\varphi = \varphi + \varphi^{-1} = \sqrt{5}$, we can see that the compositon $\eta_{\sqrt{5},\varphi^2}(x) = (5x+5)/(x+5)$.

Lastly, we calculate $q_{-1}(x) := q_0(x)$ and $q_1(x)$:

$$q_1(x) = \frac{F_0(x^2+\tilde{\Delta}) - (4F_2 - 2\tilde{a}_1F_0)x}{x^2-\tilde{\Delta}} = \frac{-4x}{x^2-5},$$

and

$$q_{-1}(x) = \frac{F_1(x^2+\tilde{\Delta}) - (4F_3 - 2\tilde{a}_1F_1)x}{x^2-\tilde{\Delta}} = \frac{x^2+5-(8-6)x}{x^2-5}.$$

All that is left is a straightforward application of the theorem, and the following remarks: We note that when d is even, $\frac{\tilde{N}_j}{\tilde{\Delta}\alpha^d} = \pm(5\alpha^d)^{-1}$ is never a square, and so the Dickson polynomials of even degree do not appear in the theorem and we may only consider odd d for this case. Thus, per Remark 3.2, we can both forgo the ± sign, and take $\alpha = 5/N_j$. More explicitly, we take $\alpha = -5$ whenever there are infinitely many even indexed Fibonacci numbers in the image of ϕ, and $\alpha = 5$ when there are infinitely many odd indexed Fibonacci numbers in the image. □

Chapter 4: Reducibility of $R_n(x) - a$ and $D_n(x) - a$

Throughout this chapter let K be a field of characteristic 0, let $\delta \in \bar{K}^\times$ be such that $\delta^2 \in K$, let $\alpha \in K^\times$ and let $n \in \mathbb{N}$ be a natural number. We sometimes write $R_n(x) = R_{\delta,n}(x)$ for the Rédei function, and $D_n(x) = D_{\alpha,n}(x)$ for the Dickson polynomial.

The purpose of this chapter is to prove the following two theorems:

Theorem 4.1. *Suppose that the numerator of $R_n(x) - a \in K(x)$ is reducible over K for some $a \in K$. Then either*

- *$a = R_p(b)$ for some $p \mid n$ and $b \in K$, or*
- *$4 \mid n$, and $a = \eta_{-4}(R_4(b))$ for some $b \in K[\delta]$.*

Theorem 4.2. *Suppose that $D_{\alpha,n}(x) - a \in K[x]$ is reducible over K for some $a \in K$. Then either*

- *$a = D_{\alpha^{n/p},p}(b)$ for some $p \mid n$ and $b \in K$, or*
- *$4 \mid n$, and $a = -\frac{1}{4}D_{2\alpha^{n/4},4}(b)$ for some $b \in K$.*

Remark 4.3. The converses of both theorems hold. The first cases of each theorem imply reducibility due to the fact that $R_{\delta,n}(x) = R_{\delta,p} \circ R_{\delta,n/p}(x)$ and $D_{\alpha,n}(x) = D_{\alpha^{n/p},p} \circ D_{\alpha,n/p}(x)$.

To see that the second case implies reducibility for the Rédei functions, we refer the reader to Appendix A.2, for a computation of the decomposition of (the numerator of)

$R_{\delta,4}(x) - \eta_{\delta,-4} R_{\delta,4}(y)$ over $K[\delta]$. To demonstrate reducibility in the second case for the Dickson polynomials, we first note that $D_{\alpha,4}(x) = 16x^4 - 16\alpha x^2 + 2\alpha^2$, and therefore

$$\begin{aligned} D_{\alpha,4}(x) + \frac{1}{4} D_{2\alpha,4}(y) &= 16x^4 - 16\alpha x^2 + 4\alpha^2 - 8\alpha y^2 + 4y^4 \\ &= 4(2x^2 + 2xy + y^2 - \alpha)(2x^2 - 2xy + y^2 - \alpha) \in K[x]. \end{aligned}$$

Remark 4.4. The reducibility of $R_4(x) - \eta_{-4} R_4(y)$ is a twisted version of the fact that

$$x^4 + 4y^4 = (x^2 - 2xy + 2y^2)(x^2 + 2xy + 2y^2).$$

We begin the proof of Theorem 4.1 by starting with the simple cases $n = p$ and $n = 4$:

Lemma 4.5. *Let p be a prime, and suppose that $R_p(x) - a \in K(x)$ is reducible. Then $a = R_p(b)$ for some $b \in K$.*

Proof. We first treat the case where a is ramified under $R_p(x)$. This occours only for $a = \pm\delta$, in which case, since we assumed $a \in K$, we can simply take $b = a$, as both ramification points are fixed points of $R_p(x)$.

If a is unramified, consider a decomposition group D of the splitting field of $R_p(x) - t$ at $t \to a$. Proposition 2.54, describes the monodromy group of $R_p(x)$, and says that D is a subgroup of $\mathrm{AGL}_1(\mathbb{Z}_p)$, and that its action on the roots of $R_p(x) - t$ is induced by the action of $\mathrm{AGL}_1(\mathbb{Z}_p)$ on $\{0, \ldots, p-1\}$. Since $t \to a$ is unramified, D is also the Galois group of the splitting field of $R_p(x) - a$ over K. By the reducibility assumption, D must act intransitively on the roots of $R_p(x) - a$ in the splitting field. Thus, by Lemma 2.5, there must be a root which is fixed by the action of D. This fixed point is a root $b \in K$ of $R_p(x) - a$, in particular $a = R_p(b)$. □

Lemma 4.6. *If the numerator of $R_4(x) - a \in K(x)$ is reducible over K, then either*

1. *$a = R_2(b)$ for some $b \in K$, or*

2. *$a = \eta_{-4}(R_4(b))$ for some $b \in K[\delta]$.*

Proof. As before, we start by treating the case where a is a ramification point of $R_4(x)$. Again, this is happens only for $a = \pm\delta$, in which case $a = R_2(a)$.

From now on assume $R_4(x)$ is unramified at a. Let $\xi = \mu^{-1} i = i\delta$ denote the primitive pole of $R_4(x)$, where $i = \sqrt{-1}$.

We first treat the case where $\xi \in K$. In this case, all the finite poles of $R_4(x)$ lie in K. Then the degree 4 extension $K(z)/K(t)$ defined by $t = R_4(z)$ is the splitting field of $R_4(x) - t$, and has Galois group $\mathbb{Z}_4$. A decomposition group D at $t \to a$ is a subgroup of $\mathbb{Z}_4$, which, by the reducibility assumption, acts intransitively on the roots of $R_4(x) - t$. Thus, it must be a subgroup of $\mathbb{Z}_2$. If $D = 1$ is trivial, then all the roots of $R_4(x) - a$ are in K, and for any such root $\bar{z}$ we can set $b = R_2(\bar{z})$, yielding $R_2(b) = R_2(R_2(\bar{z})) = a$. Otherwise, let $\tau \in \mathbb{Z}_4$ be the generator of $\mathrm{Gal}\left({}^{K(z)}/_{K(t)}\right)$ given by $\tau z = \eta_i z$ (see Lemma 2.52). Then $D = \{1, \tau^2\}$. By Lemma 2.35, we can compute $\tau^2 z = \eta_{-1} z = \delta^2/z$. Let $\bar{z} \in \bar{K}$ be some root of $R_4(x) - a$, for which D is the decomposition group of $z \to \bar{z}$. Then the Galois group of $K[\bar{z}]/K$ is D, with $\tau^2 \bar{z} = \delta^2/\bar{z}$. Then, $b = R_2(\bar{z}) = \bar{z} + \delta^2/\bar{z} \in K$, and we have that $R_2(b) = R_4(\bar{z}) = a$.

For the rest of this proof, assume that $\xi \notin K$. Again, consider the field extension $K(z)/K(t)$ defined via $t = R_4(z)$.

$$\begin{tikzcd}
& K(z,\xi) \arrow[dl, dash, "4"'] \arrow[dr, dash, "2"] & \\
K(\xi,t) \arrow[dr, dash, "2"'] & & K(z) \arrow[dl, dash, "4"] \\
& K(t) &
\end{tikzcd}$$

Since $\xi \notin K$, the Galois group of $R_4(x) - t$ is a subrgoup of $\mathrm{AGL}_1(\mathbb{Z}_4)$ which contains both $\mathbb{Z}_4$ and the automorphism sending ξ to $-\xi$. Thus, it must be of order at least 8, and therefore be all of $\mathrm{AGL}_1(\mathbb{Z}_4)$. Again, due to reducibility assumption, a decomposition group D at $t \to a$ must act intransitively on the roots of $R_4(x) - a$.

Now, D either does or does not act transitively on the roots of $R_2(x) = a$. By Proposition 2.55, this is equivalent to acting transitivily mod 2. If it does not act transitively, then as in the previous lemma, it must have some fixed point, which gives a root of $R_2(x) - a$ over K. If however the action is transitive mod 2, then by Corollary 2.9, we have that D must be conjugate to the subgroup generated by the involution $\tau = -x + 1$. Since D is defined up to conjugation, we may without loss of generality assume equality. The residue degree at $t \to a$ must be at least two, as $[K(\xi) : K] = 2$. As D is of order two, the residue degree must be in fact equal to two. Therefore, if we pick some root $\bar{z} \in \bar{K}$ of $R_4(x) - a$, then $K(\xi, \bar{z}) = K(\xi)$. In particular, $\bar{z} \in K(\xi)$. Observe that both $\bar{z}\tau\bar{z}$ and $\bar{z} + \tau\bar{z}$ are preserved by the action of D, hence both belong to K.

Recall (Lemma 2.52) that τ acts as $\tau z = \eta_i(z)$, where $i = \sqrt{-1}$, and the same holds for $\bar{z}$. Applying μ to both sides, this means that $\mu(\tau\bar{z}) = \mu(i\bar{z})$.

We shall show that $\eta_{1+i}(\bar{z})$ is defined over $K[\delta]$. We can see that this is the case by applying Lemma 2.31 to the last term in the following equation:

$$\begin{aligned}
\eta_{1+i}\bar{z} &= \mu^{-1}((1+i)\mu(\bar{z})) && \text{Definition 2.33} \\
&= \mu^{-1}(\mu(\bar{z}) + i\mu(\bar{z})) \\
&= \mu^{-1}(\mu(\bar{z}) + \mu(\tau\bar{z})) \\
&\in K[\delta, \bar{z}\tau\bar{z}, \bar{z} + \tau\bar{z}] && \text{Lemma 2.31 (3)} \\
&= K[\delta].
\end{aligned}$$

Thus, we define $b = \eta_{1+i}(\bar{z}) \in K[\delta]$. Finally, by Lemma 2.36, we find that $R_4(b) = R_4(\eta_{(1+i)}(\bar{z})) = \eta_{-4}R_4(\bar{z}) = a$ shows the result. □

We now turn to the proof of the general case:

Proof of Theorem 4.1. Indeed, suppose that the numerator of $R_n(x) - a \in K(x)$ is reducible over K. Consider the extension $K(z)$ of $K(t)$ defined by $t = R_n(z)$. Write $\Omega = F_n(z)$ for the Galois closure of $R_n(x) - t$, and G for its Galois group. Again, $t \to a$ is ramified in this extension if and only if $a = \pm\delta$, in which case $a = R_p(a)$ for any $p \mid n$.

From now on assume that $t \to a$ is unramified. Since the numerator of $R_4(x) - a$ is reducible, a decomposition group $D \leq G \leq \mathrm{AGL}_1(\mathbb{Z}_n)$ at $t \to a$ must act intransitively on the roots of $R_n(x) - t$. Again, this action is isomorphic with the action induced by $\mathrm{AGL}_1(\mathbb{Z}_n)$ acting on $\{0, \ldots, n-1\}$. By Lemma 2.12, we can assume that D acts intransitively mod p, for some $p \,|\, n$, or that $4 \,|\, n$ and D acts intransitivily mod 4. By Proposition 2.55, the fixed field of $G \cap \ker q_{n,n'}$ is the splitting field of $R_{n'}(x) - t$. Now, $q_{n,n'}(D) \leq \mathrm{AGL}_1(\mathbb{Z}_{n'})$ is a decomppposition group at $t \to a$ of the extension $\Omega^{G \cap \ker q_{n,n'}}/K(t)$. Intransitivity of the action mod n' means that the numerator of $R_{n'}(x) - t$ is reducible. Thus we reduce to the cases where $n = p$ or $n = 4$, which are treated by Lemmas 4.5 and 4.6 respectively, yielding the result. □

The proof for Theorem 4.2 follows much of the same ideas. We start by considering the cases where $n = p$ and $n = 4$:

Lemma 4.7. *Let p be a prime, and suppose that $D_{\alpha,p}(x) - a \in K[x]$ is reducible over K. Then $a = D_{\alpha,p}(b)$ for some $b \in K$.*

Proof. The case $p = 2$ is trivial, as a quadratic function may only factor into linear factors, giving a rational root.

From now on we assume that $p > 2$. Again, we first treat the case where a is a branch point of $D_{\alpha,p}(x)$. This implies $a = \pm 2\alpha^{p/2} \in K$. Since p is odd, we have that $\alpha^{1/2} \in K$, in which case

$$2\alpha^{p/2} = D_{\alpha,p}(\alpha^{1/2} + \alpha/\alpha^{1/2}),$$

and

$$-2\alpha^{p/2} = D_{\alpha,p}((-\alpha)^{1/2} + \alpha/(-\alpha^{1/2}) = D_{\alpha,p}(0)$$

yield approprirate $b \in K$.

Now, assume that a is not a branch point of $D_{\alpha,p}(x)$. Consider the extension ${}^{K(z)}/_{K(t)}$ defined by $t = D_p(z)$, and let Ω denote its Galois closure. By Proposition 2.58, it has Galois group $G \leq \mathrm{AGL}_1(\mathbb{Z}_p)$. Since the specialization of $D_{\alpha,p}(x) - t$ at $t \to a$ is reducible, a decomposition group $D \leq \mathrm{AGL}_1(\mathbb{Z}_p)$ at $t \to a$ must act intransitively on the roots of $R_p(x) - a$. Then by Lemma 2.5, there must be a root of $R_p(x) - a$ which is fixed under the action of D, which gives a rational $b \in K$ such that $a = R_p(b)$. □

Lemma 4.8. *If $D_{\alpha,4}(x) - a$ is reducible over K, then either*

1. $a = D_{\alpha^2,2}(b)$ *for some* $b \in K$, *or*

2. $a = -\frac{1}{4}D_{2\alpha,4}(b)$ *for some* $b \in K$.

Proof. Again, we first treat the case where a is a branch point of $D_{\alpha,4}(x)$. This is the case only for $a = \pm 2\alpha^2$. Then the computations

$$2\alpha^2 = D_{\alpha^2,2}(\alpha + \alpha^2/\alpha),$$

and

$$-2\alpha^2 = D_{\alpha^2,2}(i\alpha + \alpha^2/(i\alpha)) = D_{\alpha^2,2}(0)$$

provide appropriate $b \in K$.

Now assume that a is not a branch point of $D_{\alpha,4}(x)$. Again, let $K(z)$ be the extensnion of $K(t)$ given by $t = D_{\alpha,4}(z)$, and let Ω be its Galois closure, which again has Galois group $G \leq \mathrm{AGL}_1(\mathbb{Z}_4)$.

Let D be a decomposition group over $t \to a$. Again, due to the reducibility assumption, D acts intransitively on the roots of $D_{\alpha,4}(x) - a$. Since a is unramified, there are exactly 4 roots which correspond to $\{0, \dots, 3\}$ under the action of G.

Now, D either does or does not act transitively modulo two (i.e., when factored through the quotient morphism $\mathrm{AGL}_1(\mathbb{Z}_4) \to \mathrm{AGL}_1(\mathbb{Z}_2)$). If it does not act transitively mod two, we again have that a decomposition group for $\Omega^{\ker q_{4,2}}$ (which is the splitting field of $D_{\alpha^2,2}(x) - t$) must have a fixed point. The specialization of this fixed point is a root of $D_{\alpha^2,2}(x) - a$ which belongs to K.

If D *does* act transitively modulo two, it is conjugate to $\langle -x + 1\rangle$ by Corollary 2.9. Without loss of generality we may assume equality. Write σ for the unique non-identity element of D. Let us work in the larger field $\Omega(v, i)$, defined by $z = v + \alpha/v$ and $i^2 = -1$, and extend σ to this larger field via $\sigma v = iv$, as in the proof of Proposition 2.58.

We compute $\sigma z = iv + \alpha/iv$, and note that $t = v^4 + \alpha^4/v^4$. The group D preserves the set $\{z, \sigma z\}$, and thus also preserves the sum

$$B := z + \sigma z = (1+i)v + \frac{(1-i)\alpha}{v} = (1+i)v + \frac{2}{(1+i)v}.$$

Now, clearly

$$D_{2\alpha,4}(B) = -4v^4 + 2^4/(-4v^4) = -4(v^4 + \alpha^4/v^4) = -4t,$$

and hence $b = \bar{B} \in K$ satisfies $D_{2\alpha,4}(b) = -4a$, as desired. □

We now turn to the proof of the general case:

Proof of Theorem 4.2. Again we begin with special treatment for the branch points. If n is odd, then $a = \pm 2\alpha^{n/2} \in K$ implies that $\alpha^{1/2} \in K$, and as in the odd prime case $2\alpha^{n/2} = D_{\alpha,n}(2\alpha)$ and $-2\alpha^{n/2} = D_{\alpha,n}(0)$. By Remark 2.57, which states that $D_{\alpha,n}(x) = D_{\alpha^{n/p},p} \circ D_{\alpha,n/p}(x)$, we are done.

Now, if n is even and $p \,|\, n$ is an odd prime, then again

$$2\alpha^{n/2} = D_{\alpha^{n/p},p}(2\alpha^{n/2p})$$

and

$$-2\alpha^{n/2} = D_{\alpha^{n/p},p}(0)$$

provide appropriate $b \in K$. The case $n = 2$ was treated in the previous lemma. Lastly, if $n > 2$ is a power of 2, then $\alpha^{n/4} \in K$ and the idenities

$$2\alpha^{n/2} = D_{\alpha^{n/2},2}(2\alpha^{n/4})$$

and

$$-2\alpha^{n/2} = D_{\alpha^{n/2},2}(0)$$

provide appropriate $b \in K$.

From now on we assume that a is not a branch point of $D_{\alpha,n}(x)$. As before, consider the extension $K(z)$ of $K(t)$ defined $t = D_{\alpha,n}(z)$, and its Galois closure Ω, and its Galois group $G \leq \mathrm{AGL}_1(\mathbb{Z}_n)$. Since the specialization at $t \to a$ is reducible, a decomposition group $D \leq G$ at $t \to a$ must act intransitively on the roots of $R_n(x) - a$.

By Lemma 2.12, it follows that D acts intransitively modulo p for some $p \,|\, n$, or modulo 4, in which case $4 \,|\, n$. By Proposition 2.55, the fixed field of $G \cap \ker q_{n,n'}$ is the splitting field of $D_{\alpha^{n/n'},n'}(x) - t$. Now, $q_{n,n'}(D) \leq \mathrm{AGL}_1(\mathbb{Z}_{n'})$ is a decomposition group at $t \to a$ of the extension $\Omega^{G \cap \ker q_{n,n'}}/K(t)$. Intransitivity of the action modulo n' means that the polynomial $D_{\alpha^{n/n'},n'}(x) - a$ is reducible, and we may reduce to the cases where $n = p$ or $n = 4$, which are treated by Lemmas 4.7 and 4.8 respectively, yielding the result. □

Chapter 5: Polynomials reducible at infinitely many values of a recurrence sequence

As in Chapter 3, let K be a number field, and let $(r_n)_{n\in\mathbb{Z}}$ be a rank-two recurrence sequence satisfying $r_{n+2} = a_1 r_{n+1} + a_2 r_n$, in which $a_1 \in K$ and $a_2 = -\zeta \in K$ where ζ is an m-th root of unity. Likewise, recall our notations $\tilde{N}_j = r_{2m+j} r_j - r_{m+j}^2$ and $\tilde{\Delta} = D_{\zeta,m}(a_1)^2 - 4$, where $D_{\zeta,m}(x)$ is the degree-m Dickson polynomial with parameter ζ.

Recall that we are interested in describing the irreducible polynomials $P(t, x) \in K(t)[x]$ for which the specializations $P(r_n, x) \in K[x]$ are reducible for infinitely many $n \in \mathbb{Z}$. Due to Hilbert's irreducibility theorem, it suffices to classify all such $P(t, x)$ for which $P(\phi(z), x) \in K(z)[x]$ is reducible for some rational function $\phi(z) \in K(z)$ whose image contains infinitely many numbers from $\{r_n \mid n \in \mathbb{Z}\}$. Now that Theorem 3.1 classifies all such functions $\phi(x)$, we describe the irreducible polynomials $P(t, x)$ for which $P(\phi(z), x) \in K(z)[x]$ become reducible for one of those ϕ's. Therefore, we will split the proof along the two cases given in Theorem 3.1: The case where ϕ is linearly equivalent to a Dickson polynomial, and the case where ϕ is the composition of a degree-two function with a Rédei function $R_{\delta,n}(z)$. These cases are treated in Proposition 5.3 and Proposition 5.4, respectively. The combined description is given in the following theorem.

Given a recurrence sequence satisfying the recurrence relation $r_{n+2} = a_1 r_{n+1} + a_2 r_n$, let φ be a root of the recurrence sequence, i.e., a solution to $x^2 = a_1 x + a_2$. Restrict to the case where $a_2 = -\zeta$, where ζ is an m-th root of unity. Let $\tilde{\Delta}$ and $\tilde{N}_j$ be as defined at the start of the chapter, let $\delta = \sqrt{\tilde{\Delta}}$, and define, as in Theorem 3.1,

$$q_j(x) = \frac{r_j(x^2 + \tilde{\Delta}) - (4r_{m+j} - 2\tilde{a}_1 r_j)x}{x^2 - \tilde{\Delta}} \in K(x)$$

for $i = 0, \dots, m-1$,

$$\mu_\delta(x) = \frac{x+\delta}{x-\delta}, \quad R_{\delta,n}(x) = \mu_\delta^{-1}(\mu_\delta(x)^n), \quad \eta_{\delta,c}(x) = \mu_\delta^{-1}(c\mu_\delta(x)).$$

Theorem 5.1. *Let K be a number field, and let $r_{n+2} = a_1 r_{n+1} + a_2 r_n$ be a recurrence sequence with $a_1 \in K$ and $a_2 = -\zeta \in K$, where ζ is an m-th root of unity. Assume that both $\tilde{\Delta}$ and all the subsequence norms (c.f. Chapter 3) $\tilde{N}_j$ are not 0, for $0 \leq j < m$.*

Now, suppose that $P(t,x) \in K(t)[x]$ is an irreducible polynomial over $K(t)$ such that the specializations $P(r_n, x) \in K[x]$ are reducible for infinitely many $n \in \mathbb{Z}$. Let X_P be the projective variety defined by $P(t,x) = 0$ and denote by $\pi_x : X_P \to \mathbb{P}^1$ the projection to the x-coordinate. Then either

1. *π_x factors as $q_j \circ \pi'$ for some $\pi' : X_P \to \mathbb{P}^1$ defined over K, or*

2. *π_x factors as $\pm\alpha^{-(p+1)/2} D_{\alpha,p} \circ \pi'$ for some $\pi' : X_P \to \mathbb{P}^1$ defined over K, and some odd prime $p \,|\, \deg_x P$ and where $\alpha = \sqrt{\frac{\tilde{\Delta}}{\tilde{N}_j}}$ whenever this value belongs to K, or*

3. *π_x factors as $\pm\sqrt{\frac{\tilde{N}_j}{\tilde{\Delta}\alpha^d}} D_{\alpha,d} \circ \pi'$ for some $\pi' : X_P \to \mathbb{P}^1$ defined over K, and where $d = 2$ or 4, and for some $\alpha \in K$ such that $\tilde{N}_j / \tilde{\Delta}\alpha^d$ is a square in K, or*

4. *the pullback $q_j^* \pi_x$ factors as $\eta_{\delta,\varphi^{mk}} \circ R_{\delta,p} \circ \pi'$ for some $\pi' : X_P \to \mathbb{P}^1$ defined over K, and some prime $p \,|\, \deg_x P$, and for some $k < p$, or*

5. *the pullback $q_j^* \pi_x$ factors as $\eta_{\delta,-4\varphi^{mk}} \circ R_{\delta,4} \circ \pi'$ for some $\pi' : X_P \to \mathbb{P}^1$ defined over $K[\delta]$ and for some $k < 4$, when $4 \,|\, \deg_x P$,*

for some $0 \leq j < m$. Moreover, for this particular j, there are infinitely many elements of the form r_{mn+j} in $\mathrm{Red}_P(K)$.

Remark 5.2. As shown in Remark 3.8, the converse statement holds for functions of the form 1, and for functions of the form 2 or 3 for particular sequences and particular values of α. For the other forms we do not know whether the converse holds and intend to tackle the question in future work.

We begin the proof for the case where $\phi(x)$ is linearly related to a Dickson polynomial.

Proposition 5.3. *Let $\phi(z) = C\alpha^{-n/2}D_{\alpha,n}(\ell(z))$ for some $C, \alpha \in K$ and $\ell(z)$ a rational degree-one function. Suppose $P(t,x) \in K(t)[x]$ is an irreducible polynomial over $K(t)$ such that $P(\phi(z), x) \in K(z)[x]$* is *reducible over $K(z)$, where this is the extension of $K(t)$ defined by $\phi(z) = t$. As before, let X_P be the projective variety defined by $P(t,x) = 0$ and let $\pi_x : X_P \to \mathbb{P}^1$ be the projection to the x-coordinate. Then the projection $\pi_x : X_P \to \mathbb{P}^1$ factors as either*

- *$C\alpha'^{-p/2}D_{\alpha',p} \circ \pi'$ for some $\pi' : X_P \to \mathbb{P}^1$ and some prime $p \mid n$, and where $\alpha' = \alpha^{n/p}$, or as*
- *$-\frac{C}{\alpha'^2}D_{\alpha',4} \circ \pi'$ for some $\pi' : X_P \to \mathbb{P}^1$, and where $\alpha' = 2\alpha^{n/4}$, and $4 \mid n$.*

Proof. We may assume without loss of generality that $\ell(z) = z$, since two polynomials which differ by a degree-one map will be reducible or irreducible simultaneously, and this change of variables would only amount to a similar change of variables in the input of the resulting π'. Consider the following field diagram, in which we describe the field extensions defined by $\phi(z) = t$ and $P(t,x) = 0$.

$$\begin{tikzcd}
 & K(z,x) \arrow[dl, dash] \arrow[dr, dash] & \\
K(z) \arrow[dr, dash] & & K(t,x) \arrow[dl, dash] \\
 & K(t) &
\end{tikzcd}$$

The fact that $P(\phi(z), x)$ is reducible over $K(z)$, but not over $K(t)$, implies that the extension obtained via adjoining to $K(z)$ an x which satisfies $P(\phi(z), x) = 0$ will have smaller rank than the extension obtained via adjoining to $K(t)$ such an x. That is,

$$[K(z,x) : K(z)] < [K(t,x) : K(t)],$$

which in turn implies that

$$[K(z,x) : K(t,x)] < [K(z) : K(t)],$$

i.e., that (the numerator of) $\phi(Z) - t \in K(t)[Z]$ is reducible over $K(t,x)$. Now, since ϕ is linearly related to a Dickson polynomial we can apply Theorem 4.2 over the field $K(t)$ and setting $a = t$. We find that $t = C\alpha^{-n/2} D_{\alpha^{n/p},p}(b)$ for some prime $p \mid n$, some $b \in K(t,x)$, or that $t = -\frac{C}{4\alpha^{n/2}} D_{2\alpha^{n/4},4}(b)$. Rewrite with $\alpha' = \alpha^{n/p}$ or $2\alpha^{n/4}$ to get that either $t = C\alpha'^{-p/2} D_{\alpha',p}(b)$ or $t = -C\alpha'^{-2} D_{\alpha',4}(b)$ for some $b \in K(t,x)$. This implies that π_x factors through these functions. Clearly, in this case p (or 4, respectively) divides $\deg \pi_x = \deg_x P$.

$$\begin{tikzcd}
 & K(z,x) \arrow[dl, dash] \arrow[dr, dash] & \\
K(z) \arrow[ddr, dash] & & K(t,x) \arrow[dl, dash] \arrow[ddl, dash] \\
 & K(b) \arrow[d, dash] & \\
 & K(t) &
\end{tikzcd}$$

□

We now turn to the case where ϕ is linearly related to the composition of a quadratic map and a Rédei function.

Proposition 5.4. *Let $\phi(z) = q(R_{\delta,d}(\ell(z)))$ for arbitrary degree-one and degree-two maps $\ell(x), q(x) \in K(x)$, and some $\delta^2 \in K$.*

Suppose $P(t,x) \in K(t)[x]$ is an irreducible polynomial over $K(t)$ such that $P(\phi(z),x) \in K(z)[x]$ is reducible *over $K(z)$. As before, let X_P be the projective variety defined by $P(t,x) = 0$ and let $\pi_x : X_P \to \mathbb{P}^1$ be the projection to the x-coordinate. Let*

$P_q(z,x) = P(q(z),x) \in K(z)[x]$. *Observe that the variety defined by* $P_q(t,x) = 0$ *is birational to the pullback along* $q : \mathbb{P}^1 \to \mathbb{P}^1$ *of* X_P*. Let* $q^*\pi_x : q^*X_P \to \mathbb{P}^1$ *be the pullback of the projection* π_x *along* q*.*

Then either

- $\pi_x = q \circ \pi'$ *for some* $\pi' : X_P \to \mathbb{P}^1$ *defined over* K*, or*

- $q^*\pi_x = R_{\delta,p} \circ \pi'$ *for some* $\pi' : q^*X_P \to \mathbb{P}^1$ *defined over* K*, and for some prime* $p \mid \deg_x P$*, or*

- $q^*\pi_x = \eta_{\delta,-4} \circ R_{\delta,4} \circ \pi'$ *for some* $\pi' : q^*X_P \to \mathbb{P}^1$ *defined over* $K[\delta]$ *and* $4 \mid \deg_x P$*.*

Remark 5.5. We remark that the function $\eta_{\delta,-4}(x) = (3\delta x + 5\delta^2)/(5x + 3\delta^2)$ is defined over $K[\delta]$.

Proof. As in the proof of Proposition 5.3, we may assume $\ell(z) = z$, since a linear change in variables does not affect reducibility. We begin by showing that (since q is a degree-two map) π_x factors through $q(w)$ if and only if $P_q(w,x)$ is reducible over $K(w)$: Indeed, let

$$K(X_P) = K(t,x) \subset K(q^*X_P) = K(w,x)$$

denote the corresponding function fields, where we have $t = q(w)$. The polynomial $P(q(w),x)$ is reducible over $K(w)$ if and only if $[K(w,x) : K(w)] < \deg_x P$, which, in view of the diagram below holds if and only if $[K(w,x) : K(t,x)] < 2$, i.e., if and only if $K(w,x) = K(t,x)$. This holds if and only if $K(w) \subset K(t,x)$, which is the field-theoretic reformulation of the factoring claim.

$$\begin{tikzcd}
& K(w,x) \arrow[dl, dash, "\deg_x P >"'] \arrow[dr, dash, "2 >"] & \\
K(w) \arrow[dr, dash, "2"'] & & K(t,x) \arrow[dl, dash, "\deg_x P"] \\
& K(t) &
\end{tikzcd}$$

Thus, from now on, suppose that $P_q(w,x)$ is irreducible. However, by our assumption, $P_q(R_{\delta,n}(z),x)$ *is* reducible over $K(z)$. By the same logic as in the proof for the Dickson case, this is equivalent to the numerator of $R_{\delta,n}(Z)-w \in K(w,x)(Z)$ being reducible over $K(w,x)$. By Theorem 4.1, the reducibility of the numerator $R_n(z)-w$ implies that $w = R_p(b)$ for some prime $p \,|\, n$ and some $b \in K(w,x)$, or that $w = \eta_{-4}R_4(b)$ for some $b \in K(\delta,w,x)$, in which case $4 \,|\, n$. The diagram below depicts the case where $w = R_p(b)$. Either way, in both cases this implies the prescribed factorization of π_x as described in the theorem.

$$\begin{tikzcd}
 & K(z,x) \arrow[dl, dash] \arrow[dr, dash] & & \\
K(z) \arrow[ddr, dash] & & K(w,x) \arrow[dl, dash] \arrow[ddl, dash] \arrow[ddr, dash] & \\
 & K(b) \arrow[d, dash] & & \\
 & K(w) \arrow[dr, dash] & & K(t,x) \arrow[dl, dash] \\
 & & K(t) &
\end{tikzcd}$$

As for the divisibility claim: In the prime case, clearly $p \,|\, \deg \pi_x = \deg_x P$. However, in the case where π_x factors through $R_4(x)$ over $K[\delta]$ we find that 4 divides $[K(\delta,w,x) : K(\delta,w)]$. If $\delta \notin K(w,x)$, this quantity equals $[K(w) : K(w,x)]$, which (by our assumption of irreducibility with q) is equal to $\deg \pi_x$. If $\delta \in K(w,x)$, we find that (in view of the diagram below):

$$\begin{aligned}
4 \,|\, &[K(\delta,w,x) : K(\delta,w)] \\
&\,|\, [K(\delta,w,x) : K(w)] \\
&= [K(w,x) : K(w)] \\
&= \deg \pi_x,
\end{aligned}$$

which finishes the proof.

$$\begin{tikzcd}
& K(w,x) = K(\delta,w,x) \arrow[dl, dash] \arrow[dd, dash] \\
K(\delta,w) \arrow[dr, dash, "2"'] & \\
& K(w)
\end{tikzcd}$$

□

We can now turn to the proof of the main theorem of this chapter:

Proof of Theorem 5.1. Indeed, by Hilbert's irreducibility theorem (Theorem 2.26), we have that

$$\mathrm{Red}_P(K) = \bigcup_i \phi_i(V_i(K)) \cup F$$

for a finite set F and a finitely many smooth projective ramified coverings $\phi_i : V_i \to \mathbb{P}^1$. Moreover, the theorem gives us that $P(\phi_i(v), x) \in K(V_i)[x]$ is reducible for all i. For at least one such i the image $\phi_i(V_i(K))$ will contain infinitely many elements from $\{r_n \mid n \in \mathbb{Z}\}$. Note that all these elements lie in the finitely generated subring of K generated by a_1, a_2, r_0 and r_1. Thus, by Siegel's theorem (Theorem 2.24), for this particular i we have that $V = V_i$ is birational with $\mathbb{P}^1$, and that $\phi = \phi_i$ is a rational function. By our choice of i, this function attains infinitely many elements from $\{r_n\}$.

Thus, by Theorem 3.1, we must have that for some $0 \leq j < m$, and some degree-one map $\ell(x) \in K(x)$, the function $\phi = \pm\sqrt{\frac{\tilde{N}_j}{\tilde{\Delta}\alpha^n}} D_{\alpha,n} \circ \ell$ or $\phi = q_j \circ \eta_c \circ R_{\delta,n} \circ \ell$ where $c = \varphi^k$ for some $0 \leq k < n$. We have that for this particular j, infinitely many of the values attained by $\phi(x)$ are of the form r_{nm+j}. These are, in particular, reducible values for $P(t,x)$,

The case where ϕ is linearly related to a Dickson polynomial is a direct application of Proposition 5.3, and the case where ϕ is the composition of a quadratic and a Rédei function is treated by Proposition 5.4, with $q = q_j \circ \eta_c$. Lastly, we note that $q_j^* \pi_x = \eta_c \circ q^* \pi_x$, yielding the result.

We remark that in the application of Proposition 5.3 we may freely ignore the sign differences in the two factorizations, as the constant in front of our Dickson polynomial is already defined only up to sign. Likewise, for the odd prime case we may set $\alpha = \tilde{\Delta}/\tilde{N}_j$ as in Remark 3.2. □

Lastly, we prove the theorem stated in the introduction, which is the special case of the Fibonacci sequence.

Proof of Theorem 1.3. As in the proof of Theorem 1.1, we have that $\zeta = -1$, that the roots of the recurrence sequence are the golden ratio $\varphi = (1+\sqrt{5})/2$ and its conjugate $-\varphi^{-1} = (1-\sqrt{5})/2$. Thus, we need to consider the cases $j = 0$ and $j = 1$. The same calculations from the proof of Theorem 1.1 yielded that $\tilde{a}_1 = 3$, $\tilde{\Delta} = 5$, $\delta = \sqrt{5}$, and that $\tilde{N}_0 = -1$ and $\tilde{N}_1 = 1$. Likewise, that $\eta_{\sqrt{5},\varphi^2}(x) = (5x+5)/(x+5)$, and that

$$q_0(x) = \frac{F_0(x^2+\tilde{\Delta}) - (4F_2 - 2\tilde{a}_1 F_0)x}{x^2-\tilde{\Delta}} = \frac{-4x}{x^2-5},$$

and

$$q_1(x) = \frac{F_1(x^2+\tilde{\Delta}) - (4F_3 - 2\tilde{a}_1 F_1)x}{x^2-\tilde{\Delta}} = \frac{x^2+5-(8-6)x}{x^2-5}.$$

We can now apply Theorem 5.1. Observe that since we assumed that $\deg_x P(t,x)$ is odd, we may discard the case where π_x factors through the quadratic maps $q_j(x)$ and the case where $q_j^*\pi_x$ factors through the degree-four map $R_{\delta,4}(x)$. □

Chapter A: Code

A.1 Verification of the parameterization in Lemma 3.12

Recall the parameterization for $V : y^2 = \Delta x^2 - 4N$ given in the lemma:

$$(x(w), y(w)) = \left(\frac{r_0 \cdot (w^2 + \Delta) - (4r_1 - 2a_1 r_0)w}{w^2 - \Delta}, \frac{(a_1 r_0 - 2r_1)w^2 + 2\Delta r_0 w + (a_1 r_0 - 2r_1)\Delta}{w^2 - \Delta} \right).$$

The following Python code evaluates the parameterization, showing that indeed $(x(w), y(w))$ gives a point on V for every w:

```
import sympy
a1, a2, r0, r1, w = sympy.symbols('a1, a2, r0, r1, w')
Delta = a1**2 + 4*a2
N = a2*r0**2 + a1*r0*r1 - r1*r1
x = (r0*(w**2 + Delta) - (4*r1 - 2*a1*r0)*w) /
                (w**2 - Delta)
y = ((a1*r0 - 2*r1)*w**2 + 2*Delta*r0*w
                                + (a1*r0 - 2*r1)*Delta) /
                (w**2 - Delta)
print((y**2 - Delta * x**2 + 4*N).simplify())
```

The code prints out 0.

A.2 Reducibility of $R_4(x) - \eta_{-4}R_4(y)$

The following Mathematica code shows that the numerator of $R_4(x) - \eta_{-4}R_4(y)$ is a reducible polynomial:

```
mu[x_] := (x + d)/(x-d)
muinv := InverseFunction[mu]
R[n_, x_]  := muinv[mu[x]^n]
eta[c_, x_] := muinv[c * mu[x]]
(R[4,x]-eta[-4,R[4,y]]) // Factor \
// Numerator // IrreduciblePolynomialQ
```

This code prints out the value False.

Further, the result of the following additional line:

```
(R[4,x] - eta[-4, R[4, y]]) // Factor // Numerator // FactorList
```

comes out to be:

```
{{1,1},
{d^4-2d^3x+5d^2x^2+2d^3y-12d^2xy+2dx^2y+5d^2y^2-2dxy^2+x^2y^2,1},
{5d^4-2d^3x+d^2x^2+2d^3y-12d^2xy+2dx^2y+d^2y^2-2dxy^2+5x^2y^2,1}}
```

which gives the decomposition.

Bibliography

[1] S. Lang. Division points on curves. *Annali di Matematica Pura ed Applicata*, 70(1):229–234, 1965.

[2] J. H. E. Cohn. On square fibonacci numbers. *Journal of the London Mathematical Society*, s1-39(1):537–540, 1964.

[3] Y. Bugeaud, M. Mignotte, and S. Siksek. Classical and modular approaches to exponential diophantine equations i. fibonacci and lucas perfect powers. *Annals of Mathematics*, 163(3):969–1018, 2006.

[4] Y. Bugeaud, F. Luca, M. Mignotte, and S. Siksek. Fibonacci numbers at most one away from a perfect power. *Elemente der Mathematik*, 63(2):65–75, 2008.

[5] P. M. Voutier. Bounds on the number of squares in recurrence sequences. *Journal of Number Theory*, 265:291–343, 2024.

[6] P. Corvaja and U. Zannier. Diophantine equations with power sums and universal hilbert sets. *Indagationes Mathematicae*, 9(3):317–332, 1998.

[7] I. Nemes and A. Pethö. Polynomial values in linear recurrences, ii. *Journal of Number Theory*, 24(1):47–53, 1986.

[8] A. Ostrov, D. Neftin, A. Berman, and R. Abed Elrazik. Polynomial values in fibonacci sequences. *Involve, a Journal of Mathematics*, 13:597–605, 2020.

[9] P. Dèbes and U. Zannier. Universal hilbert subsets. *Mathematical Proceedings of the Cambridge Philosophical Society*, 124(1):127–134, 1998.

[10] M. Filaseta and R. Wilcox. An explicit dense universal hilbert set. *Mathematical Proceedings of the Cambridge Philosophical Society*, 167(3):531–547, 2019.

[11] Y. Bilu. A note on universal hilbert sets. *Journal für die reine und angewandte Mathematik*, 479:195–204, 1996.

[12] M. Fried. On the sprindžuk-weissauer approach to universal hilbert subsets. *Israel Journal of Mathematics*, 51(4):347–363, 1985.

[13] P. Dèbes. On the irreducibility of the polynomials p(tm, y). *Journal of Number Theory*, 42(2):141–157, 1992.

[14] L. Bary-Soroker, D. Garzoni, and V. Matei. On the irreducibility of $f(2^n, 3^m, x)$ and other such polynomials. *Mathematische Zeitschrift*, 310(1), 2025.

[15] H. Stichtenoth. *Algebraic function fields and codes.* Springer-Verlag, 1993.

[16] M. E. Zieve and P. Müller. On ritt's polynomial decomposition theorems, 2008.

[17] P. Müller. Finiteness results for hilbert's irreducibility theorem. *Annales de l'institut Fourier*, 52(4):983–1015, 2002.

נתעניין בשאלה מי הם הפולינומים $P(t,x) \in \mathbb{Q}(t)[x]$ עבורם $P(r_n,x) \in \mathbb{Q}[x]$ פריק עבור אינסוף איברים מסדרה r_n. בחלק השני של עבודה זו נענה על השאלה הזו.

במקרה הדומה של הסדרה ההנדסית $G_n = \alpha^n$ שאלה זו נפתרה ע"י פייר דבס. הוא נתן איפיון גיאומטרי לפולינומים יוצאי הדופן, אלו שעבורם יש אינסוף נקודות פריקות מהסדרה: הם בדיוק אלו שנמשכים אחורה לפולינום פריק על ידי ההעתקות $x \mapsto x^p$ או $x \mapsto -4x^4$.

נקודת מבט נוספת על שאלה זו מגיעה מהמחקר של קבוצות הילברט אוניברסליות. אלו קבוצות $U \subset \mathbb{Q}$ המקיימות את התכונה שלכל פולינום אי פריק $P(t,x) \in \mathbb{Q}(t)[x]$, יש רק מספר סופי של ייחודים פריקים $P(u,x) \in \mathbb{Q}[x]$ עבור $u \in U$. בהרבה מקרים, קבוצת הערכים של סדרת נסיגה מהווה קבוצת הילברט אוניברסלית. עם זאת, קבוצת הערכים של סדרת נסיגה כללית מדרגה 2 אינה קבוצת הילברט אוניברסליות. למרות זאת, בעבודה זו אנחנו נראה כי הכשל הזה של אוניברסליות מוגבל במידת מה, ושהוא נובע מתנאים גיאומטריים היחודיים לסדרות דמויות-פיבונאצ'י. ספציפית, היא מוגבלת לאי אילו $P(t,x)$ אשר נמשכים לאחור לפולינום פריק על ידי פונקציות ראציונליות מסוימות.

תקציר

סדרת פיבונאצ'י היא אחת מסדרות הנסיגה המוכרות והנחקרות ביותר בתורת המספרים. היא נתונה על ידי ערכי ההתחלה $F_0 = 0$ ו־$F_1 = 1$, ומקיימת את כלל הנסיגה $F_{n+2} = F_{n+1} + F_n$.

ב־1964 הוכיח קון בשיטות אלמנטריות שהריבועים השלמים היחידים שמופיעים בסדרת פיבונאצ'י הם 0, 1 ו־144. בכך פתר שאלה שהייתה פתוחה זה מכבר. באותה הזדמנות הוא גם תיאר את כל איברי הסדרה שהם פעמיים ריבוע, וכן פתר את אותן השאלות עבור סדרת לוקס הנתונה על ידי ערכי ההתחלה $L_0 = 2$ ו־$L_1 = 1$, וכלל הנסיגה $L_{n+2} = L_{n+1} + L_n$. את המשוואות $F_n = x^p$ ו־$F_n = x^p \pm 1$ פתרו בוז'ו, מיניוט וסיקסק בעזרת כלים קלאסיים בתחום כגון תבניות לינאריות בלוגריתמים, כמו גם בעזרת רעיונות מהתורה של תבניות מודולריות, כשם שהשתמשו בהן בהוכחה של משפט פרמה האחרון. בכל המקרים הללו למשוואות יש רק מספר סופי של פתרונות שלמים. תוצאות חדשות יותר של ווטייה נותנות חסמים על מספר הריבועים השלמים בסדרות נסיגה נוספות מדרגה שתיים, כלומר שבהן כל איבר בסדרה תלוי בשני האיברים הקודמים בסדרה.

בחלק הראשון של עבודה זו, אנו נמשיך את המחקר של משוואות דיופנטיות המערבות סדרות נסיגה מדרגה שתיים. בהינתן סדרת נסיגה r_n המקיימת כלל נסיגה מדרגה 2, אנו נתאר את כל הפונקציות הראציונליות $\phi(x) \in \mathbb{Q}(x)$ עבורן יש אינסוף פתרונות $(n, x) \in \mathbb{Z} \times \mathbb{Q}$ למשוואה $R_n = \phi(x)$. בייחוד נתעניין בדוגמה של סדרת פיבונאצ'י, עבורה, למרות התוצאות שצוינו, ישנן $\phi(x)$ שתמונתן מכילה אינסוף ערכים מסדרת פיבונאצ'י.

בחלק השני של עבודה זו, אנו נחקור את בעיית הפריקות בערכים מסדרת נסיגה מדרגה שתיים: בהינתן פולינום $P(t, x) \in \mathbb{Q}(t)[x]$ ומספר רציונלי $t_0 \in \mathbb{Q}$, נתבונן בייחוד של P ב־t_0, כלומר בפולינום $P(t_0, x) \in \mathbb{Q}[x]$. אם $P(t, x)$ הוא אי-פריק מעל $\mathbb{Q}(t)$, אזי הייחודים $P(t_0, x) \in \mathbb{Q}[x]$ עלולים להישאר אי-פריקים מעל $\mathbb{Q}$, או להפך לפריקים. לדוגמה, אם ל־$P(t_0, x)$ יש שורש רציונלי $x \in \mathbb{Q}$, אזי הוא חייב להתפרק כמכפלה של רכיב לינארי ופולינום נוסף. אם כך, נתייחס לפריקות של הייחודים בתור גרסה עדינה יותר של פתירות. בעקבות זאת, בהינתן סדרה דמויית-פיבונאצ'י r_n,

עבודה זו נעשתה בהדרכתם של

פרופסור דני נפטין

מן הפקולטה למתמטיקה

הטכניון

ודוקטור אייל סובג

מן המחלקה למתמטיקה

אוניברסיטת בר-אילן

המחלקה למתמטיקה
בדרך שלנו התוצאה שלך מוכחת!

אוניברסיטת
בר־אילן
Bar-Ilan University

אוניברסיטת בר אילן

מספרי פיבונאצ'י כערכים מיוחדים של פולינומים

עדי אוסטרוב

עבודה זו מוגשת כחלק מהדרישות לשם קבלת תואר מוסמך

במחלקה למתמטיקה, אוניברסיטת בר-אילן

רמת גן התשפ"ה