UTRECHT UNIVERSITY
DEPARTMENT OF MATHEMATICS

Master's thesis

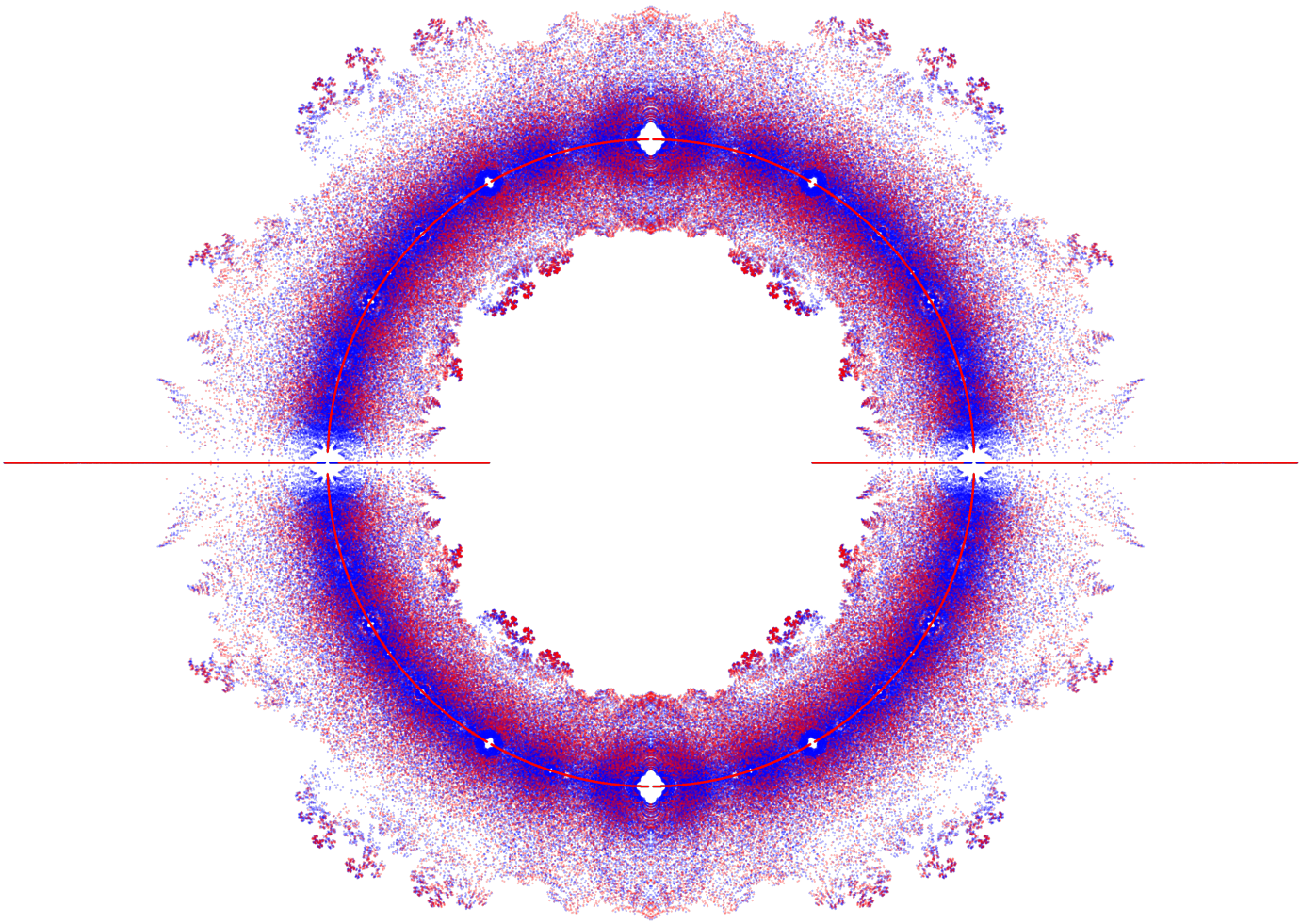
Littlewood polynomials with square discriminant

David Hokken

Supervisor:
prof. dr. G.L.M. Cornelissen

Second reader:
dr. L. Thompson

July 2020



Contents

Introduction

What are the odds that a given monic polynomial f with integer coefficients has maximal Galois group?

Fixing the degree of f and uniformly sampling its coefficients from $\{-H, \dots, H\}$ with H a positive integer, a classical 1934 result by Van der Waerden [**49**, **50**] states that that probability tends to 1 as H tends to infinity. This is the *large box model*.

In the *restricted coefficient model*, one instead fixes H (or more generally any 'coefficient set') and lets the degree n of f grow. In this approach, much less is known, but it is generally expected that

$$\mathbb{P}(\mathrm{Gal}(f) = S_n) \to 1 \quad \text{as} \quad n \to \infty$$

as well. The state-of-the-art conditional result is by Breuillard and Varjú [**11**], who showed that the Galois group of the noncyclotomic part of f contains A_n with probability tending to 1 as n tends to infinity – assuming that the Riemann Hypothesis for Dedekind zeta functions holds. Bary-Soroker, Koukoulopoulos and Kozma [**6**] showed that, for various coefficient sets, the polynomial f has Galois group containing the alternating group with positive probability as the degree n tends to infinity; if the coefficient set is in some sense large enough, this probability tends to 1.

All mentioned results rely on probabilistic methods to demonstrate that the Galois group $\mathrm{Gal}(f)$ of f must be highly transitive (more precisely, k-transitive for $k > 5$). As a result from the classification of finite simple groups, such a highly transitive group must be either the symmetric group S_n or the alternating group A_n.

To exclude the alternating group A_n, one is bound to consider the discriminant

$$\Delta(f) = \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2$$

of f (where the α_i denote the roots of f). Indeed, recall that if f does not have multiple roots, then $\mathrm{Gal}(f)$ is contained in A_n if and only if $\Delta(f)$ is the square of an integer.

However, it is not clear how to employ this criterion in a probabilistic approach to the general question.

In this thesis, we will consider *Littlewood polynomials*, which are the monic, single-variable polynomials all of whose coefficients lie in the rather small coefficient set $\{\pm 1\}$. Motivated by the above, we are especially interested in such polynomials with square discriminant. In the following, we give an overview of the thesis, including a sample of new conjectures and theorems (here denoted by the 'lettered conjecture and theorems' A to D) that it contains.

Denote by $\mathscr{F}_n$ the set of Littlewood polynomials of degree n. We further define the subsets $\mathrm{Sq}_n \subset \mathscr{F}_n$, consisting of those polynomials with square discriminant, and Ir_n, containing all irreducible polynomials in $\mathscr{F}_n$. Recall that the Galois group is transitive if and only if f is irreducible. Hence any polynomial with Galois group A_n or S_n must be irreducible. So we are interested in the intersection $\mathrm{SI}_n = \mathrm{Sq}_n \cap \mathrm{Ir}_n$. It seems that having square discriminant and being irreducible are properties that repel each other: for example, any even degree polynomial with square discriminant is reducible modulo any prime – see Lemma 1.2.4.

The following main conjecture of this thesis has been verified computationally for all Littlewood polynomials of degree at most 34 (i.e., roughly 34 billion polynomials).

Conjecture A (= Conjecture 4.1.1)**.** *Let $n > 1$ be an integer and $f \in \mathrm{SI}_n$. Then f is balanced and $n \equiv 0, 6 \bmod 8$. Furthermore, the set SI_n is nonempty for any $n \equiv 0, 6 \bmod 8$.*

Here, a degree-n polynomial $f \in K[X]$ (where $K = \mathbb{Q}$ or $\mathbb{F}_p$ with p prime) is called *balanced* if n is even and

$$f(X) = X^n f(X^{-1}) \quad \text{or} \quad f(X) = \pm X^n f(-X^{-1}),$$

where the sign is negative if and only if $n \equiv 2 \bmod 4$. In the former case, we call f *reciprocal*, and in the latter case f is called *skew-reciprocal*. We will investigate balanced polynomials in Chapter 2, where we establish and employ a square discriminant criterion for them.

Out of the 2^{2n} Littlewood polynomials in degree $2n$, only 2^{n+1} are balanced. The fraction $2^{n+1}/2^{2n} = 2^{1-n}$ tends to 0 as n tends to infinity; in this sense, Conjecture A implies that only 'a few' Littlewood polynomials are both irreducible and have square discriminant.

In our algebraic approach, it will be of great help that any Littlewood polynomial $f = X^n \pm X^{n-1} \pm \cdots \pm X \pm 1$ satisfies

$$f(X) \equiv X^n + X^{n-1} + \cdots + X + 1 \bmod 2,$$

which is for even n both a reciprocal polynomial, as well as a product of cyclotomic polynomials; we study cyclotomic polynomials from the 'balanced point of view' in Chapter 3. On the other hand, for odd n this polynomial congruence shows that 2 is a ramified prime; as a result, it is much harder to make any progress on Conjecture A for odd-degree Littlewood polynomials than for even-degree Littlewood polynomials.

In Chapter 4, we study the implications of Chapter 2 and Chapter 3 for Littlewood polynomials. This leads for example to the following theorem, where we again encounter the tension between irreducibility and square discriminants.

Theorem B (= Theorem 4.2.9)**.** *Let $2n+1$ be a prime number congruent to 7 mod 8. Suppose that 2 has order n in $(\mathbb{Z}/(2n+1)\mathbb{Z})^\times$. Then every reciprocal Littlewood polynomial in $\mathscr{F}_{2n}$ is irreducible over $\mathbb{Q}$, and every skew-reciprocal Littlewood polynomial in $\mathscr{F}_{2n}$ is irreducible over $\mathbb{Q}$ or has square discriminant.*

In addition, Chapter 4 contains results regarding the irreducibility and Galois group of Littlewood polynomials with one or two sign changes, such as the following.

Theorem C (= Theorem 4.3.1)**.** *Let $n > k$ be positive integers. The Littlewood polynomial $f = X^n + X^{n-1} + \cdots + X^k - X^{k-1} - \cdots - 1$ is irreducible if and only if $\gcd(n+1,k) = 1$ unless $(n,k) = (6,2)$ or $(6,5)$. If we further suppose that n is even, then the discriminant of $f_{n,k}$ is not a square for any k, and the Galois group of $f_{n,k}$ is the symmetric group S_n if $f_{n,k}$ is irreducible.*

Given a reciprocal Littlewood polynomial f with two sign changes, we also establish an asymptotic upper bound on the number of factors that f can have, assuming Lehmer's conjecture and a conjecture of our own concerning the asymptotic Mahler measure of f.

In Chapter 5, we study the topology of the set Γ of *all* roots of *all* Littlewood polynomials. We give an account of both Odlyzko and Poonen's proof [**39**] and of Bousch' proof [**10**] that the closure $M = \overline{\Gamma}$ is a connected subset of the plane.

A last result is the following.

Theorem D (= part of Theorem 5.2.4)**.** *Suppose that $\alpha \in M$. Then there exist a sequence $(f_k)_{k\geq 0}$ of reciprocal Littlewood polynomials with, for each k, the following properties:*

(1) f_k has nonvanishing square discriminant;
(2) f_k has a root α_k such that $\alpha_k \to \alpha$ as $k \to \infty$.

Furthermore, we can also find a sequence $(f_k)_{k\geq 0}$ of skew-reciprocal polynomials satisfying properties (1) *and* (2)*.*

Write $M^\square$ for the closure of the set of all roots of all Littlewood polynomials f whose Galois group is contained in the alternating group $A_{\deg f}$. Theorem D shows that $M = M^\square$,

because Littlewood polynomials of even degree cannot have multiple roots – a known fact that we establish in Lemma 4.2.1. From the topological point of view, one could thus say that there are 'many' Littlewood polynomials with square discriminant.

Many of the results and conjectures in this thesis originate in experimenting with the computer. The appendices include an overview of computational results, as well as a `Sage` script to reproduce them. The results and proofs in this thesis are new, unless a reference is given.

Acknowledgements

I would like to thank my supervisor Gunther, who introduced me to this subject and gave me a lot of freedom to pursue whatever interested me in this thesis, while encouraging me at the right moments to keep track of the 'big picture'. He was a source of many ideas and great enthusiasm: I always left our meetings (for which he would always take whatever time was needed) with renewed energy and motivation (and sometimes a new novel to read or music to listen to!). Thank you above all for approaching the supervisor-student relation as, first and foremost, a relation between two human beings.

I would also like to thank Lola for reading this thesis carefully and giving thoughtful feedback in its final stages, as well as on an early draft in January.

Berend and Jan-Willem, thanks to both of you for your interest in my thesis and for involving me with your own projects!

Thinking back of the years studying Mathematics in Utrecht, it is first of all my study friends Lennert, Robert, Jaco, Wilmer and Martijn that come to mind. Your presence is worth a thousand theorems.

Thank you, Mar, for being on my side. Your support is something truly unhoped-for. (And I promise to typeset all of your LaTeX documents.)

CHAPTER 1

Preliminaries

This introductory chapter consists of six parts. Sections 1.1 and 1.2 contain concepts and theorems that lie at the very heart of this thesis. Sections 1.3 and 1.4 serve as a recapitulation of some concepts in algebraic number theory that are needed in Chapter 4. Sections 1.5 and 1.6 contain some basic results in topology and complex analysis, most of which are only needed in Chapter 5.

1.1 The discriminant of a polynomial

Two classical tools for calculations with polynomials are the resultant and discriminant. The definitions and properties mentioned here can be found in [**51**, §25-27].

Definition 1.1.1. Let $f = a_n X^n + \cdots + a_1 X + a_0$ and $g = b_m X^m + \cdots + b_1 X + b_0$ be two polynomials with coefficients and zeros in a field K. Denote by α_i and β_j the zeros of f and g (repeated according to their multiplicities), respectively. The *resultant* $\mathrm{Res}(f,g)$ of f and g is defined as the product

$$\mathrm{Res}(f,g) = a_n^m b_m^n \prod_{\substack{1\le i\le n\\ 1\le j\le m}} (\alpha_i - \beta_j).$$

Since the resultant of f and g is a symmetric expression in the roots of f and g, it can also be expressed as a polynomial in the coefficients of f and g. Thus $\mathrm{Res}(f,g)$ lies in K. A practical form of the resultant is

$$\mathrm{Res}(f,g) = \prod_{1\le i\le n} g(\alpha_i). \tag{1.1}$$

The resultant of f and g vanishes if and only if f and g have a root in common. In particular, $\mathrm{Res}(f,f')$ vanishes if and only if f has a double root, motivating the definition of the discriminant, which will play a key role in this thesis.

Definition 1.1.2. Let $f = a_n X^n + \cdots + a_1 X + a_0$ be a polynomial with coefficients and zeros in a field K. Denote by α_i the zeros of f (repeated according to their multiplicities). The *discriminant* $\Delta(f)$ of f is

$$\Delta(f) = \frac{(-1)^{\frac{n(n-1)}{2}}}{a_n} \operatorname{Res}(f, f'). \tag{1.2}$$

Again, we see that $\Delta(f)$ lies in K. Expanding the resultant using (1.1) shows that

$$\Delta(f) = a_n^{2n-2} \prod_{\substack{1 \le i,j \le n \\ i \ne j}} (\alpha_i - \alpha_j) = a_n^{2n-2} \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2. \tag{1.3}$$

This thesis concerns particular polynomials whose discriminant is a square. In this light, we may think of the result in the next lemma as 'the discriminant is a multiplicative function modulo squares'.

Lemma 1.1.3. *We have*

$$\Delta(fg) = \Delta(f)\Delta(g)\operatorname{Res}(f, g)^2.$$

Proof. Write n and m for the degrees of f and g, respectively, and call their respective leading coefficients a_n and b_m. Let $\alpha_1, \ldots, \alpha_n$ be the roots of f and $\alpha_{n+1}, \ldots, \alpha_{n+m}$ those of g. Using (1.3), the discriminant $\Delta(fg)$ equals

$$(a_n b_m)^{2(n+m)-2} \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2 \prod_{n+1 \le i < j \le n+m} (\alpha_i - \alpha_j)^2 \prod_{\substack{1 \le i \le n \\ n+1 \le j \le n+m}} (\alpha_i - \alpha_j)^2. \tag{1.4}$$

Since $(a_n b_m)^{2(n+m)-2} = a_n^{2n-2} \cdot b_m^{2m-2} \cdot (a_n^m b_m^n)^2$, the expression (1.4) can be reordered into the product of the discriminant of f, the discriminant of g, and the square of the resultant of f and g. □

The last lemma of this section states that the sign of the discriminant of a polynomial f is determined by the parity of half of the nonreal roots of f. In particular, the discriminant of f is positive if all roots of f are real.

Lemma 1.1.4. *Let $f \in \mathbb{Z}[X]$. Then f has positive discriminant if and only if it has an even number of pairs of complex conjugate roots.*

Proof. Consider two distinct roots of f that are not complex conjugates, say α and β, and consider (1.3). If α and β are both real, then $(\alpha - \beta)^2$ is real and positive. If only one of them is real, say α, then $((\alpha - \beta)(\alpha - \overline{\beta}))^2$ is real and positive. If they are both nonreal, then $((\alpha - \beta)(\alpha - \overline{\beta})(\overline{\alpha} - \beta)(\overline{\alpha} - \overline{\beta}))^2$ is real and positive. So all distinct, nonconjugate pairs of roots give a real and positive contribution to (1.3). This leaves us with the factors $(\alpha - \overline{\alpha})$ (where α is complex), which always square to a negative real number. □

1.2 Galois theory and the discriminant

The main result of Galois theory is summarised in the following theorem. We will only need it once in this explicit form, namely in Chapter 3.

Theorem 1.2.1 (Fundamental theorem of Galois theory)**.** *Let L/K be a finite Galois extension. The map $M \mapsto \mathrm{Gal}(L/M)$ defines an inclusion-reversing bijection between*

$$\{\textit{Extensions of } K \textit{ contained in } L\} \longleftrightarrow \{\textit{Subgroups of } \mathrm{Gal}(L/K)\}$$

with inverse $H \mapsto L^H$. It restricts to an inclusion-reversing bijection between

$$\{\textit{Galois extensions of } K \textit{ contained in } L\} \longleftrightarrow \{\textit{Normal subgroups of } \mathrm{Gal}(L/K)\}.$$

Proof. See [**20**, Thm. 14.2.14]. □

In the special case that L is the splitting field of a separable polynomial $f \in K[X]$, we denote $\mathrm{Gal}(L/K)$ by $\mathrm{Gal}(f/K)$ (or simply $\mathrm{Gal}(f)$ if this doesn't lead to ambiguity). The Galois group of a polynomial is determined by its action on the roots of f. If the degree of f equals n, and we fix a labelling $\alpha_1, \ldots, \alpha_n$ of the roots of f, then we can think of an element in $\mathrm{Gal}(f)$ as a permutation of the indices $\{1, \ldots, n\}$ of the roots of f. In other words, $\mathrm{Gal}(f)$ is a subgroup of S_n.

Lemma 1.2.2. *Let f be a polynomial of degree n over a field K whose characteristic does not equal 2. Suppose that f has no multiple roots. Then the discriminant $\Delta(f)$ of f is a square in K if and only if $\mathrm{Gal}(f/K)$ is contained in the alternating group A_n.*

Proof. Denote the roots of f by α_i and the leading term of f by a_n. Consider the expression $D = a_n^{n-1} \prod_{i<j}(\alpha_i - \alpha_j)$, which is nonzero as f does not have multiple roots. Recall that $\Delta(f) = D^2$. Hence $\Delta(f)$ is a square in K if and only if $D \in K$. A transposition $\tau \in S_n$ sends D to $-D$. So if $\sigma \in S_n$ is any permutation, then it sends D to $(-1)^{\mathrm{sgn}(\sigma)}D$, meaning that $D \neq 0$ is fixed precisely when σ is an even permutation. (This is false in characteristic 2, where the equality $D = -D$ ensures that D is fixed by any $\sigma \in S_n$.) □

The following theorem is a weak version of a classical result of Dedekind. It is a very useful tool when calculating the Galois group of a polynomial. Its proper context is that of algebraic number theory. However, the required terminology needed to state this weak version is already at our disposal.

Theorem 1.2.3 (Dedekind)**.** *Let $f \in \mathbb{Z}[X]$ be a monic, irreducible polynomial over $\mathbb{Q}$ of degree n and $p \nmid \Delta(f)$ a prime number. Write*

$$f(X) = f_1(X) \cdots f_r(X) \bmod p$$

for the factorisation of f into monic, irreducible factors and set $d_i = \deg f_i$, so that $d_1 + \cdots + d_r = n$. Then $\mathrm{Gal}(f/\mathbb{Q})$*, viewed as a permutation group, contains a permutation that is the product of cycles of length $d_1, \ldots, d_r$.*

Proof. See [37, Thm. 8.23] (take $K = \mathbb{Q}$ so that $\mathcal{O}_K = \mathbb{Z}$, $\mathfrak{p} = (p)$ for a prime number p, and $k = \mathbb{F}_p$). □

Dedekind's theorem implies that even-degree polynomials with square discriminant are reducible modulo *any* prime.

Lemma 1.2.4. *Let $f \in \mathbb{Z}[X]$ be a polynomial of even degree without double roots, whose discriminant is a square. Then f is reducible modulo any prime p.*

Proof. We prove the contrapositive. Suppose that f is irreducible modulo a prime p. Then in particular, the reduction $\bar{f} = f \bmod p \in \mathbb{F}_p[X]$ does not have multiple factors modulo p, i.e., $\Delta(\bar{f})$ is not divisible by p. Since $\Delta(f)$ is a polynomial expression in the coefficients of f, we have $\Delta(f) \equiv \Delta(\bar{f}) \bmod p$. Hence p does not divide $\Delta(f)$. Dedekind's theorem thus implies that $\mathrm{Gal}(f)$ contains a cycle of length n, which is an odd permutation since n is even. Hence $\mathrm{Gal}(f)$ is not contained in the alternating group A_n, and therefore f does not have square discriminant. □

The converse of Lemma 1.2.4 does not hold: simply pick any reducible polynomial whose discriminant is not a square. However, there are also irreducible counterexamples, such as the polynomial $f(X) = X^6 - 3X^5 - 2X^4 + 9X^3 - 5X + 1$. The Galois group of f is isomorphic to S_3, which clearly does not contain a 6-cycle. Furthermore, the discriminant of f is $2^4 \cdot 37^3$, which is not a square. More generally, any irreducible polynomial f of even degree n with $C_n \not\subset \mathrm{Gal}(f) \not\subset A_n$ is a counterexample to the converse of Lemma 1.2.4 by Dedekind's theorem and Lemma 1.2.2. Irreducible counterexamples do not exist in degree 2 and 4.

Lemma 1.2.5. *Let $f \in \mathbb{Z}[X]$ be an irreducible polynomial of degree n with all but an odd number of pairs of complex conjugate roots in $\mathbb{R}$. Then* $\mathrm{Gal}(f) \not\subset A_n$.

Proof. This is a consequence of Lemma 1.1.4; alternatively, complex conjugation corresponds to taking the product of an odd number of disjoint transpositions, which is an odd permutation. □

1.3 Some local field theory

The goal of this and the next section is to state Hensel's lemma and the definition of the inertia group of a Galois extension of local fields. The exposition is thus heavily specialized and does not aim to be a comprehensive introduction to local fields. This section is largely based on [38, 45].

Definition 1.3.1. An *absolute value* of a field K is a function $|\cdot| : K \to \mathbb{R}$ with the properties

(1) $|x| \geq 0$, and $|x| = 0$ if and only if $x = 0$,
(2) $|xy| = |x||y|$,
(3) $|x + y| \leq |x| + |y|$

for any $x, y \in K$. The last property is the well-known triangle inequality. When $|\cdot|$ satisfies the strong triangle inequality $|x + y| \leq \max\{|x|, |y|\}$, we call $|\cdot|$ *nonarchimedean*.

Any absolute value induces a topology on K coming from a basis of open balls in the usual way.

Definition 1.3.2. A *discrete valuation* on field K is a function $\nu : K \to \mathbb{Z} \cup \{\infty\}$ that enjoys the properties

(1) $\nu(xy) = \nu(x) + \nu(y)$,
(2) $\nu(x + y) \geq \min\{\nu(x), \nu(y)\}$,
(3) $\nu(x) = \infty$ if and only if $x = 0$,

for all $x, y \in K$. In addition, we exclude the trivial valuation that takes the value 0 at each $x \neq 0$.

Any discrete valuation ν induces a nonarchimedean absolute value $|\cdot|_\nu$ via $|x|_\nu = c^{-\nu(x)}$ for any fixed real number $c > 1$. (Here, we set the convention that $c^{-\infty} = 0$.) Suppose that K is complete with respect to the topology induced by $|\cdot|_\nu$ (or equivalently, by ν).

Define the sets

$$\mathcal{O}_K = \{x \in K \mid \nu(x) \geq 0\}$$

and

$$\mathfrak{p} = \{x \in K \mid \nu(x) > 0\} \subset \mathcal{O}_K.$$

Then $\mathcal{O}_K$ is a discrete valuation ring and $\mathfrak{p}$ is the unique maximal ideal of $\mathcal{O}_K$; see [**38**, Prop. II.3.8 & II.3.9]. The field $\kappa = \mathcal{O}_K/\mathfrak{p}$ is called the *residue class field* of K.

Definition 1.3.3. Let K be a field which is complete with respect to a discrete nonarchimedean valuation ν, such that κ is a finite field. Then K is called a *nonarchimedean local field*.

Choosing a prime p, the most important example of a local field in the context of this thesis is the p-adic field $K = \mathbb{Q}_p$ with $\nu(x) = v_p(x)$ defined as the unique integer such that $x = p^{v_p(x)}a/b$ with a and b not divisible by p.

In the remainder of this section, we assume that K is a nonarchimedean local field.

Lemma 1.3.4 (Hensel's Lemma)**.** *Let $f \in \mathcal{O}_K[X]$ have at least one coefficient not in $\mathfrak{p}$. Suppose that f factors mod $\mathfrak{p}$ into the product of two relatively prime polynomials $\bar{g}, \bar{h} \in \kappa[X]$ (i.e., $\bar{g}$ and $\bar{h}$ have no root in common in an algebraic closure of κ). Then f admits a factorisation $f = gh$ into polynomials $g, h \in \mathcal{O}_K[X]$ such that $\deg g = \deg \bar{g}$, $\deg h = \deg \bar{h}$ and $g \equiv \bar{g} \bmod \mathfrak{p}$, $h \equiv \bar{h} \bmod \mathfrak{p}$.*

Proof. See [38, Lem. II.4.6]. □

Now let L be a finite extension of the field K. Since K is complete, the valuation v extends to a unique valuation w on L by [38, Thm. II.4.8] via the formula

$$w(\alpha) = \frac{1}{n} v(N_{L/K}(\alpha))$$

where $N_{L/K}$ denotes the norm function of the field extension L/K. The formula immediately shows that w is discrete as well. Let $\mathfrak{P}$ be the unique maximal ideal of the discrete valuation ring $\mathcal{O}_L$ of L. Then $\mathfrak{P}$ must lie above $\mathfrak{p}$. As there is no other prime above $\mathfrak{p}$, there must be an integer $e = e_{\mathfrak{p}}$ such that

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}^e.$$

The integer $e_{\mathfrak{p}}$ is called the *ramification index*.

Consider the residue class fields λ and κ of L and K, respectively. Then λ/κ is a field extension as well. The index $[\lambda : \kappa]$ is known as the *inertia degree* $f = f_{\mathfrak{p}}$.

Lemma 1.3.5 (Fundamental identity)**.** *The equality $[L : K] = ef$ holds whenever L/K is separable.*

Proof. See [38, Prop. II.6.8]. □

A finite extension L/K is called *unramified* if the extension λ/κ of associated residue class fields is separable and $[L : K] = [\lambda : \kappa]$. Equivalently, the extension L/K is unramified if $e_{\mathfrak{p}} = 1$.

Lemma 1.3.6. *The compositum of finitely many unramified extensions of K is again unramified.*

Proof. See [38, Cor. II.7.3]. □

From here on, we assume that the extension L/K is also Galois. The fact that any element σ of the Galois group $\mathrm{Gal}(L/K)$ must send $\mathfrak{P}$ to itself, leads to the following lemma.

Lemma 1.3.7. *The extension λ/κ is Galois, and there is a canonical surjection*

$$\mathrm{Gal}(L/K) \to \mathrm{Gal}(\lambda/\kappa)$$

whose kernel is the inertia group

$$I(L/K) = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(x) \equiv x \bmod \mathfrak{P} \text{ for all } x \in \mathcal{O}_L\} \tag{1.5}$$

of cardinality $e_\mathfrak{p}$.

Proof. See [38, Prop. II.9.9] for a proof in a more general setting. □

When L/K is a finite, unramified Galois extension, the fundamental identity shows that $e_\mathfrak{p} = 1$. Hence $I(L/K)$ is trivial, and we arrive at the following conclusion.

Lemma 1.3.8. *Let L/K be a finite, unramified Galois extension. Then* $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(\lambda/\kappa)$.

1.4 Inertia groups of extensions of number fields

Now let L/K be a finite Galois extension of number fields and $\mathfrak{p}$ a prime ideal of $\mathcal{O}_K$. The main goal of this section is to define another 'inertia group', associated with a prime ideal $\mathfrak{P}$ extending $\mathfrak{p}$ in $\mathcal{O}_L$, and show that it coincides with a particular inertia group in the sense of Lemma 1.3.7.

The Galois group $\mathrm{Gal}(L/K)$ acts transitively on the set of primes ideals in $\mathcal{O}_L$ extending $\mathfrak{p}$, see [38, Prop. I.9.1]. Furthermore, the ideal $\mathfrak{p}$ factors in $\mathcal{O}_L$ as

$$\mathfrak{p}\mathcal{O}_L = \prod_{\sigma \in \mathrm{Gal}(L/K)} (\sigma(\mathfrak{P}))^{e_\mathfrak{p}}$$

where the integer $e_\mathfrak{p}$ is the *ramification index* and $\mathfrak{P}$ is any prime ideal extending $\mathfrak{p}$. The *inertia degree* is the integer $f_\mathfrak{p} = [\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p}]$ and does not depend on the choice of $\mathfrak{P}$ – see [38, p. 55] for all this.

The *decomposition group* of $\mathfrak{P}$ is the subgroup

$$D_\mathfrak{P} = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}$$

of $\mathrm{Gal}(L/K)$. Let $\lambda = \mathcal{O}_L/\mathfrak{P}$ and $\kappa = \mathcal{O}_K/\mathfrak{p}$. Then the extension λ/κ is Galois and admits a surjective homomorphism

$$D_\mathfrak{P} \to \mathrm{Gal}(\lambda/\kappa)$$

that is 'reduction modulo $\mathfrak{P}$', see [38, Prop. I.9.4]. The kernel of this homomorphism is the *inertia group*

$$I_{\mathfrak{P}} = \{\sigma \in D_{\mathfrak{P}} \mid \sigma(x) \equiv x \bmod \mathfrak{P} \text{ for all } x \in \mathcal{O}_L\}. \tag{1.6}$$

The prime ideal $\mathfrak{p}$ induces a discrete valuation on K via $\nu_{\mathfrak{p}}(x) = n$ if the ideal (x) factors as $\mathfrak{p}^n J$, where J is an ideal that contains no power of $\mathfrak{p}$. Denote by $K_{\mathfrak{p}}$ the completion of K with respect to $\nu_{\mathfrak{p}}$. Then $K_{\mathfrak{p}}$ is a local field with maximal ideal $\mathfrak{p}\mathcal{O}_{K_{\mathfrak{p}}}$, and the completion $L_{\mathfrak{P}}$ of L with respect to $\mathfrak{P}$ is a Galois extension of $K_{\mathfrak{p}}$. Let σ be an element of the Galois group of $L_{\mathfrak{P}}/K_{\mathfrak{p}}$. Then σ must fix K (as K lies in $K_{\mathfrak{p}}$) and $\mathfrak{P}$ (as it is the only prime ideal). Thus we can see $\sigma\big|_L$ as an element of $D_{\mathfrak{P}}$. Conversely, any element of $D_{\mathfrak{P}}$ can be seen as an element of $\mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$. So the explicit forms in (1.5) (where we now substitute $L_{\mathfrak{P}}$ and $K_{\mathfrak{p}}$ for L and K) and (1.6) show the following:

Lemma 1.4.1. *$I(L_{\mathfrak{P}}/K_{\mathfrak{p}})$ and $I_{\mathfrak{P}}$ coincide.*

A more detailed account is given in [38, Prop. II.9.6], which features a proof of Lemma 1.4.1 (and more) for arbitrary (finite and infinite) Galois extensions.

1.5 A few results in topology

This section contains a few basic results and constructions in topology that we will need in Chapter 5.

Lemma 1.5.1. *The union of two connected sets X and Y is connected if and only if $X \cap Y$ is nonempty.*

Proof. The 'only if' part is immediate. Suppose that $X \cup Y$ is disconnected. Write $X \cup Y = A \cup B$ where A and B are disjoint, nonempty sets that are each open – and hence also closed – in $X \cup Y$. Suppose that X and Y have nonempty intersection; without loss of generality, we may assume that $X \cap Y \cap A$ is nonempty. Since $A \cap X$ is open and closed in X, it must be the whole of X; otherwise the union of $A \cap X$ with its complement inside X would be a partitioning of X into disjoint, nonempty opens. So X is contained in A. In similar fashion we can show that Y must be contained in A. Hence $A = X \cup Y$ and B must be empty. □

Lemma 1.5.2. *Let $(X_i)_{i\geq 0}$ be a descending collection of closed, nonempty, connected subsets of a compact metric space X. Then $\bigcap_i X_i$ is nonempty and connected.*

Proof. See [22]. □

Definition 1.5.3. Let $\epsilon > 0$. A metric space X is called *ϵ-chain connected* if for any two points $x, y \in X$ there is a finite sequence $x = x_0, x_1, \ldots, x_n = y$ of points in X such that $d(x_{i+1}, x_i) < \epsilon$ for every i; such a sequence is called an *ϵ-chain* from x to y. The metric space X is called *chain connected* if it is ϵ-chain connected for every $\epsilon > 0$.

Lemma 1.5.4. *A compact metric space X is chain connected if and only if it is connected.*

Proof. Suppose $X = U \cup V$ is chain connected and U and V are open, nonempty and disjunct. Then U and V are also closed, and hence compact by compactness of X. Hence $r = \inf_{x \in U, y \in V} d(x, y)$ is strictly positive, implying that X is not ϵ-chain connected for any $0 < \epsilon < r$.

Conversely, if X is not ϵ-chain connected for some $\epsilon > 0$, then X consists of at least two chain components (i.e., nonempty maximally chain connected subsets of X). Note that each chain component C is open, as for $x \in C$ necessarily each y with $d(x, y) < \epsilon$ is contained in C. Write $X = U \cup V$ with U and V a union of such chain components, such that U and V are disjoint. Then U and V are also open and nonempty, so X is disconnected. □

A *multiset* is collection of elements in which each element is allowed to occur multiple times. We will denote a multiset by double curly brackets, e.g. $\{\{a, b, c, \ldots, \}\}$. Equivalently, one can think of a multiset as an unordered tuple. Fixing an integer n, the following construction gives a topology on the collection of multisets of n elements of a topological space Y.

Definition 1.5.5. Let Y be a topological space and $n > 1$ an integer. Consider the product space Y^n, endowed with the product topology. The symmetric group S_n acts on Y^n by permuting the coordinates. The ensuing quotient Y^n/S_n is called the *n-th symmetric product* of Y.

Given an n-tuple $x = (x_1, \ldots, x_n)$ of elements of Y, the orbit $S_n \cdot x$ of x (which is the image of x under the quotient map $Y^n \to Y^n/S_n$) is a set of $n!$ different tuples, each of which corresponds to a particular order of the coordinates of x. So we can indeed think of $S^n \cdot x$ as the multiset $\{\{x_1, \ldots, x_n\}\}$.

Theorem 1.5.6 (Contraction mapping theorem)**.** *Let X be a nonempty, complete metric space and $f : X \to X$ a contraction mapping, i.e., there is a $0 < c < 1$ such that $d(f(x), f(y)) \leq c\,d(x, y)$ for all $x, y \in X$. Then f has a unique fixed point in X.*

Proof. See [18]. □

1.6 A few results in complex analysis

Let f be a power series with integral coefficients. Suppose that the coefficients of f are bounded in absolute value by some integer $B > 0$; we say that f has *bounded coefficients*. Then

$$|f(z)| \leq B(1 + |z| + |z|^2 + \cdots) = \frac{B}{1-|z|}$$

for any z in the open unit disk $\mathbb{D}$. In particular, the radius of convergence of f is at least 1 and the set of roots of f within $\mathbb{D}$ is well-defined. In Chapter 5, we will require the following approximation result on the roots in $\mathbb{D}$ of power series with bounded coefficients.

Lemma 1.6.1. *Let $f, g \in \mathbb{Z}[\![X]\!]$ be two power series with bounded coefficients. Suppose $\delta \in (0,1)$ and $0 < \epsilon < 1-\delta$. Then there exists an $N \in \mathbb{N}$ such that $X^N \mid (f-g)$ implies the following: for each zero α of f of modulus smaller than $1-\delta$ and multiplicity r, there are (possibly nondistinct) zeroes $\beta_1, \ldots, \beta_r$ of g such that $|\alpha - \beta_i| < \epsilon$ for each i.*

We start with a few results that are needed to prove Lemma 1.6.1, and state a lemma needed in Chapter 4 along the way.

Theorem 1.6.2 (Rouché's theorem)**.** *Let f and g be two holomorphic functions on a simply-connected domain U. If*

$$|f(z) - g(z)| < |g(z)|$$

for all $z \in \partial U$, then f and g have the same number of zeros (counting multiplicity) in the interior of U.

Proof. See [**24**, Chap. VI, §1, Thm. 1.6] (in our case $\gamma = \partial U$, which satisfies the required properties since we assume U to be simply-connected). □

We will need the following result at the end of Chapter 4.

Lemma 1.6.3. *Let α be a complex number. Then*

$$\int_0^1 \log|e^{2\pi i t} - \alpha| \, \mathrm{d}t = \log^+|\alpha|,$$

where $\log^+(x) = \max\{0, \log(x)\}$.

Proof. See [**12**, Prop. 1.4] or the first step in the proof of [**24**, Chap. XII, §1, Thm. 1.2]. □

Lemma 1.6.3 is a key ingredient of the proof of Jensen's well-known formula.

Theorem 1.6.4 (Jensen's formula)**.** *Let f be holomorphic and nonconstant and suppose $f(0) \neq 0$. Let $R > 0$. Denote the roots of f of modulus at most R by z_j, repeated according to their multiplicities. Then*

$$\frac{1}{2\pi}\int_0^{2\pi} \log|f(Re^{i\theta})|\,\mathrm{d}\theta = \log|f(0)| + \sum_j \log(R/|z_j|). \tag{1.7}$$

Proof. See [24, Chap. XII, §1, Thm. 1.2]. □

A first consequence of Jensen's formula is the following, which is a slight generalisation of [39, Prop. 2.1].

Lemma 1.6.5. *Suppose that f is a nonconstant power series with $|f(0)| \geq 1$ such that all coefficients of f are bounded in absolute value by some positive integer B. Then f has at most*

$$\frac{2\log\frac{1-\sqrt{r}}{B}}{\log r}$$

zeros of modulus at most r for any $r \in (0,1)$.

Proof. Since

$$|f(Re^{i\theta})| \leq B\sum_{k\geq 0} R^k = \frac{B}{1-R}$$

for any $R < 1$, the radius of convergence of the power series f is at least 1, and we obtain

$$\frac{1}{2\pi}\int_0^{2\pi} \log|f(Re^{i\theta})|\,\mathrm{d}\theta \leq \log\left(\frac{B}{1-R}\right). \tag{1.8}$$

Now suppose $r < R < 1$ and denote by z_j the roots of f of modulus smaller than R, repeated according to their multiplicities. Since the left-hand side in Jensen's formula (1.7) is finite, there are only finitely many zeros of f whose modulus is at most r. In particular, if m is the number of such zeros,

$$\sum_j \log\frac{R}{|z_j|} \geq \sum_{|z_j|\leq r} \log\frac{R}{|z_j|} \geq m\log\frac{R}{r}. \tag{1.9}$$

Since $\log|f(0)|$ is nonnegative, combining (1.8) and (1.9) yields

$$m \leq \frac{\log(B/(1-R))}{\log(R/r)}.$$

Choosing $R = \sqrt{r}$ gives the claimed bound. □

We are now ready to prove Lemma 1.6.1.

Proof of Lemma 1.6.1. Since the coefficients of f and g are bounded, there is an integer B such that the coefficients of the difference $f-g$ are at most B in absolute value. If f and g have the same first N coefficients, then

$$|f(z)-g(z)| \leq |z|^N B \sum_{j\geq 0} |z|^j \leq \frac{B|z|^N}{1-|z|} < \frac{B(1-\delta)^N}{\delta}$$

for all z of modulus smaller than $1-\delta$. Let α be a (possibly multiple) root of f of modulus smaller than $1-\delta$. Note that there are only finitely many such roots by Lemma 1.6.5. Consider an open disk D_α of radius $r \leq \epsilon$ centered at a α. Make r small enough such that no root of f lies on the boundary of $\overline{D}_\alpha$. By compactness, $|f|$ attains some positive minimum m on the boundary of D_α. Choosing $N = N_\alpha$ large enough, we can ensure that $|f(z)-g(z)| < m \leq |f(z)|$ for any z lying on the boundary of D_α. By Rouché's theorem 1.6.2, the power series f and g have the same number of roots within D_α, so there are (possibly nondistinct) roots $\beta_1, \ldots, \beta_r$ of g satisfying the conditions. Finally, observe that N can be chosen uniformly via $N = \max_\alpha N_\alpha$. □

CHAPTER 2

Balanced polynomials

2.1 Preliminaries

In this chapter we introduce and study *balanced polynomials*, which come in two different types that share similar properties. This section sets out the fundamentals of these two flavours, and is loosely based on the introduction to one of these types found in [13].

Let K be the field $\mathbb{Q}$ or $\mathbb{F}_p$ (where p is a prime number) and $f \in K[X]$ a polynomial of degree n whose constant term does not vanish. The *reversal polynomial* of f is

$$f_{\mathsf{rev}}(X) := X^n f(X^{-1}) \in K[X] \tag{2.1}$$

and the *skew-reversal polynomial* of f is

$$f_{\mathsf{srev}}(X) := (-1)^{\frac{n(n-1)}{2}} X^n f(-X^{-1}) \in K[X]. \tag{2.2}$$

The polynomial f_{rev} has the same coefficients of f but reversed (or 'read backwards'); f_{srev} is formed by first changing the signs of the odd-degree terms, then reversing the coefficients, and then changing *all* signs if and only if $n \equiv 2, 3 \bmod 4$. This last flipping of the signs corresponds to the term $(-1)^{\frac{n(n-1)}{2}}$, which ensures that the middle coefficient of f and f_{srev} are always the same when f has even degree (in fact, we could also have chosen $(-1)^{\frac{n(n+1)}{2}}$ instead).

The *reversal transformation* $f \mapsto f_{\mathsf{rev}}$ is an involution. The same holds for the *skew-reversal transformation* $f \mapsto f_{\mathsf{srev}}$ if the degree of f is even. The even-degree polynomials that stay fixed under these involutions deserve a special name; their study is the content of this chapter.

Definition 2.1.1. Let $f \in K[X]$ be a polynomial whose constant term does not vanish. Then f is *reciprocal* if $f = f_{\mathsf{rev}}$ and f is of even degree. Similarly, f is *skew-reciprocal* if $f = f_{\mathsf{srev}}$ and f is of even degree. Furthermore, f is called *balanced* if it is either reciprocal or skew-reciprocal.

If f is reciprocal *and* skew-reciprocal (and $\operatorname{char} K \neq 2$), all coefficients of odd-degree terms of f vanish. Hence f is an *even* polynomial, that is, of the form $g(X^2)$. In addition, the degree of f must be a multiple of 4.

Remark 2.1.2. In many texts, reciprocal polynomial are defined in a slightly different manner. Reciprocality is often defined up to sign, i.e., a polynomial f is reciprocal if $f = \pm f_{\mathsf{rev}}$. In addition, the condition that the degree of f be even is often left out. There are several reasons to restrict ourselves to even-degree polynomials. First, 'reciprocal polynomials of odd degree' do exist, but each such polynomial factors as $X+1$ times a reciprocal polynomial of even degree, as an immediate consequence of the definition of the reversal polynomial. So the study of 'reciprocal polynomials of odd degree' boils down to the study of reciprocal polynomials of even degree. Secondly, it is easy to check that 'skew-reciprocal polynomials of odd degree' cannot exist – even up to sign.

There are two more ways to think of balanced polynomials: in terms of the coefficients and in terms of the roots. The former is best illustrated by taking two examples of balanced polynomials, such as

$$+X^6+X^5-X^4+X^3-X^2+X+1 \quad \text{and} \quad +X^6+X^5+X^4-X^3-X^2+X-1. \tag{2.3}$$

These are reciprocal and skew-reciprocal, respectively. The color coding highlights the fact that the coefficients of balanced polynomials come in pairs (except for the middle coefficient). This is shown in the next proposition.

Proposition 2.1.3 (Coefficient characterisation of balanced polynomials)**.** *Let $f \in K[X]$ be a polynomial of degree $2n$ for some integer n. Then f is reciprocal if and only if it is of the form*

$$f(X) = a_0 X^n + X^n \sum_{j=1}^{n} a_j (X^j + X^{-j}). \tag{2.4}$$

Similarly, f is skew-reciprocal if and only if it can be written as

$$f(X) = a_0 X^n + X^n \sum_{j=1}^{n} a_j (X^j + (-X)^{-j}). \tag{2.5}$$

Proof. Write $f = b_0 + b_1 X + \cdots + b_{2n} X^{2n}$ and assume f is reciprocal. Then $f(X) = X^{2n} f(X^{-1}) = b_{2n} + b_{2n-1} X + \cdots + b_0 X^{2n}$. Hence $b_j = b_{2n-j}$ for all j. The claim thus holds with $a_j = b_{n-j}$. Conversely, any polynomial as in (2.4) is clearly reciprocal. The proof for skew-reciprocals proceeds analogously: here, we find $b_j = (-1)^{n-j} b_{2n-j}$, so that (2.5) holds with $a_j = b_{n-j}$. □

Depending on whether f is reciprocal or skew-reciprocal, we call the a_j the *reciprocal* or *skew-reciprocal coefficients* of f. Since reciprocal polynomials have the same coefficient list read forward and backward, they are also called palindromic polynomials. This adds to a long list of other adjectives, such as self-reciprocal, inversive, self-inversive or symmetric instead of reciprocal, and skew-palindromic or skew-symmetric instead of skew-reciprocal.

For the second characterisation of balanced polynomials we need the following lemma, which is stated for reciprocals (without proof) in [**13**, Lem. 3].

Lemma 2.1.4. *Suppose that f, g and h lie in $K[X]$. If $f = gh$ and f and g are reciprocal (resp. skew-reciprocal), then h is also reciprocal (resp. skew-reciprocal).*

Proof. Reversal commutes with products of polynomials since

$$(gh)_{\mathsf{rev}}(X) = X^{\deg(gh)}(gh)(X^{-1}) = X^{\deg g} g(X^{-1}) X^{\deg h} h(X^{-1}) = g_{\mathsf{rev}}(X) h_{\mathsf{rev}}(X).$$

The series of equalities

$$gh = f = f_{\mathsf{rev}} = (gh)_{\mathsf{rev}} = g_{\mathsf{rev}}\, h_{\mathsf{rev}} = g h_{\mathsf{rev}}$$

thus shows that $h = h_{\mathsf{rev}}$. Since f and g are of even degree, so is h. So h is reciprocal.

For the skew-reciprocal case, start by noting that f, g and h have even degree. Write $\deg g = 2m$ and $\deg h = 2n$. We have

$$\begin{aligned}(gh)_{\mathsf{srev}}(X) &= (-1)^{(m+n)(2m+2n-1)} X^{\deg(gh)}(gh)(-X^{-1}) \\ &= (-1)^{4mn} \cdot (-1)^{m(2m-1)} X^m g(-X^{-1}) \cdot (-1)^{n(2n-1)} X^n h(-X^{-1}) \\ &= g_{\mathsf{srev}}(X) h_{\mathsf{srev}}(X),\end{aligned}$$

so taking the skew-reversal commutes with products of even-degree polynomials. Hence

$$gh = f = f_{\mathsf{srev}} = (gh)_{\mathsf{srev}} = g_{\mathsf{srev}}\, h_{\mathsf{srev}} = g h_{\mathsf{srev}}$$

shows that h is skew-reciprocal. □

The 'root characterisation' of balanced polynomials is spelled out as follows. Here and throughout this thesis we denote by $i \in \overline{K}$ a root of the polynomial $X^2 + 1 \in K[X]$; note that i lies in K if and only if the characteristic of K is congruent to 1 mod 4. The reciprocal case is mentioned (without proof) in [**13**, Prop. 2].

Proposition 2.1.5 (Root characterisation of balanced polynomials)**.** *Let $f \in K[X]$ be a polynomial of even degree whose constant term does not vanish. Then f is reciprocal if and only if both of the following hold:*

(1a) If 1 *is a root of* f*, then its multiplicity is even. The same holds for* -1*.*
(1b) If α *is a root of* f*, then* α^{-1} *is a root of* f *of the same multiplicity.*

Similarly, f *is skew-reciprocal if and only if both of the following hold:*

(2a) If i *is a root of* f*, then its multiplicity is even. The same holds for* $-i$*.*
(2b) If α *is a root of* f*, then* $-\alpha^{-1}$ *is a root of* f *of the same multiplicity.*

Proof. We only consider the reciprocal case: the skew-reciprocal case is entirely analogous. Suppose $\deg f = n$ is even. Denote by α_j the roots of f (in an algebraic closure of K) and by m_j the corresponding multiplicities. Write $f = a_n \cdot \prod_{j=1}^{2n}(X-\alpha_j)^{m_j}$. Then

$$\begin{aligned} f_{\mathsf{rev}} &= X^{2n} \cdot a_{2n} \cdot \prod_{j=1}^{2n}(X^{-1}-\alpha_j)^{m_j} \\ &= a_{2n} \cdot \prod_{j=1}^{2n}(1-\alpha_j X)^{m_j} \\ &= a_{2n} \cdot \prod_{j=1}^{2n}\Big((-\alpha_j)^{m_j}(X-\alpha_j^{-1})^{m_j}\Big). \end{aligned}$$

The expression $a_{2n} \cdot \prod_{j=1}^{2n}(-\alpha_j)^{m_j}$ equals the constant term of f, so that

$$f_{\mathsf{rev}}(X) = f(0) \cdot \prod_{j=1}^{2n}(X-\alpha_j^{-1})^{m_j}. \tag{2.6}$$

Suppose that f satisfies conditions (1a) and (1b). We may relabel the roots of f such that

$$f = a_{2n}(X-1)^{2a}(X+1)^{2b}\prod_{j=1}^{n}(X-\alpha_j)^{m_j}(X-\alpha_j^{-1})^{m_j}.$$

for some integers $a, b \geq 0$. Therefore

$$\begin{aligned} f_{\mathsf{rev}} &= a_{2n}(1-X)^{2a}(1+X)^{2b}\prod_{j=1}^{n}\Big((1-\alpha_j X)^{m_j}(1-\alpha_j^{-1}X)^{m_j}\Big) \\ &= a_{2n}(X-1)^{2a}(X+1)^{2b}\prod_{j=1}^{n}\Big((\alpha_j X-1)^{m_j}(\alpha_j^{-1}X-1)^{m_j}\Big) \\ &= a_{2n}(X-1)^{2a}(X+1)^{2b}\prod_{j=1}^{n}\Big(\alpha_j^{m_j}\alpha_j^{-m_j}(X-\alpha_j^{-1})^{m_j}(X-\alpha_j)^{m_j}\Big), \end{aligned}$$

which equals f. Hence f is reciprocal.

Conversely, suppose that f is reciprocal. Then $f = f_{\mathsf{rev}}$, so from (2.6) we see that $f(0) = a_n$ and $\alpha \neq \pm 1$ is a root if and only if $\alpha^{-1} \neq \alpha$ is a root of the same multiplicity. Choose $a, b \geq 0$ maximal such that $(X-1)^a(X+1)^b$ divides f, and write $g = (X-1)^{-a}(X+1)^{-b}f$. Then g lies in $K[X]$ and is reciprocal, since it satisfies conditions (1) and (2). Hence $\deg f$ and $\deg g$ are both even, so that also $a+b$ is even. We need to show that a and b must be both even.

Note that $(X+1)^2$ and $(X-1)^2$ are both reciprocal polynomials. The product of reciprocal polynomials is again reciprocal. If a and b are both odd, we find that the reciprocal polynomial f is the product of a reciprocal polynomial with $(X+1)(X-1) = X^2-1$, which is not reciprocal. This contradicts Lemma 2.1.4. □

The following lemma lists a few basic properties of a polynomial $f \in K[X]$ that are preserved under (skew-)reversing. With the *factorisation pattern* of f we mean the set of tuples of the degrees and multiplicities of each irreducible factor of f.

Lemma 2.1.6. *Let $f \in K[X]$ be a polynomial whose constant term does not vanish. Then f_{rev} and f_{srev} have the same factorisation pattern, discriminant, and Galois group (over K) as f.*

Proof. Let $f \in K[X]$ be a polynomial with $f(0) \neq 0$. Suppose that f is irreducible and f_{rev} is reducible. Write $f_{\mathsf{rev}} = gh$ where $g, h \in K[X]$ are polynomials of degree at least 1 (whose constant coefficients are necessarily nonzero). Since $f(0) \neq 0$, the reversal operation is an involution, which means that $f = (gh)_{\mathsf{rev}}$. Since reversal commutes with taking products of polynomials (see the proof of Lemma 2.1.4), we see that $f = g_{\mathsf{rev}}h_{\mathsf{rev}}$ is a factorisation of f into polynomials of degree at least 1. This contradicts the irreducibility of f. More generally, if $f = f_0 f_1 \cdots f_k$ is the factorisation of f into irreducibles, then the above shows that $f_{\mathsf{rev}} = (f_0)_{\mathsf{rev}}(f_1)_{\mathsf{rev}} \cdots (f_k)_{\mathsf{rev}}$ is the factorisation of f_{rev} into irreducibles. This shows that reversal fixes the factorisation pattern of f.

Next, we consider the discriminant. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be the roots of f (which has degree n), repeated according to their multiplicities. Denote by a_n and a_0 the leading and constant coefficient of f, respectively. Then the roots of f_{rev} are $\alpha_1^{-1}, \alpha_2^{-1}, \ldots, \alpha_n^{-1}$, and hence

$$\begin{aligned}\Delta(f_{\mathsf{rev}}) &= a_0^{2n-2} \prod_{1 \leq i < j \leq n} (\alpha_i^{-1} - \alpha_j^{-1})^2 \\ &= a_0^{2n-2} \prod_{1 \leq i < j \leq n} \left(\frac{\alpha_j - \alpha_i}{\alpha_i \alpha_j} \right)^2 .\end{aligned}$$

Each α_i appears $n-1$ times in the denominator of the last expression. Taking them out we obtain

$$\begin{aligned}\Delta(f_{\mathsf{rev}}) &= a_0^{2n-2}\prod_{1\le i\le n}\alpha_i^{-2(n-1)}\prod_{1\le i<j\le n}(\alpha_j-\alpha_i)^2\\ &= a_0^{2n-2}\cdot(a_n/a_0)^{2n-2}\cdot\prod_{1\le i<j\le n}(\alpha_j-\alpha_i)^2\\ &= \Delta(f).\end{aligned}$$

Similar proofs apply in the case of the skew-reversal polynomial.

Regarding the Galois group, we note that any $\sigma\in\mathrm{Gal}(f)$ is a field automorphism and thus $\sigma(\pm\alpha^{-1})=\pm\sigma(\alpha)^{-1}$ for any root α of f. Therefore the action on the roots of f_{rev} and f_{srev} is completely determined by the action on the roots of f, and vice versa, and the relations between the roots of f, f_{rev} and f_{srev} correspond to each other. □

2.2 The trace polynomial

Any balanced polynomial f comes equipped with a so-called *trace polynomial* of half the degree of f. Questions on the irreducibility and discriminant of a balanced polynomial can often be solved by considering the associated trace polynomial: it is thus worth studying the latter, which is the aim of this section.

Define $\mathcal{R}_{2n}$ and $\mathcal{S}_{2n}$ as the set of reciprocal and skew-reciprocal polynomials of degree $2n$ with coefficients in K, respectively. Denote by $K[X]_n$ the polynomials in $K[X]$ of degree n. The Q-transformation or reciprocal mapping

$$(-)^{\mathsf{Q}}: K[X]_n\to\mathcal{R}_{2n},\quad f(X)\mapsto f^{\mathsf{Q}}(X)=X^n f(X+X^{-1})$$

and the S-transformation or skew-reciprocal mapping

$$(-)^{\mathsf{S}}: K[X]_n\to\mathcal{S}_{2n},\quad f(X)\mapsto f^{\mathsf{S}}(X)=X^n f(X-X^{-1})$$

associate with any degree n polynomial f the reciprocal polynomial f^{Q} and skew-reciprocal polynomial f^{S}, both of degree $2n$. That f^{S} and f^{Q} are balanced follows straight from the definition. (The letter Q stands for 'quadratic' and goes back at least to [35].)

Proposition 2.1.5 asserts that the roots of f^{Q} come in pairs α, α^{-1} of the same multiplicity m; this happens if and only if $\alpha+\alpha^{-1}$ is a root of f with multiplicity m. Likewise, if α is a root of f^{S}, then so is $-\alpha^{-1}$, and $\alpha-\alpha^{-1}$ is then a root of f, all of the same multiplicity. In the literature, the transformation $f\mapsto f^{\mathsf{Q}}$ is mostly studied over finite fields, see e.g. [35], but also over $\mathbb{Q}$ in [13]. The transformation $f\mapsto f^{\mathsf{S}}$ has not

been studied thoroughly, but has similar properties, as we will show in this chapter. The main goal of this section is to show that the Q- and S-transformations are bijective.

Lemma 2.2.1. *The reciprocal and skew-reciprocal mapping are injective.*

Proof. Write r_i (with $1 \leq i \leq n$) for the n (not necessarily distinct) roots of $f \in K[X]_n$. The $2n$ (not necessarily distinct) roots of f^{Q} are the solutions to the n quadratic equations $\alpha + \alpha^{-1} = r_i$ and are hence uniquely determined by the r_i. We also see that f and f^{Q} have the same leading coefficient. Since polynomials with the same roots, corresponding multiplicities, and leading coefficients are equal, the Q-transformation is injective. The injectivity of the S-map follows likewise. □

For surjectivity, we construct the right inverse of the reciprocal and skew-reciprocal mapping explicitly, denoted respectively by

$$(-)_{\mathsf{RQ}} : \mathcal{R}_{2n} \to K[X]_n, \quad f \mapsto f_{\mathsf{RQ}}$$

and

$$(-)_{\mathsf{RS}} : \mathcal{S}_{2n} \to K[X]_n, \quad f \mapsto f_{\mathsf{RS}}.$$

The *trace polynomial* of f is f_{RQ} when f is reciprocal and f_{RS} when f is skew-reciprocal. The maps $(-)^{\mathsf{Q}}$ and $(-)^{\mathsf{S}}$ are described explicitly in the following lemma, which is the main result of this section.

Lemma 2.2.2 (Inversion formula)**.** *The reciprocal and skew-reciprocal mappings are surjective. The right inverse $(-)_{\mathsf{RQ}}$ of $(-)^{\mathsf{Q}}$ sends $f \in \mathcal{R}_{2n}$ with reciprocal coefficients $a_0, a_1, \ldots, a_n$ to $f_{\mathsf{RQ}}(X) = b_0 + b_1 X + \cdots + b_n X^n$ with coefficients*

$$b_i = a_i + \sum_{j=1}^{\lfloor \frac{n-i}{2} \rfloor} (-1)^j \frac{i+2j}{i+j} \binom{i+j}{j} a_{i+2j}. \tag{2.7}$$

Similarly, the right inverse $(-)_{\mathsf{RS}}$ of $(-)^{\mathsf{S}}$ sends $f \in \mathcal{S}_{2n}$ with skew-reciprocal coefficients a_0, $a_1, \ldots, a_n$ to $f_{\mathsf{RS}}(X) = b_0 + b_1 X + \cdots + b_n X^n$ with coefficients given by

$$b_i = a_i + \sum_{j=1}^{\lfloor \frac{n-i}{2} \rfloor} \frac{i+2j}{i+j} \binom{i+j}{j} a_{i+2j}. \tag{2.8}$$

The fractions of binomials in the summands satisfy a particular relation, captured in the following lemma.

Proposition 2.2.3. *Define*

$$t_{j,k} = \frac{k}{k-j}\binom{k-j}{j} \tag{2.9}$$

for any integers $j, k \geq 1$ such that $2j \leq k$. Then $t_{j,k}$ is an integer and satisfies the recurrence relation

$$t_{j,k+1} = t_{j,k} + t_{j-1,k-1}. \tag{2.10}$$

Proof. Two ways to write $t_{j,k}$ are

$$\frac{k(k-j-1)!}{j!(k-2j)!} = t_{j,k} = \binom{k-j}{j} + \binom{k-j-1}{j-1}.$$

The rightmost expression shows that $t_{j,k}$ is indeed an integer. With the leftmost expression in mind, we multiply both sides of (2.10) by $j!(k-2j+1)!/(k-j-1)!$ to obtain the claimed equality

$$(k+1)(k-j) = k(k-2j+1) + (k-1)j$$

which indeed holds. □

The next lemma shows how $X^k \pm X^{-k}$ is expressed in terms of $X \pm X^{-1}$, which we can then combine with (2.4) and (2.5).

Lemma 2.2.4. *For any $k \geq 1$, we have*

$$X^k + X^{-k} = (X + X^{-1})^k + \sum_{j=1}^{\lfloor k/2 \rfloor} (-1)^j \frac{k}{k-j}\binom{k-j}{j}(X + X^{-1})^{k-2j}, \tag{2.11}$$

$$X^k + (-X)^{-k} = (X - X^{-1})^k + \sum_{j=1}^{\lfloor k/2 \rfloor} \frac{k}{k-j}\binom{k-j}{j}(X - X^{-1})^{k-2j} \tag{2.12}$$

Proof. We only show (2.11), as the proof of (2.12) is analogous. We use the notation from Proposition 2.2.3 and write $Y = X + X^{-1}$ and $P_k = Y^k + \sum_{j=1}^{\lfloor k/2 \rfloor} (-1)^j t_{j,k} Y^{k-2j}$, which equals the right-hand side in (2.11). The claim certainly holds for $k = 0$ or 1. Furthermore, we have

$$X^{k+1} + X^{-(k+1)} = (X + X^{-1})(X^k + X^{-k}) - (X^{k-1} + X^{-(k-1)})$$

for any $k \geq 1$. We will show that P_k also satisfies the recurrence $P_{k+1} = YP_k - P_{k-1}$, immediately implying the claimed equalities. When k is even, we find

$$YP_k - P_{k-1} = Y^{k+1} - (t_{1,k} + 1)Y^{k-1} + \sum_{j=2}^{\lfloor k/2 \rfloor} (-1)^j (t_{j,k} + t_{j-1,k-1}) Y^{k+1-2j}$$

while P_{k+1} equals

$$P_{k+1} = Y^{k+1} - t_{1,k+1}Y^{k-1} + \sum_{j=2}^{\lfloor k/2 \rfloor} (-1)^j t_{j,k+1} Y^{k+1-2j}.$$

When k is odd, the term $2 \cdot (-1)^{(k+1)/2}$ must be added to both expressions above, coming from $j = (k+1)/2$. Regardless of the parity of k, the coefficients of degree $k \pm 1$ and 0 indeed match, and the coefficients in the sums match by Proposition 2.2.3. This proves (2.11). □

We are now ready to demonstrate Lemma 2.2.2.

Proof of Lemma 2.2.2. Let f be a reciprocal polynomial of degree $2n$ with reciprocal coefficients $a_0, a_1, \ldots, a_n$. We need to show that the given definition of the map $(-)_{\mathsf{RQ}}$ satisfies

$$(f_{\mathsf{RQ}})^{\mathsf{Q}} = f.$$

Using (2.4) and (2.11), we find that

$$\frac{f(X)}{X^n} - \sum_{i=0}^{n} a_i (X + X^{-1})^i = \sum_{i=0}^{n} \sum_{j=1}^{\lfloor i/2 \rfloor} (-1)^j t_{j,i} a_i (X + X^{-1})^{i-2j}.$$

We want to gather terms in the sum on the right-hand side by degree. Write $k = i - 2j$ for the exponent of $X + X^{-1}$ in the summand. Whenever k appears as exponent, its coefficient equals $(-1)^l t_{l,k+2l} a_{k+2l}$ for some l. Note that l can attain any value between 1 and $\lfloor (n-k)/2 \rfloor$; if l is smaller or larger, then $t_{l,k+2l}$ or a_{k+2l} is not defined. Hence

$$\sum_{i=0}^{n} \sum_{j=1}^{\lfloor i/2 \rfloor} (-1)^j t_{j,i} a_i (X + X^{-1})^{i-2j} = \sum_{k=0}^{n} \sum_{l=1}^{\lfloor \frac{n-k}{2} \rfloor} (-1)^l t_{l,k+2l} a_{k+2l} (X + X^{-1})^k. \tag{2.13}$$

On the other hand, the definition of the Q-transformation and its inverse says that

$$\begin{aligned} \frac{(f_{\mathsf{RQ}})^{\mathsf{Q}}}{X^n} - \sum_{i=0}^{n} a_i (X + X^{-1})^i &= f_{\mathsf{RQ}}(X + X^{-1}) - \sum_{i=0}^{n} a_i (X + X^{-1})^i \\ &= \sum_{i=0}^{n} \sum_{j=1}^{\lfloor \frac{n-i}{2} \rfloor} (-1)^j t_{j,i+2j} a_{i+2j} (X + X^{-1})^i, \end{aligned}$$

which coincides with (2.13). The proof of the skew-reciprocal case proceeds in analogous fashion. □

Remark 2.2.5. Recall that for any $k \geq 0$, the Chebyshev polynomial $T_k(Y)$ is the unique k-th degree polynomial satisfying $T_k(\cos\theta) = \cos k\theta$. Hence $T_0 = 1$ and $T_1 = Y$. It satisfies the recurrence relation

$$T_{k+1}(Y) = 2Y\,T_k(Y) - T_{k-1}(Y).$$

Consider the scaled Chebyshev polynomial $\widetilde{T}_k(Y) = 2T_k(Y/2)$. Then $\widetilde{T}_0 = 2$, $\widetilde{T}_1 = Y$, and $\widetilde{T}_k$ satisfies the recurrence relation

$$\widetilde{T}_{k+1}(Y) = Y\,\widetilde{T}_k(Y) - \widetilde{T}_{k-1}(Y), \tag{2.14}$$

which is the recurrence relation shown for the polynomials P_k in Lemma 2.2.4. Since the initial values of P_k and $\widetilde{T}_k$ also agree, the right-hand side in (2.11) equals $\widetilde{T}_k(X + X^{-1})$.

Corollary 2.2.6. *Let $f \in \mathbb{Z}[X]$ be a balanced polynomial with balanced coefficients $a_0, a_1, \ldots, a_n$. Denote by b_i the coefficients of the trace polynomial of f. Then b_0 and a_0 have the same parity, as do b_1 and the sum $a_1 + a_3 + a_5 + \cdots$ of the balanced coefficients with odd index.*

Proof. Since $t_{j,2j} = 2$ is even and $t_{j,2j+1} = 2j+1$ is odd, the results follow from (2.7) and (2.8). □

2.3 Discriminants

In this section, we relate the discriminant of a balanced polynomial to that of its trace polynomial.

Theorem 2.3.1 (Square discriminant criterion)**.** *Let $f \in K[X]$ be a balanced polynomial of degree $2n$. Suppose that f is reciprocal. Then*

$$\Delta(f) = f_{\mathsf{RQ}}(-2)f_{\mathsf{RQ}}(2)\Delta(f_{\mathsf{RQ}})^2 = (-1)^n f(1)f(-1)\Delta(f_{\mathsf{RQ}})^2,$$

which, assuming that f is separable, is a square if and only if $(-1)^n f(1)f(-1)$ is a square. If f is skew-reciprocal, then

$$\Delta(f) = f_{\mathsf{RS}}(2i)f_{\mathsf{RS}}(-2i)\Delta(f_{\mathsf{RS}})^2 = f(i)f(-i)\Delta(f_{\mathsf{RS}})^2$$

which, assuming that f is separable, is a square if and only if $f(i)f(-i)$ is a square, that is, if $|f(i)|$ lies in K.

Proof. Write a_n for the leading coefficient of f. If f is not monic, then $\Delta(f) = a_n^{2n-2}\Delta(f/a_n)$. Since a_n^{2n-2} is a square, we may assume without loss of generality that f is in fact monic.

First suppose that f is inseparable, so that $\Delta(f) = 0$. Assume that f is reciprocal. Then either 1 or -1 is a root of f (since these always occur with even multiplicity by Proposition 2.1.5) or f has a root α such that both α and α^{-1} have multiplicity higher than 1 (since these always have the same multiplicity by Proposition 2.1.5). In the former case, either 2 or -2 is a root of f_{RQ} (indeed, the Q-transformation of $X \pm 2$ equals $(X \pm 1)^2$), so the claim holds. In the latter case, f_{RQ} has a multiple root, so the claim holds as well. For skew-reciprocals a similar proof works, again by invoking Proposition 2.1.5.

Now assume that f is separable. First suppose that f is reciprocal and has no roots in $\{\pm 1\}$. Hence its $2n$ distinct roots come in pairs α, α^{-1}. Label these as $\alpha_1, \ldots, \alpha_n, \alpha_{n+1} = \alpha_1^{-1}, \ldots, \alpha_{2n} = \alpha_n^{-1}$. Then

$$\Delta(f) = \prod_{1 \le i < j \le n} \left((\alpha_i - \alpha_j)(\alpha_i - \alpha_j^{-1})(\alpha_i^{-1} - \alpha_j^{-1})(\alpha_i^{-1} - \alpha_j)\right)^2 \prod_{1 \le i \le n} (\alpha_i - \alpha_i^{-1})^2.$$

The first of the two products above equals the square of the discriminant of f_{RQ}, since

$$(\alpha_i - \alpha_j)(\alpha_i - \alpha_j^{-1})(\alpha_i^{-1} - \alpha_j^{-1})(\alpha_i^{-1} - \alpha_j) = (\alpha_i + \alpha_i^{-1} - \alpha_j - \alpha_j^{-1})^2.$$

The latter product can be expanded as

$$\begin{aligned}\prod_{1 \le i \le n} (\alpha_i - \alpha_i^{-1})^2 &= \prod_{1 \le i \le n} (-2 - (\alpha_i + \alpha_i^{-1}))(2 - (\alpha_i + \alpha_i^{-1})) \\ &= f_{\mathsf{RQ}}(-2) f_{\mathsf{RQ}}(2) = (-1)^n f(1) f(-1),\end{aligned}$$

as claimed.

When f is a skew-reciprocal polynomial of degree $2n$, the proof proceeds in similar fashion. Let again α_i and $\alpha_{n+i} = -\alpha_i^{-1}$ be the roots of f (with $1 \le i \le n$). Since

$$(\alpha_i - \alpha_j)(\alpha_i + \alpha_j^{-1})(-\alpha_i^{-1} + \alpha_j^{-1})(-\alpha_i^{-1} - \alpha_j) = -(\alpha_i - \alpha_i^{-1} - \alpha_j + \alpha_j^{-1})^2$$

we can again write

$$\Delta(f) = \Delta(f_{\mathsf{RS}})^2 \cdot \prod_{1 \le i \le n} (\alpha_i + \alpha_i^{-1})^2.$$

The product on the right-hand side equals $f_{\mathsf{RS}}(2i) f_{\mathsf{RS}}(-2i) = f(i) f(-i)$, as we had to show. □

The following corollary of Theorem 2.3.1 provides an easy way to identify balanced polynomials that do not have square discriminant.

Theorem 2.3.2. *Suppose $K = \mathbb{Q}$ and let $f \in \mathcal{R}_{2n}$ (or $\mathcal{S}_{2n}$) have integral (skew-)reciprocal coefficients a_i. Assume that both a_0 and $a_1 + a_3 + a_5 + \cdots$ are odd. If f has no double roots*

and no roots in $\{\pm 1\}$ *(if* f *is reciprocal) or in* $\{\pm i\}$ *(if* f *is skew-reciprocal), then* f *does not have square discrimininant.*

Proof. We only prove the reciprocal case, but the skew-reciprocal case is shown in the same way. Let $f_{\mathsf{RQ}} = b_n X^n + \cdots + b_0$. Recall that a_0 and $a_1 + a_3 + \cdots$ have the same parity as b_0 and b_1, respectively, by Corollary 2.2.6; assume these are both odd. In particular, b_0^2 and b_1^2 are congruent to 1 mod 8. If f has square discriminant, Theorem 2.3.1 implies that $f_{\mathsf{RQ}}(2) f_{\mathsf{RQ}}(-2)$ is a square. Reducing modulo 8, this gives

$$\begin{aligned} f_{\mathsf{RQ}}(2) f_{\mathsf{RQ}}(-2) &= (b_0 + 2b_1 + 4b_2 + \cdots)(b_0 - 2b_1 + 4b_2 + \cdots), \\ &\equiv b_0^2 - 4b_1^2 \equiv 5 \bmod 8. \end{aligned}$$

Since 5 is not a square modulo 8, we conclude that $f_{\mathsf{RQ}}(2) f_{\mathsf{RQ}}(-2)$ cannot be the square of an integer. □

2.4 Galois theory of balanced polynomials

How large can the Galois group of a balanced polynomial be? We have already seen that the roots of a balanced polynomial f come in pairs $\{\alpha, \pm\alpha^{-1}\}$ (at least when assuming that f is irreducible and of degree greater than 2). As any $\sigma \in \mathrm{Gal}(f)$ is a field automorphism, it must obey $\sigma(\pm\alpha^{-1}) = \pm\sigma(\alpha)^{-1}$. How exactly this affects the Galois group of f is the content of this section. As the Galois group of an extension of finite fields is cyclic, we only study the case of balanced polynomials over $\mathbb{Q}$.

Let $s_1, \ldots, s_n$ be n distinct indeterminates and denote $\boldsymbol{s} = (s_1, \ldots, s_n)$. Let $f = f(\boldsymbol{s}, X) \in \mathbb{Q}(\boldsymbol{s})[X]$ be the balanced polynomial of degree $2n$ with balanced coefficients $s_1, \ldots, s_n$. Then we call f the *general (skew-)reciprocal polynomial* of degree $2n$ (depending on whether it is reciprocal or skew-reciprocal).

The main goal of this section is to prove the isomorphism (Theorem 2.4.6 below)

$$\mathrm{Gal}(f/\mathbb{Q}(\boldsymbol{s})) \cong C_2 \wr S_n, \tag{2.15}$$

where the group on the right-hand side, realised as a so-called *wreath product* of C_2 and S_n, is known as the *hyperoctahedral group*. This implies (see [**51**, §61]) that any separable specialization of $f(\boldsymbol{s}, X)$ (i.e., replacement of the indeterminates s_i by numbers $a_i \in \mathbb{Q}$ such that the resulting polynomial $f(X) \in \mathbb{Q}[X]$ is separable) has Galois group contained in $C_2 \wr S_n$.

The realisation of $C_2 \wr S_n$ as a wreath product is the most suitable to show that the isomorphism above holds. Two other ways to view the hyperoctahedral group, namely as the *Coxeter group* $\mathcal{B}_n$ or as the *signed permutation group*, are useful in other contexts;

we introduce these perspectives in the second part and show that a balanced polynomial has square discriminant precisely when its Galois group is contained in a certain group known as the Coxeter group $\mathcal{D}_n$.

The results here are independent from the previous sections.

2.4.1 Semidirect products and wreath products

Here, we review two group-theoretic constructions, called the *semidirect product* and *wreath product*.

Definition 2.4.1. Given two groups N and H and a homomorphism

$$\varphi : H \ni h \mapsto \varphi_h \in \mathrm{Aut}(N),$$

the *semidirect product* $N \rtimes_\varphi H$ is the group with elements $N \times H$ and operation

$$(n,h) \bullet (n',h') = (n\varphi_h(n'), hh').$$

Definition 2.4.2. Let K be a group and $H < S_n$ a group, thought of as a permutation group on n elements. The *wreath product* $K \wr H$ is the semidirect product $K^n \rtimes_\varphi H$, where H acts on the n copies of K by permuting its coordinates. That is,

$$\varphi : H \ni \sigma \mapsto \varphi_\sigma \in \mathrm{Aut}(K^n),$$

where the automorphism φ_σ is given by

$$\varphi_\sigma(k_1, \ldots, k_n) = (k_{\sigma(1)}, \ldots, k_{\sigma(n)}).$$

It turns out that the Galois group of a balanced polynomial is contained in a certain wreath product known as the hyperoctahedral group.

Example 2.4.3. The *hyperoctahedral group* is the wreath product $C_2 \wr S_n$, i.e., the group

$$C_2^n \rtimes_\varphi S_n,$$

where φ is the action $S_n \to \mathrm{Aut}(C_2^n)$ sending $\sigma \mapsto \varphi_\sigma$, with

$$\varphi_\sigma : C_2^n \to C_2^n, \quad (\epsilon_1, \ldots, \epsilon_n) \mapsto (\epsilon_{\sigma(1)}, \ldots, \epsilon_{\sigma(n)})$$

i.e., given by permuting the n copies of C_2. Equivalently, $C_2 \wr S_n$ is the group with elements $C_2^n \times S_n$ and operation

$$((\epsilon_1, \ldots, \epsilon_n), \sigma) \cdot ((\epsilon'_1, \ldots, \epsilon'_n), \sigma') = ((\epsilon_1 \epsilon'_{\sigma(1)}, \ldots, \epsilon_n \epsilon'_{\sigma(n)}), \sigma\sigma').$$

To prove the isomorphism (2.15), we also need the following.

Definition 2.4.4. A short exact sequence $1 \to N \to G \xrightarrow{\beta} H \to 1$ is called *split* if there is a group homomorphism $\beta' : H \to G$ such that $\beta \circ \beta' = \mathrm{id}_H$.

Lemma 2.4.5. *A short exact sequence* $1 \to N \xrightarrow{\alpha} G \xrightarrow{\beta} H \to 1$ *is split if and only if there is a homomorphism* $\varphi : H \to \mathrm{Aut}(N)$ *and an isomorphism* $\theta : G \to N \rtimes_\varphi H$ *such that the diagram*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \xrightarrow{\alpha} & G & \xrightarrow{\beta} & H & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \theta} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 1 & \longrightarrow & N & \xrightarrow{\mathrm{incl}} & N \rtimes_\varphi H & \xrightarrow{\mathrm{proj}} & H & \longrightarrow & 1 \end{array}$$

commutes (where maps in the bottom short exact sequence are inclusion $\mathrm{incl} : n \mapsto (n,1)$ *and projection* $\mathrm{proj} : (n,h) \mapsto h$*). In that case, the map* φ *is given by*

$$\varphi_h(n) = \alpha^{-1}\left(\beta'(h)\alpha(n)\beta'(h^{-1})\right), \tag{2.16}$$

where β' *is a section of* β.

Proof. See e.g. [17, Theorem 3.3]. □

Theorem 2.4.6. *Let* $f(\boldsymbol{s},X) \in \mathbb{Q}(\boldsymbol{s})[X]$ *be the general (skew-)reciprocal polynomial of degree* $2n$*. Then*

$$\mathrm{Gal}(f/\mathbb{Q}(\boldsymbol{s})) \cong C_2 \wr S_n.$$

For the proof we partly follow [48], supplying some more details.

Proof. Denote the $2n$ roots of f by r_i and $r_{n+i} = \upsilon r_i^{-1}$, where $\upsilon \in \{\pm 1\}$ is a fixed sign that equals 1 if f is reciprocal and -1 if f is skew-reciprocal. Write $G = \mathrm{Gal}(f/\mathbb{Q}(\boldsymbol{s}))$ for the Galois group of the splitting field of $f(\boldsymbol{s},X)$ over $\mathbb{Q}(\boldsymbol{s})$, and set $t_i = r_i + \upsilon r_i^{-1}$. Note that the t_i are the roots of the trace polynomial $\widetilde{f}$ of f.

Each element τ of the Galois group G is determined by its action on the roots of f. Since such elements are field homomorphisms, they satisfy $\tau(\upsilon r_i^{-1}) = \upsilon\tau(r_i)^{-1}$. Hence τ is determined by its action on just n roots of f, and we obtain a homomorphism

$$\beta : G \to S_n, \quad \beta(\tau)(i) = j \quad \text{if} \quad \tau(\{r_i, \upsilon r_i^{-1}\}) = \{r_j, \upsilon r_j^{-1}\}.$$

Equivalently, $\beta(\tau)(i) = j$ if $\tau(t_i) = t_j$. But this is a condition on the roots of $\widetilde{f}$. We want to show that β is surjective; from the above, it is clear that this is equivalent to showing that the Galois group of $\widetilde{f}$ over $\mathbb{Q}(\boldsymbol{s})$ is S_n.

To this end, denote the indeterminate coefficients of $\widetilde{f}$ by $\boldsymbol{e} = (e_1, \ldots, e_n)$. We know from Lemma 2.2.2 that the e_i are $\mathbb{Z}$-linear combinations of the s_i, and certainly the converse is also true. Hence

$$\mathbb{Q}(\boldsymbol{s}) = \mathbb{Q}(\boldsymbol{e}).$$

Note that $\mathbb{Q}(\boldsymbol{t})$ is the splitting field of $\widetilde{f}$ over $\mathbb{Q}(\boldsymbol{e})$, and is contained in the splitting field L of f. We claim that

$$\mathrm{Gal}(\mathbb{Q}(\boldsymbol{t})/\mathbb{Q}(\boldsymbol{e})) \cong S_n.$$

Indeed, since the e_i are, up to sign, the elementary symmetric polynomials of the t_i, the field $\mathbb{Q}(\boldsymbol{e})$ is fixed by the action of any permutation in the symmetric group S_n on the t_i. So $\mathbb{Q}(\boldsymbol{e})$ lies in the fixed field $\mathbb{Q}(\boldsymbol{t})^{S_n}$. Since the extension $\mathbb{Q}(\boldsymbol{e}) \subset \mathbb{Q}(\boldsymbol{t})$ has degree not exceeding $n!$, but

$$\mathbb{Q}(\boldsymbol{e}) \subset \mathbb{Q}(\boldsymbol{t})^{S_n} \subset \mathbb{Q}(\boldsymbol{t})$$

and $[\mathbb{Q}(\boldsymbol{t}) : \mathbb{Q}(\boldsymbol{t})^{S_n}] = |S_n| = n!$, we must conclude that $\mathbb{Q}(\boldsymbol{t})^{S_n} = \mathbb{Q}(\boldsymbol{e}) = \mathbb{Q}(\boldsymbol{s})$. Hence β is surjective.

Now we demonstrate that the Galois group of f has the claimed structure. The kernel of β consists of all τ such that $\tau(r_i)$ is r_i or υr_i^{-1} for each i. Each such τ is completely characterised by a choice of n signs, with the i-th sign being positive if $\tau(r_i) = r_i$ and negative if $\tau(r_i) = \upsilon r_i^{-1}$. This corresponds to an element of C_2^n. Conversely, each element of C_2^n prescribes an element of τ in the kernel of β according to

$$\alpha : C_2^n \to G, \quad (\epsilon_1, \ldots, \epsilon_n) \mapsto \tau : r_i \mapsto \begin{cases} r_i & \text{if } \epsilon_i = 1, \\ \upsilon r_i^{-1} & \text{if } \epsilon_i = -1, \end{cases}$$

which is an injective group homomorphism. Hence $\ker\beta \cong C_2^n \cong \mathrm{im}\,\alpha$. The resulting short exact sequence

$$1 \to C_2^n \xrightarrow{\alpha} G \xrightarrow{\beta} S_n \to 1$$

splits, since

$$\beta' : S_n \to G, \quad \sigma \mapsto (\beta'(\sigma) : r_i \mapsto r_{\sigma(i)})$$

is a homomorphism and a right-inverse of β. By Lemma 2.4.5, the group G is isomorphic to the semi-direct product $C_2^n \rtimes_\varphi S_n$, where the the homomorphism $\varphi : S_n \to \mathrm{Aut}(C_2^n)$ as in (2.16) is given by

$$\begin{aligned} \varphi_\sigma((\epsilon_i)_i) &= \alpha^{-1}\left(\beta'(\sigma)\alpha((\epsilon_i)_i)\beta'(\sigma^{-1})\right) \\ &= \alpha^{-1}\left(\beta'(\sigma^{-1}) \circ \alpha((\epsilon_i)_i) \circ \beta'(\sigma)\right) \\ &= (\epsilon_{\sigma(i)})_i. \end{aligned}$$

This is exactly the map φ that makes the semi-direct product $C_2^n \rtimes_\varphi S_n$ into the wreath product $C_2 \wr S_n$ (see Example 2.4.3). □

2.4.2 Square discriminants and Coxeter groups

Theorem 2.4.6 implies that the Galois group of a separable balanced polynomial f of degree $2n$ is contained in $C_2 \wr S_n$. We are now interested to know what further restrictions we find when such a polynomial has square discriminant. In that case, $\mathrm{Gal}(f) \subset A_{2n}$ must have even index in the hyperoctahedral group, because

$$\frac{|A_{2n}|}{|C_2 \wr S_n|} = \frac{(2n)!/2}{2^n n!} = \frac{1}{2} \cdot 1 \cdot 3 \cdot 5 \cdot \ldots \cdot (2n-1)$$

is half an integer. One would maybe guess that the index-2 group we look for is $C_2 \wr A_n$, but that is not true.

Definition 2.4.7. We say that $\tau = ((\epsilon_i)_i, \sigma) \in C_2 \wr S_n$ is *even-signed* when the product of all ϵ_i's equals 1 (equivalently, when $\epsilon_i = -1$ for an even number of ϵ_i's).

The set of even-signed elements of $C_2 \wr S_n$ forms a subgroup of index 2, which we will denote by D_n (note that this is not the dihedral group!).

Lemma 2.4.8. *Let f be an irreducible balanced polynomial of degree $2n$. Then f has square discriminant if and only if its Galois group is contained in the subgroup D_n of even-signed elements of $C_2 \wr S_n$.*

Proof. Denote by r_i and υr_i^{-1} the roots of f, where υ is a fixed sign depending on whether f is skew-reciprocal. Recall from the proof of Theorem 2.3.1 that

$$W = \prod_i \left(r_i - \upsilon r_i^{-1}\right)$$

lies in $\mathbb{Z}$ if and only if f has square discriminant. A signed permutation $\tau = ((\epsilon_i)_i, \sigma) \in \mathrm{Gal}(f) \subset C_2 \wr S_n$ maps

$$r_i \mapsto \begin{cases} r_{\sigma(i)} & \text{if } \epsilon_i = 1, \\ \upsilon r_{\sigma(i)}^{-1} & \text{if } \epsilon_i = -1, \end{cases}$$

so

$$\tau(r_i - \upsilon r_i^{-1}) = \epsilon_i (r_{\sigma(i)} - \upsilon r_{\sigma(i)}^{-1}).$$

Therefore τ fixes W precisely when the product of all ϵ_i equals 1, that is, when τ is even-signed. □

The groups $C_2 \wr S_n$ and D_n can be represented as so-called Coxeter groups, which is shown in the remainder of this section.

Definition 2.4.9. A *Coxeter group* is a group with a presentation of the form

$$\langle \tau_1, \ldots, \tau_n \mid (\tau_i \tau_j)^{c_{ij}} = 1 \rangle,$$

where $c_{ii} = 1$ and $c_{ij} \geq 2$ for $i \neq j$. For $n \geq 2$, the group $\mathcal{B}_n$ is the Coxeter group with n generators, $c_{i,i+1} = 3$ for $i \leq n-2$, and $c_{n-1,n} = 4$. For $n \geq 4$, the group $\mathcal{D}_n$ is the Coxeter group with n generators, such that $c_{i,i+1} = 3$ for $i \leq n-2$ and $c_{n-2,n} = 3$.

Lemma 2.4.10. *The groups $C_2 \wr S_n$ and $\mathcal{B}_n$ are isomorphic for $n \geq 4$.*

Proof. The idea of this proof comes from [33, p. 5]. Define for each $i \leq n-1$ the element $\tau_i = (1, \ldots, 1, (i\ i{+}1))$ in the wreath product $C_2 \wr S_n$. Then $\tau_i \tau_{i+1} = (1, \ldots, 1, (i\ i{+}1\ i{+}2))$, which has order 3, for all $i \leq n-2$. Setting $\tau_n = (1, \ldots, 1, -1, \mathrm{id})$ in addition, the elements τ_i all have order 2 and $\tau_{n-1}\tau_n = (1, \ldots, 1, -1, 1, (n-1\ n))$ has order 4 since

$$(\tau_{n-1}\tau_n)^2 = (1, \ldots, 1, -1, -1, \mathrm{id}).$$

Hence the τ_i generate a subgroup of $C_2 \wr S_n$ isomorphic to $\mathcal{B}_n$ for $n \geq 4$. Do they also generate $C_2 \wr S_n$? Since the adjacent transpositions $(i\ i{+}1)$ with $i \leq n-1$ generate S_n, any element of the form $(1, \ldots, 1, \sigma)$ is a product of elements of the form $(1, \ldots, 1, (i\ i{+}1)) = \tau_i$. The identities

$$\tau_i \cdots \tau_{n-1}\tau_n\tau_{n-1} \cdots \tau_i = (1, \ldots, 1, -1, 1, \ldots, 1, \mathrm{id})$$

(with the -1 in the i-th place) and

$$(1, \ldots, 1, -1, 1, \ldots, 1, \mathrm{id}) \cdot (\epsilon_1, \ldots, \epsilon_n, \sigma) = (\epsilon_1, \ldots, -\epsilon_i, \ldots, \epsilon_n, \sigma)$$

show that the τ_i indeed generate the full group $C_2 \wr S_n$. □

Lemma 2.4.11. *The group of even-signed permutations $D_n \subset C_2 \wr S_n$ is isomorphic to the Coxeter group $\mathcal{D}_n$.*

Proof. The idea of this proof comes from [33, p. 5]. Define the τ_i with $i \leq n-1$ as above, but set $\tau_n = (1, \ldots, 1, -1, -1, (n-1\ n))$. We want to show that the τ_i generate both $\mathcal{D}_n$ and D_n.

Again all τ_i have order 2. To demonstrate that the τ_i generate $\mathcal{D}_n$, it only remains to show that $\tau_{n-2}\tau_n$ has order 3. Now

$$\tau_{n-2}\tau_n = (1, \ldots, 1, -1, 1, -1, (n-2\ n-1\ n))$$

and

$$(\tau_{n-2}\tau_n)^2 = (1, \ldots, 1, -1, -1, 1, (n-2\ n\ n-1)).$$

One more calculation shows that $\tau_{n-2}\tau_n$ indeed has order 3.

Since all τ_i are even-signed elements of $C_2 \wr S_n$, they generate a subgroup of D_n; to show that all of D_n is generated, first note that, again, the τ_i with $i \leq n-1$ generate any element of the form $(1,\dots,1,\sigma)$ with $\sigma \in S_n$. Conjugating

$$\tau_n\tau_{n-1} = (1,\dots,1,-1,-1,\mathrm{id})$$

with $\tau_{i,j} = (1,\dots,1,(i\ n-1)(j\ n))$ gives

$$(1,\dots,-1,\dots,-1,\dots,1,\mathrm{id})$$

with -1 in the i-th and j-th places. It is now not hard to see that any element of D_n is generated by the τ_i: indeed, after conjugating $\tau_n\tau_{n-1}$ with $\tau_{1,2}$, we can again multiply with $\tau_n\tau_{n-1}$ to introduce two more entries with -1; conjugating this with $\tau_{3,4}$ and repeating, we can first form any element of D_n of the form $(-1,-1,\dots,-1,1,1,\dots,1,\mathrm{id})$ with an even number $2k$ initial -1s followed by $n-2k$ entries containing 1s; conjugating this by an element of the form $(1,\dots,1,\sigma')$ moves the $2k$ entries with -1 to any position; postmultiplying this by $(1,\dots,1,\sigma)$ thus gives the element of D_n with $2k$ entries containing -1 in any desired position, paired with the permutation σ. This is any element of D_n, so the τ_i generate D_n. □

2.5 Irreducibility

In this section, we discuss some characteristics of the factorisation of balanced polynomials over $K = \mathbb{Q}$, $\mathbb{F}_p$. The results are largely based on the overview of factorisation properties of reciprocal polynomials over $\mathbb{Q}$ listed in [**13**], and we supply references where suitable; there is, however, a slight difference between the definitions in [**13**] and in this thesis, already addressed in Remark 2.1.2.

Throughout this section, we let f, g and h be nonconstant polynomials in $K[X]$ unless stated otherwise. One elementary property regarding the factorisation of balanced polynomials was already discussed in Lemma 2.1.4: if $f = gh$ and f and g are (skew-)reciprocal, then h is (skew-)reciprocal too.

Lemma 2.5.1. *Suppose that f is reciprocal (resp. skew-reciprocal) and of degree $2n$. Let g be an irreducible factor of f over K that is nonreciprocal (resp. non-skew-reciprocal). Then $f = g\,g_{\mathsf{rev}}\,h$ (resp. $f = g\,g_{\mathsf{srev}}\,h$) with h reciprocal (resp. skew-reciprocal) and possibly constant.*

Proof. We prove the skew-reciprocal case; this is based on [**13**, Prop. 5], which concerns the reciprocal case. Let g be a non-skew-reciprocal degree-m irreducible factor of f. Then g_{srev} is also irreducible and of degree m by Lemma 2.1.6. If α is a root of g, then $-\alpha^{-1}$ is

a root of g_{srev}; both are roots of f, so g_{srev} is a factor of f. Supposing that g and g_{srev} do not share a root, we find that $g\,g_{\mathsf{srev}}$ is a factor of f — and a skew-reciprocal one since

$$\begin{aligned}(g\,g_{\mathsf{srev}})_{\mathsf{srev}}(X) &= (-1)^{\frac{2m(2m-1)}{2}} X^{2m} g(-X^{-1}) g_{\mathsf{srev}}(-X^{-1}) \\ &= (-1)^m X^{2m} g(-X^{-1}) \cdot (-1)^{\frac{m(m-1)}{2}} (-X^{-1})^m g(X) \\ &= (-1)^{\frac{m(m-1)}{2}} X^m g(-X^{-1}) g(X) \\ &= g\,g_{\mathsf{srev}}(X).\end{aligned}$$

Now suppose that g and g_{srev} do share a root. By irreducibility, the polynomials g and g_{srev} must coincide up to multiplication by a unit in K (note that irreducible polynomials over K are separable). So if α is a root of g, then $-\alpha^{-1}$ is so too (both with multiplicity 1 since g is separable). There are two possibilities: First, if i is not a root of g, then g is skew-reciprocal by Proposition 2.1.5, contradicting our assumptions. Secondly, if i is a root, then $g = u(X^2+1)$ or $g = u(X-i)$ with $u \in K^\times$ a unit, depending on whether i lies in K or not. Hence $g_{\mathsf{srev}} = -g$ or $g_{\mathsf{srev}} = -ig$, respectively. So g is not skew-reciprocal. However, Proposition 2.1.5 says that $g\,g_{\mathsf{srev}}$ is a skew-reciprocal factor of f nonetheless, since the multiplicity of i as a root of a skew-reciprocal polynomial is even. Lemma 2.1.4 shows that h is thus also skew-reciprocal. □

Lemma 2.5.2. *Let $f \in K[X]$ be a balanced polynomial of degree $2n$ with $f(1) \neq 0$ if f is reciprocal or $f(i) \neq 0$ if f is skew-reciprocal. Then the trace polynomial of f is reducible over K if and only if f is reducible over K and f cannot be written as $u\,g\,g_{\mathsf{rev}}$ (or $u\,g\,g_{\mathsf{srev}}$) where g is irreducible and not (skew-)reciprocal, and $u \in K^\times$.*

Proof. We prove the skew-reciprocal case; this is based on [**13**, Prop. 8], which concerns the reciprocal case. If $f_{\mathsf{RS}} = f_0 f_1$ is reducible, then $f = f_0^{\mathsf{S}} f_1^{\mathsf{S}}$, so f is also reducible and factors as the product of skew-reciprocal polynomials. Assume that f also factors as $u\,g\,g_{\mathsf{srev}}$, where g is an irreducible, non-skew-reciprocal and $u \in K^\times$. Then g_{srev} is also irreducible and $\deg g = \deg g_{\mathsf{srev}} = n$. In particular, f_0^{S} and f_1^{S} must also be of degree n, and in fact equal to g and g_{srev} (up to multiplication by a unit) respectively, by irreducibility of the latter. But then g is a skew-reciprocal polynomial, contrary to our assumptions.

Conversely, assume that f is reducible but does not factor as $u\,g\,g_{\mathsf{srev}}$ with u and g as before. Write $f = hk$ with h irreducible. If h is not skew-reciprocal, then $k = h_{\mathsf{srev}}\,\widetilde{k}$ with $\widetilde{k}$ skew-reciprocal by Lemma 2.5.1. Note that $\widetilde{k}$ is nonconstant — otherwise f would factor as uhh_{srev}, contrary to our assumptions. Setting $\widetilde{h} = hh_{\mathsf{srev}}$ yields $f = \widetilde{h}\widetilde{k}$, which is a product of skew-reciprocal polynomials (of degree larger than 1). Since skew-reversal commutes with products, we obtain the factorisation $f_{\mathsf{RS}} = \widetilde{g}_{\mathsf{RS}}\widetilde{h}_{\mathsf{RS}}$ at the trace level, so also f_{RS} is reducible. □

Lemma 2.5.3. *Let f be a separable balanced polynomial whose trace polynomial is irreducible over K. If f is reducible over K, then the discriminant of f is a square. (Phrased in Galois-theoretic terms, the Galois group $\mathrm{Gal}(f)$ is transitive if it is not contained in A_{2n}.)*

Proof. Consider such f and assume that f is reducible over K. Lemma 2.5.2 implies that $f = u g g_{\mathsf{rev}}$. Hence $\Delta(f)$ is a square, because

$$\Delta(f) = \Delta(g g_{\mathsf{rev}}) = \Delta(g)\Delta(g_{\mathsf{rev}})\operatorname{Res}(g, g_{\mathsf{rev}})^2 = \Delta(g)^2 \operatorname{Res}(g, g_{\mathsf{rev}})^2$$

by Lemma 1.1.3. In the last step we used that the discriminant is invariant under reversion of the coefficients. The same proof also holds for skew-reciprocal polynomials, since the discriminant also satisfies $\Delta(f(X)) = \Delta(f(-X))$.

Alternatively, invoking the square-discriminant criteria given in Theorem 2.3.1 gives the same result. □

Using Theorem 2.3.2, we conclude the following.

Corollary 2.5.4. *Let $f \in \mathbb{Z}[X]$ be a separable balanced polynomial of degree $2n$ with balanced coefficients denoted by a_i. Suppose that f has no roots in $\{\pm 1\}$ or $\{\pm i\}$ depending on whether f is reciprocal or skew-reciprocal. If a_0 and $a_1 + a_3 + a_5 + \cdots$ are odd, then f is irreducible if and only if the trace polynomial of f is irreducible.*

We also record the following irreducibility criteria for reciprocal polynomials, which will be particularly helpful in in Chapter 4. This is Theorem 11 in [**13**].

Lemma 2.5.5. *Let $f \in \mathbb{Z}[X]$ be a monic reciprocal polynomial whose trace polynomial f_{RQ} is irreducible over $\mathbb{Q}$. Then f is irreducible if one (or more) of the following conditions are satisfied:*

(1) The value $|f(1)|$ or $|f(-1)|$ is not a square;
(2) The value $f(1)$ and the middle coefficient of f have opposite signs;
(3) The middle coefficient of f lies in $\{-1, 0, 1\}$.

Proof. Suppose to the contrary that f is reducible. If f is reducible, then it factors as $u g g_{\mathsf{rev}}$ with g some irreducible polynomial by Lemma 2.5.2. By Gauss' lemma, the unit $u \in \mathbb{Q}^\times$ lies in $\mathbb{Z}^\times = \{\pm 1\}$.

Since $g(1) = g_{\mathsf{rev}}(1)$ we find that $|f(1)| = |g(1)|^2$; similarly, $|g(-1)| = |g_{\mathsf{rev}}(-1)|$ implies that $|f(-1)| = |g(-1)|^2$. This shows (1). For (3), expanding the product $\pm g g_{\mathsf{srev}}$ reveals that the middle coefficient of f is plus or minus the sum of the squares of the coefficients of g, which is at least 2 in absolute value since the leading and constant coefficient of g must be at least 1 in absolute value. For (2), if $f(1) = \pm g(1) g_{\mathsf{rev}}(1) = \pm g(1)^2$ is positive, then $f = g g_{\mathsf{rev}}$. Hence the middle coefficient of f equals the sum of the squares of the coefficients of g, which is positive. Similarly, if $f(1)$ is negative, then $f = -g g_{\mathsf{rev}}$, so the middle coefficient of f is negative by a similar argument as before. □

The following theorem from Meyn [35] implies that over finite fields of odd characteristic, the converse of Lemma 2.5.3 also holds. Over $\mathbb{Q}$, this is certainly false – the polynomials in (2.3) are both separable, balanced, irreducible and have square discriminant! In Chapter 4 we will see that many more examples exist.

Theorem 2.5.6. *Let q be an odd prime power and f an irreducible monic polynomial over $\mathbb{F}_q$. Then f^{Q} is reducible over $\mathbb{F}_q$ if and only if $f(2)f(-2)$ is a square in $\mathbb{F}_q$.*

The term $f(2)f(-2)$ appearing in Theorem 2.5.6 originates in the square discriminant criterion Theorem 2.3.1: if $f(2)f(-2)$ is a square in $\mathbb{F}_q$, then the discriminant of f^{Q} is a square in $\mathbb{F}_q$.

The following results combine what we have seen in this section, and will be of importance in Chapter 4 – see Theorem 4.2.9.

Theorem 2.5.7. *Let f and g be two separable reciprocal polynomials in $\mathbb{Z}[X]$. Let p be a prime such that $f \equiv g \bmod p$. Suppose that the middle coefficient of f lies in $\{-1, 0, 1\}$ and that g_{RQ} is irreducible over $\mathbb{F}_p$. Then f is irreducible over $\mathbb{Q}$. Furthermore, if the middle coefficient does not lie in $\{-1, 0, 1\}$ and f is reducible, then f has square discriminant.*

Proof. Lemma 2.2.2 shows that the image of f_{RQ} in $\mathbb{F}_p[X]$ only depends on the values of the coefficients of f modulo p. That is, it is equal to the image of g_{RQ} in $\mathbb{F}_p[X]$. Therefore f_{RQ} is irreducible over $\mathbb{F}_p$, and thus over $\mathbb{Q}$. Therefore f is irreducible by Lemma 2.5.5. The last statement follows from Lemma 2.5.3. □

Theorem 2.5.8. *Let f be a separable skew-reciprocal polynomial and g a separable reciprocal polynomial. Suppose that $f \equiv g \bmod 2$ and that g_{RQ} is irreducible over $\mathbb{F}_2$. If f is reducible over $\mathbb{Q}$, then f has square discriminant.*

Proof. Lemma 2.2.2 shows that the images of f_{RS} and g_{RQ} in $\mathbb{F}_2[X]$ coincide. Therefore f_{RS} is irreducible over $\mathbb{F}_2$, and thus over $\mathbb{Q}$. The claim follows from Lemma 2.5.3. □

The formulation of Theorems 2.5.7 and 2.5.8 is perhaps a little mysterious: the introduction of the polynomial g seems unnecessary. It is best to think of g as a polynomial with sufficiently nice properties (such as cyclotomic polynomials, see the next chapter) so that irreducibility of the trace polynomial can be easily determined.

CHAPTER 3

Applications to cyclotomic polynomials

Let again $K = \mathbb{Q}$ or $K = \mathbb{F}_p$ (where p is a prime number). For any positive integer m, the roots of the polynomial $X^m - 1 \in K[X]$ are the *m-th roots of unity* in K. If $K = \mathbb{Q}$, the irreducible factors of $X^m - 1$ with m varying are the extensively studied *cyclotomic polynomials*. Equivalently, cyclotomic polynomials can be defined as follows.

Definition 3.0.1. Let $n \in \mathbb{Z}_{\geq 1}$. The *n-th cyclotomic polynomial* $\Phi_n(X) \in \mathbb{Z}[X]$ is the minimal polynomial of $\zeta = \zeta_n = \exp(2\pi i/n)$ over $\mathbb{Q}$.

We refer to [**26**, pp. 63-66, 76–77] and [**52**, pp. 12-14] for some historical background and basic results pertaining to cyclotomic polynomials, most of which will be reproduced in this chapter.

Since Φ_n is reciprocal for all $n \geq 3$ (see Lemma 3.2.1), cyclotomic polynomials function as a toy model for general reciprocal polynomials. In this chapter, we apply the results from Chapter 2 to cyclotomic polynomials and their trace polynomials to obtain a few results about their discriminants and factorisation patterns over finite fields. Combined with Theorem 2.5.7 and Theorem 2.5.8, this yields irreducibility results about more general balanced polynomials in the next chapter – see Theorem 4.2.9.

3.1 Factorisation over finite fields

Let $n \geq 1$ be an integer. Then the roots of Φ_n are ζ_n^k for each $k \leq n$ coprime with n; these are called the *primitive n-th roots of unity*. That is,

$$\Phi_n(X) = \prod_{\substack{1 \leq k \leq n \\ \gcd(k,n)=1}} (X - \zeta_n^k).$$

The polynomial Φ_n is of degree $\varphi(n)$, where $\varphi(n)$ is the Euler-totient function, defined to be the number of integers between 1 and n that are coprime with n. For example, $\varphi(p^k) = p^{k-1}(p-1)$ for any prime p and positive integer k (only the powers of p are

not coprime with p^k). Writing $n = p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}$ for the factorisation of n into primes, φ enjoys the property

$$\varphi(n) = \varphi(p_1^{k_1}) \cdots \varphi(p_t^{k_t}) = p_1^{k_1-1}(p_1-1) \cdots p_t^{k_t-1}(p_t-1). \tag{3.1}$$

In particular, $\varphi(n)$ is even for all $n \geq 3$ and divisible by 4 unless $n = 1, 2, 4$, or of the form p^k or $2p^k$ where $p \equiv 3 \bmod 4$ is prime and $k \geq 1$. If n is divisible by three distinct odd primes, then $\varphi(n)$ is divisible by 8.

As a direct consequence of the definition, any n-th root of unity is a primitive d-th root of unity for a unique d dividing n. Therefore

$$X^n - 1 = \prod_{d|n} \Phi_d(X). \tag{3.2}$$

For example, if p is prime, the polynomial $X^p - 1$ factors as $\Phi_1(X)\Phi_p(X) = (X-1)\Phi_p(X)$, so that $\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$. Another useful lemma is the following.

Lemma 3.1.1. *Let n be an odd integer. Then $\Phi_{2n}(X) = \Phi_n(-X)$.*

Proof. Let ζ be a primitive n-th root of unity. Then $(-\zeta)^n = -1$. The order of $-\zeta$ cannot be anything else than $2n$, meaning that $-\zeta$ must be a primitive $2n$-th root of unity. Since $\varphi(2n) = \varphi(n)$, the roots of Φ_{2n} are exactly $-\zeta^k$ for k coprime with n. □

We are interested in the factorisation pattern of cyclotomic polynomials over finite fields. This information can be used to study the irreducibility of their trace polynomials over finite fields, which is the content of the next section. The core of this section is the following particular property of the factorisation of cyclotomic polynomials.

Proposition 3.1.2. *Let n be an integer and p a prime not dividing n. Denote by $\operatorname{ord}_n(p)$ the order of p in $(\mathbb{Z}/n\mathbb{Z})^\times$. Then Φ_n splits into $\varphi(n)/\operatorname{ord}_n(p)$ irreducible factors over $\mathbb{F}_p$, each of degree $\operatorname{ord}_n(p)$.*

The following two lemmas prove that the Galois group of $\mathbb{F}_p(\zeta)/\mathbb{F}_p$ has order $\operatorname{ord}_n(p)$, by exhibiting the structure of that Galois group. This is needed in the proof of Proposition 3.1.2.

Lemma 3.1.3. *The Galois group of a finite extension of $\mathbb{F}_p$ is generated by the Frobenius automorphism $\operatorname{Frob}_p : a \mapsto a^p$.*

Proof. Recall that any finite extension of $\mathbb{F}_p$ is isomorphic to $\mathbb{F}_{p^n}$ for some n, and that this extension has degree n. The Frobenius map – considered as a map from $\mathbb{F}_{p^n}$ to itself – certainly fixes $\mathbb{F}_p$. No field has zero divisors, guaranteeing that Frob_p is injective and thus bijective (as $\mathbb{F}_{p^n}$ is finite). Therefore Frob_p is contained in the Galois group of $\mathbb{F}_{p^n}/\mathbb{F}_p$.

By Lagrange's theorem, any $a \in \mathbb{F}_{p^n}$ has order dividing p^n. If all a have order dividing p^k with $k < n$, then the polynomial $X^{p^k} - X \in \mathbb{F}_{p^n}[X]$ would have p^n roots, exceeding its degree. Thefore Frob_p has order n in $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. □

Lemma 3.1.4. *Let n be an integer, p a prime not dividing n, and ζ a primitive n-th root of unity. Then Φ_n is separable over $\mathbb{F}_p$. Its splitting field $\mathbb{F}_p(\zeta)$ is an extension of $\mathbb{F}_p$ whose Galois group is isomorphic to the cyclic subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$ generated by p mod n, under the map*

$$\mathrm{Gal}(\mathbb{F}_p(\zeta)/\mathbb{F}_p) \to (\mathbb{Z}/n\mathbb{Z})^\times, \quad \sigma \mapsto a_\sigma \bmod n.$$

Here, a_σ denotes any integer that satisfies $\sigma(\zeta) = \zeta^{a_\sigma}$.

Proof. The roots of $X^n - 1$ are exactly the powers of ζ, so the splitting fields of $X^n - 1$ and Φ_n coincide. Since p does not divide n, the polynomial $X^n - 1$ and its derivative nX^{n-1} are coprime in $\mathbb{F}_p[X]$. Hence Φ_n is separable over $\mathbb{F}_p$.

For the second part, we follow [**15**, §2]. Take $\sigma \in \mathrm{Gal}(\mathbb{F}_p(\zeta)/\mathbb{F}_p)$. Since σ is an automorphism, it is multiplicative, so $\sigma(\zeta)^k = \sigma(\zeta^k)$ for any k; in particular, for $k = n$ we retrieve $\sigma(\zeta)^n = 1$. An automorphism is also injective, meaning that $\sigma(\zeta^k) \neq 1$ for any $0 < k < n$. Therefore $\sigma(\zeta)$ must be a primitive n-th root of unity, that is, of the form $\zeta^{a_{\sigma,\zeta}}$ for some $a_{\sigma,\zeta}$ coprime to n. It remains to show that $a_{\sigma,\zeta}$ does not depend on ζ. Let $\xi = \zeta^k$ be another root of unity. Then

$$\sigma(\xi) = \sigma(\zeta^k) = \sigma(\zeta)^k = \zeta^{a_{\sigma,\zeta} k} = \xi^{a_{\sigma,\zeta}},$$

so $a_{\sigma,\zeta} = a_\sigma$ is indeed independent of choice of ζ. Furthermore, we can interpret a_σ as an element of $(\mathbb{Z}/n\mathbb{Z})^\times$ since $\zeta^k = \zeta^{k+n}$ for any k. The map

$$\mathrm{Gal}(\mathbb{F}_p(\zeta)/\mathbb{F}_p) \to (\mathbb{Z}/n\mathbb{Z})^\times, \quad \sigma \mapsto a_\sigma \bmod n$$

is thus well-defined. By definition $a_\sigma a_\tau = a_{\sigma\tau}$ in $(\mathbb{Z}/n\mathbb{Z})^\times$, so it is a homomorphism. The automorphism σ is assigned to the integer 1 if and only if σ sends ζ to itself, so the kernel is trivial. The Galois group of $\mathbb{F}_p(\zeta)/\mathbb{F}_p$ is generated by Frob_p by Lemma 3.1.3, and $a_{\mathrm{Frob}_p} = p$. Therefore the image of $\mathrm{Gal}(\mathbb{F}_p(\zeta)/\mathbb{F}_p)$ is isomorphic to the cyclic subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$ generated by p mod n. □

We are now ready to prove Proposition 3.1.2.

Proof of Proposition 3.1.2. Let ζ be a primitive n-th root of unity over $\mathbb{F}_p$. By Lemma 3.1.4, the Galois group of $\mathbb{F}_p(\zeta)/\mathbb{F}_p$ has order $\mathrm{ord}_n(p)$. Therefore the minimal polynomial of ζ over $\mathbb{F}_p$ has degree $\mathrm{ord}_n(p)$. As each root of Φ_n is a primitive n-th root of unity, each irreducible factor of Φ_n over $\mathbb{F}_p$ has degree $\mathrm{ord}_n(p)$, proving the statement. □

3.2 Factorisation of trace polynomial over finite fields

In this section, we show that cyclotomic polynomials are reciprocal and study the irreducibility of their trace polynomials over finite fields.

Lemma 3.2.1. *Each cyclotomic polynomial Φ_n with $n \geq 3$ is reciprocal.*

Proof. Let ζ be a primitive n-th root of unity. Recall that the degree of Φ_n is $\varphi(n)$. Since Φ_n is irreducible, so is $(\Phi_n)_{\mathsf{rev}}$ by Lemma 2.1.6. Moreover, they must be of the same degree as the constant coefficient of the irreducible polynomial Φ_n can not vanish. Since ζ^{-1} is the multiplicative inverse of ζ as well as a primitive n-th root of unity, it must be a root of $(\Phi_n)_{\mathsf{rev}}$ as well as of Φ_n. Since both polynomials are irreducible, we conclude that they are the same up to multiplication by a constant. The result thus follows if $\Phi_n(0)$ equals the leading coefficient of Φ_n, which is 1. We have

$$\begin{aligned}\Phi_n(0) &= \prod_{\substack{1\leq k\leq n\\ \gcd(k,n)=1}} -\zeta^k = (-1)^{\varphi(n)} \prod_{\substack{1\leq k\leq n\\ \gcd(k,n)=1}} \zeta^k \\ &= \prod_{\substack{1\leq k\leq n\\ \gcd(k,n)=1}} \zeta^k = \prod_{\substack{1\leq k<n/2\\ \gcd(k,n)=1}} \zeta^k\zeta^{n-k} = \prod_{\substack{1\leq k<n/2\\ \gcd(k,n)=1}} 1 = 1.\end{aligned}$$

Here, the first equality follows from plugging 0 into the factorisation of Φ_n; the second equality holds since there are $\varphi(n)$ numbers coprime with n; and the third and fourth equality since $\gcd(n,k) = \gcd(n-k,k)$ and $\gcd(n,n/2) \neq 1$ for all $n \geq 3$ whenever it is defined (and thus $\varphi(n)$ is even for all $n \geq 3$). □

The trace polynomial $(\Phi_n)_{\mathsf{RQ}}$ is usually denoted by Ψ_n, a convention that we adopt here. It has the $\varphi(n)/2$ roots $\zeta^k + \zeta^{-k} = 2\cos(2\pi k/n)$, where $k < n/2$ is a positive integer coprime with n.

We introduce some (partly nonstandard) terminology to simplify the exposition. Write C_k for the cyclic group with k elements. Recall that $(\mathbb{Z}/n\mathbb{Z})^\times$ has $\varphi(n)$ elements. The integer n is called *cyclic* if the group $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic, i.e., isomorphic to $C_{\varphi(n)}$; any integer a that generates the cyclic group $(\mathbb{Z}/n\mathbb{Z})^\times$ is called a *primitive root* modulo n. By analogy, we say that n is *semi-cyclic* if the group $(\mathbb{Z}/n\mathbb{Z})^\times$ is isomorphic to $C_2 \times C_{\varphi(n)/2}$. Any integer a that has order $\varphi(n)/2$ in $(\mathbb{Z}/n\mathbb{Z})^\times$ is called a *semi-primitive root* modulo n.

In the following lemma, we use these concepts to show under what conditions Ψ_n is irreducible over $\mathbb{F}_p$. In the context of this thesis, the main point of obtaining such conditions is to combine them with Theorem 2.5.7 and Theorem 2.5.8 (as will be done in Chapter 4) to obtain irreducibility results on balanced Littlewood polynomials.

Lemma 3.2.2. *The polynomial Ψ_n is irreducible over $\mathbb{F}_p$ if and only one of the following holds:*

(1) *The prime p is a semi-primitive root modulo n and the two irreducible factors of Φ_n over $\mathbb{F}_p$ are not reciprocal, or*
(2) *The prime p is a primitive root modulo n.*

Proof. The reciprocal polynomial Φ_n splits into $\varphi(n)/\operatorname{ord}_n(p)$ irreducible factors of equal degree over $\mathbb{F}_p$ by Proposition 3.1.2. By Lemma 2.5.1, the factors are each either reciprocal or come in pairs g, g_{rev}. If there are more than two factors, then Φ_n can be written as the product of two reciprocal polynomials $f_1 f_2$ over $\mathbb{F}_p$. Hence Ψ_n can be written as the product of the two trace polynomials of f_1 and f_2 over $\mathbb{F}_p$. If p is a primitive root modulo n, then Φ_n is irreducible over $\mathbb{F}_p$, and therefore also Ψ_n is irreducible over $\mathbb{F}_p$. Lastly, if p is a semi-primitive root modulo n, then Ψ_n is reducible over $\mathbb{F}_p$ if and only if the two reducible factors of Φ_n over $\mathbb{F}_p$ are both reciprocal by Lemma 2.5.2. □

The following lemma describes which numbers n are cyclic or semi-cyclic.

Lemma 3.2.3. *We have*

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong C_{\varphi(n)}$$

if and only if n equals 1, 2, 4, q^k or $2q^k$ with q an odd prime and $k \geq 1$. Furthermore, we have

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong C_2 \times C_{\varphi(n)/2}$$

precisely when n is of the form 2^k with $k \geq 3$, $4q^k$ with q an odd prime, $q_1^{k_1} q_2^{k_2}$ or $2q_1^{k_1} q_2^{k_2}$ with q_1, q_2 odd primes and $(q_1-1)/2$ and $(q_2-1)/2$ coprime, and $k_1, k_2 \geq 1$.

Proof. The Chinese remainder theorem implies that

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong \prod_i (\mathbb{Z}/p_i^{k_i}\mathbb{Z})^\times \tag{3.3}$$

when $n = p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}$ is the prime factorisation of n. Recall that each of the factors on the right-hand side is cyclic if p_i is odd, and $(\mathbb{Z}/2\mathbb{Z})^\times = C_1$, $(\mathbb{Z}/4\mathbb{Z})^\times = C_2$, and $(\mathbb{Z}/2^k\mathbb{Z})^\times = C_2 \times C_{2^{k-2}}$ if $k \geq 3$. Furthermore, recall that $C_a \times C_b \cong C_{ab}$ if and only if a and b are coprime. All factors on the right-hand side of (3.3) have order $\varphi(p_i^{k_i}) = p_i^{k_i-1}(p_i-1)$, which is even for all $p_i^{k_i} > 2$ and larger than 2 for all $p_i^{k_i} > 4$; hence all these pairs are not coprime. If 2 divides n, but 4 does not, then the trivial factor $(\mathbb{Z}/2\mathbb{Z})^\times = C_1$ occurs on the right-hand side of (3.3). It is thus immediately clear that $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic if and only if n equals 1, 2, 4, p^k or $2p^k$ with p an odd prime and $k \geq 1$.

We now consider the semi-cyclic case. It is easy to check that $(\mathbb{Z}/n\mathbb{Z})^\times$ is indeed semi-cyclic in all mentioned cases; as an example, note that if $n = p^k q^l$ then

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p^k\mathbb{Z})^\times \times (\mathbb{Z}/q^l\mathbb{Z})^\times \cong C_{p^{k-1}(p-1)} \times C_{q^{l-1}(q-1)}.$$

If $(p-1)/2$ and $(q-1)/2$ are coprime, then at least one of p and q is congruent to 3 mod 4. Assuming without loss of generality that $p \equiv 3 \bmod 4$, then

$$C_{p^{k-1}(p-1)} \times C_{q^{l-1}(q-1)} \cong C_2 \times C_{p^{k-1}(p-1)/2} \times C_{q^{l-1}(q-1)} \cong C_2 \times C_{q^{l-1}(q-1)p^{k-1}(p-1)/2}.$$

The last isomorphism does not hold when $(p-1)/2$ and $(q-1)/2$ are not coprime, and we quickly see that n cannot be semi-cyclic in that case. More generally, rewriting this product required that, combined, there are not too many factors 2 in the order of the cyclic groups. Indeed, it is not hard (but tedious) to show that $(\mathbb{Z}/n\mathbb{Z})^\times$ has $C_2 \times C_2 \times C_2$ as a subgroup in all other cases. But if $(\mathbb{Z}/n\mathbb{Z})^\times$ has $C_2 \times C_2 \times C_2$ as a subgroup then it cannot be semi-cyclic, as a consequence of the rule that $C_a \times C_b \cong C_{ab}$ if and only if a and b are coprime. □

Applying Lemma 3.2.2 and Lemma 3.2.3 gives the following few results.

Theorem 3.2.4. *Supppose that p is a semi-primitive root modulo n and that $\varphi(n)$ is not divisible by 4. Then Ψ_n is irreducible over $\mathbb{F}_p$.*

Proof. Since $\varphi(n)$ is not divisible by 4, the order of p in $(\mathbb{Z}/n\mathbb{Z})^\times$ is odd. Hence the two irreducible factors of Φ_n over $\mathbb{F}_p$ are not reciprocal. Therefore Ψ_n is irreducible over $\mathbb{F}_p$ by Lemma 3.2.2. □

Theorem 3.2.5. *Suppose that p is a semi-primitive root modulo n and that $\varphi(n)$ is divisible by 4. Then Ψ_n is irreducible over $\mathbb{F}_p$ if and only if $p^{\varphi(n)/4} \not\equiv -1 \bmod n$.*

Proof. Write $\Phi_n = f_1 f_2$ for the factorisation of Φ_n over $\mathbb{F}_p$ into irreducibles. Let ζ be a root of f_1. Then the other roots of f_1 are $\zeta^p, \zeta^{p^2}, \ldots, \zeta^{p^{\varphi(n)/2-1}}$. Therefore f_1 is reciprocal if and only if $\zeta^{p^k} = \zeta^{-1}$ for some $k \in \{1, 2, \ldots, \varphi(n)/2-1\}$. This happens if and only if $p^k \equiv -1 \bmod n$. Suppose that this congruence holds. Recall that the order of p in $(\mathbb{Z}/n\mathbb{Z})^\times$ is $\varphi(n)/2$. It is clear that k cannot be smaller than $\varphi(n)/4$, as otherwise $2k < \varphi(n)/2$ while $p^{2k} \equiv 1 \bmod n$. If k is larger than $\varphi(n)/4$, then $p^{2k-\varphi(n)/2} \equiv 1 \bmod n$, but also $2k - \varphi(n)/2 < \varphi(n)/2$. Therefore k must equal $\varphi(n)/4$. The result follows from Lemma 3.2.2. □

Recall that -1 is a quadratic residue modulo n if and only if -1 is a quadratic residue modulo each of the prime powers dividing n (by the Chinese remainder theorem). It immediately follows that -1 is a quadratic residue modulo n if and only if $n = p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}$ or $n = 2p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}$, where all $k_i \geq 1$ and the p_i are primes congruent to 1 mod 4.

Proposition 3.2.6. *Suppose that n is of the form*

- *$q_1^{k_1} q_2^{k_2}$ where q_1 and q_2 are primes such that $(q_1-1)/2$ and $(q_2-1)/2$ are coprime, $q_1 \equiv 1 \bmod 4$, and k_1, $k_2 \geq 1$ are integers, or*

- $2q_1^{k_1}q_2^{k_2}$ *with* q_1, q_2, k_1, *and* k_2 *as above, or*
- 2^k *with* $k \geq 4$, *or*
- $4q^k$ *with* $q \equiv 1 \bmod 4$ *a prime number.*

Then Ψ_n *is irreducible over* $\mathbb{F}_p$ *whenever* p *is a semi-primitive root modulo* n.

Proof. In each of these cases, -1 is not a quadratic residue modulo n. (In the first two cases, the prime q_2 must be congruent to 3 mod 4 by the coprimality condition.) On the other hand, $\varphi(n)/4$ is always even by (3.1). Therefore $p^{\varphi(n)/4}$ cannot be congruent to $-1 \bmod n$ for any prime p which is a semi-primitive root modulo n. Theorem 3.2.5 thus implies the claim. □

Proposition 3.2.7. *Suppose that* n *is of the form* q^k *or* $2q^k$ *where* q *is a prime. Let* p *be a semi-primitive root modulo* n. *Then* Ψ_n *is reducible over* $\mathbb{F}_p$ *if* $q \equiv 1 \bmod 4$, *and irreducible over* $\mathbb{F}_p$ *if* $q \equiv 3 \bmod 4$.

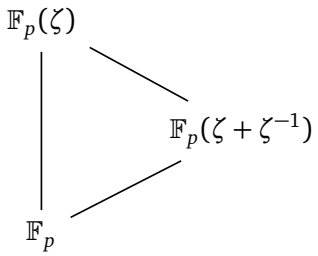
Proof. If $q \equiv 3 \bmod 4$, the result follows immediately from Theorem 3.2.4.

Now suppose that $q \equiv 1 \bmod 4$ and $n = q^k$. Then $\mathbb{F}_n = \mathbb{F}_{q^k}$ is a field and the polynomial $X^2 - 1 \in \mathbb{F}_{q^k}[X]$ has exactly two roots. Write $a = p^{\varphi(n)/4} \in \mathbb{F}_{q^k}$. Since $a^2 = 1$ we find that a is either 1 or -1; however, the order of a in $\mathbb{F}_{q^k}$ is 2, so $a = -1$. The result follows from Theorem 3.2.5 and Lemma 3.1.1. □

We present one additional proof of the case $q \equiv 3 \bmod 4$ in Proposition 3.2.7 by means of Galois theory.

Lemma 3.2.8. *Let* $n = q^k$ *where* $q \equiv 3 \bmod 4$ *is a prime number. Let* p *be a semi-primitive root modulo* n. *Then* Ψ_n *is irreducible over* $\mathbb{F}_p$.

Proof. Let ζ be a primitive q^k-th root of unity. We will show that the minimal polynomial of $\zeta + \zeta^{-1}$ over $\mathbb{F}_p$ is of degree $\varphi(q^k)/2$, which must then be equal to Ψ_{q^k}. Consider the following diagram of field extensions.



First consider the extension $\mathbb{F}_p(\zeta)/\mathbb{F}_p$. This is a finite Galois extension, so its degree equals the order of its Galois group $G = \mathrm{Gal}(\mathbb{F}_p(\zeta)/\mathbb{F}_p)$. By virtue of Lemma 3.1.4, this group is isomorphic to the cyclic subgroup of $(\mathbb{Z}/q^k\mathbb{Z})^\times$ generated by p. Hence the

degree of $\mathbb{F}_p(\zeta)/\mathbb{F}_p$ is $\varphi(q^k)/2 = q^{k-1}(q-1)/2$. In particular, the degree is odd, since $q \equiv 3 \bmod 4$. The fundamental theorem of Galois theory 1.2.1 thus dictates that $\mathbb{F}_p(\zeta)$ has no subfield of index 2.

Now consider the extension $\mathbb{F}_p(\zeta)/\mathbb{F}_p(\zeta+\zeta^{-1})$. The polynomial

$$X^2 - (\zeta+\zeta^{-1})X + 1 \in \mathbb{F}_p(\zeta+\zeta^{-1})[X]$$

has ζ as a root, showing that the index of $\mathbb{F}_p(\zeta+\zeta^{-1})$ in $\mathbb{F}_p(\zeta)$ is at most 2. By the previous paragraph, it must have index 1, i.e., the fields $\mathbb{F}_p(\zeta)$ and $\mathbb{F}_p(\zeta+\zeta^{-1})$ are equal. Therefore $\mathbb{F}_p(\zeta+\zeta^{-1})/\mathbb{F}_p$ is an extension of degree $\varphi(q^k)/2$. Hence the degree of the minimal polynomial of $\zeta+\zeta^{-1}$ is $\varphi(q^k)/2$. Since the reduction of Ψ_{q^k} modulo p in $\mathbb{F}_p[X]$ is monic and of degree $\varphi(q^k)/2$, it must be the minimal polynomial of $\zeta+\zeta^{-1}$ over $\mathbb{F}_p$, and hence it is irreducible. □

Let n be semi-cyclic and p a semi-primitive root modulo n. If n is not of any form described in Proposition 3.2.6 and Proposition 3.2.7, then Ψ_n can be either reducible or irreducible over $\mathbb{F}_p$, depending on p. By Lemma 3.2.3, the only remaining semi-cyclic numbers are $n = 4q^k$, $q_1^{k_1}q_2^{k_2}$ or $2q_1^{k_1}q_2^{k_2}$ with $q \equiv q_1 \equiv q_2 \equiv 3 \bmod 4$ all prime numbers.

3.3 Discriminants

In this section, we study when the discriminant of a cyclotomic polynomial is a square in $\mathbb{Q}$ or $\mathbb{F}_p$. The following lemma provides an explicit expression for the discriminant of a cyclotomic polynomial.

Lemma 3.3.1. *Let Φ_n be the n-th cyclotomic polynomial. Then*

$$\Delta(\Phi_n) = (-1)^{\frac{\varphi(n)}{2}} n^{\varphi(n)} \prod_{p \mid n} p^{-\frac{\varphi(n)}{p-1}}.$$

Proof. See [**52**, Prop. 2.7]. □

Using Lemma 3.3.1, it is not hard to show when the discriminant of a cyclotomic polynomial is a square. The proof of Lemma 3.3.1 requires some field theory and algebraic number theory. However, we will take a slightly different approach, namely via the square discriminant criterion Theorem 2.3.1. In order to use Theorem 2.3.1, we first need to calculate the values $\Phi_n(1)$ and $\Phi_n(-1)$ for any $n \geq 3$, which is the content of Lemma 3.3.3. We use the following lemma to carry out the calculation.

Lemma 3.3.2. *Let p be a prime and let $m, k \geq 1$ be integers. Then*

$$\Phi_{p^k m}(X) = \begin{cases} \Phi_m(X^{p^k})/\Phi_m(X^{p^{k-1}}) & \text{if } p \nmid m \\ \Phi_m(X^{p^k}) & \text{if } p \mid m. \end{cases}$$

Proof. This lemma is usually demonstrated using Möbius inversion, but what follows is an alternative proof. First suppose that p does not divide m. Note that $\Phi_m(X^{p^k})$, which is of degree $\varphi(m)p^k$, has roots $\exp(2\pi il/(p^k m))$ with l varying between 1 and $p^k m$ and coprime to m. The roots of $\Phi_{p^k m}(X)$, which is of degree $\varphi(p^k m) = p^{k-1}(p-1)\varphi(m)$ since p and m are coprime, are exactly $\exp(2\pi il/(p^k m))$ with l varying between 1 and $p^k m$ and *coprime to* $p^k m$. So α is a root of $\Phi_m(X^{p^k})$ but not of $\Phi_{p^k m}(X)$ if and only if it is of the form $\exp(2\pi il/(p^{k-1}m))$ with l varying between 1 and $p^{k-1}m$ and coprime to m. But these are precisely the roots of $\Phi_m(X^{p^{k-1}})$, which is of degree $\varphi(m)p^{k-1}$. Moreover, all mentioned roots are simple. Lastly, the degrees and leading coefficients on both sides match, so the two polynomials must be equal.

Now suppose that p divides m. Then the leading coefficients and degrees of the left-hand side and right-hand side also match (this time because $\varphi(p^k m) = p^k \varphi(m)$), and it is clear that any $p^k m$-th primitive root of unity is also a root on the right-hand side. This implies that the left-hand side and right-hand side must coincide, since the left-hand side is a minimal polynomial. □

Lemma 3.3.3. *Let $n \geq 3$. Then*

$$\Phi_n(1) = \begin{cases} p & \text{if } n = p^k \text{ with } p \text{ any prime and } k \geq 1 \\ 1 & \text{else} \end{cases}$$

and

$$\Phi_n(-1) = \begin{cases} p & \text{if } n = 2p^k \text{ with } p \text{ any prime and } k \geq 1 \\ 1 & \text{else.} \end{cases}$$

Proof. First note that ± 1 are roots of Φ_1 and Φ_2, and can therefore not be roots of Φ_n for $n \geq 3$. Let p be a prime. We already remarked that

$$\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + 1.$$

First suppose that $p = 2$, and let $k \geq 2$. Lemma 3.3.2 implies that

$$\Phi_{2^k}(\pm 1) = \Phi_2((\pm 1)^{2^{k-1}}) = \Phi_2(1) = 2.$$

Now suppose that p is odd. We know that $\Phi_p(1) = p$ and $\Phi_p(-1) = 1$. Lemma 3.3.2 implies that $\Phi_{p^k}(\pm 1) = \Phi_p((\pm 1)^{p^{k-1}}) = \Phi_p(\pm 1)$.

It remains to show that $\Phi_n(\pm 1) = 1$ for all n not of the form p^k or $2p^k$. Assume that n is indeed not of the form p^k or $2p^k$ and, moreover, that $n > 2$ is odd. Let p be a prime divisor of n and write $n = p^k m$, with $k \geq 1$ and $m \geq 3$, such that m is not divisible by p. Then

$$\Phi_{p^k m}(\pm 1) = \Phi_m((\pm 1)^{p^k})/\Phi_m((\pm 1)^{p^{k-1}}) = \Phi_m(\pm 1)/\Phi_m(\pm 1) = 1,$$

which shows the claim for odd n. Lastly, suppose that $n > 2$ is even. Write $n = 2^k m$ with $m > 1$ odd and $k \geq 1$. Invoking Lemma 3.3.2 again, we obtain $\Phi_{2^k m}(1) = \Phi_m(1)/\Phi_m(1) = 1$, and if $k > 1$ also $\Phi_{2^k m}(-1) = \Phi_m(1)/\Phi_m(1) = 1$. If $k = 1$, we have

$$\Phi_{2m}(-1) = \Phi_m(1)/\Phi_m(-1).$$

Now m is odd, but by assumption not a prime power. We have just seen that in that case, $\Phi_m(\pm 1) = 1$, so also their ratio equals 1. □

We thus obtain the following statement regarding the discriminant of a cyclotomic polynomial.

Lemma 3.3.4. *Let $n \geq 3$. The discriminant of Φ_n is not a square over $\mathbb{Q}$ if and only if $n = 4, p^k$, or $2p^k$, where p is an odd prime. More precisely, the following are equivalent:*

(1) $\Delta(\Phi_n)$ is not a square in $\mathbb{Z}$;
(2) $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic;
(3) $n = 4, p^k$ or $2p^k$ for some odd prime p and positive integer k.

Proof. By the square discriminant criterion, the discriminant of Φ_n is a square if and only if $(-1)^{\frac{\varphi(n)}{2}}\Phi_n(1)\Phi_n(-1)$ is a square. Note that $(-1)^{\frac{\varphi(n)}{2}}$ is negative if $\varphi(n)$ is not divisible by 4, and recall that this is the case if and only if $n = 4, p^k$, or $2p^k$ with $p \equiv 3 \bmod 4$ prime. In addition, Lemma 3.3.3 shows that $\Phi_n(1)\Phi_n(-1)$ is positive, and equals a square if and only if n is not of the form $n = p^k$ or $n = 2p^k$ where p is an odd prime. The first claim follows after combining these observations.

For the second claim, note that statements (2) and (3) are equivalent by Lemma 3.2.3. □

Lastly, we show over which finite fields $\mathbb{F}_p$ (with p prime) the discriminant of a cyclotomic polynomial is square. If $\Delta(\Phi_n)$ is a square, then it is a square modulo any prime. Lemma 3.3.4 implies that only the cases $n = 4, p^k$ and $2p^k$ are left, where p is an odd prime and $k \geq 1$ an integer. Since $\Phi_4(X) = X^2 + 1$, its discriminant is -4, which is a square modulo a prime q if and only if q is congruent to 1 mod 4. For the last two cases, we use the following closed-form expression for the discriminant of a cyclotomic polynomial.

Lemma 3.3.5. *Let p be an odd prime and $n = p^k$ or $n = 2p^k$. Then*

$$\left(\frac{\Delta(\Phi_n)}{q}\right) = \left(\frac{q}{p}\right)$$

for any prime q.

Proof. Let n be equal to p^k or $2p^k$. Note that $\varphi(2p^k) = \varphi(p^k) = p^{k-1}(p-1)$. Lemma 3.3.3 and Theorem 2.3.1 imply that $\Delta(\Phi_n)$ equals $(-1)^{\frac{p-1}{2}}p$ times a square. Hence

$$\left(\frac{\Delta(\Phi_n)}{q}\right) = \left(\frac{(-1)^{\frac{p-1}{2}}p}{q}\right) = \left(\frac{(-1)^{\frac{p-1}{2}}}{q}\right)\left(\frac{p}{q}\right).$$

Recall that -1 is a quadratic nonresidue modulo q if and only if $q \equiv 3 \bmod 4$, whereas 1 is always a quadratic residue modulo q. Therefore $(-1)^{\frac{p-1}{2}}$ is a quadratic nonresidue modulo q if and only if both p and q are congruent to 3 mod 4. In other words,

$$\left(\frac{(-1)^{\frac{p-1}{2}}}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}},$$

which yields

$$\left(\frac{\Delta(\Phi_n)}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$$

after applying quadratic reciprocity. □

3.4 The polynomial $p_n(X) = (X^{n+1}-1)/(X-1)$

The polynomial

$$p_n(X) = \frac{X^{n+1}-1}{X-1} = X^n + X^{n-1} + \cdots + 1$$

is reciprocal whenever n is even. It is also a product of cyclotomic polynomials, and will feature prominently in Chapter 4. In this section, we study the discriminant of p_n and its trace polynomial.

Lemma 3.4.1. *Let $n \in \mathbb{Z}_{\geq 1}$. The discriminant of p_n equals $(-1)^{\frac{n(n-1)}{2}}(n+1)^{n-1}$.*

Proof. Lemma 1.1.3 implies that

$$\Delta(X^{n+1}-1) = \Delta((X-1)p_n) = \Delta(p_n)\Delta(X-1)\operatorname{Res}(p_n, X-1)^2.$$

The roots of p_n are $\zeta = \exp(\frac{2\pi i}{n+1})$ and $\zeta^2, \ldots, \zeta^n$. Using (1.1) and (1.2) yields

$$\operatorname{Res}(p_n, X-1) = \prod_{k=1}^{n}(\zeta^k - 1) = (-1)^n \prod_{k=1}^{n}(1-\zeta^k) = (-1)^n p_n(1) = (-1)^n(n+1)$$

and

$$\begin{aligned}\Delta(X^{n+1}-1) &= (-1)^{\frac{n(n+1)}{2}} \prod_{k=0}^{n}((n+1)\zeta^{kn}) \\ &= (-1)^{\frac{n(n+1)}{2}}(n+1)^{n+1}\prod_{k=0}^{n}\zeta^{-k} \\ &= (-1)^{\frac{n(n+1)}{2}}(n+1)^{n+1}(-1)^{n+2}\end{aligned}$$

(the product in the penultimate line extends over all roots of $X^{n+1}-1$, which is $(-1)^{n+1}$ times the constant coefficient of $X^{n+1}-1$). Hence

$$\Delta(p_n) = \frac{\Delta(X^{n+1}-1)}{\Delta(X-1)\operatorname{Res}(p_n, X-1)^2} = (-1)^{\frac{n(n-1)}{2}}(n+1)^{n-1},$$

as claimed. □

Corollary 3.4.2. *Let f be an even-degree polynomial that is congruent to some p_n modulo a prime p. If f has a multiple root, then $n \equiv -1 \bmod p$.* □

Although we won't need the following corollary, it is a nice application of the square discriminant criterion Theorem 2.3.1.

Corollary 3.4.3. *The discriminant of the trace polynomial of p_{2n} equals $(2n+1)^{n-1}$.*

Proof. The square discriminant criterion Theorem 2.3.1 implies that

$$\Delta(p_{2n}) = (-1)^n p_{2n}(1)p_{2n}(-1)\Delta((p_{2n})_{\mathsf{RQ}})^2.$$

Hence

$$\Delta((p_{2n})_{\mathsf{RQ}})^2 = \frac{\Delta(p_{2n})}{(-1)^n p_{2n}(1)p_{2n}(-1)} = \frac{(-1)^{n(2n-1)}(2n+1)^{2n-1}}{(-1)^n(2n+1)} = (2n+1)^{2n-2},$$

which shows that $\Delta((p_{2n})_{\mathsf{RQ}})$ is one of $\pm(2n+1)^{n-1}$; since all roots of $(p_{2n})_{\mathsf{RQ}}$ are real, the sign is indeed positive (see Lemma 1.1.4). □

The following proposition, which is much akin to Lemma 3.3.5, provides a succinct description of all odd primes p such that p_n has square discriminant over $\mathbb{F}_p$.

Proposition 3.4.4. *Let p be an odd prime and $n \in \mathbb{Z}_{\geq 1}$ a positive integer not congruent to -1 mod p. If n is even, then*

$$\left(\frac{\Delta(p_n)}{p}\right) = \left(\frac{p}{n+1}\right).$$

In other words, p_n does not have square discriminant over $\mathbb{F}_p$ if p is a quadratic nonresidue for an odd number of prime factors of $n+1$. Furthermore, p_n does not have square discriminant if $n \equiv p \equiv 3 \bmod 4$.

Proof. Recall from before that

$$\Delta(p_n) = (-1)^{\frac{n(n-1)}{2}}(n+1)^{n-1} \tag{3.4}$$

(i.e., the sign is negative if and only if $n \equiv 2, 3 \bmod 4$). Suppose that $n \not\equiv -1 \bmod p$. Then $\Delta(p_n) \not\equiv 0 \bmod p$. When $n \equiv p \equiv 3 \bmod 4$, the discriminant of p_n is minus a square, which is not a square modulo p by the sum of two squares theorem.

For even n, the last equality in

$$\left(\frac{\Delta(p_n)}{p}\right) = \left(\frac{(-1)^{\frac{n(n-1)}{2}}}{p}\right)\left(\frac{n+1}{p}\right)^{n-1} = \left(\frac{(-1)^{\frac{n}{2}}}{p}\right)\left(\frac{n+1}{p}\right) = \left(\frac{p}{n+1}\right)$$

is ensured by quadratic reciprocity. □

A similar result holds when $p = 2$, but its proof requires passing through the p-adics. This result, along with its implications on other polynomials congruent modulo 2 to p_n, will be discussed in the next chapter – see Lemma 4.2.3.

CHAPTER 4

Littlewood and related polynomials: algebra

4.1 Introduction

Littlewood polynomials are monic polynomials all of whose coefficients lie in $\{\pm 1\}$. They were first studied extensively by Littlewood in his papers [27, 28, 29]. He denoted the set of degree-n Littlewood polynomials by $\mathscr{F}_n$, and we will stick with his notation. Note that the cardinality of $\mathscr{F}_n$ is 2^n. The subset $\mathrm{Sq}_n \subset \mathscr{F}_n$ consists of those Littlewood polynomials whose discriminant is a square, and $\mathrm{Ir}_n \subset \mathscr{F}_n$ is the subset of irreducible Littlewood polynomials. Finally, the intersection $\mathrm{Sq}_n \cap \mathrm{Ir}_n$ is denoted by SI_n. We also recall from Chapter 2 the notation $\mathcal{R}_n$ and $\mathcal{S}_n$ for the sets of reciprocal and skew-reciprocal polynomials of degree n, respectively.

Denote by $Z(S)$ the set of zeroes in the complex plane of a set $S \subset \mathbb{Z}[X]$ of polynomials. A picture of

$$\bigcup_{n=1}^{30} Z(\mathrm{SI}_n) = \bigcup_{n=1}^{30} (Z(\mathrm{SI}_n \cap \mathcal{R}_n) \cup Z(\mathrm{SI}_n \cap \mathcal{S}_n)) \tag{4.1}$$

adorns the second page of this thesis. This fascinating picture is ample reason to study Littlewood polynomials, but we refer to the introduction of this thesis for a short primer on Littlewood polynomials, including some recently established results. Many other beautiful pictures of roots of Littlewood (and other) polynomials can be found in [4]. The decomposition at the right-hand side in (4.1) corresponds to the two colors in the picture: red for reciprocal, blue for skew-reciprocal. That these are the *only* irreducible Littlewood polynomials with square discriminant is not at all obvious – in fact, it was shown computationally for this limitied range of values of n. Indeed, numerical evidence has led to the following conjecture.

Conjecture 4.1.1. *Let $n > 1$ be an integer and $f \in \mathrm{SI}_n$. Then f is balanced and $n \equiv 0, 6 \bmod 8$. Furthermore, the set SI_n is nonempty for any $n \equiv 0, 6 \bmod 8$.*

Conjecture 4.1.1 has been verified using Sage for all Littlewood polynomials of degree ≤ 34 (which are $2^{35}-1$, or more than 34 billion polynomials). In addition, a short argument – first outlined in [7] and ascribed to Alexei Entin – shows that Conjecture 4.1.1 holds for $n \equiv 2, 4 \bmod 8$; see Lemma 4.2.3. This numerical result formed the starting point for the work on this thesis. In this chapter, we obtain partial results on Conjecture 4.1.1; however, the full conjecture remains out of reach, especially for odd n. We refer to Appendices A and B for a full overview of the numerical results in this thesis.

4.2 Consequences of Chapter 2 & 3

In this section, we establish a few consequences of the propositions in previous chapters for Littlewood polynomials, and supplement them with other general observations.

Lemma 4.2.1. *Let $f \in \mathscr{F}_n$ be a Littlewood polynomial of even degree. Then f has odd discriminant. In particular, f is separable.*

Proof. The polynomial f is congruent modulo 2 to the distinguished polynomial p_n studied in Section 3.4. The expression for the discriminant of p_n in Lemma 3.4.1 shows that the discriminant of any $f \in \mathscr{F}_n$ of even degree is odd, implying that f does not have multiple roots. □

Littlewood polynomials with multiple cyclotomic factors do exist (for example $X^3 - X^2 - X + 1 = (X-1)^2(X+1)$), but it is an open question whether noncyclotomic algebraic integers can occur as multiple root of a Littlewood polynomial.

In contrast with Lemma 4.2.1, the discriminant of f is even when n is odd. Bary-Soroker and Kozma [7, §4] list some surprising numerical results regarding the exact degree of 2 that divides the discriminant of f. They also mention the following result, due to Shoni Gilboa.

Lemma 4.2.2. *The discriminant of a Littlewood polynomial of odd degree n is divisible by 2^{n-1}.*

Proof. Denote the roots of f by α_i, the elementary symmetric polynomials by e_k (with $e_0 = 0$ and $e_k = 0$ for $k > n$) and define the power sums $s_k = \sum \alpha_i^k$ (for $k \geq 0$). Let V be the Vandermonde matrix $(\alpha_i^{j-1})_{i,j=1}^n$. Recall that $\Delta(f) = \det(V)^2$, and note that

$$\det(V)^2 = \det(V^T V) = \det(s_{i+j-2})_{i,j=1}^n.$$

One consequence of Newton's identities is that the s_k and e_k satisfy the relation

$$s_k = (-1)^{k-1} k e_k + \sum_{i=1}^{k-1} (-1)^{k-1+i} e_{k-i} s_i$$

for all $k \geq 1$. Since $e_k \equiv 1 \pmod 2$ for all $1 \leq k \leq n$ we have $s_k \equiv k + \sum_{i=1}^{k-1} s_i \pmod 2$ for all $k \leq n$. Hence if s_i is odd for all $1 \leq i < k \leq n$ then $s_k \equiv k + k - 1 \equiv 1 \pmod 2$ is odd as well. Since $s_1 = e_1 \in \{\pm 1\}$ we deduce that s_k is odd for all $k \leq n$. When $k > n$, we have $e_k = 0$, so

$$\begin{aligned} s_k &= \sum_{i=1}^{k-1} (-1)^{k-1+i} e_{k-i} s_i \equiv \sum_{i=1}^{k-1} e_{k-i} \equiv \sum_{i=k-n}^{k-1} e_{k-i} \\ &\equiv (k-1) - (k-n-1) \equiv n \equiv 1 \pmod 2 \end{aligned}$$

assuming that all s_i with $1 \leq i < k$ are odd. Therefore all the s_i are odd (indeed, also $s_0 = n$ is odd). Subtracting the first row in $(s_{i+j-2})_{i,j=1}^n$ from all the others, we can pull out a factor of 2 from every row except the first one while keeping the entries of the matrix integral. □

Most of the results in this section are based on calculations modulo 2. Lemma 4.2.2 foreshadows that these methods are hard to apply for Littlewood polynomials of odd degree, since the prime 2 ramifies.

Returning to the case that n is even, the following lemma is ascribed to Alexei Entin in [7, §4].

Lemma 4.2.3. *Let $n \equiv 2, 4 \bmod 8$. Then there is no $f \in \mathscr{F}_n$ with square discriminant – in other words, Sq_n is empty.*

Proof. Suppose that n is even and $f \in \mathscr{F}_n$. We claim that $\mathrm{Gal}(f/\mathbb{F}_2)$, which is contained in $\mathrm{Gal}(f/\mathbb{Q})$, is isomorphic to $\mathrm{Gal}(p_n/\mathbb{Q}_2)$. Suppose that the claim holds. Since the discriminant of p_n is odd by Lemma 3.4.1, it is a square in $\mathbb{Z}_2$ if and only if it is 1 mod 8. A calculation shows that the discriminant is congruent to 5 mod 8 if $n \equiv 2, 4 \bmod 8$ (and congruent to 1 mod 8 otherwise), showing that f cannot have square discriminant over $\mathbb{Q}$.

To prove the claim, first note that the reduction of p_n over the finite field $\mathbb{F}_2$ does not have a multiple root (again because p_n has odd discriminant). Denote the irreducible factors of p_n over $\mathbb{F}_2$ by $\bar{g}_1, \ldots, \bar{g}_t$. By Hensel's lemma 1.3.4, the factors $\bar{g}_i$ lift to factors g_i of p_n over $\mathbb{Z}_p[X]$, such that for each i the degrees of g_i and $\bar{g}_i$ coincide and $g_i \equiv \bar{g}_i \bmod p$. The latter condition implies that the g_i are separable and, since the $\bar{g}_i$ share no roots, also p_n is separable over $\mathbb{Q}_2$. Hence the splitting field of p_n over $\mathbb{Q}_2$ is an unramified extension of $\mathbb{Q}_2$. This implies that its Galois group is isomorphic to the Galois group of p_n over $\mathbb{F}_2$ by Lemma 1.3.8. □

Entin's lemma 4.2.3 says in particular that SI_n is empty whenever $n \equiv 2, 4 \bmod 8$, confirming Conjecture 4.1.1 in those degrees. The special case of Entin's lemma 4.2.3 for balanced polynomials of those degrees can also be deduced from Theorem 2.3.2.

Corollary 4.2.4. *No balanced Littlewood polynomial of degree* $2n \equiv 2, 4 \bmod 8$ *has square discriminant.*

Proof. Let $f \in \mathbb{Z}[X]$ be such a balanced Littlewood polynomial, with (skew-)reciprocal coefficients $a_0, a_1, \ldots, a_n$. These are all odd, so in particular a_0 is odd. Assume f is reciprocal. Since $f(\pm 1)$ has odd parity, it is nonzero. If f is skew-reciprocal, then $f(\pm i)/(\pm i)^n$ has odd real part by (2.5), so $f(\pm i)$ also doesn't vanish. In both cases, the sum of the coefficients with odd index has the same parity as the number of such coefficients, which is $\lfloor \frac{n-1}{2} \rfloor + 1$; and this is odd precisely when $n \equiv 1, 2 \bmod 4$. The result follows from Theorem 2.3.2 and the fact that no Littlewood polynomial of even degree has multiple roots. □

In Appendix A, an overview of numerical results pertaining to the irreducibility and Galois groups of Littlewood polynomials is included. Table A.2 shows that, in small and even degree, 'most' Littlewood polynomials are irreducible – although there is a lot of variation. In particular, observe that $\mathscr{F}_n$ and Ir_n coincide when $n = 1, 2, 4, 10, 12, 18$. In each of these cases (apart from $n = 1$), notice that $n+1$ is a prime for which 2 is a primitive root. This means that $\mathrm{ord}_{n+1}(2) = \varphi(n)$, and thus that $\Phi_{n+1} = p_n$ is irreducible over $\mathbb{F}_2$ by Proposition 3.1.2. We obtain the following consequence, first observed by Poonen in [41].

Lemma 4.2.5. *If* 2 *is a primitive root for* $n+1$*, each Littlewood polynomial in* $\mathscr{F}_n$ *is irreducible over* $\mathbb{F}_2$*, and thus over* $\mathbb{Q}$*.* □

What about the converse? When $n+1$ is not a prime number, the polynomial p_n is reducible since it is the product of more than one cyclotomic polynomial by (3.2). In fact, this is a special case of the following well-known construction: take Littlewood polynomials f and g of degree n and $d \geq 1$, respectively. Then the polynomial $h(X) = f(X^{d+1})g(X)$ is a Littlewood polynomial of degree $N = n(d+1) + d = (n+1)(d+1) - 1$. Varying n and d, it is clear that reducibles in $\mathscr{F}_N$ exist when $N+1$ is not prime (at least 2^{n+d} of them). We can also make h reciprocal by choosing both f and g reciprocal. That leaves the case when f is a Littlewood polynomial of degree $N = p-1$, where p is a prime for which 2 is not a primitive root. It is not known whether reducible Littlewood polynomials always exist in that case, but it can be shown that any such $f \neq \Phi_p, \Phi_{2p}$ has no cyclotomic factor.

Lemma 4.2.6. *Suppose* $f \in \mathbb{Z}[X]$ *is a Littlewood polynomial of degree* n *and the cyclotomic polynomial* Φ_r *divides* f*. Then* $r \mid 2(n+1)$*.*

Proof. See [8, Lemma 2.3] (the set $\mathcal{D}_2$ is the set of polynomials with all coefficients odd, and thus contains all Littlewood polynomials). The proof ultimately relies on Lemma 3.3.2, which gives a factorisation of $(X-1)f$ modulo 2 in terms of cyclotomic polynomials, and on the fact that two cyclotomic polynomials Φ_n and Φ_m are coprime in $\mathbb{F}_2[X]$ if m and n are both odd. □

We will use Lemma 4.2.6 further on to show that certain Littlewood polynomials with two sign changes don't have cyclotomic factors, see Lemma 4.4.3. But we also obtain the following corollary.

Corollary 4.2.7. *Let f be a Littlewood polynomial of degree $p-1$, with p an odd prime. Then f does not have cyclotomic factors, unless $f = \Phi_p(X)$ or $\Phi_{2p}(X) = \Phi_p(-X)$.*

Proof. Apply Lemma 4.2.6 and the fact that even-degree Littlewood polynomials do not vanish at ± 1. □

The first few values of N such that $N+1$ is a prime for which 2 is not a primitive root, are 16 and 22. In Table A.2 we see that 99.8% of the polynomials in $\mathscr{F}_{16}$ is irreducible, and 99.995% of the polynomials in $\mathscr{F}_{22}$ are irreducible. Since $\varphi(17)/\operatorname{ord}_{17}(2) = \varphi(23)/\operatorname{ord}_{23}(2) = 2$, any reducible Littlewood polynomial can only have two factors in those degrees by Proposition 3.1.2, which intuitively seems to be a serious restriction; perhaps there is a way to capitalise on this, but the author is not aware of such a possibility.

Recall from Lemma 1.2.4 that every separable, even-degree polynomial with square discriminant is reducible modulo any prime. Hence none of the polynomials addressed in Lemma 4.2.5 has square discriminant. Again, this leads to a special case of Entin's lemma 4.2.3. Indeed, the following lemma shows that 2 is only a primitive root of $n+1$ if $n \equiv 2, 4 \bmod 8$, since 2 is a quadratic residue modulo the prime $n+1$ if and only if $n \equiv 2, 4 \bmod 8$ (compare Proposition 3.4.4).

Lemma 4.2.8. *Let p be an odd prime and $a \in (\mathbb{Z}/p\mathbb{Z})^\times$. Then a has order dividing $(p-1)/2$ modulo p if and only if a is a quadratic residue modulo p. In particular, if a is a primitive root modulo p, then a is a quadratic nonresidue modulo p.*

Proof. Recall that

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p,$$

also known as Legendre's formula. The right-hand side is 1 if and only if a has order dividing $(p-1)/2$ modulo p, so the result is immediate. □

Another observation we can make from Table A.2 is that all reciprocal polynomials in degrees $2, 4, 6, 10, 12, 18$ and 22 are irreducible. Apart from 6 and 22, all these instances can be ascribed to Lemma 4.2.5. However, 6 and 22 come from the following theorem, that combines results from Chapter 2 and 3.

Theorem 4.2.9. *Let $2n+1$ be a prime number congruent to 3 mod 4. Suppose that 2 has order n in $(\mathbb{Z}/(2n+1)\mathbb{Z})^\times$. Then every reciprocal Littlewood polynomial in $\mathscr{F}_{2n}$ is irreducible over $\mathbb{Q}$, and every skew-reciprocal Littlewood polynomial in $\mathscr{F}_{2n}$ is irreducible over $\mathbb{Q}$ or has square discriminant.*

Proof. By Proposition 3.2.7, we find that Ψ_{2n+1} is irreducible over $\mathbb{F}_2$. Let f be a balanced polynomial in $\mathscr{F}_{2n}$. Then f does not have double roots by Lemma 4.2.1, and $f \equiv \Phi_{2n+1} \bmod 2$. If f is reciprocal, then f is irreducible over $\mathbb{Q}$ by Theorem 2.5.7; if f is skew-reciprocal and reducible over $\mathbb{Q}$, then f has square discriminant by Theorem 2.5.8. □

Combined with Theorem 2.3.1, Theorem 4.2.9 shows that for each such n the set SI_{2n} is quite large. It is not known whether infinitely many such values of n exist, but this would be a consequence of Artin's primitive root conjecture.

By Lemma 4.2.8, the number 2 can only have order n in $(\mathbb{Z}/(2n+1)\mathbb{Z})^\times$ if 2 is a quadratic residue modulo $2n+1$. This is the case if and only if $n \equiv 0, 3 \bmod 4$. Hence the prime $2n+1$ in Theorem 4.2.9 must actually be congruent to 7 mod 8, so that n is congruent to 3 mod 4.

Definition 4.2.10. Let n be an integer. Then n is called a *Queneau number* if $2n+1$ is a prime and one of the following holds:

(1) $n \equiv 1, 2 \bmod 4$ and 2 is a primitive root for $(\mathbb{Z}/(2n+1)\mathbb{Z})^\times$, or
(2) $n \equiv 3 \bmod 4$ and 2 has order n in $(\mathbb{Z}/(2n+1)\mathbb{Z})^\times$.

Lemma 4.2.5, Lemma 4.2.8, and Theorem 4.2.9 together show that all reciprocal polynomials in $\mathscr{F}_{2n}$ are irreducible if n is a Queneau number. The first few Queneau numbers are $n = 1, 2, 3, 5, 6, 9, 11, 14, 18, 23, \ldots$ (OEIS [23], A054639). Another characterisation of Queneau numbers is given in the following lemma.

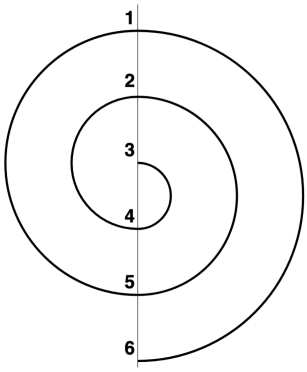
Lemma 4.2.11. *Let n be a natural number. The* Queneau-Daniel *or* spiral *permutation is, in two-line notation, the permutation*

$$Q_n = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots & n \\ n & 1 & n-1 & 2 & n-2 & \cdots & \cdots \end{pmatrix} \in S_n. \tag{4.2}$$

If the order of the cyclic subgroup generated by Q_n in S_n equals n, then n is a Queneau number.

The name *spiral* permutation stems from the following fact: Write the numbers from 1 to n in a straight line and connect n with 1, 1 with $n-1$, $n-1$ with 2, 2 with $n-2$, and so on – that is, exactly in the order in which these numbers appear in the bottom line of the permutation Q_n in (4.2). The result is a spiral (for any n), see Figure 4.1. There is an interesting history [43] attached to the name 'Queneau-Daniel': the second comes from Arnaut Daniel, Occitan troubadour of the 12th century. His poem *Lo ferm voler qu'el cor m'intra* (see Appendix C for the original in Old Occitan, together with an English translation by Ezra Pound) is written in a form nowadays known as a sestina: six

Figure 4.1: Spiral corresponding to the Queaneau-Daniel permutation Q_6 (picture taken from [19, p. 11]).



stanzas of six lines each, followed by a short stanza (or envoi) of three lines. The final words in each of the six lines of the first stanza should also be the final words of the six lines in each of the other stanzas, but in order of occurrence permuted according to the permutation Q_6. In the case of 'Lo ferm voler', keep track of the way the six words *intra, ongla, arma, veria, oncle*, and *cambra* are permuted. Since 6 is a Queneau-Daniel number, each of the six orders of occurrence is unique.

The 20th-century French poet Raymond Queneau generalized this concept to n stanzas consisting of n lines, with final words permuted by Q_n; he asked for which n the permutation Q_n has order n, and showed this is not the case when n is a power of 2 or of the form $2ab+a+b$, with integers $a, b \geq 1$. For more information on the historical background and development of the mathematical understanding of Queneau numbers, we again refer to [43].

The following proof is due to Dumas [19, Thm. 2]; an English translation is available in [43, Thm. 2].

Proof of Lemma 4.2.11. For $n = 1$ the problem is trivial, so suppose $n \geq 2$. Denote by δ_n the inverse of Q_n. Then for any integer i between 1 and $2n$, we have

$$\delta_n(i) = \begin{cases} 2i & \text{if } 2i \leq n, \\ 2n+1-2i & \text{otherwise.} \end{cases}$$

Note in particular that $\delta_n(i) \equiv \pm 2i \bmod 2n+1$ for all i.

Suppose that Q_n has order n; we wish to show that n is a Queneau number. We first show that $2n+1$ is prime. If not, let q be a nontrivial divisor of $2n+1$. Then δ_n sends q to a multiple of q. Repeating, we observe that the orbit of q under δ_n only contains

multiples of q. Since q is odd, the number $q-1$ does not divide q, and is thus fixed under δ_n. But then δ_n (and subsequently Q_n) has order smaller than n, which is a contradiction.

To show that 2 has the right order in $(\mathbb{Z}/(2n+1)\mathbb{Z})^\times$, we first prove the following claim.

Claim: Let $j < n$. If $\delta_n^j(2) \equiv \pm 2 \bmod 2n+1$ then Q_n has order smaller than n. Indeed, if $\delta_n^j(2) = 2$, then the orbit of 2 under δ_n contains less than n integers, so δ_n has order smaller than n. If $\delta_n^j(2) = -2$, then $\delta_n^{j-1}(2)$ must be equal to 1 and $2 > n$, but we assumed that $n \geq 2$. This concludes the proof of the claim.

We use the claim twice. Suppose that 2 is of order $j < n$ in $(\mathbb{Z}/(2n+1)\mathbb{Z})^\times$. Then $\delta_n^j(2) \equiv \pm 2^{j+1} \equiv \pm 2 \bmod 2n+1$. So Q_n has order smaller than n, contradicting our assumptions. So 2 has order n or $2n$. If 2 has order $2n$, we are done by Lemma 4.2.8. If 2 has order n, we have to exclude the possibility that n is divisible by 4. But then $2^{n/2} \equiv -1 \bmod 2n+1$ and thus $\delta_n^{n/2}(2) = \pm 2 \bmod 2n+1$, which again leads to the contradictory statement that Q_n has order smaller than n via the claim above. So we conclude that n is a Queneau number.

For the converse, suppose that n is a Queneau number. Let ω be the cardinality of the smallest orbit of δ_n; note that $\omega \leq n$, and we need to show that $\omega = n$. Take an element u of order ω in $(\mathbb{Z}/n\mathbb{Z})^\times$. Then $u = \delta_n^\omega(u) \equiv (-1)^k 2^\omega u \bmod 2n+1$ for some k. Hence $2^\omega \equiv \pm 1 \bmod 2n+1$. If $2^\omega \equiv 1$, then $\omega = n$ since n is a Queneau number, and we are done. If $2^\omega \equiv -1$, then ω equals n (if 2 has order $2n$) or $n/2$ (if 2 has order n). In the latter case n must be even, which never happens when 2 has order n. So again $\omega = n$. □

Let n be a Queneau number. Then we call $2n+1$ a *Queneau prime number*. Asveld [2, Thm. 6.8] shows (under the Generalized Riemann Hypothesis) the following density statement (within the set of primes) for Queneau prime numbers associated with Queneau numbers congruent to 3 mod 4. This is also mentioned in his overview [3] of results and articles pertaining to Queneau numbers.

Lemma 4.2.12. *Assuming the Generalized Riemann Hypothesis, the Queneau prime numbers associated with Queneau numbers congruent to* 3 mod 4 *have a density of* $\mathbf{A}/2 \approx 0.187$ *in the prime numbers. Here* $\mathbf{A}$ *is Artin's constant, which is*

$$\mathbf{A} = \prod_p \left(1 - \frac{1}{p(p-1)}\right),$$

where the product extends over all prime numbers p.

We stress that this result depends not 'just' on Artin's primimitive root conjecture (which has been proven conditionally by assuming the Generalized Riemann Hypothesis), but on the full strength of the Generalized Riemann Hypothesis. Note that a Queneau

prime number is congruent to 7 mod 8 if the associated Queneau number is congruent to 3 mod 4. By the prime number theorem for arithmetic progressions, the density of the primes in the congruence class 7 mod 8 in the set of primes is $1/\varphi(8) = 1/4$.

Corollary 4.2.13. *Assuming the Generalized Riemann Hypothesis, the density of Queneau prime numbers congruent to* 7 mod 8 *is* $(\mathbf{A}/2)\big/(1/4) = 2\mathbf{A} \approx 0.748$.

To wrap up this section, we turn to the question of *counting* balanced Littlewood polynomials with square discriminant (that are not necessarily irreducible). Theorem 2.3.1 is most useful for this purpose. In degree 0 or 6 mod 8, balanced Littlewood polynomials with square discriminant do exist, and using Theorem 2.3.1 it is a fun exercise to write some down. But how many are there?

To count them efficiently, we recall that any polynomial f can be written as the sum $f(X) = f_{\mathrm{e}}(X^2) + Xf_{\mathrm{o}}(X^2)$ of its even and odd parts. Therefore

$$f(1)f(-1) = (f_{\mathrm{e}}(1) + f_{\mathrm{o}}(1))(f_{\mathrm{e}}(1) - f_{\mathrm{o}}(1)) = f_{\mathrm{e}}(1)^2 - f_{\mathrm{o}}(1)^2 \tag{4.3}$$

and

$$f(i)f(-i) = (f_{\mathrm{e}}(i^2) + if_{\mathrm{o}}(i^2))(f_{\mathrm{e}}((-i)^2) - if_{\mathrm{o}}((-i)^2)) = f_{\mathrm{e}}(-1)^2 + f_{\mathrm{o}}(-1)^2. \tag{4.4}$$

If f is a Littlewood polynomial and we want this expression to equal a square (or minus a square – see Theorem 2.3.1), we can count the possible choices of signs giving rise to (possibly degenerate) Pythagorean triples. As an example, we show the following lemma.

Lemma 4.2.14. *The number of reciprocal Littlewood polynomials of degree* $8n$ *with square discriminant equals*

$$2^{2n}\binom{2n}{n} + 2\sum_{\substack{k>0\\ k\ odd}} \sum_{\substack{r>s>0\\ r,s\ coprime\\ r-s\equiv 1 \bmod 2}} \binom{2n}{n+\frac{1}{2}krs}\binom{2n}{n+\frac{1}{4}(kr^2+ks^2+(-1)^{\frac{k+1}{2}})} \tag{4.5}$$

Here, we adopt the convention that $\binom{n}{k} = 0$ *if* $k > n$.

For the sake of clarity, we reiterate that here, with 'Littlewood polynomial' we mean a monic polynomial all of whose coefficients lie in $\{\pm 1\}$.

Proof of Lemma 4.2.14. Consider a reciprocal polynomial $f = a_{4n}X^{8n} + \cdots + a_1X^{4n+1} + a_0X^{4n} + a_1X^{4n-1} + \cdots + a_{4n-1}X + a_{4n}$ of degree $8n$. Set

$$\begin{aligned} c &:= f_{\mathrm{e}}(1) = a_0 + 2(a_2 + a_4 + \cdots + a_{4n}), \\ b &:= f_{\mathrm{o}}(1) = 2(a_1 + a_3 + \cdots + a_{4n-1}). \end{aligned}$$

By Theorem 2.3.1 and (4.3), we need to choose the a_i such that $c^2 - b^2$ is a square, say equal to a^2. Suppose that f is Littlewood (so in particular, monic). In the $\binom{2n}{n}$ cases that exactly half of the odd-index coefficients $a_1, a_3, \ldots, a_{4n-1}$ are equal to 1 and thus $b = 0$, we find that any choice of the coefficients $a_0, a_2, \ldots, a_{4n-2}$ will make f a Littlewood polynomial with square discriminant. Hence there are in total $2^{2n}\binom{2n}{n}$ reciprocal Littlewood polynomials f of degree $8n$ whose discriminant is a square and with the property $f_o(1) = 0$. This is the first term in (4.5).

From here on we assume that $b \neq 0$. Furthermore, we remove (for the sake of symmetry) the condition that f is monic; since f has square discriminant if and only if $-f$ has square discriminant, we must simply divide whatever final expression we obtain by 2. Recall that if $a^2 + b^2 = c^2$ is a Pythagorean triple, then there are *unique* positive integers k, r and s such that $r > s$ and the numbers r and s are coprime and not both odd. Since we treat each of the *four* triples $(a, \pm b, \pm c)$ separately (we care if $c^2 - b^2$ is a square, so the sign of a doesn't matter; but the polynomials corresponding to the four tuples $(\pm b, \pm c)$ are genuinely different) we multiply whatever final expression we obtain by 4. We thus conclude that the final expression must be multiplied by $4/2 = 2$.

It remains to show that the second summand in (4.5) is correct. That is, we must count all choices of the a_i that lead to the equalities $c = k(r^2 + s^2)$ and $b = 2krs$. Notice that

$$a_2 + a_4 + \cdots + a_{4n} = \frac{c - a_0}{2} = \frac{k(r^2 + s^2) - a_0}{2}. \tag{4.6}$$

Since all a_i lie in $\{\pm 1\}$, the left-hand side in (4.6) is even. As $r^2 + s^2 \equiv 1 \bmod 4$, we find that $a_0 \equiv k \bmod 4$. Hence $a_0 = (-1)^{\frac{k-1}{2}}$ and

$$a_2 + a_4 + \cdots + a_{4n} = \frac{k(r^2 + s^2) + (-1)^{\frac{k+1}{2}}}{2}. \tag{4.7}$$

Therefore a total of $n + (k(r^2 + s^2) + (-1)^{\frac{k+1}{2}})/4$ of the even-index coefficients must be chosen equal to 1 (and the other $n - (k(r^2 + s^2) + (-1)^{\frac{k+1}{2}})/4$ thus equal -1). This yields

$$\binom{2n}{n + (k(r^2 + s^2) + (-1)^{\frac{k+1}{2}})/4}$$

options for the even-index coefficients. Similarly, there are $2n$ choices to be made for the even-index coefficients $a_2, a_4, \ldots, a_{4n}$; since the sum of the latter equals $b/2 = krs$, we find that $n + krs/2$ of the odd-index coefficients must be equal to 1. So we have in total $\binom{2n}{n+krs/2}$ options for the odd-index coefficients. This gives

$$\binom{2n}{n + krs/2}\binom{2n}{n + (k(r^2 + s^2) + (-1)^{\frac{k+1}{2}})/4}$$

combinations of the coefficients $a_0, a_1, a_2, \dots, a_{4n-1}$ of such that the resulting polynomial f satisfies $f_e(1) = c$ and $f_o(1) = b$, which is exactly the summand in (4.5). □

It is an interesting question how the fraction

$$\frac{\#\{f \in \mathscr{F}_n \mid f \text{ is balanced and } \Delta(f) = \square\}}{\#\{f \in \mathscr{F}_n \mid f \text{ is balanced}\}}$$

behaves asymptotically; numerical computations using (4.5) for $n < 100$ show that the fraction

$$\frac{\#\{f \in \mathscr{F}_{8n} \mid f \text{ is reciprocal and } \Delta(f) = \square\}}{\#\{f \in \mathscr{F}_{8n} \mid f \text{ is reciprocal}\}}$$

drops steadily from $1/2$ (for $n = 2$) to $\approx 1/3$ (for $n = 5$) to $\approx 1/5$ (for $n = 18$) to $\approx 1/10$ (for $n = 94$).

4.3 One sign change

In this section, we will demonstrate some results and formulate some conjectures about Littlewood polynomials with one sign change.

We say that a polynomial $f \in \mathbb{Z}[X]$ *changes sign at* X^k if the coefficients of the terms X^k and X^{k-1} in the expansion of f are nonzero and of different sign, and write $f_{n,k}$ for the Littlewood polynomial of degree n that changes sign at X^k. That is,

$$f_{n,k}(X) = X^n + X^{n-1} + \cdots + X^k - X^{k-1} - \cdots - X - 1.$$

We also define the related trinomial $F_{n,k} = (X-1)f_{n,k} = X^{n+1} - 2X^k + 1$. When $d = \gcd(n+1, k) > 1$, the polynomial $f_{n,k}$ is divisible by $X^{d-1} + \cdots + X + 1$. The main aim of this section is to prove that this is the only obstruction to the irreducibility of $f_{n,k}$ (barring two exceptional cases); moreover, $f_{n,k}$ has maximal Galois group when it is irreducible and n is even.

Theorem 4.3.1. *The polynomial $f_{n,k}$ is irreducible if and only if $\gcd(n+1, k) = 1$ unless $(n, k) = (6, 2)$ or $(6, 5)$ (corresponding to the reversal $f_{6,5}$ of $f_{6,2}$). Now suppose that n is even. Then the discriminant of $f_{n,k}$ is not a square for any k, and the Galois group of $f_{n,k}$ is S_n if $f_{n,k}$ is irreducible.*

Theorem 4.3.1 implies that $|\mathrm{Ir}_n| \geq \varphi(n+1)$ for all n (this also holds for $n = 6$, see Table A.2).

The proof of Theorem 4.3.1 is split into several parts. First, we show in Theorem 4.3.3 that $f_{n,k}$ is irreducible when $n+1$ and k are coprime. The proof is inspired by Keith Conrad's proof [16] of the irreducibility of $X^n - X - 1$ (first shown by Selmer [44] in

1956); it seems that this proof technique is due to Ljunggren in [30, Lem. 1] (also see [36]). Maximality of the Galois group of $f_{n,k}$ in case n is even and $f_{n,k}$ is irreducible is shown in Theorem 4.3.6. Here, we follow the argument presented in [34], where Theorem 4.3.1 is shown for the polynomials $f_{n,n-1}$.

Ljunggren's proof technique relies on the following trick, also shown in [16].

Lemma 4.3.2 (Ljunggren's trick)**.** *Let $f \in \mathbb{Z}[X]$ be a monic polynomial with $f(0) = \pm 1$ and such that f and its reversal f_{rev} have no root in common. If $f = \varphi\psi$ for some nonconstant $\varphi, \psi \in \mathbb{Z}[X]$, then there exists a monic $g \in \mathbb{Z}[X]$ different from $\pm f, \pm f_{\mathsf{rev}}$ with $\deg g = \deg f$, $g(0) = \pm 1$, and $f f_{\mathsf{rev}} = g g_{\mathsf{rev}}$.*

Proof. Since f is monic and $f(0) = \pm 1$, the constant and leading coefficients of φ and ψ also lie in $\{\pm 1\}$. Consider $g = \pm\varphi\psi_{\mathsf{rev}}$, where the sign is chosen so that g is monic. If g equals one of $\pm f$ or $\pm f_{\mathsf{rev}}$, then f and f_{rev} must share either φ or ψ as a factor, which is a contradiction. It also satisfies all other properties, thus showing the lemma. □

Theorem 4.3.3. *If $\gcd(n+1, k) = 1$ then $f_{n,k}$ is irreducible unless $(n,k) = (6,2)$ or $(n,k) = (6,5)$.*

Proof. For ease of notation, we replace n by $n-1$ and write $f = f_{n-1,k}$ and $F = F_{n-1,k} = X^n - 2X^k + 1$ throughout the proof. Assume $\gcd(n,k) = 1$. After possibly replacing f by $-f_{\mathsf{rev}}$, we may assume that $2 \le 2k < n$. We need to show that f is irreducible unless $(n,k) = (7,2)$. We will argue by contradiction and assume that f is reducible.

The proof is split in two parts. In the first part, we show that if f is reducible, then a certain polynomial G is a hexanomial (i.e., consisting of six monomials). In the second part, we show that the latter is impossible.

Reduction to the hexanomial case. Assume that f is reducible. Lemma 4.3.2 is an essential ingredient of the proof, and so we first show that f and f_{rev} share no roots. Equivalently, F and its reversal F_{rev} have no common root except $\alpha = 1$. Indeed, if α is a common root of F and F_{rev}, it satisfies the relation $\alpha^k = \alpha^{n-k}$. On the one hand, this shows that α is an $n-2k$-th root of unity. On the other hand, we have $\alpha^{2k} = \alpha^n$. From $F(\alpha) = 0$ we know that $1 = \alpha^k \cdot (2 - \alpha^k)$; so $\alpha^k = 1$, i.e., α is also a k-th root of unity. Hence $1 = \alpha^{\gcd(n-2k,k)} = \alpha^{\gcd(n,k)} = \alpha$.

Write $f f_{\mathsf{rev}} = g g_{\mathsf{rev}}$ with g as in Lemma 4.3.2. Set $G = (X-1)g$, so that $G_{\mathsf{rev}} = (-X+1)g_{\mathsf{rev}}$ and

$$G G_{\mathsf{rev}} = F F_{\mathsf{rev}} = X^{2n} - 2X^{2n-k} - 2X^{n+k} + 6X^n - 2X^{n-k} - 2X^k + 1. \tag{4.8}$$

The expansion on the right-hand side really does consist of seven terms of different degrees, ordered from highest to lowest degree.

Say $G = b_n X^n + \cdots + b_1 X + b_0$. The coefficient of the monomial X^n in GG_{rev} equals $b_0^2 + \cdots + b_n^2 = 6$. Both b_0 are b_n are 1 since G and G_{rev} are monic. Hence $b_1^2 + \cdots + b_{n-1}^2 = 4$. There are two cases: either there is an $0 < i < n$ such that $b_i = \pm 2$, or there are $0 < q < r < s < t < n$ such that $b_q, b_r, b_s, b_t = \pm 1$. For the former case, assume that $G = X^n + b_i X^i + 1$. Note that $b_i = -2$ as 1 is a root of G. Expanding GG_{rev} shows that either $i = k$ or $i = n-k$, in which case G equals F or F_{rev}, respectively; but this contradicts that $g \neq \pm f, f_{\mathsf{rev}}$. We conclude that the second case must hold, that is, G is a hexanomial.

Claim: G is not a hexanomial. Now assume that G is a hexanomial $G = X^n + b_t X^t + b_s X^s + b_r X^r + b_q X^q + 1$ with $0 < q < r < s < t < n$ and $b_q, b_r, b_s, b_t = \pm 1$. We may assume that $t \geq n - q > n/2$, possibly after replacing G by G_{rev}. Since $G(1) = 2 + b_t + b_s + b_r + b_q = 0$, exactly one of b_t, b_s, b_r and b_q equals 1.

Assume first that $n - q \neq t$. Then $b_t X^{n+t}$ is the monomial of second-highest degree occurring in the expansion of GG_{rev}, and it receives no other contribution. But b_t is odd, contradicting that all coefficients (barring the leading and constant ones) in (4.8) have even coefficients.

Now consider the case that $n - q = t$. The monomial of second-highest degree occurring in the expansion of GG_{rev} is $(b_q + b_t)X^{n+t}$. Comparing with (4.8) shows that either $t = n - k$ and $b_q = b_t = -1$, or else $b_q + b_t = 0$.

In the former situation, we deduce that $b_r = -b_s$ and

$$GG_{\mathsf{rev}} = (X^n - X^{n-k} + b_s X^s - b_s X^r - X^k + 1)(X^n - X^{n-k} - b_s X^{n-r} + b_s X^{n-s} - X^k + 1).$$

Expanding this product and comparing with (4.8), we see that the monomials $-b_s X^{2n-r}$ and $b_s X^{n+s}$ are certainly of degree larger than $n + k$ and hence have to cancel in the product. They can only cancel by each other or by X^{2n-2k}, since all other terms are certainly of smaller degree; but if they don't cancel each other, then one of them is left over, which is impossible. Hence $n = r + s$. Expanding GG_{rev} shows that

$$GG_{\mathsf{rev}} = X^{2n} - 2X^{2n-k} - 2X^{n+k} + X^{2n-2k} - X^{2s} + O(X^n).$$

Comparing with (4.8) we conclude that $X^{2n-2k} - X^{2s} = 0$ as polynomials, and hence $n - s = k$. However, $n - s = r > k$ by assumption, and we have derived a contradiction.

The last and most laborious case is $b_q = -b_t$. Now

$$GG_{\mathsf{rev}} = (X^n + b_t X^t - X^s - X^r - b_t X^{n-t} + 1)(X^n - b_t X^t - X^{n-r} - X^{n-s} + b_t X^{n-t} + 1).$$

Assume without loss of generality that $s \geq n - r$. Then the new candidate terms for the second-highest-degree monomial in the expansion of GG_{rev} are $-X^{2t}$, $-X^{2n-r}$, and $-X^{n+s}$.

No sum of these can possibly vanish, so precisely two of these terms must sum to $-2X^{2n-k}$. There are two cases.

Case 1: $s = n-r$. In this case we have $2t < n+s$, $s = n-k$, $r = k$; expanding GG_{rev} gives

$$GG_{\mathsf{rev}} = X^{2n} - 2X^{2n-k} - X^{2t} - 2X^{n+k} + X^{2n-2k} + O(X^n).$$

This means that $2t = 2n-2k$, i.e., $t = n-k = s$, which contradicts that $s < t$.

Case 2: $s > n-r$. In this case we have $n+s = 2t = 2n-k$. Note in particular that then $k < r$. Again expanding GG_{rev} gives

$$\begin{aligned} GG_{\mathsf{rev}} = X^{2n} - X^{2n-r} - X^{n+k} - 2X^{2n-k} - b_t X^{2n-r-k/2} - b_t X^{n+k/2} \\ + b_t X^{2n-3k/2} + X^{2n-k-r} - X^{n+r} + b_t X^{n+r-k/2} + O(X^n), \end{aligned}$$

Comparing with (4.8) gives

$$-X^{n+k} \doteq -X^{2n-r} - b_t X^{2n-r-k/2} - b_t X^{n+k/2} + b_t X^{2n-3k/2} + X^{2n-k-r} - X^{n+r} + b_t X^{n+r-k/2}.$$

(Here, note that $2n-r-k/2 > 2n-r-k > n+s-r > n$ since $n-k = s > r$.) Define by A the set of exponents occurring on the right-hand side after dividing by X^n, i.e.,

$$A := \{n-r, n-r-k/2, n-r-k, k/2, n-3k/2, r, r-k/2\}.$$

Then A cannot have cardinality larger than 4 as six terms must cancel, and it cannot be smaller than 3 because $n-r, n-r-k/2$, and $n-r-k$ are certainly distinct. If $|A| = 3$ then $3k/2 \in \{r, r+k/2, r+k\}$ so $2r \in \{k, 2k, 3k\}$; since $k < r$ we must have $3k = 2r$. Hence

$$A = \{n-3k/2, n-2k, n-5k/2, k/2, 3k/2, k\}$$

and again because $|A| = 3$ we have $n-3k/2 = 3k/2$, but then $n = 3k$, which contradicts $\gcd(n,k) = 1$ unless $(n,k) = (3,1)$. This corresponds to the polynomial $f_{2,1} = X^2 + X - 1$, which is irreducible.

Hence $|A| = 4$ and in particular $n-3k/2 \notin \{n-r, n-r-k/2, n-r-k\}$. For the elements of A, we find that $n-3k/2, n-r > n-r-k/2 > n-r-k$ and $r > r-k/2 > k/2$. The monomials corresponding to the latter three expressions must all cancel with three of the monomials corresponding to the former expressions. In particular, we find that $k/2$ is either $n-r-k/2$ or $n-r-k$. In the former case we have $n-k = r$, which contradicts that $n-k = s > r$. Hence $3k/2 = n-r$ and

$$A = \{3k/2, k, k/2, n-3k/2, n-2k\}.$$

Since $|A| = 4$ and $n - 3k/2 \notin \{n - r = 3k/2, n - r - k/2 = k, n - r - k = k/2\}$ we deduce that $n - 2k$ must equal one of the other elements of A and that can only be $3k/2$. Hence $2n = 7k$ and $\gcd(n,k) = 1$ is only respected when $k = 2$ and $n = 7$. This corresponds to the polynomial $f_{6,2} = (X^3 + X + 1)(X^3 + X^2 - 1)$.

This concludes the proof of Theorem 4.3.3. □

The remainder of this section is devoted to showing Theorem 4.3.6, which states that $\mathrm{Gal}(f_{n,k}) = S_n$ when n is even and $f_{n,k}$ is irreducible. The following auxiliary lemma shows that $f_{n,k}$ ramifies in a very particular way at its ramiying primes, which we then exploit in the proof of Theorem 4.3.6.

Lemma 4.3.4. *Suppose that n is even and $(n,k) \neq (6,2), (6,5)$ and let p be a prime divisor of $\Delta(f_{n,k})$. Then the reduction of $f_{n,k}$ modulo p has a unique double root that lies in $\mathbb{F}_p$, and all other roots of $f_{n,k}$ are simple.*

Proof. Again, we replace n with $n-1$. Consider $f = f_{n-1,k}$ and suppose we are in the setting of the statement. Note that $p > 2$, since the discriminant of f is odd by Lemma 4.2.1. Since p divides the discriminant $\Delta(f)$, the polynomial f has multiple roots modulo p; write α for such a multiple root. Define $F = (X-1)f = X^n - 2X^k + 1$ (and note that the splitting field of F and f coincide) and $h = nF - XF' = -2(n-k)X^k + n$ and note that f, f', F, F' and h all vanish at α.

First, we show that α is not congruent to 1 mod p. (This implies that the multiplicity of α as a root of f equals the multiplicity of α as a root of F.) Observe that $f(1) = n - 2k$ and

$$f'(1) = (n-1) + (n-2) + \cdots + k - (k-1) - \cdots - 1 = \frac{n(n-1)}{2} - k(k-1).$$

If both $f(1)$ and $f'(1)$ vanish modulo p, then $n \equiv 2k \bmod p$ and hence $f'(1) \equiv k(n-1-(k-1)) \equiv k^2 \bmod p$. So p divides k. But then $n \equiv 2k \equiv 0 \bmod p$, i.e., the integer n is also divisible by p. But this contradicts $\gcd(n,k) = 1$.

Secondly, the integers n, k and $n-k$ are nonzero in $\mathbb{F}_p$; we show that the contrary assertions lead to contradictions with the condition $\gcd(n,k) = 1$. Note that $F(0) = 1$, so α is certainly not congruent to 0. Suppose p divides n, then $0 \equiv h(\alpha) \equiv 2k\alpha^k \bmod p$. So p divides k, contradicting the gcd condition. Similarly, if p divides k, then $0 \equiv F'(\alpha) \equiv n\alpha^{n-1} \bmod p$, so p divides n as well. Lastly, if p divides $n-k$, then $0 \equiv h(\alpha) \equiv n \bmod p$, so p divides n. Hence p also divides $n - (n-k) = k$.

Lastly, we show that α is the unique multiple root of f, lies in $\mathbb{F}_p$, and has multiplicity 2. Since $\alpha \not\equiv 1 \bmod p$, the multiplicity of α as a root of f and as a root of F is the same.

Notice that $h'(\alpha) \equiv -2k(n-k)\alpha^{k-1} \not\equiv 0 \bmod p$ by the above. On the other hand,

$$h'(\alpha) \equiv nF'(\alpha) - F'(\alpha) - \alpha F''(\alpha) \equiv -\alpha F''(\alpha) \bmod p,$$

so $F''(\alpha) \not\equiv 0 \bmod p$. We conclude that α has multiplicity 2 as a root of f.

For unicity, the congruence $F'(\alpha) \equiv 0 \bmod p$ implies that $\alpha^{n-k} \equiv 2k/n \bmod p$. Similarly, we obtain from $h(\alpha) \equiv 0 \bmod p$ that $\alpha^k \equiv n/(2(n-k)) \bmod p$. Hence $\alpha^n \equiv k/(n-k) \bmod p$. Therefore $\alpha^{\gcd(n,k)} = \alpha$ also lies in $\mathbb{F}_p$. If γ is another multiple root of F, then $(\alpha/\gamma)^n \equiv (\alpha/\gamma)^k \equiv 1$, so $\gamma = \alpha$. Thus α is unique. □

We also need the following group-theoretic lemma, taken from [40, Lem. 5].

Lemma 4.3.5. *Let H be a permutation group that is generated by transpositions and acts transitively on a set Ω of n elements. Then H is the symmetric group S_n.*

Proof. Recall that S_n is generated by all transpositions of elements of Ω, since it is generated by all cycles and the equality

$$(a_1\, a_2\, \ldots\, a_n) = (a_1\, a_2)(a_2\, a_3)\cdots(a_{n-1}\, a_n)$$

for distinct a_i holds. So it suffices to show that H contains all transpositions.

For this, we claim that it is enough to show that H acts *doubly transitively* on Ω: that is, for any two pairs $(a,b), (c,d) \in \Omega \times \Omega$ there is a $\sigma \in H$ such that $\sigma(a) = c$ and $\sigma(b) = d$. Indeed, if H acts doubly transitively on Ω and we choose $(a,b) \in \Omega \times \Omega$ such that $(a\, b)$ lies in H, then $\sigma(a\, b)\sigma^{-1} = (c\, d)$ lies in H. So H contains all transpositions, as (c,d) can be chosen arbitrarily.

To show that H indeed acts doubly transitively on Ω, first note that there is a series of transpositions $(b\, a_1)$, $(a_1\, a_2)$, …, $(a_m d)$ connecting b to d, as H acts transitively on Ω and is generated by transpositions. If there are $i < j$ such that $a_i = a_j$, then

$$\begin{aligned}(a_i\, a_{i+1})(a_{i+1}\, a_{i+2})\cdots(a_{j-1} a_j) &= (a_i\, a_{i+1})(a_{i+1}\, a_{i+2}\, \ldots\, a_{j-1})(a_{j-1}\, a_j)\\ &= (a_{i+1}\, a_{i+2})(a_{i+2}\, a_{i+3})\cdots(a_{j-2}\, a_{j-1}).\end{aligned}$$

So we can assume that all a_i are distinct. If also $a \neq a_i$ for all i then $\sigma(a\, c)\sigma^{-1} = (a\, d)$ for $\sigma = (b\, a_1)(a_1\, a_2)(a_m\, d)$. If $a = a_i$ for some i, then

$$(a\, c)\sigma(a\, c)\sigma^{-1}(a\, c) = (a\, d)$$

for $\sigma = (a\, a_{i+1})(a_{i+1}\, a_{i+2})\cdots(a_m\, d)$. So $(a\, d)$ is contained in H. There is also a series of transpositions connecting a to c, so by repeating the above procedure with these transpositions shows that $(b\, d)$ is contained in H as well. □

For the proof of the next theorem, we borrow some tools from algebraic number theory. These can be found in Section 1.3 and Section 1.4.

Theorem 4.3.6. *Suppose that n is even and $(n,k) \neq (6,2),(6,5)$. Then $f_{n,k}$ does not have square discriminant, and* $\mathrm{Gal}(f_{n,k}) = S_n$ *if* $\gcd(n+1,k) = 1$.

Proof. Write $f = f_{n-1,k}$ and suppose we are in the setting of the statement. Again, let p be a prime dividing the discriminant $\Delta(f)$ (which is then necessarily at least 3 by Lemma 4.2.1). Suppose that L is the splitting field of f and $\mathfrak{p}$ a prime ideal of $\mathcal{O}_L$ lying over p.

Claim 1: The inertia group $I_\mathfrak{p}$ of $\mathfrak{p} \mid p$ is generated by a transposition. In Lemma 4.3.4 we showed that f has a unique double root α lying in $\mathbb{F}_p$ and that all other roots of f are simple. Hence f is of the form

$$f \equiv \bar{g}_1 \bar{g}_2 \bmod p,$$

where $\bar{g}_2 \in \mathbb{F}_p[X]$ is separable and relatively prime with $\bar{g}_1 \equiv (X-\alpha)^2 \in \mathbb{F}_p[X]$ (as they share no root in an algebraic closure of $\mathbb{F}_p$). By Hensel's lemma 1.3.4, the polynomial f admits a factorisation

$$f = g_1 g_2 \in \mathbb{Z}_p[X]$$

over the local ring $\mathbb{Z}_p$ such that the degrees of g_i and $\bar{g}_i$ match and $g_i \equiv \bar{g}_i \bmod p$ for $i = 1,2$. The latter implies that g_2 is monic and separable over $\mathbb{Z}_p$. In a moment we will see that, in addition, the monic polynomial g_1 is irreducible.

Consider the extensions $\mathbb{Q}_p \subset T \subset L_\mathfrak{p}$, where T is the compositum generated by the roots of g_2, and $L_\mathfrak{p}$ the completion of L with respect to the prime ideal $\mathfrak{p}$ extending p (equivalently, it is the splitting field of f over $\mathbb{Q}_p$). Then $L_\mathfrak{p}$ is a local field with prime ideal $\mathfrak{p}\mathcal{O}_{L_\mathfrak{p}}$, whose inertia group $I(L_\mathfrak{p}/\mathbb{Q}_p)$ coincides with the inertia group $I_\mathfrak{p}$ by Lemma 1.4.1. We claim that the extension $T/\mathbb{Q}_p$ is unramified. Indeed, fix a root θ of g_2 in an algebraic closure of $\mathbb{Q}_p$. It suffices to show that the separable extension $\mathbb{Q}_p(\theta)$ of $\mathbb{Q}_p$ is unramified as the compositum of finitely many unramified extensions is unramified by Lemma 1.3.6. Recall the fundamental identity

$$[\mathbb{Q}_p(\theta) : \mathbb{Q}_p] = e_p f_p,$$

where e_p and $f_p = [\mathbb{F}_p(\theta) : \mathbb{F}_p]$ are the ramification index and the inertia degree of the extension $\mathbb{Q}_p(\theta) \mid \mathbb{Q}_p$, respectively (see Lemma 1.3.5). Again by Hensel's lemma, the minimal polynomial of θ over $\mathbb{F}_p$ lifts to a (necessarily irreducible) polynomial in $\mathbb{Z}_p[X]$ that shares its degree with and is congruent modulo p to the minimal polynomial of θ. Thus $[\mathbb{Q}_p(\theta) : \mathbb{Q}_p] = f_p$ and $e_p = 1$.

However, the extension $L_\mathfrak{p}$ over $\mathbb{Q}_p$ generated by the roots of both g_1 and g_2 does ramify, as $\mathfrak{p}$ ramifies. Therefore the root $\alpha \in \mathbb{F}_p$ of $\bar{g}_1$ does not lift to a root of g_1 that lies

in $\mathbb{Q}_p$, so g_1 is an irreducible quadratic. Hence $|I_\mathfrak{p}| = e_p = 2$ and the nontrivial element of $I_\mathfrak{p}$ must be the automorphism transposing the two roots of g_1. ■

In particular, the Galois group of f contains a transposition. Hence $f_{n,k}$ does not have square discriminant.

Claim 2: $\mathrm{Gal}(f)$ *is isomorphic to* S_n *if* $\gcd(n+1,k) = 1$. Here, we use some results from Osada's paper [40], relying on the fact that the splitting fields of f and F coincide.

By Theorem 4.3.3, the polynomial f is irreducible over $\mathbb{Q}$, so $\mathrm{Gal}(L/\mathbb{Q})$ is a transitive subgroup of S_n. Let p be now be an arbitrary prime number and $\mathfrak{p}$ a prime in L lying above p. If p doesn't ramify in L, the inertia subgroup of $\mathfrak{p}$ is trivial. If p does ramify in L, Claim 1 asserts that the inertia group of $\mathfrak{p}$ contains a transposition. Hence the inertia group of any prime in L is either trivial or generated by a transposition. Now consider the subgroup H of $\mathrm{Gal}(L/\mathbb{Q})$ generated by the inertia groups of all primes lying over any rational prime p. The fundamental theorem of Galois theory implies that H corresponds to a fixed field L^H. But this must be an unramified extension of $\mathbb{Q}$, which is impossible. Hence $L^H = \mathbb{Q}$ and $\mathrm{Gal}(L/\mathbb{Q}) = H$. Since H is generated by transpositions and is a transitive subgroup of S_n by the irreducibility of $f_{n,k}$, it must be all of S_n by Lemma 4.3.5. ■

This concludes the proof of Theorem 4.3.6 and hence of Theorem 4.3.1. □

4.4 Two sign changes

4.4.1 A conjecture and cyclotomy

By analogy of the developments in the previous section, we write $f_{n,k,l}$ with $1 \le l < k \le n$ for the Littlewood polynomial of degree n that changes sign at X^k and X^l and define the related quadrinomial $F_{n,k,l} = (X-1)f_{n,k,l} = X^{n+1} - 2X^k + 2X^l - 1$. We conjecture the following.

Conjecture 4.4.1. *Let* $n \not\equiv 2 \bmod 6$. *Then* $f_{n,k,l}$ *is irreducible if and only if* $\gcd(n+1, k-l) = 1$, *unless* (n,k,l) *is one of* $(6,4,1),(6,3,2),(6,6,3),(6,5,4)$. *If* $n \equiv 2 \bmod 6$, *then* f *is reducible if* $\gcd(n+1, k-l) \neq 1$, *but the converse does not hold.*

How many such pairs (k,l) are there for any given n?

Lemma 4.4.2. *Let* n *be an integer. There are* $(n-1)\varphi(n+1)/2$ *pairs* (k,l) *such that* $\gcd(n+1, k-l) = 1$ *and* $1 \le l < k \le n$.

Proof. For any integer a coprime with $n+1$, there are $n-a$ pairs (k,l) with $k-l=a$ and $1 \le l < k \le n$. Note that a is coprime with $n+1$ if and only if $n+1-a \neq a$ is coprime with $n+1$. Hence there are $(n-a)+(n-(n+1-a)) = n-1$ pairs (k,l) with $k-l \in \{a, n+1-a\}$ and $1 \le l < k \le n$. We conclude that, in total, there are $(n-1)\varphi(n+1)/2$ pairs (k,l) with $\gcd(n+1, k-l) = 1$ and $1 \le l < k \le n$. □

The next lemma shows that $f_{n,k,l}$ does not have cyclotomic factors when $n \not\equiv 2 \bmod 6$ is even.

Lemma 4.4.3. *Let $n \not\equiv 2 \bmod 6$ be even. Then the polynomial $f_{n,k,l}$ does not have cyclotomic factors if $\gcd(n+1, k-l) = 1$.*

Proof. Again, we replace n by $n-1$, meaning that we show the following statement: let $n \not\equiv 3 \bmod 6$ be odd. Then the polynomial $f = f_{n-1,k,l}$ does not have cyclotomic factors if $\gcd(n, k-l) = 1$.

Assume that $l < k$ and $2 \le 2l < n$. Let α be a primitive t-th root of unity with $t < n$; since ± 1 cannot be a root of a Littlewood polynomial of even degree, we certainly have $t > 2$. Write $F = F_{n-1,k,l}$ and assume $F(\alpha) = \alpha^n - 2\alpha^k + 2\alpha^l - 1 = 0$. By Lemma 4.2.6 we know that $t \mid 2n$. First assume $t \mid n$. From $F(\alpha) = 0$ we obtain $\alpha^{k-l} = 1$. So $t \mid (k-l)$ and $\gcd(n, k-l) \ge t > 1$.

Now assume t divides $2n$ but not n. Since $\alpha^n \neq 1$ but $\alpha^{2n} = 1$, it is clear that $\alpha^n = -1$. The relation $F(\alpha) = 0$ implies that $\alpha^l - \alpha^k = 1$. Phrased differently, the imaginary parts of α^l and α^k are equal while their real parts differ by one. Considering that both α^k and α^l lie on the unit circle, a short computation shows that

$$\alpha^l = \frac{1 \pm \sqrt{-3}}{2}, \quad \alpha^k = \frac{-1 \pm \sqrt{-3}}{2} = \alpha^{2l}$$

where the signs are chosen equal (notice that k is of the form $2l + ct$). Hence α^l is a primitive sixth root of unity—in other words, t divides $6l$. Hence $\gcd(2n, 6l) = 2\gcd(n, 3l) \ge t$. Since $t > 2$ divides $2n$ but not n, it is twice an odd number and hence $\gcd(n, 3l) > 1$. Hence if $3 \nmid n$ then $\gcd(n, k-l) = \gcd(n, l+ct) = \gcd(n, 3l+3ct) > 1$. □

4.4.2 Reciprocality and Mahler measures

In contrast with the case of one sign change, there are reciprocal Littlewood polynomials with two sign changes.

Lemma 4.4.4. *Let n be even and $2 \le 2k < n$. The reciprocal polynomial $f_{n,n-k+1,k}$ has square discriminant if and only if*

$$(-1)^{n/2}(4k-n)(1-2\cdot(-1)^k)$$

is a square.

Proof. Write $f = f_{n,n-k+1,k}$. As usual, we apply the square discriminant criterion Theorem 2.3.1: the polynomial f has square discriminant if and only if $(-1)^{n/2} f(1) f(-1)$ is a square. It is easy to see that $f(1) = n+1-2(n-k+1)+2k = 4k-n+1$ and, writing $F = F_{n,n-k+1,k} = X^{n+1} - 2X^{n+1-k} + 2X^k - 1$, that

$$f(-1) = \frac{F(-1)}{-2} = 1 - 2 \cdot (-1)^k,$$

thus proving the claim. □

For example, the family

$$\frac{X^{8n+v} - 2X^{6n+v(1+t+t^2)} + 2X^{2n-v(t+t^2)} - 1}{X-1} \tag{4.9}$$

has square discriminant for any $v \in \{\pm 1\}$ and nonnegative integer t satisfying $t + t^2 < 2n$. Under Conjecture 4.4.1, it is also irreducible unless $\gcd(n, 1+2t+2t^2) \neq 1$ when $v = 1$ and $\gcd(4n-1, t(t+1)) \neq 1$ when $v = -1$.

It seems hard to prove irreducibility directly; in the following, we consider another approach that, again conditionally, gives an asymptotic upper bound on the number of factors of $f_{n,n+1-k,k}$.

The *Mahler measure* $M(f)$ of a polynomial $f(X) \in \mathbb{C}[X]$ is

$$M(f) = \prod \max\{1, |\alpha_i|\}, \tag{4.10}$$

where the product extends over all roots α_i of f (repeated according to multiplicity). Note that $M(f)$ is a multiplicative function, i.e., $M(fg) = M(f)M(g)$. The quantity $M(f)$ first showed up in Lehmer's paper [**25**] (published in 1933), one of many of his hand on primality tests. Here, he proposed a method to find large primes which would be optimal in case $M(f)$ was very close to 1. Lehmer did not find a polynomial whose Mahler measure was smaller than $\theta^\star = 1.176\ldots$, which is the Mahler measure of $f^\star = X^{10} + X^9 - X^7 - X^6 - X^5 - X^4 - X^3 + X + 1$. This naturally led to the following conjecture.

Conjecture 4.4.5 (Lehmer's conjecture)**.** *Let $f \in \mathbb{Z}[X]$ be a noncyclotomic polynomial. Then $M(f) \geq \theta^\star$.*

Notice that $f^\star$ is a reciprocal polynomial. This is perhaps no coincidence, as Smyth [**46**] showed that Lehmer's conjecture holds for nonreciprocal polynomials. In fact, he showed the following.

Theorem 4.4.6 (Smyth's theorem)**.** *Let $f \in \mathbb{Z}[X]$ be a nonreciprocal polynomial. Then $M(f) \geq M(X^3 - X - 1) = 1.324\ldots$.*

For reciprocal Littlewood polynomials with two sign changes, computational results suggest that the following should be true.

Conjecture 4.4.7. *We have*

$$\lim_{(n,k)\to\infty} M(f_{n,n+1-k,k}) = 2. \tag{4.11}$$

We stress that the conjecture claims that the limit in (4.11) equals 2 regardless of the way n and k approach infinity. Together with Lehmer's conjecture, it would imply the following lemma.

Lemma 4.4.8. *Assume that both Lehmer's conjecture 4.4.5 and Conjecture 4.4.7 hold. Let $(t_i)_{i\in\mathbb{N}}$ be a sequence of tuples (n,k) such that $t_i \to \infty$ (i.e., both n and k go to infinity) as $i \to \infty$. Then there is an integer N such that, for every $i \geq N$, the polynomial $f_{n,n+1-k,k}$ has at most four factors for every pair of values of (n,k) taken by t_i.*

Proof. Write $f_{n,n+1-k,k} = g_1 \cdot \ldots \cdot g_r$ for the factorisation of $f_{n,n+k-1,k}$ into irreducibles. As $f_{n,n+1-k,k}$ has middle coefficient in $\{\pm 1\}$, each g_i is again reciprocal by Lemma 2.5.1 and the argument in the proof of Lemma 2.5.5, part (3). Hence by Lehmer's conjecture, the Mahler measure of each g_i is at least $\theta^\star$. Therefore

$$M(f_{n,n+1-k,k}) = M(g_1) \cdot \ldots \cdot M(g_r) \geq (\theta^\star)^r.$$

Since $(\theta^\star)^4 = 1.914\ldots$ and $(\theta^\star)^5 = 2.251\ldots$, the integer r cannot exceed 4 assuming Conjecture 4.4.7. □

Restricting how the limit in (4.11) is taken, it can be computed more easily. The goal of this section is to calculate a few examples of this. In order to do so, we need to introduce multivariate Mahler measures, which were first introduced by Mahler in [**32**].

Definition 4.4.9. Define for any nonzero polynomial $f(X_1,\ldots,X_k) \in \mathbb{C}[X_1,\ldots,X_k]$ the *logarithmic Mahler measure* as

$$m(f(X_1,\ldots,X_k)) = \int \cdots \int_{[0,1]^k} \log|f(e(t_1),\ldots,e(t_k))|\,\mathrm{d}x_1 \cdots \mathrm{d}x_k$$

where $e(t) = e^{2\pi i t}$. The *Mahler measure* of f is the quantity

$$M(f(X_1,\ldots,X_k)) = \exp(m(f(X_1,\ldots,X_k))).$$

Previously, Mahler [31] had shown that this definition is in accordance with (4.10) when taking $k = 1$, as an application of the corollary of Jensen's formula mentioned in Lemma 1.6.3. We will also repeatedly use Lemma 1.6.3 in this section.

There is one last lemma that we need in order to calculate limit values of multivariate Mahler measures.

Lemma 4.4.10. *For a nonzero polynomial $f(X_1,\dots,X_k) \in \mathbb{C}[X_1,\dots,X_k]$, the limit*

$$\lim_{m_2\to\infty} \cdots \lim_{m_k\to\infty} M(f(X, X^{m_2},\dots,X^{m_k}))$$

exists and is equal to $M(f(X_1,\dots,X_k))$.

Proof. See [12, Thm. 3.7]. □

We are now ready to prove certain cases of Conjecture 4.4.7.

Lemma 4.4.11. *Fix an integer k. Then*

$$\lim_{n\to\infty} M(f_{n,n+1-k,k}) = 2.$$

In particular, the double limit

$$\lim_{k\to\infty} \lim_{n\to\infty} M(f_{n,n+1-k,k})$$

equals 2.

Proof. Write $f_n = f_{n,n+1-k,k}$ and $F_n = (X-1)f_n = X^n - 2X^{n-k} + 2X^k - 1$, so that $M(F_n) = M(f_n)$. Consider $\hat{F}(X,Y) = (X^k-2)Y + X^k(2X^k-1)$, so that $\hat{F}(X,X^n) = X^k(X^n - 2X^{n-k} + 2X^k - 1)$ has the same Mahler measure as F_n. Hence

$$\lim_{n\to\infty} M(f_n(X)) = M(\hat{F}(X,Y))$$

by Lemma 4.4.10. Write $e(t) = e^{2\pi i t}$. Then

$$\begin{aligned} m(\hat{F}) &= \iint_{[0,1]^2} \log|e(s)(e(kt)-2) + e(kt)(2e(kt)-1)|\,\mathrm{d}s\,\mathrm{d}t \\ &= \iint_{[0,1]^2} \log|e(kt)-2| + \log\left|e(s) + e(kt)\frac{2e(kt)-1}{e(kt)-2}\right|\mathrm{d}s\,\mathrm{d}t \\ &= \int_0^1 \log|e(kt)-2| + \log^+\left|e(kt)\frac{2e(kt)-1}{e(kt)-2}\right|\mathrm{d}t. \end{aligned}$$

Since $|2e(kt)-1| = |e(kt)-2|$ for all t, the second term of the last integrand vanishes. We evaluate the remaining integral after the substitution $u = kt$ as

$$\begin{aligned} m(\hat{F}) &= \frac{1}{k}\int_0^k \log|e(u)-2|\,\mathrm{d}u \\ &= \frac{1}{k}\cdot k\cdot\int_0^1 \log|e(u)-2|\,\mathrm{d}u \\ &= \log 2, \end{aligned} \tag{4.12}$$

where the penultimate equality relies on the periodicity of the integrand and the last equality on Lemma 1.6.3. □

A similar result is the following.

Lemma 4.4.12. *For any fixed integers $a, b \geq 1$ and c, we have*

$$\lim_{n\to\infty} M(f_{(a+b)n+c,\,bn+c+1,\,an}) = 2.$$

Proof. Now consider $\hat{F}(X,Y) = X^cY^b(Y^a-2)+2Y^a-1$. Then $\hat{F}(X,X^n) = X^{c+bn+an} - 2X^{c+bn}+2X^{an}-1$. We have

$$\begin{aligned} m(\hat{F}) &= \iint_{[0,1]^2} \log|e(cs)e(bt)(e(at)-2)+2e(at)-1|\,\mathrm{d}s\,\mathrm{d}t \\ &= \iint_{[0,1]^2} \log|e(bt)(e(at)-2)| + \log\left|e(cs)+\frac{2e(at)-1}{e(bt)(e(at)-2)}\right|\mathrm{d}s\,\mathrm{d}t. \end{aligned}$$

The integrand on the last line is obtained by pulling out $|e(bt)(e(at-2))|$ from the logarithm in the integrand on the previous line. Note that all terms are independent of s, except for $e(cs)$. The term containing $e(cs)$ can thus be evaluated in the same way as the derivation in (4.12), after substituting $u = cs$. We thus obtain

$$\begin{aligned} m(\hat{F}) &= \int_0^1 \log|e(bt)(e(at)-2)| + \log^+\left|\frac{2e(at)-1}{e(bt)(e(at)-2)}\right|\mathrm{d}t \\ &= \int_0^1 \log|e(bt)(e(at)-2)|\,\mathrm{d}t \\ &= \int_0^1 \log|e(at)-2|\,\mathrm{d}t \\ &= \log 2. \end{aligned}$$

where the second equality again follows from the fact that $|2e(at)-1| = |e(bt)(e(at)-2)|$, and the last equality from the same derivation as in (4.12). □

Picking $a = 2$, $b = 6$, $c = \upsilon \in \{\pm 1\}$ in Lemma 4.4.12 corresponds to (4.9) with $t = 0$.

CHAPTER 5

Littlewood and related polynomials: topology

5.1 Introduction

So far, we have regarded Littlewood polynomials mainly as algebraic objects. But they are also interesting from a topological point of view, illustrated by the following warm-up example. Suppose f is a Littlewood polynomial with a root $z \in \mathbb{C}$ of modulus smaller than 1. The modulus of z is bounded from below by $1/2$ since

$$1 = \pm z \pm z^2 \pm \cdots \pm z^n \leq |z| + |z|^2 + \cdots + |z|^n < \frac{|z|}{1-|z|}. \tag{5.1}$$

Since f_{rev} is also a Littlewood polynomial, the set of *all* roots of *all* Littlewood polynomials is closed under $z \mapsto 1/z$. In particular, any root of a Littlewood polynomial lies in the annulus $\{z \in \mathbb{C} \mid 1/2 \leq |z| \leq 2\}$.

In this chapter we will adopt a topological point of view and prove certain topological statements related to the set of all roots of all Littlewood polynomials. We first introduce a few pieces of notation that allow us to state these results.

Definition 5.1.1. Let $S \subset \mathbb{Z}$ be a finite set of cardinality at least 2; we shall refer to S as a/the *coefficient set*. Define the *polynomial set* L_S as the set of polynomials with nonvanishing constant term and coefficients in S, and the *root set* as

$$\Gamma_S = \{z \in \mathbb{C} \mid f(z) = 0 \text{ for some } f \in L_S\}.$$

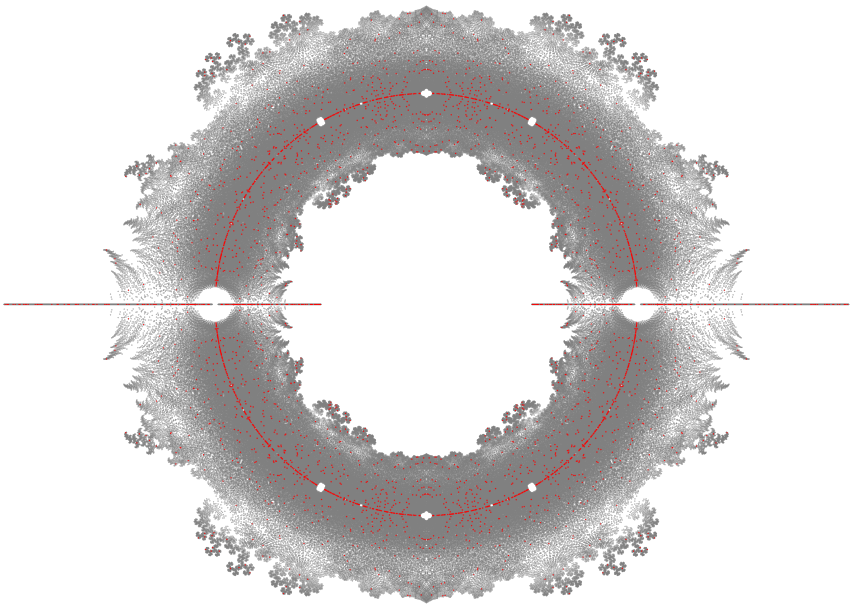
Similarly, we define the *square discriminant polynomial set* $L_S^{\square}$ as the set of polynomials with square discriminant, nonvanishing constant term, and coefficients in S, and the corresponding *square discriminant root set* as

$$\Gamma_S^{\square} = \{z \in \mathbb{C} \mid f(z) = 0 \text{ for some } f \in L_S^{\square}\}.$$

We explicitly exclude the case that S has only one element, as the root set will then be either empty (if $S = \{0\}$) or else consist of the roots of unity. Note in particular that this implies that S always contains a nonzero element. As the set S in the above definition is finite, the sets Γ_S and $\Gamma_S^{\square}$ are countable and we cannot hope to say much about their topology. Instead, we consider their closures, which we shall denote by M_S and $M_S^{\square}$, respectively. In practice, the set S is fixed and we simply write L, Γ, and so on instead of L_S, Γ_S, and so on.

The main results in this chapter are as follows. First, we prove in Theorem 5.2.4 that $M_S = M_S^{\square}$ whenever $S = -S = \{-s \mid s \in S\}$, such as in the case $S = \{\pm 1\}$. Secondly, we use Odlyzko and Poonen's methods [**39**] to show in Theorem 5.3.3 that M_S is connected for $S = \{\pm 1\}$, $\{0, \pm 1\}$, and $\{0, 1\}$; the proof techniques are very similar in these cases. Thirdly, we follow Bousch' manuscript [**10**] to give in Theorem 5.4.4 another proof of the connectedness of M_S for $S = \{\pm 1\}$ and $\{0, \pm 1\}$, this time from the point of view of complex dynamics. His methods also show in Theorem 5.4.1 and Theorem 5.4.2 that the closures M_S are not just contained in annuli, but also *contain* certain annuli, and that there is a wonderful relationship between $M_{\{\pm 1\}}$ and $M_{\{0,\pm 1\}}$, giving yet another motivation to study the latter set in the first place.

Figure 5.1: All roots of Littlewood polynomials of degree 16 (grey) and those with square discriminant (red). The amount of red dots seems rather small; however, they will fill up the whole grey area as the degree tends to infinity, as shown in Theorem 5.2.4.



5.2 Power series and square discriminants

Let $S \subset \mathbb{Z}$ be a coefficient set. As S will be fixed in this section, we simply write L, Γ, M, $\Gamma^\square$ and $M^\square$ for the corresponding polynomial set, root set, the closure of the root set, the square discriminant root set, and the closure of the square discriminant root set – see Definition 5.1.1. Denote $B = \max_{s\in S} |s|$ and note that $B \geq 1$ as S contains a nonzero integer. In this section, we recast the problems stated above in terms of power series and show that $M = M^\square$ if $S = -S = \{-s \mid s \in S\}$.

The *power series set corresponding to* L is the set $L^\star$ of power series whose constant term is nonvanishing and whose set of coefficients coincides with the set of coefficients of the polynomials in L. If $f \in L^\star$, then

$$|f(z)| \leq B(1 + |z| + |z|^2 + \cdots) = \frac{B}{1-|z|}$$

for any z in the open unit disk $\mathbb{D}$. In particular, the radius of convergence of f is at least 1 and the set of roots of f within $\mathbb{D}$ is well-defined. We write

$$\Gamma^\star = \{z \in \mathbb{D} \mid f(z) = 0 \text{ for some } f \in L^\star\} \cup \mathbb{S}^1.$$

It will soon be made clear why the unit circle $\mathbb{S}^1$ is included here. But first, we define the *cyclotomic power series* as

$$p_\infty(X) = 1 + X + X^2 + \cdots = \frac{1}{1-X}.$$

The power series $Bp_\infty(X)$ lies in $L^\star$, but has no roots in $\mathbb{D}$.

If $0 \in S$, then it is clear that we can think of L as a subset of $L^\star$. However, we only really care about the *roots* of the polynomials in L, not so much about the polynomials themselves. This brings us to the *hat operator*, which is defined as the map $L \to L^\star$ given by

$$g(X) \mapsto \hat{g}(X) = g(X)p_\infty(X^{1+\deg g}).$$

The power series $\hat{g}$ has the same roots within $\mathbb{D}$ as g. This shows we can always think of L as a 'subset' of $L^\star$, or more precisely, that $\Gamma^\star$ contains $\Gamma \cap \overline{\mathbb{D}}$. The following lemma and proposition strengthen this result.

Lemma 5.2.1. *The unit circle* $\mathbb{S}^1$ *is contained in* M.

Proof. For any positive integer n, the polynomial $Bp_n = B(1 + X + \cdots + X^n)$ is contained in L, so its roots lie in Γ. The roots of Bp_n are exactly the $n+1$-th roots of unity, the union of which lie dense in $\mathbb{S}^1$ as n goes to infinity. Hence $\mathbb{S}^1$ lies in M. □

Proposition 5.2.2. *We have*

$$M \cap \overline{\mathbb{D}} = \Gamma^\star,$$

where $\overline{\mathbb{D}}$ *denotes the closed unit disk.*

Proof. In [5, Prop. 1.2], it is shown that $M \cap \mathbb{D} = \Gamma^\star \cap \mathbb{D}$. The result follows from Lemma 5.2.1 and the definition of $\Gamma^\star$. □

In addition, we have the following.

Lemma 5.2.3. *The set* M *is connected if and only if* $\Gamma^\star$ *is connected.*

Proof. Since L is closed under reversal $f \mapsto f_{\mathsf{rev}}$, the sets Γ and M are closed under the inversion map

$$\mathsf{inv}\colon M \to M, \quad z \mapsto z^{-1}.$$

Inversion is clearly a homeomorphism away from 0, so it is a homeomorphism on M if Γ lies in the complement of an open disk around 0. This holds because Γ lies in an annulus centered at 0: indeed, Γ lies in the annulus $\{z \in \mathbb{C} \mid 1/(B+1) \le |z| \le B+1\}$, by an argument similar to the one leading up to (5.1).

Recall that the union of two connected sets is connected if and only if their intersection is nonempty. Lemma 5.2.1 shows that

$$(M \cap \overline{\mathbb{D}}) \cup (M \setminus \mathbb{D}) = M, \qquad (M \cap \overline{\mathbb{D}}) \cap (M \setminus \mathbb{D}) = \mathbb{S}^1,$$

so the set M is connected if and only if both $M \cap \overline{\mathbb{D}}$ and $M \setminus \mathbb{D}$ are connected. Since inversion maps $M \cap \overline{\mathbb{D}}$ continuously to $M \setminus \mathbb{D}$, and the continuous image of a connected set is connected, we conclude that M is connected if and only if $M \cap \overline{\mathbb{D}}$ is connected. The result follows from Proposition 5.2.2. □

The connectedness of $\Gamma^\star \cap \overline{\mathbb{D}}$ will be established in Section 5.3. In the remainder of the present section, we show that M and $M^\square$ coincide.

Theorem 5.2.4. *Let* $S \subset \mathbb{Z}$ *be a coefficient set such that* $S = -S = \{-s \mid s \in S\}$. *Suppose that* $\alpha \in \mathbb{D}$ *is a root of a power series* $f \in L^\star$. *Then there exist a sequence* $(f_k)_{k \ge 0}$ *of reciprocal polynomials with, for each* k, *the following properties:*

(1) f_k *has square discriminant;*
(2) The coefficients of f_k *lie in* S *for each* k*;*
(3) f_k *has a root* α_k *such that* $\alpha_k \to \alpha$ *as* $k \to \infty$.

In particular, the equality $M_S = M_S^\square$ *holds whenever* $S = -S$. *Furthermore, we can also find a sequence* $(f_k)_{k \ge 0}$ *of skew-reciprocal polynomials satisfying properties* (1)–(3).

The idea of the proof is to take the first k coefficients of f_k to be equal to those of f, so that Lemma 1.6.1 gives property (3). The remaining part of the proof consists of manipulating the terms of f_k of degree $\geq k$ enough while maintaining property (2), until property (1) pops out.

Proof of Theorem 5.2.4. Write $f = a_0 + a_1X + a_2X^2 + \cdots$. If $0 \in S$ and all a_i are 0 from some point onwards, then we replace f by $\hat{f}$ (we can think of f as an element of L, so this is possible).

Consider for each even k the polynomial

$$g_k(X) = a_0 + a_1X + \cdots + a_{k-1}X^{k-1}$$

obtained by truncating f at the $k-1$-th term. Define

$$f_k(X) = g_k(X) + X^k g_k(-X) + aX^{2k} - X^{2k+1}(g_k)_{\mathsf{rev}}(-X) + X^{3k+1}(g_k)_{\mathsf{rev}}(X)$$

where $a \in S$ can be chosen at will. Then the coefficients of f_k lie in S, and $\deg f_k = 4k$. Note that $(g_k)_{\mathsf{rev}}(-X) = (-X)^{k-1}g_k(-X^{-1}) = -X^{k-1}g_k(-X^{-1})$ since k is even. Hence f_k is reciprocal since

$$\begin{aligned}(f_k)_{\mathsf{rev}} &= X^{4k}g_k(X^{-1}) + X^{3k}g_k(-X^{-1}) + aX^{2k} - X^{2k-1}(g_k)_{\mathsf{rev}}(-X^{-1}) + X^{k-1}(g_k)_{\mathsf{rev}}(X^{-1}) \\ &= X^{3k+1}(g_k)_{\mathsf{rev}}(X) - X^{2k+1}(g_k)_{\mathsf{rev}}(-X) + aX^{2k} + X^k g_k(-X) + g_k(X) \\ &= f_k.\end{aligned}$$

Furthermore, $f - f_k$ is divisible by X^k. Hence we obtain a root α_k of f_k arbitrarily close to α by Lemma 1.6.1 as k tends to infinity. Lastly, we need to show that f_k has square discriminant. As $\deg f_k = 4k$ is divisible by 4, Theorem 2.3.1 says that f_k has square discriminant if and only if f_k is inseparable or $f_k(1)f_k(-1)$ is a square. But it is not hard to check that

$$f_k(1) = f_k(-1) = g_k(1) + g_k(-1) + a - (g_k)_{\mathsf{rev}}(-1) + (g_k)_{\mathsf{rev}}(1)$$

so $f_k(1)f_k(-1)$ is a square. (By choosing a well, we can also ensure that $f_k(1)f_k(-1)$ is nonzero, but that doesn't guarantee that f_k is separable, as its trace polynomial may also have double roots.)

For the skew-reciprocal case, an analogous argument works. Take k divisible by 4, leave g_k as before, and set

$$f_k(X) = g_k(X) + X^k g_k(-X) + aX^{2k} + X^{2k+1}(g_k)_{\mathsf{srev}}(-X) - X^{3k+1}(g_k)_{\mathsf{srev}}(X)$$

where again $a \in S$ can be chosen freely. Then the coefficients of f_k lie in S. Since $\deg f_k = 4k$ is divisible by 4, we have $(f_k)_{\mathsf{srev}}(X) = X^{4k} f(-X^{-1})$. Note that

$$(g_k)_{\mathsf{srev}}(X) = (-1)^{\frac{(k-1)(k-2)}{2}} X^{k-1} g_k(-X^{-1}) = -X^{k-1} g_k(-X^{-1})$$

since k is divisible by 4. Hence f_k is skew-reciprocal, since

$$\begin{aligned}(f_k)_{\mathsf{srev}} &= X^{4k} g_k(-X^{-1}) + X^{3k} g_k(X^{-1}) + aX^{2k} + X^{2k-1}(g_k)_{\mathsf{srev}}(X^{-1}) - X^{k-1}(g_k)_{\mathsf{srev}}(-X^{-1}) \\ &= -X^{3k+1}(g_k)_{\mathsf{srev}}(X) + X^{2k+1}(g_k)_{\mathsf{srev}}(-X) + aX^{2k} + X^k g_k(-X) + g_k(X) \\ &= f_k.\end{aligned}$$

Again, $f - f_k$ is divisible by X^k, so f_k has a root α_k that converges to α as k tends to infinity by Lemma 1.6.1. Theorem 2.3.1 says that f_k has square discriminant if f_k is inseparable or $f_k(i)f_k(-i)$ is a square. In this case

$$f_k(i) = f_k(-i) = g_k(i) + g_k(-i) + a + i \cdot (g_k)_{\mathsf{srev}}(-i) - i \cdot (g_k)_{\mathsf{srev}}(i),$$

so that $f_k(i)f_k(-i)$ is indeed a square. (Again, by choosing a well we can also ensure that $f_k(i)f_k(-i)$ is nonzero, but that doesn't guarantee that f_k is separable, as its trace polynomial can also have double roots.) □

Corollary 5.2.5. *We have the equalities $M^{\square}_{\{0,\pm1\}} = M_{\{0,\pm1\}}$ and $M^{\square}_{\{\pm1\}} = M_{\{\pm1\}}$. In particular, the closure of the root set of Littlewood polynomials whose Galois group is contained in the Coxeter group $\mathcal{D}_n$, itself contained in the alternating group A_{2n}, equals the closure of the root set of all Littlewood polynomials.*

Proof. The first part is an immediate consequence of Theorem 5.2.4. Note that Littlewood polynomials of even degree are separable since they have odd discriminant, see Lemma 4.2.1. Hence the second part of the statement is a consequence of Lemma 1.2.2, Lemma 2.4.8, and Lemma 2.4.11. □

5.3 Proof of connectedness (after Odlyzko & Poonen)

In this section, we give an exposition of the proof of Odlyzko and Poonen [39] of the connectedness of M_S when $S = \{0, 1\}$. We slightly generalise their methods and show the same claim for $S = \{\pm1\}$ and $S = \{0, \pm1\}$. From now on, we assume that S is any of these three sets.

We start with the following lemma, which is a key ingredient of the proof of connectedness of M_S. First some notation: Let l be a positive integer and denote by $[l]$ any set of l integers. Endow $[l]$ with the discrete topology and $[l]^{\mathbb{N}}$ with the product topology. If

$v \in [l]^n$ for some $n \geq 0$, then we write S_v for the set of elements of $[l]^{\mathbb{N}}$ that start with v, i.e., whose first n 'digits' coincide with v. If $i \in [l]$, then S_{vi} is the set of elements of $[l]^{\mathbb{N}}$ that start with v and are then followed by an i. The following lemma is a slight generalisation of [39, Lem. 4.1].

Lemma 5.3.1. *Let Y be a topological space. Suppose $h\colon [l]^{\mathbb{N}} \to Y$ is a continuous map such that*

$$h(S_{vi}) \cap h(S_{vj}) \neq \varnothing$$

for all $v \in [l]^n$, $n \geq 0$, and $i, j \in [l]$. Then $\mathrm{im}(h)$ *is path-connected.*

Proof. Suppose $n \geq 1$ is an integer and the first $n-1$ coordinates of two sequences $x', x \in [l]^{\mathbb{N}}$ agree. Then there exists an ordered tuple (s, s') of elements in $[l]^{\mathbb{N}}$—which we call the n-midtuple of (x', x)—such that the first n coordinates of s agree with those of x' and the first n coordinates of s' agree with those of x, and $h(s) = h(s')$. (Note that the order of decorated and undecorated symbols in the tuples swaps; hopefully the reader will acknowledge that this is justified at the end of the proof!) Indeed, if the n-th coordinate of x and x' are the same, take $s = s' = x$; otherwise, apply the hypothesis with v as the first $n-1$ coordinates of x. The sequences s and s' do not have to be unique, but their first $n-1$ coordinates agree.

Suppose x'_0 and x_1 are two elements of $[l]^{\mathbb{N}}$. Define a path $\gamma : [0,1] \to \mathrm{im}(h)$ from $\gamma(0) = h(x'_0)$ to $\gamma(1) = h(x_1)$ as follows. Recursively pick for any $n \geq 1$ and any odd $d < 2^n$ some n-midtuple $(x_{d/2^n}, x'_{d/2^n})$ of $(x'_{(d-1)/2^n}, x_{(d+1)/2^n})$, and set

$$\gamma(d/2^n) = h(x_{d/2^n}) = h(x'_{d/2^n}).$$

At each

$$r = \sum_{i=1}^{\infty} \epsilon_i 2^{-i} \in [0,1], \quad \epsilon_i \in \{0,1\}$$

that is not a dyadic rational, set

$$x_r = x'_r = \lim_{n\to\infty} x'_{\pi_n(r)}, \quad \text{where} \quad \pi_n(r) = \sum_{i=1}^{n} \epsilon_i 2^{-i}$$

and take $\gamma(r) = h(x_r) = h(x'_r)$. The 2-adic expansion of r is unique, so this is well-defined.

Observe that $x'_{e/2^m}$ has the same first $m-1$ coordinates as $x_{(e+1)/2^m} = x_{f/2^k}$, which has the same first $k-1$ coordinates as $x'_{f/2^k}$, which has the same first $k-1$ coordinates as $x_{(f+1)/2^k}, \ldots$. Inductively we conclude that certainly the first n coordinates of $x'_{d/2^n}$ and $x'_{e/2^m}$ agree if $m \geq n$ and d, e are odd.

Denote by $v \in [l]^n$ the first n coordinates of $x_{(d+1)/2^n}$, or equivalently, those of $x'_{d/2^n}$. Let $r \in [d/2^n, (d+1)/2^n)$. If $r = e/2^m$ is a dyadic rational, then $m \geq n$ and the discussion above shows that the first n coordinates of x'_r agree with those of $x'_{d/2^n}$. If r is not a dyadic rational, then x'_r has the same first n coordinates as $x'_{\pi_n(r)} = x'_{d/2^n}$ all the same. Hence γ maps the interval $[d/2^n, (d+1)/2^n]$ into $h(S_v)$.

It remains to show that γ is indeed continuous. Let $U \subset Y$ be an open neighbourhood of $\gamma(r)$. Then $h^{-1}(U)$ contains x_r and x'_r and is open, i.e., of the form $\prod_i U_i$ with $U_i \subset [l]$ for all i and $U_i = [l]$ from some i onwards, by continuity. Therefore $h^{-1}(U)$ contains S_v for some finite substring v of x_r onwards. Similarly, we find a substring v' of x'_r such that $S_{v'} \subset h^{-1}(U)$. Hence $\gamma^{-1}(U)$ contains $\gamma^{-1}(h(S_v) \cup h(S_{v'}))$. The last sentence of the previous paragraph implies that the latter set contains an interval containing r. □

Again, let L be one of $L_{\{0,1\}}$, $L_{\{\pm 1\}}$ and $L_{\{0,\pm 1\}}$. Set $L^\star$ for the corresponding power series set, and again we consider Γ, M, $M^\square$ and $\Gamma^\star$ as before. Consider the closed set

$$\Gamma^\star_\delta = (\Gamma^\star \cap \overline{\mathbb{D}}) \cup \{z \in \mathbb{C} \mid 1 - \delta \leq |z| \leq 1\}$$

where $\delta \in (0,1)$ is a real number.

Proposition 5.3.2. *The set $\Gamma^\star_\delta$ is connected for any $\delta \in (0,1)$.*

Before showing Proposition 5.3.2, we show that it implies that $\Gamma^\star$ is connected.

Theorem 5.3.3. *The set $\Gamma^\star \cap \overline{\mathbb{D}}$ is connected. Therefore M is connected, and $M^\square$ too if $S = -S$.*

Proof. Consider the collection $(\Gamma^\star_{1/k})_{k \geq 2}$. Each of its elements is a closed, nonempty, connected subset of the compact metric space $\overline{\mathbb{D}}$ by Proposition 5.3.2. Hence

$$\bigcap_{k \geq 2} \Gamma^\star_{1/k} = (\Gamma^\star \cap \overline{\mathbb{D}}) \cup \mathbb{S}^1 = \Gamma^\star \cap \overline{\mathbb{D}}$$

is connected by Lemma 1.5.2 (recall that $\mathbb{S}^1 \subset \Gamma^\star$ by Lemma 5.2.1). The last statements follow from Lemma 5.2.3 and Theorem 5.2.4. □

The following lemma, which is Lemma 4.2 in [39], is another prerequisite for the proof of Proposition 5.3.2.

Lemma 5.3.4. *Let X be a topological space and $A \subset X^n/S_n$ a connected subset. Suppose that $P \in X$ is a point such that the multiset $\{\{P, P, \ldots, P\}\}$ is in A, and write $B \subset X$ for the subset consisting of all coordinates of all points in A. Then B is connected.*

Proof. We show the contrapositive. Suppose that B is disconnected. Then there are opens U and V of X such that $U \cap B$ and $V \cap B$ are disjoint, nonempty sets whose union equals B. Assume without loss of generality that P lies in U. Consider the open subsets

$$U' = \{p = (p_1, \ldots, p_n) \in X^n \mid p_i \in U \text{ for all } i\},$$
$$V' = \{p = (p_1, \ldots, p_n) \in X^n \mid p_i \in V \text{ for some } i\}$$

of X^n. The definitions of U' and V' imply that $\sigma \cdot U' = U'$ and $\sigma \cdot V' = V'$ for any $\sigma \in S_n$. Therefore the quotient map $\pi : X^n \to X^n/S_n$ sends U' and V' to opens in X^n/S_n. Set $U'' = \pi(U') \cap A$ and $V'' = \pi(V') \cap A$. We will show that $A = U'' \cup V''$ is a partitioning of A into open, nonempty, disjoint sets. This shows that A is disconnected and thus proves the lemma.

First, the sets U'' and V'' are open by definition. Secondly, U'' is nonempty: indeed, the tuple $(P, \ldots, P)$ lies in U', so the multiset $\{\{P, \ldots, P\}\}$ lies in U''. Since $V \cap B$ is nonempty, the set V'' is also nonempty. Thirdly, any mulitset $x \in A$ must lie either in U'' or in V'', but not in both, as either all the coordinates of tuples in $\pi^{-1}(x)$ lie in U or at least one coordinate of each tuple lies in $B \setminus U = V \cap B$, but not both. □

In the following two lemmas, we will construct a specific metric space X and show how its metric d induces a metric D_n on the symmetric product X^n/S_n. It is the space X^n/S_n to which we will apply Lemma 5.3.4 in the proof of Proposition 5.3.2. The definition of the metric d in Lemma 5.3.5 is taken from [**9**, p. 18], although there it is not shown to be a metric.

Lemma 5.3.5. *Let $\delta \in (0,1)$ and write $r = 1 - \delta$. Define X_δ to be the unit disk with the outer annulus $\{z \in \mathbb{C} \mid r \leq |z| \leq 1\}$ collapsed to a point P. Then X_δ is a metric space with metric $d : X_\delta \times X_\delta \to \mathbb{R}_{\geq 0}$ defined for any $x, y \in X_\delta$ by*

$$d(x,y) = \begin{cases} \min\{|x-y|, 2r - |x| - |y|\} & \text{if } x, y \neq P \\ r - |x| & \text{if } y = P, \end{cases} \tag{5.2}$$

and such that $d(x,P) = d(P,x)$ and $d(P,P) = 0$. Here, $|\cdot|$ denotes the usual, Euclidean absolute value.

Proof. Write $X = X_\delta$. We need to demonstrate that d is a metric on X. Intuitively, the function d compares the usual Euclidean distance to the distance obtained by passing through P. Let $x, y \in X$. We certainly have $d(x,y) \geq 0$ (since $|x|, |y| \leq r$), and $d(x,y) = d(y,x)$. Furthermore, $d(x,x) = 0$. It remains to show that d satisfies the triangle inequality, which requires more effort. Let $x, y, z \in X$. First consider the case that $x, y, z \neq P$. We need to show in each case that $d(x,y) + d(y,z) \geq d(x,z)$. There are four

subcases, corresponding to each of the four possible combinations that the values $d(x,y)$ and $d(y,z)$ take. We will use without mention the triangle inequality for $|\cdot|$.

If $d(x,y) = |x-y|$ and $d(y,z) = |y-z|$, then their sum is at least $|x-z| \geq d(x,z)$.

If $d(x,y) = 2r - |x| - |y|$ and $d(y,z) = 2r - |y| - |z|$, then

$$d(x,y) + d(y,z) = 2r - |x| - |z| + (2r - 2|y|) \geq 2r - |x| - |z| \geq d(x,z).$$

The third subcase is $d(x,y) = 2r - |x| - |y|$ and $d(y,z) = |y-z|$. If $|y| \leq |z|$, then already $d(x,y) \geq 2r - |x| - |z| \geq d(x,z)$. If $|y| > |z|$, then by the reversed triangle inequality,

$$\begin{aligned} d(x,y) + d(y,z) &\geq 2r - |x| - |y| + ||y| - |z|| \\ &= 2r - |x| - |y| + |y| - |z| \\ &= 2r - |x| - |z| \\ &\geq d(x,z). \end{aligned}$$

Swapping the role of x and z gives the fourth and last subcase.

When $y = P$ and $x, z \neq P$, the triangle inequality follows quickly since

$$d(x,y) + d(y,z) = r - |x| + r - |z| = 2r - |x| - |z| \geq d(x,z).$$

Now consider the case that $x = P$ and $y, z \neq P$. If $|y| \leq |z|$, then already $d(x,y) = r - |y| \geq r - |z| = d(x,z)$. If instead $|y| > |z|$, there are again two subcases. If $d(y,z) = |y-z|$, then by the reversed triangle inequality we have $d(y,z) \geq ||y| - |z|| = |y| - |z|$, so

$$d(x,y) + d(y,z) \geq r - |y| + |y| - |z| = r - |z| = d(x,z).$$

If $d(y,z) = 2r - |y| - |z|$, then

$$\begin{aligned} d(x,y) + d(y,z) &\geq r - |y| + 2r - |y| - |z| \\ &= r - |z| + 2(r - |y|) \\ &\geq r - |z| \\ &= d(x,z). \end{aligned}$$

By symmetry, also the case $z = P$ and $x, y \neq P$ follows.

In all cases where at least two of x, y and z are equal to P, the result is immediate. □

The next step is to extend the metric d on X_δ to a metric D_n on the symmetric product X_δ^n / S_n.

Lemma 5.3.6. *The map* $D_n : X_\delta^n/S_n \times X_\delta^n/S_n \to \mathbb{R}_{\geq 0}$ *given by*

$$D_n(\{\{x_1,\dots,x_n\}\},\{\{y_1,\dots,y_n\}\}) \mapsto \min_{\sigma\in S_n}\max_i d(x_i, y_{\sigma(i)}).$$

defines a metric on X_δ^n/S_n *for any* $n > 1$.

Proof. Again, write $X = X_\delta$. We need to show that D_n is a metric. Take the elements $x = \{\{x_1,\dots,x_n\}\}$, $y = \{\{y_1,\dots,y_n\}\}$ and $z = \{\{z_1,\dots,z_n\}\}$ of X^n/S_n. Since d is a metric, we immediately obtain that $D_n(x,y) \geq 0$. Choosing the identity permutation for σ, we find $D_n(x,x) \leq \max_i d(x_i,x_i) = 0$. For symmetry, we find that

$$\begin{aligned} D_n(x,y) &= \min_{\sigma\in S_n}\max_i d(x_i, y_{\sigma(i)}) \\ &= \min_{\sigma\in S_n}\max_i d(x_{\sigma^{-1}(i)}, y_i). \end{aligned}$$

Since $\sigma \in S_n$ if and only if $\sigma^{-1} \in S_n$, we have

$$\begin{aligned} D_n(x,y) &= \min_{\sigma\in S_n}\max_i d(x_{\sigma(i)}, y_i) \\ &= \min_{\sigma\in S_n}\max_i d(y_i, x_{\sigma(i)}) \\ &= D_n(y,x) \end{aligned}$$

since d is symmetric. For the triangle inequality, we have

$$\begin{aligned} D_n(x,y) + D_n(y,z) &= D_n(y,x) + D_n(y,z) \\ &= \min_{\sigma\in S_n}\max_i d(y_i, x_{\sigma(i)}) + \min_{\tau\in S_n}\max_j d(y_j, z_{\tau(j)}) \\ &\geq \min_{\sigma,\tau\in S_n}\max_i d(y_i, x_{\sigma(i)}) + d(y_i, z_{\tau(i)}) \\ &\geq \min_{\sigma,\tau\in S_n}\max_i d(x_{\sigma(i)}, z_{\tau(i)}) \end{aligned}$$

since the triangle inequality holds for d. After relabelling, the last expression equals

$$\min_{\tau\in S_n}\max_i d(x_i, z_{\tau(i)}) = D_n(y,z),$$

so the triangle inequality holds for D_n. □

We are now ready to prove Proposition 5.3.2.

Proof of Proposition 5.3.2. Let $f \in L^\star$. Write $\mathbb{D}_\delta = \{z \in \mathbb{C} \mid |z| < 1-\delta\}$. By Lemma 1.6.5, there is a finite upper bound n on the number of zeros that f can have within $\mathbb{D}_\delta$, which

is independent of the choice of a particular f. Let (X_δ, d) and $(X_\delta^n/S_n, D_n)$ be the metric spaces defined in Lemma 5.3.5 and Lemma 5.3.6. Let $[l] = S$ (i.e., one of $\{0,1\}$, $\{\pm 1\}$, and $\{0,\pm 1\}$). Define the map

$$\mathsf{rts}\colon [l]^{\mathbb{N}} \to X_\delta^n/S_n$$

by assigning to the coefficient list of f the multiset M_f of cardinality n, that we construct in two steps. First, we construct the multiset $\widetilde{M}_f$ consisting of the roots of f inside $\mathbb{D}_\delta = \{z \in \mathbb{C} \mid |z| < 1-\delta\}$ (repeated according to multiplicity), and write $n' \le n$ for the cardinality of $\widetilde{M}_f$. Then M_f is defined as the union of $\widetilde{M}_f$ with $n-n'$ copies of P.

We claim that the map rts is continuous. Indeed, if $f, g \in L^\star$ share N initial coefficients with N large enough, then by Lemma 1.6.1, each root α of f lying in $\mathbb{D}_\delta$ of multiplicity m will be within ϵ (according to the Euclidean metric) of some (possibly nondistinct) roots $\beta_1, \dots, \beta_m$ of g. So α will certainly be within ϵ of β_i in X_δ if both α and β_i lie in $\mathbb{D}_\delta$. If β_i lies outside of $\mathbb{D}_\delta$, then its distance to α on X_δ only decreases. By definition of the metric D_n, we thus find $D_n(\mathsf{rts}(f), \mathsf{rts}(g)) < \epsilon$.

Notice that $\mathsf{rts}(1,1,\dots) = (P,P,\dots,P)$. So if $A = \mathrm{im}(\mathsf{rts}) \subset X_\delta^n/S_n$ is connected, then Lemma 5.3.4 shows that the subset $B \subset X_\delta$ consisting of all coordinates of all points in A is connected. But B is precisely equal to $\Gamma_\delta^\star$ with the annulus $\{z \in \mathbb{C} \mid 1-\delta \le |z| \le 1\}$ collapsed to a point. This implies that $\Gamma_\delta^\star$ is connected.

It remains to show that im(rts) is connected: for this, we show that Lemma 5.3.1 holds with $Y = X_\delta^n/S_n$ and $h = \mathsf{rts}$. We adopt the notation from that lemma, and write $v = (v_0, \dots, v_{n-1}) \in [l]^n$ with $n \ge 0$ and $i, j \in [l]$ distinct. We have to construct an $f \in S_{vi}$ and $g \in S_{vj}$ with the property that $\mathsf{rts}(f) = \mathsf{rts}(g)$. In the following, we will describe all possible cases, depending on the coefficient set S. First assume $S = \{0, \pm 1\}$. Write $v(X) = v_0 + \cdots + v_{n-1}X^{n-1}$, and pick

$$S_{vi} \times S_{vj} \ni (f,g) = \begin{cases} (v(X),\ v(X)p_\infty(jv_0X^n)) & \text{if } i = 0 \\ (v(X)p_\infty(iv_0X^n),\ v(X)) & \text{if } j = 0 \\ (v(X)p_\infty(iv_0X^n),\ v(X)p_\infty(jv_0X^n)) & \text{if } i, j \neq 0. \end{cases} \tag{5.3}$$

These are slightly tweaked versions of the hat operator. As p_∞ does not have roots in the unit disk, we find that $\mathsf{rts}(f) = \mathsf{rts}(v(X)) = \mathsf{rts}(g)$. Furthermore, the first line in (5.3) describes the desired construction when $S = \{0,1\}$, and the last line describes the desired construction if $S = \{\pm 1\}$. □

5.4 Proof of connectedness (after Bousch)

In this section, we look at the root sets Γ and their closures M from the point of view of iterated function systems (IFS). We mainly follow Bousch' unpublished manuscript

[10], but also borrow notation, definitions and proofs from [14]. Bousch' proof of the connectedness of $M_{\{0,\pm1\}}$ and $M_{\{\pm1\}}$ depends on the fact that both of these sets contain annuli of the form

$$\{z \in \mathbb{C} \mid R \le |z| \le 1/R\}$$

for some $R < 1$. The existence of these annuli is established using methods from iterated function systems and complex dynamics, which are quite different from the proof of Odlyzko and Poonen in Section 5.3.

These methods lead to the following beautiful theorems of Bousch; see [10, Prop. 2] and [14, Prop. 4.1.3].

Theorem 5.4.1. *If $z \in \mathbb{D}$ has modulus at least $1/\sqrt{2}$, then $z \in M_{\{0,\pm1\}}$.*

Theorem 5.4.2. *If $z^2 \in M_{\{0,\pm1\}}$ then $z \in M_{\{\pm1\}}$. In particular, the closure of the set of roots of Littlewood polynomials contains the annulus $\{z \in \mathbb{C} \mid 2^{-1/4} \le |z| \le 2^{1/4}\}$.*

The proofs of these theorems will be given later in this section, although we will only be able to give a conditional proof for the latter theorem. We first show how the existence of these annuli implies that the closures of the root sets are connected. The kind of argument required to establish that implication is, by contrast, muck akin to the reasoning in the proof of Odlyzko and Poonen.

Write $H = L^\star_{\{0,\pm1\}}$ for the collection of $\{0,\pm1\}$-power series, $H_1 = L^\star_{\{\pm1\}}$ for the collection of $\{\pm1\}$-power series, and H_N and $H_{1,N}$ for the images of H and H_1 under the truncation map

$$\pi_N : \sum_{i\in\mathbb{N}} a_i X^i \mapsto \sum_{i<N} a_i X^i.$$

Lastly, write W for the collection of power series whose coefficients are at most 2 in absolute value. The following is Lemma 3 in [10]; we reproduce Bousch' proof.

Lemma 5.4.3. *Let N be a positive integer and A, B polynomials in H_N (resp. $H_{1,N}$). Then there is a finite sequence $P_0 = A, Q_0, \ldots, P_{t-1}, Q_{t-1}, P_t = B$ of power series in W, satisfying for every i the following properties:*

(1) P_i is in H_N (respectively, in $H_{1,N}$);
(2) P_i divides Q_i;
(3) $P_{i+1} = \pi_N(Q_i)$.

This is much akin to the construction in (5.3).

Proof. We say that A and B *connect* if there is a sequence $P_0 = A, Q_0, \ldots, P_{t-1}, Q_{t-1}, P_t = B$ of power series in W, satisfying for every i the properties (1), (2) and (3).

Denote the coefficients of A by a_i, and those of B by b_i. After possibly replacing A by $-A$ and B by $-B$, we can assume that $a_0 = b_0 = 1$. Write $(s_0, s_1, \ldots)$ for the power series $s_0 + s_1 X + \cdots$. Set $\mathrm{err}(A,B) = \min\{N, \mathrm{val}_X(A-B)\}$ where $\mathrm{val}_X(A-B)$ is the maximal integer k such that X^k divides $A-B$. If $\mathrm{err}(A,B) = N$, then the lemma is true for trivial reasons. We proceed by induction. Suppose there is a $k < N$ such that the lemma is true for every $\mathrm{err}(A,B) > k$, and assume that $\mathrm{err}(A,B) = k$. Then $a_i = b_i$ for every $i < k$ and $a_k \neq b_k$. Write $S = (1, a_1, \ldots, a_k, 0, 0, \ldots) \in H_N$. Then $\mathrm{err}(A,S) > k$, so A and S connect. If $|a_k - b_k| = 1$, then the sequence $P_0 = S$, $Q_0 = S(1 + (b-a)X^k)$, $P_1 = \pi_N(Q_0) = (1, b_1, \ldots, b_k, \pm b_1, \pm b_2, \ldots)$ connects S to a polynomial that connects with B, again by the induction hypothesis. So A and B connect. If $|a_k - b_k| = 2$, then the sequence $P_0 = S$, $Q_0 = S(1 - aX^k)$ connects S to a polynomial $(1, a_1, \ldots, a_{k-1}, 0, -a, -a, \ldots)$, which connects to $U = (1, a_1, \ldots, a_{k-1}, 0, 0, \ldots)$ by the induction hypothesis. Now $P_0 = U$ and $Q_0 = U(1 + bX^k)$ connects U to a polynomial that connects to B. So A and B connect.

For $H_{1,N}$, write $A = (1, a_1, \ldots, a_{k-1}, \upsilon, a_{k+1}, \ldots) \in H_{1,N}$ and consider the polynomial $S = (1, a_1, \ldots, a_{k-1}, \upsilon, \upsilon a_1, \upsilon a_2, \ldots) \in H_{1,N}$, where $\upsilon \in \{\pm 1\}$. Then again A and S connect by the induction hypothesis. The sequence $P_0 = S$, $Q_0 = S(1 - 2\upsilon X^k)$ connects S to a polynomial P_1 that connects to B by the induction hypothesis, so A and B connect. □

Theorem 5.4.4. *The sets $M_{\{0,\pm 1\}}$ and $M_{\{\pm 1\}}$ are connected.*

Proof. Assume Theorem 5.4.1 and Theorem 5.4.2. We first prove that $M_{\{0,\pm 1\}}$ is connected. Set $R = 1/\sqrt{2}$ and $0 < \epsilon < 1 - R$. Let $z \in M_{\{0,\pm 1\}}$ be of modulus smaller than R, and suppose f is a $\{0, \pm 1\}$-power series such that $f(z) = 0$. Let N be large enough such that the roots of power series that have the same first N coefficients as f are within ϵ of the roots of f. We want to connect z to an element of $M_{\{0,\pm 1\}}$ of modulus at least R by means of an ϵ-chain in $M_{\{0,\pm 1\}}$ (see Definition 1.5.3). The result then follows since the annulus $\{z \in \mathbb{C} \mid R \leq |z| \leq 1/R\}$ is contained in $M_{\{0,\pm 1\}}$ by Lemma 5.4.1, so that $M_{\{0,\pm 1\}}$ is chain-connected and thus connected by Lemma 1.5.4.

Consider a sequence $P_0, Q_0, \ldots, P_t$ as in Lemma 5.4.3 with $P_0 = \pi_N(f)$ and $P_t = B = p_n(X) = 1 + X + X^2 + \cdots + X^N$. Since P_0 divides Q_0 and $P_1 = \pi_N(Q_0)$, the polynomial P_1 must have a root $z_1 \in M_{\{0,\pm 1\}}$ such that $|z_1 - z| < \epsilon$ by Lemma 1.6.1. By induction, we can find a root $z_{i+1} \in M_{\{0,\pm 1\}}$ of P_{i+1} for z_i as long as $|z_i| < R$. As soon as $|z_i| \geq R$, we are done. Lastly, the sequence $z, z_1, z_2, \ldots$ must be finite since the sequence $P_0, Q_0, \ldots, P_t$ is finite.

The connectedness of $M_{\{\pm 1\}}$ follows likewise after changing R to $2^{-1/4}$, now by Theorem 5.4.2. □

We now present the setup of Bousch' method in [**10**] used to show the existence of the annuli contained in $M_{\{0,\pm 1\}}$ and $M_{\{\pm 1\}}$. Fix again a coefficient set S. For a subset $L \subset \mathbb{C}$, denote by L_ϵ the set $\{x \in \mathbb{C} \mid \inf_{y \in L} |x - y| < \epsilon\}$. Let $\mathcal{K}$ be the collection of nonempty,

compact subsets of the complex plane. Then $\mathcal{K}$ is a metric space under the Hausdorff metric

$$d_H : \mathcal{K} \times \mathcal{K} \to \mathbb{R}_{\geq 0}, \quad (K, L) \mapsto \min\{\epsilon > 0 \mid K \subset L_\epsilon,\, L \subset K_\epsilon\},$$

see [**21**, pp. 189-190]. In fact, it is even complete, see [**42**]. For any $z \in \mathbb{C}$ the map

$$\varphi : \mathcal{K} \to \mathcal{K}, \quad A \mapsto zA + S = \{za + s \mid a \in A,\, s \in S\}$$

is $|z|$-Lipschitz under the Hausdorff metric (that is, $d_H(\varphi(A), \varphi(A')) \leq |z| d_H(A, A')$). If z lies in $\mathbb{D}$, the map φ is thus a contraction on a nonempty, complete metric space, so that it has a unique fixed point by the contraction mapping theorem, see Theorem 1.5.6. This fixed point, denoted by A_z and called the *attractor* or *limit set* of z, satisfies

$$A_z = S + zA_z = S + z(S + zA_z) = \ldots = S + zS + z^2 S + \cdots$$

– in other words, it is the set of values that power series in $L^\star$ attain in the point z. In particular, we derive the following.

Lemma 5.4.5. *We have* $M_{\{\pm 1\}} \cap \mathbb{D} = \{z \in \mathbb{D} \mid 0 \in A_z\}$. □

For any $z \in \mathbb{D}$ and $s \in S$, the map

$$z^s : \mathbb{C} \to \mathbb{C}, \quad x \mapsto zx + s$$

is a so-called *(contracting) similarity*, the adjective 'contracting' referring to the fact that z^s is a contraction mapping. Note that A_z equals the union $\bigcup_{s \in S} z^s(A_z)$. From now on, we only consider the case $S = \{\pm 1\}$ and thus study the similarities

$$z^+ : \mathbb{C} \to \mathbb{C}, \quad x \mapsto zx + 1 \qquad \text{and} \qquad z^- : \mathbb{C} \to \mathbb{C}, \quad x \mapsto zx - 1.$$

Set $A_z^+ = z^+(A_z)$ and $A_z^- = z^-(A_z)$, so that $A_z^+ = -A_z^-$. Bousch [**10**, Prop. 1] proved the following.

Lemma 5.4.6. *For any nonzero $z \in \mathbb{D}$, the following are equivalent:*

(a) A_z *is connected.*
(b) $A_z^+ \cap A_z^- \neq \emptyset$.
(c) $z \in M_{\{0,\pm 1\}} \cap \mathbb{D}$.

In particular, $M_{\{0,\pm 1\}} \cap \mathbb{D} = \{z \in \mathbb{D} \mid A_z \text{ is connected}\}$.

Proof. (a) $\Longrightarrow$ (b). Suppose that A_z^+ and A_z^- do not intersect. As the union of A_z^+ and A_z^- equals A_z, the complement of A_z^+ within A_z must be A_z^- (and vice versa). Hence the sets A_z^+ and A_z^-, which are both closed, are also both open. Thus A_z is disconnected.

(b) $\implies$ (a). Suppose $A_z^+ \cap A_z^-$ is nonempty. Because $A_z \subset \mathbb{C}$ is compact, it must be bounded. Hence there is a maximal distance t between points in A_z. So A_z is t-chain connected – see Definition 1.5.3. But $A_z = A_z^+ \cup A_z^-$ consists of copies of itself, scaled by a factor $|z|$, so A_z is $|z|t$-chain connected. By induction, A_z is $|z|^n t$-chain connected for every n. So A_z is chain connected and compact, which implies that it is connected by Lemma 1.5.4.

(b) $\iff$ (c). Suppose that (b) holds, and take sequences (a_i) and (a_i') in $\{\pm 1\}^{\mathbb{N}}$ with $a_0 = 1$ and $a_0' = -1$, such that $\sum a_i z^i = \sum a_i' z^i$. If $b_i = (a_i - a_i')/2$ for each i, then $(b_i) \in \{0, \pm 1\}^{\mathbb{N}}$ has the properties $b_0 \neq 0$ and $\sum b_i z^i = 0$. Conversely, any such sequence (b_i) gives sequences (a_i) and (a_i') in $\{\pm 1\}^{\mathbb{N}}$ with $a_0 = 1$ and $a_0' = -1$: indeed, define $a_0 = 1$, $a_0' = -1$, and for $i > 0$ set $-a_i' = a_i = b_i$ if $b_i \neq 0$ and $a_i = a_i' = 1$ if $b_i = 0$. □

The following proof is part of [**10**, Prop. 2].

Proof of Theorem 5.4.1. The ϵ-neighborhood $(A_z)_\epsilon$ of A_z satisfies $z^+((A_z)_\epsilon) \cup z^-((A_z)_\epsilon) \subset (A_z)_\epsilon$. As A_z is nonempty, the set $(A_z)_\epsilon$ has positive Lebesgue measure $\mu((A_z)_\epsilon)$. Suppose $z \notin M_{\{0,\pm 1\}}$. Then A_z^+ and A_z^- do not intersect by Lemma 5.4.6, so by compactness there is an $\epsilon > 0$ such that A_ϵ^+ does not intersect A_ϵ^-. Hence

$$\mu((A_z)_\epsilon) \geq \mu((A_z)_\epsilon^+ \cup (A_z)_\epsilon^-) = \mu((A_z)_\epsilon^+) + \mu((A_z)_\epsilon^-) = 2\mu((A_z)_\epsilon^+) = 2|z|^2 \mu((A_z)_\epsilon),$$

implying that z has modulus at most $1/\sqrt{2}$. □

For the proof of Theorem 5.4.2, we require the following results.

Lemma 5.4.7. *Let K and L be two compact subsets of $\mathbb{C}$. If L_ϵ intersects K_ϵ for every $\epsilon > 0$, then L and K intersect as well.*

Proof. Let $\epsilon > 0$ and suppose $L_\epsilon \cap K_\epsilon$ is nonempty. By the triangle inequality, the distance $d(K, L) = \min_{x \in K, y \in L} |x - y|$ is smaller than 2ϵ. This holds for any such ϵ, so $d(K, L) = 0$. By compactness, there are $x \in K$ and $y \in L$ such that $d(x, y) = d(L, K) = 0$, meaning that $x = y$. □

Lemma 5.4.8. *Let $L \subset \mathbb{C}$ be connected. Then L_ϵ is path-connected.*

Proof. Assume to the contrary that x and y are two points of L_ϵ lying in dinstinct path components U and V of L_ϵ. The set L_ϵ is locally path-connected by definition, which has two consequences: First, there are points x' and y' of L lying in U and V, respectively; secondly, the path components of L_ϵ are open. So $U' = U \cap L$ and $V' = V \cap L$ partition L in two open, disjoint, nonempty subsets of L, contradicting the hypothesis that L is connected. □

Proposition 5.4.9. *Let $K \subset \mathbb{C}$ be a compact and connected set such that $(K+1) \cap (K-1)$ is nonempty. Then K intersects the union $(K+1) \cup (K-1)$.*

Proof. After possibly replacing K by K_ϵ for an $\epsilon > 0$ we may assume that K is path-connected; Lemma 5.4.7 and Lemma 5.4.8 show that this does not lead to loss of generality. Since K is Hausdorff, it follows that K is arc-connected – that is, any two points in K can be connected by a path in K homeomorphic to the closed unit interval.

Since K is closed and bounded, it contains (not-necessarily unique) points a and b whose imaginary parts are minimal and maximal, respectively. Let $B = \{z \in \mathbb{C} \mid a \leq \operatorname{Im} z \leq b\}$ be the smallest horizontal strip containing K, and therefore also $K-1$ and $K+1$. Let γ be a path in K from a to b that is homeomorphic to $[0,1]$. Suppose that K does not intersect $(K+1) \cup (K-1)$. Then γ divides B into two disjunct 'half-strips' each containing one of $K+1$ and $K-1$ (this step indeed requires that the path γ is injective). So $K+1$ and $K-1$ do not intersect. □

Lemma 5.4.10. *Let X be a compact subset of the complex plane. Then $\mathbb{C} \setminus X$ has exactly one unbounded connected component. In addition, if X is also connected, then any bounded connected component of $\mathbb{C} \setminus X$ is homeomorphic to a disk.*

Proof. The second part of the lemma is a consequence of Alexander duality; see e.g. [1] for an informal explanation.

For the first part, note that X is bounded since it is compact in the complex plane. Hence there exists an $r > 0$ such that the set $A = \{z \in \mathbb{C} \mid |z| \geq r\}$ is contained in $\mathbb{C} \setminus X$. Let C be an unbounded component of $\mathbb{C} \setminus X$. Then $A \cap C$ is nonempty. Since both A and C are connected, there union must thus also be connected by Lemma 1.5.1. Since C is a connected component, it is not contained in any bigger set that is also connected. Hence $C = C \cup A$, meaning that any other connected component of $\mathbb{C} \setminus X$ must be contained in $\{z \in \mathbb{C} \mid |z| < r\}$. □

Lemma 5.4.11. *If A_z is connected then it is locally connected.*

Proof. Suppose A_z is connected. Let $x \in A_z$ and $\epsilon > 0$. Since A_z is compact, it is bounded, so there is a maximal distance t between points in A_z. Let $N > 0$ such that $|z^N| t < \epsilon$. Let $f = s_0 + s_1 X + \cdots \in L^\star$ be a power series such that $f(z) = x$. Then the set $s_0 + s_1 z + \cdots + s_{N-1} z^{N-1} + z^N A_z$ is a connected neighborhood of x of diameter smaller than ϵ. □

Unfortunately, we were not able to prove one crucial claim in the proof of Theorem 5.4.2, the truth of which we believe is implicitly asserted in [10, Prop. 2] and in [14, Prop. 4.1.3], whose proofs we follow here. It is needed in the proof of Theorem 5.4.2. That means that the truth of this theorem remains conditional in this thesis. This claim is pointed out in the course of the proof.

Conditional proof of Theorem 5.4.2. Assume to the contrary that $z^2 \in M_{\{0,\pm 1\}} \cap \mathbb{D}$ but $z \notin M_{\{\pm 1\}} \cap \mathbb{D}$. Then A_{z^2} is connected by Lemma 5.4.6 but $0 \notin A_z$ by Lemma 5.4.5. Notice that $A_z = A_{z^2} + zA_{z^2}$ by definition. So $0 \notin A_{z^2}$, otherwise $0 = 0 + z \cdot 0 \in A_z$.

It suffices to show that A_{z^2} does not intersect $K = z^2 A_{z^2}$. Indeed, since A_{z^2} is compact and connected, so too is K. But $A_{z^2} = (K+1) \cup (K-1)$, and $K+1 = A^+_{z^2}$ intersects $K - 1 = A^-_{z^2}$ by Lemma 5.4.6, which contradicts Proposition 5.4.9.

We first show that the attractor A_{z^2} does not intersect zA_{z^2}. Indeed, supposing that it would, then there are $p, p' \in A_{z^2}$ such that $p = zp'$. So $-p$ lies in A_{z^2} as well, since $A_{z^2} = -A_{z^2}$. Hence $0 = -p + p = -p + zp' \in A_{z^2} + zA_{z^2} = A_z$.

Now write C for the connected component of $\mathbb{C} \setminus A_{z^2}$ containing 0. Since A_{z^2} is compact and connected, by Lemma 5.4.10, we know that C is either bounded and homeomorphic to a disk, or unbounded and homeomorphic to a punctured disk (with the puncture corresponding to the 'point at infinity'). We want to show that C is bounded. Suppose not. Write φ for the homeomorphism mapping C to the punctured disk. Consider a straight line segment R starting from $\varphi(0)$ in the direction of the puncture, finishing at a distance ϵ from it. Then $\varphi^{-1}(R)$ is a path from 0 to a complex number of large modulus. Hence $L = \varphi^{-1}(R) \cup -\varphi^{-1}(R)$ is a path in C that divides the plane in half in the limit $\epsilon \to 0$. Since both L and A_{z^2} are point-symmetric in 0, the path L necessarily divides A_{z^2} in two parts. But this contradicts the connectedness of A_{z^2}.

Hence the connected component C is bounded. It must contain zA_{z^2}: indeed, the straight line segment from 0 to an element of zA_{z^2} of minimal modulus (which exists by compactness) cannot cross A_{z^2}, as then A_{z^2} would contain an element of modulus smaller than the minimal modulus attained in the set zA_{z^2}. So zA_{z^2} and 0 lie in the same path-component of $\mathbb{C} \setminus A_{z^2}$, and thus in the same connected component.

By Lemma 5.4.10, the interior of C is simply connected, so that Riemann's mapping theorem implies that it maps onto the open unit disk via some biholomorphism ψ. Since C is closed and A_{z^2} is locally connected, the map ψ extends continuously and bijectively to the boundary of C by the Carathéodory-Torhorst theorem. Hence the boundary of C is a non-self-intersecting continuous loop γ whose exterior contains A_{z^2} and whose interior contains zA_{z^2} by the Jordan curve theorem. Similarly, the loop $z\gamma$ has an exterior containing zA_{z^2} and an interior containing $z^2 A_{z^2}$.

Claim: The loops γ and $z\gamma$ do not intersect.

Assuming the claim, $z\gamma$ must be contained in the interior of the region bounded by γ. In particular, the exterior of $z\gamma$ contains A_{z^2}, and thus the intersection of A_{z^2} with $z^2 A_{z^2}$ is empty. □

It remains to show that the loops γ and $z\gamma$ indeed do not intersect.

APPENDIX A

Computational results

This appendix provides an overview of computational results pertaining to Littlewood polynomials. Here, we adopt a slightly different definition of Littlewood polynomials: we assume all Littlewood polynomials to be of the form $X^n + X^{n-1} \pm X^{n-2} \pm \cdots \pm 1$. That is, we require both leading and second coefficient to be equal to 1. The transformation $f(X) \mapsto (-1)^{\deg f} f(-X)$ retrieves all other Littlewood polynomials, and the properties under consideration in the tables below are invariant under this transformation; this halves the required computations. All computations were performed on a consumer-grade laptop using `Sage` and `Magma` – see the code in Appendix B.

First some notation. Denote by IRP_n and ISP_n the subsets of SI_n containing the reciprocal polynomials and skew-reciprocal polynomials, respectively; by IRNP_n we denote the set of irreducible reciprocal polynomials of degree n with positive, but nonsquare discriminant; by IrP_n the set of irreducible reciprocal polynomials; by IrRN_n the set of irreducible reciprocal polynomials with negative discriminant. See Table A.2 for an overview of the sizes of these sets for small n. We remark that all odd degree Littlewood polynomials with square discriminant and of degree at most 25 have a multiple (cyclotomic) factor or a root in $\{\pm 1\}$.

Lastly, we provide an overview of the Galois groups of irreducible Littlewood polynomials of small degree. The main results are the following:

- If f is not balanced and $n \leq 16$, then $f \in \mathrm{Ir}_n$ has as Galois group the full symmetric group, unless $n = 12$ or 14 and f is one of six exceptions.
- If f is an irreducible, balanced polynomial of even degree $2n$ between 4 and 24 (see Table A.1), the Galois group of f is
  (1) the cyclic group C_{2n} if $f = p_n$;
  (2) the wreath product $C_2 \wr S_n$ if $\Delta(f)$ is not a square and $f \neq p_n$;
  (3) the Coxeter group $\mathcal{D}_n$ if $\Delta(f)$ is a square,

  unless $n = 8$, 12, 16 or 18 and f is one of eight exceptions. (There is only one group of order 2, hence the exclusion of degree-2 polynomials.)

That means a total of 14 exceptions to 62214 cases in total (0.02%). In particular, any irreducible Littlewood polynomial of odd degree ≤ 15 has maximal Galois group.

Table A.1: Number of occurrences of the Galois groups of irreducible balanced Littlewood polynomials of low degree $2n$. All polynomials in the last two columns have square discriminant, except when marked with a dagger; and if a polynomial has square discriminant, it is in the last two columns.

$2n$	C_{2n}	$C_2 \wr S_n$	$\mathcal{D}_n$	Other
4	1	3	0	0
6	1	2	3	0
8	0	4	4	2
10	1	31	0	0
12	1	61	0	$2^\dagger$
14	0	37	44	0
16	1	123	120	3
18	1	510	0	$1^\dagger$
20	0	807	0	0
22	1	1176	866	0
24	0	2183	1675	0

Table A.2: Sizes of the sets under consideration for small n. **Note that Littlewood polynomials are here assumed to have leading and second coefficient both equal to** 1. See the introduction to Appendix A for the definitions of the various sets. The empty entries are undefined, whereas the entries labelled 'x' are defined, but have not been calculated.

n	$\lvert\mathscr{F}_n\rvert = 2^{n-1}$	$\lvert \mathrm{Ir}_n \rvert$	$\lvert \mathrm{Ir}_n \cap \mathcal{R}_n \rvert$	$\lvert \mathrm{Ir}_n \cap \mathcal{S}_n \rvert$	$\lvert \mathrm{Sq}_n \rvert$	$\lvert \mathrm{SI}_n \rvert$	$\lvert \mathrm{SI}_n \cap \mathcal{R}_n \rvert$	$\lvert \mathrm{SI}_n \cap \mathcal{S}_n \rvert$
1	1	1			1	1		
2	2	2	1	1	0	0	0	0
3	4	2			1	0		
4	8	8	2	2	0	0	0	0
5	16	6			3	0		
6	32	24	4	2	7	3	2	1
7	64	32			6	0		
8	128	96	4	6	10	6	3	3
9	256	130			13	0		
10	512	512	16	16	0	0	0	0
11	1024	564			42	0		
12	2048	2048	32	32	0	0	0	0
13	4096	2240			44	0		
14	8192	6655	29	52	68	44	14	30
15	16384	10310			320	0		
16	32768	32717	121	126	128	123	61	62
17	65536	38188			247	0		
18	131072	131072	256	256	0	0	0	0
19	262144	179266			2923	0		
20	524288	466067	313	494	0	0	0	0
21	1048576	695860			683	0		
22	2097152	2097045	1024	1019	871	866	395	471
23	4194304	2723628			32311	0		
24	8388608	8285370	1818	2040	1772	1675	793	882
25	2^{24}	x			2700	0		
26	2^{25}	x	2729	4056	0	0	0	0
27	2^{26}	x			x	0		
28	2^{27}	x	8192	8192	0	0	0	0
29	2^{28}	x			x	0		
30	2^{29}	x	16179	16332	x	12241	5599	6642
31	2^{30}	x			x	0		
32	2^{31}	x	23425	32682	x	21232	8468	12764
33	2^{32}	x			x	0		
34	2^{33}	x	58458	65498	0	0	0	0
38	2^{37}	x	194972	262008	x	x	60025	97413
40	2^{39}	x	x	x	x	x	176790	189185
46	2^{45}	x	x	x	x	x	1237181	1449198
48	2^{47}	x	x	x	x	x	2585207	x

APPENDIX B

Sage and Magma scripts

This appendix includes a few scripts that can be used to numerically study the various objects under consideration in this thesis.

B.1 A basic Sage script

We start with a minimal script in Sage that can reproduce the sets of polynomials studied in this thesis. Just as in Appendix A, we assume all Littlewood polynomials to be of the form $X^n + X^{n-1} \pm X^{n-2} \pm \cdots \pm 1$. We also show how the numerical results were established and handled, and how the picture on the second page of this thesis was obtained. A copy of this script is available online at https://github.com/davidhokken/thesis-public/.

```
# !/usr/bin/env python
# -*- coding: utf-8 -*-
#
# Author: David Hokken
# Date:   1/7/2021
#


import itertools
import numpy as np
import matplotlib.pyplot as plt

dr = '/path/to/folder' # path to wherever any output should be saved


#####################################
############# FUNCTIONS #############
#####################################


################################
```

```
#### Littlewood polynomials ####
################################

R.<x> = PolynomialRing(QQ)

def F(n):
    '''Returns a list with all Littlewood polynomials of degree n'''
    return [x^n+x^(n-1)+R(v) for v in (itertools.product((1,-1),repeat=n-1))]

def get_ir(lst):
    '''Returns the irreducibles from a list of polynomials'''
    return [f for f in lst if f.is_irreducible()]

def get_sq(lst):
    '''Returns the polynomials with square discriminant from a
    list of polynomials'''
    return [f for f in lst if f.discriminant().is_square()]

def get_sqir(lst):
    '''Returns the irreducibles with square discriminant from a
    list of polynomials.
    NOTE: get_ir(get_sq(...)) is much faster than get_sq(get_ir(...))'''
    return get_ir(get_sq(lst))


#################################
####### (Skew-)reciprocals ######
#################################

def is_reciprocal(f):
    '''Checks if a given polynomial is reciprocal'''
    if len(f.list()) % 2 == 0:
        return 'This is not a reciprocal polynomial'
    else:
        return f.list() == list(reversed(f.list()))

def is_skew(f):
    '''Check if a given polynomial is skew-reciprocal'''
    deg = f.degree()
    T = var('T')
    if deg % 2 != 0:
        return 'This is not a skew-reciprocal polynomial'
    elif deg % 4 == 2:
        skew_f = -T^deg*f(-1/T)
    elif deg % 4 == 0:
        skew_f = T^deg*f(-1/T)

    if skew_f == f(T):
```

```
70          return True
71      else:
72          return False
73
74  def f_rev(f):
75      '''Given a polynomial f, returns the reversal f_rev of f'''
76      T = var('T')
77      deg = f.degree()
78      v = ((T^deg*f(1/T)).expand()).list()
79      return R(v)
80
81  def f_srev(f):
82      '''Given a polynomial f, returns the skew-reversal f_srev of f'''
83      T = var('T')
84      deg = f.degree()
85      v = ((-1)^(deg*(deg-1)/2)*(T^deg*f(-1/T)).expand()).list()
86      return R(v)
87
88  def f_Q(f):
89      '''Given a polynomial f of degree n in the variable y=x+x^{-1},
90      returns the reciprocal polynomial f^Q of degree 2n in the variable x
91      such that f^Q(x) = x^n f_RQ(x+x^{-1})'''
92      T = var('T')
93      degree = f.degree()
94      v = ((T^degree*f(T+1/T)).expand()).list()
95      return R(v)
96
97  def f_S(f):
98      '''Given a polynomial f of degree n in the variable y=x+x^{-1},
99      returns the skew-reciprocal polynomial f^S of degree 2n in the variable x
100     such that f^S(x) = x^n f_RS(x-x^{-1})'''
101     T = var('T')
102     deg = f.degree()
103     v = ((T^deg*f(T-1/T)).expand()).list()
104     return R(v)
105
106 def Rec(n):
107     '''Returns a list of all reciprocal Littlewood polynomials of degree 2n'''
108     L = list(itertools.product((1,-1),repeat=n-1))
109     Rlist = []
110     for i in range(len(L)):
111         L[i] = list(L[i])
112         L[i].extend([1,1])
113         L[i] = tuple(L[i])
114         Rlist.append(list(reversed(L[i]))[:-1])
115         Rlist[i].extend(list(L[i]))
116     Rlist = [R(v) for v in Rlist]
117     return Rlist
```

```
118
119 def SRec(n):
120     '''Returns a list of all skew-reciprocal Littlewood polynomials of degree 2n'''
121     L = list(itertools.product((1,-1),repeat=n-1))
122     SRlist = []
123     for i in range(len(L)):
124         lst = list(L[i])
125         M = lst[::-1]
126         M.extend([1,1])
127         N = [-1*x for x in M[1::2]]
128         M = M[::2]
129         M = [x for y in zip(M, N) for x in y]
130         if n % 2 == 0:
131             M.append(1)
132         lst.extend(M[1:])
133         lst[0:0]=[1,1]
134         lst = tuple(reversed(lst))
135         SRlist.append(lst)
136     SRlist = [R(v) for v in SRlist]
137     return SRlist
138
139 def t(l, k):
140     '''helper function for f_RQ and f_RS (see below)'''
141     return k/(k-l) * binomial(k-l, l)
142
143 def f_RQ(f):
144     '''Given a reciprocal polynomial f of degree 2n in the variable x,
145     returns the trace polynomial f_R of degree n in the  variable y = x+x^{-1}
146     such that f(x) = x^n f_R(y)'''
147     if not is_reciprocal(f):
148         return "This is not a reciprocal"
149     else:
150         flist = f.list()[:(len(f.list())+1)/2]
151         deg = len(flist)-1
152         alist = flist[:]
153         for i in range(deg+1):
154             for l in range(1, int(math.floor((i)/2)+1)):
155                 alist[i] += flist[i-2*l]*(-1)**l*t(l, deg-i+2*l)
156         return S(list(reversed(alist)))
157
158 def f_RS(f):
159     '''Given a skew-reciprocal polynomial f of degree 2n in the variable x,
160     returns the trace polynomial f_RS of degree n in the  variable y = x-x^{-1}
161     such that f(x) = x^n f_RS(y)'''
162     if not is_skew(f):
163         return "This is not a skew-reciprocal"
164     else:
165         flist = f.list()[(len(f.list())-1)/2:]
```

```
        deg = len(flist)-1
        alist = flist[:]
        for i in range(deg+1):
            for l in range(1, 1+int(math.floor((deg-i)/2))):
                alist[i] += flist[i+2*l]*t(l, i+2*l)
        g = S(list(alist))
        return g


############################
######### pictures #########
############################

def picture(n):
    '''Returns a picture of all roots of all Littlewood polynomials of degree
    < n'''
    X = []
    Y = []
    for i in range(1, n):
        for f in F(n):
            roots = f.roots(ring=CDF)
            for r in roots:
                X.append(r[0].real())
                Y.append(r[0].imag())
                X.append(-(r[0].real()))
                Y.append((r[0].imag()))

    fig = plt.figure(figsize=(21, 13))
    ax = fig.add_subplot(1,1,1)
    plt.scatter(X, Y, s=0.02, color='red')
    plt.axis('equal')
    plt.axis('off')
    plt.show()
```

B.2 Determining and visualizing SI_n in Sage

Based on the script above, the set SI_n can be determined with the following command:

```
def SI(n):
        return get_sqir(F(n))
```

It takes roughly 10 seconds to determine that SI_{18} is empty. Since the cardinality of $\mathscr{F}_n$ grows exponentially, so does the computation time. However, for $n > 25$ (say) this computation can be sped up by breaking up the computation in smaller parts. The following script takes some $k < n$ and divides the set $\mathscr{F}_n$ in smaller pieces, by defining a 'head' list (consisting of the polynomials $X^n + X^{n-1} \pm X^{n-2} \pm \cdots \pm X^k$) and a 'tail' list

(consisting of the polynomials $X^{k-1} \pm X^{k-2} \pm \cdots \pm 1$) and subsequently iterating over all combinations. The found irreducible Littlewood polynomials with square discriminant, here computed in degree $n = 30$, are written to a file `SI_30.txt` in the folder `SI`, which is itself contained in the directory `dr`. For optimal computation speed, k should be chosen between, say, 11 and 14, depending on the size of n.

```
n=30
k=12

head = [x^n+x^(n-1)+x^(k)*R(v) for v in (itertools.product((1,-1),repeat=n-k-1))]
headlen = 2^(n-k-1)
tail = [R(v) for v in (itertools.product((1,-1),repeat=k))]

with open(dr+'SI/SI_30.txt', 'w+') as g:
    for i in range(headlen):
        p = head[i]
        polys = [p+f for f in tail]
        L = get_sqir(polys)
        if len(L) != 0:
            g.write(str(L)+"\n")
        if i % 10000 == 0:
            print(i)
```

Using this script, it took 2 days to determine that SI_{31} is empty, and 9.5 days to determine that SI_{33} is empty.

The following script shows how the picture of the set of roots of irreducible Littlewood polynomials with square discriminant of degree at most 30, shown on the second page of this thesis, was obtained.

```
def get_polys_from_file(path):
    '''Helper function to read polynomials from a text file'''
    with open(path, 'r') as f:
        g = f.readlines()
        polys = []
        for i in range(len(g)):
            pol = R(g[i])
            polys.append(pol)
    return polys

Xrec = []
Yrec = []
Xskew = []
Yskew = []

for n in [6, 8, 14, 16, 22, 24, 30]:
    polys = get_polys_from_file(dr+'SIn/SI_{}.txt'.format(n))
```

```
    for f in polys:
        if is_reciprocal(f):
            roots = f.roots(ring=CDF)
            for r in roots:
                Xrec.append(r[0].real())
                Yrec.append(r[0].imag())
                Xrec.append(-(r[0].real())) # root of f(-X)
                Yrec.append(r[0].imag()) # root of f(-X)
        else:
            roots = f.roots(ring=CDF)
            for r in roots:
                Xskew.append(r[0].real())
                Yskew.append(r[0].imag())
                Xskew.append(-(r[0].real())) # root of f(-X)
                Yskew.append(r[0].imag()) # root of f(-X)


fig = plt.figure(figsize=(21, 13))
ax = fig.add_subplot(1,1,1)
plt.scatter(Xskew, Yskew, s=0.02, color='blue')
plt.scatter(Xrec, Yrec, s=0.02, color='red')
plt.axis('equal')
plt.axis('off')
plt.show()
# fig.savefig("littleroots.png", bbox_inches='tight',
# pad_inches=0, transparent=True, dpi=220) # Save figure to png
```

B.3 Determining Galois groups in Magma

Lastly, the following is a simple script in Magma to determine the Galois group of a list L of k polynomials over $\mathbb{Q}$. All Magma computations were done using the free online calculator at http://magma.maths.usyd.edu.au/calc/.

```
P< x >:=PolynomialAlgebra(Rationals());
L := [**];

for i in [1 .. #L] do
    f := L[i];
    G:=GaloisGroup(f);
    print f, G;
end for;
```

Arnaut Daniel's sestina

Lo ferm voler qu'el cor m'intra

Lo ferm voler qu'el cor m'intra
no·m pot ges becx escoyssendre ni ongla
de lauzengier qui pert per mal dir s'arma;
e car po l'aus batr'ab ram ni ab veria,
sivals a frau, lai on non aurai oncle,
iauzirai ioy, en vergier o dins cambra.

Quan mi sove de la cambra
on a mon dan sai que nulhs hom non intra
ans me son tug plus que fraire ni oncle
non ai membre no·m fremisca, neis l'ongla,
aissi cum fai l'efans denan la veria:
tal paor ai no·l sia trop de l'arma.

Del cor l'i fos, non de l'arma,
e cossentis m'a celat dins sa cambra!
que plus mi nafra·l cor que colps de veria
qu'ar lo sieus sers lai on ilh es non intra:
de lieys serai aissi cum carns et ongla
e non creirai castic d'amic ni d'oncle.

Anc la seror de mon oncle
non amiei plus ni tan, per aquest'arma,
qu'aitan vezis cum es lo detz de l'ongla,
s'a lieis plagues, volgr'esser de sa cambra:
de me pot far l'amors qu'ins el cor m'intra
mielhs a son vol qu'om fortz de frevol veria.

Pus floric la seca veria
ni d'en Adam foron nebot ni oncle
tan fin amors cum selha qu'el cor m'intra
non cug qu'anc fos anc en cors ni es en arma.
on qu'ilh estey, fors en plass' o dins cambra,
mos cors no·s part de lieis tan cum ten l'ongla.

Qu'aissi s'enpren e s'enongla
mos cors en lieys cum l'escors' en la veria,
qu'ilh m'es de ioy tors e palais e cambra,
e non am tan fraire, paren ni oncle,
qu'en Paradis n'aura doble ioi m'arma,
si ia nulhs hom per ben amar lai intra.

Arnaut tramet son cantar d'ongl'e d'oncle
ab grat de lieys, que de sa veri'a l'arma,
son Dezirat, qu'a pretz dins cambra intra.

Arnaut Daniel (fl. 1180–1200)

The firm wishing that gets ingress

The firm wishing that gets ingress
To my heart fears no cad's beak or nail-tip
Of cad who by false speech doth lose his soul's hope,
And if I dare assail him not with bough or osier
On quiet I, where one admits no uncle,
Will get my joy in garden or in bower.

When I remember the bower
Where to my spite I know that no man gets ingress,
But do no more than may brothers and uncles,
I tremble all length, all save my nail-tips,
As does a child before a switch of osier,
So fear I lest I come not near my soul's hope.

Of body 'twas not of soul's hope
That consenting she hid me in her bower.
Now it hurts my heart worse than strokes of osiers
That where she now is, her slave gets no ingress.
I cling mam to her as is the flesh to the nail-tip
And take warning of neither friend nor uncle.

Ne'er love I sister of uncle
As I love her I love, by my soul's hope.
Close cling I as doth the finger to nail-tip
And would be, and it please her, in her bower;
Love that in my heart gets ingress
Can shake me, as strong man not an osier.

Since flower sprang on dry osier,
Since Adam began this line of nephews and uncles,
Such fine love as to my heart hath ingress
Was not to my belief in body or soul's hope.
If she be in piazza nor bower,
My heart leave not by a nail-tip.

The heart roots and clings like the nail-tip
Or as the bark clings that clings to the osier,
For she is joy's palace, she is joy's bower,
Nor love I so father, nor kinsman, nor kind uncle.
Double joy in Paradise, by my soul's hope,
Shall I have if ere true love there win ingress.

Arnaut sends the song of nail and uncle
With thanks to her the soul of his osier,
Son Dezirat, who to some purpose hath ingress in bower.

English translation by Ezra Pound (1885–1972)
Original and English version taken from [47]

Bibliography

[1] Anonymous. *Answer to problem "Connected closed subset in a plane"*. Answer posted by user "Jesus RS", question posted by user "stephen" on Mathematics Stack Exchange, https://math.stackexchange.com/questions/1219757/. 2015.

[2] Peter R. J. Asveld. *Permuting operations on strings and the distribution of their prime numbers*. Discrete Appl. Math. **161** (2013), 1868–1881.

[3] Peter R. J. Asveld. *Queneau Numbers—Recent Results and a Bibliography*. CTIT Technical Report Series (2013).

[4] Johan Baez, Dan Christensen, and Sam Derbyshire (with lots of help from Greg Egan). *The Beauty of Roots*. Slides from a presentation, http://math.ucr.edu/home/baez/roots/beauty.pdf. 2011.

[5] Simon Baker and Han Yu. *Root sets of polynomials and power series with finite choices of coefficients*. Comput. Methods Funct. Theory **18** (2018), 89–97.

[6] Lior Bary-Soroker, Dimitris Koukoulopoulos, and Gady Kozma. *Irreducibility of random polynomials: general measures*. Preprint arXiv:2007.14567 (2020).

[7] Lior Bary-Soroker and Gady Kozma. *Irreducible polynomials of bounded height*. Duke Math. J. **169** (2020), 579–598.

[8] Peter Borwein, Edward Dobrowolski, and Michael J. Mossinghoff. *Lehmer's problem for polynomials with odd coefficients*. Ann. of Math. (2) **166** (2007), 347–366.

[9] Thierry Bousch. *Connexité locale et par chemins hölderiens pour les systèmes itérés de fonctions*. Unpublished, available at https://www.imo.universite-paris-saclay.fr/~bousch/preprints/clh_ifs.pdf. 1993.

[10] Thierry Bousch. *Paires de similitudes*. Unpublished, available at https://www.imo.universite-paris-saclay.fr/~bousch/preprints/paires_sim.pdf. 1988.

[11] Emmanuel Breuillard and Péter P. Varjú. *Irreducibility of random polynomials of large degree*. Acta Math. **223** (2019), 195–249.

[12] François Brunault and Wadim Zudilin. *Many Variations of Mahler Measures: A Lasting Symphony*. Vol. 28. Cambridge University Press, 2020.

[13] Antonio Cafure and Eda Cesaratto. *Irreducibility criteria for reciprocal polynomials and applications*. Amer. Math. Monthly **124** (2017), 37–53.

[14] Danny Calegari, Sarah Koch, and Alden Walker. *Roots, Schottky semigroups, and a proof of Bandt's conjecture*. Ergodic Theory Dynam. Systems **37** (2017), 2487–2555.

[15] Keith Conrad. *Cyclotomic extensions*. Unpublished note, available at https://kconrad.math.uconn.edu/blurbs/galoistheory/cyclotomic.pdf (2015).

[16] Keith Conrad. *Irreducibility of x^n-x-1*. Unpublished note, available at https://kconrad.math.uconn.edu/blurbs/ringtheory/irredselmerpoly.pdf (201X).

[17] Keith Conrad. *Splitting of short exact sequences for groups*. Unpublished note, available at https://kconrad.math.uconn.edu/blurbs/grouptheory/splittinggp.pdf (201X).

[18] Keith Conrad. *The contraction mapping theorem*. Unpublished note, available at https://kconrad.math.uconn.edu/blurbs/analysis/contraction.pdf (2014).

[19] Jean-Guillaume Dumas. *Caractérisation des quenines et leur représentation spirale*. Math. Sci. Hum. Math. Soc. Sci. (2008), 9–23 (2009).

[20] David S. Dummit and Richard M. Foote. *Abstract algebra*. Third. John Wiley & Sons, Inc., Hoboken, NJ, 2004, xii+932.

[21] Felix Hausdorff. *Felix Hausdorff—gesammelte Werke. Band III*. Mengenlehre (1927, 1935): deskriptive Mengenlehre und Topologie. [Set theory (1927, 1935): descriptive set theory and topology], Edited by U. Felgner, H. Herrlich, M. Hušek, V. Kanovei, P. Koepke, G. Preuß, W. Purkert and E. Scholz. Springer-Verlag, Berlin, 2008, xxii+1005.

[22] Alexander Heyes. *Answer to problem "Understanding a proof about nested nonempty connected compact subsets"*. Posted by user "Fraïssé" on StackExchange, https://math.stackexchange.com/questions/1631126/. 2016.

[23] The OEIS Foundation Inc. *The On-Line Encyclopedia of Integer Sequences*. http://oeis.org. 1996–.

[24] Serge Lang. *Complex analysis*. Fourth. Vol. 103. Graduate Texts in Mathematics. Springer-Verlag, New York, 1999, xiv+485.

[25] Derrick H. Lehmer. *Factorization of certain cyclotomic functions*. Ann. of Math. (2) **34** (1933), 461–479.

[26] Rudolf Lidl and Harald Niederreiter. *Finite fields*. Second. Vol. 20. Encyclopedia of Mathematics and its Applications. With a foreword by P. M. Cohn. Cambridge University Press, Cambridge, 1997, xiv+755.

[27] John E. Littlewood. *On polynomials $\sum^n \pm z^m$, $\sum^n e^{\alpha_m i} z^m$, $z = e^{\theta_i}$*. J. London Math. Soc. **41** (1966), 367–376.

[28] John E. Littlewood. *On the mean values of certain trigonometric polynomials*. J. London Math. Soc. **36** (1961), 307–334.

[29] John E. Littlewood. *On the mean values of certain trigonometric polynomials. II*. Illinois J. Math. **6** (1962), 1–39.

[30] Wilhelm Ljunggren. *On the irreducibility of certain trinomials and quadrinomials*. Math. Scand. **8** (1960), 65–70.

[31] Kurt Mahler. *An application of Jensen's formula to polynomials*. Mathematika **7** (1960), 98–100.

[32] Kurt Mahler. *On some inequalities for polynomials in several variables*. J. London Math. Soc. **37** (1962), 341–344.

[33] Robert S. Maier. *The 192 solutions of the Heun equation*. Math. Comp. **76** (2007), 811–843.

[34] Paulo A. Martin. *The Galois group of* $x^n - x^{n-1} - \cdots - x - 1$. J. Pure Appl. Algebra **190** (2004), 213–223.

[35] Helmut Meyn. *On the construction of irreducible self-reciprocal polynomials over finite fields*. Appl. Algebra Engrg. Comm. Comput. **1** (1990), 43–53.

[36] W. H. Mills. *The factorization of certain quadrinomials*. Math. Scand. **57** (1985), 44–50.

[37] James S. Milne. *Algebraic Number Theory (v3.08)*. Available at www.jmilne.org/math/. 2020.

[38] Jürgen Neukirch. *Algebraic Number Theory*. Vol. 322. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder. Springer-Verlag, Berlin, 1999, xviii+571.

[39] Andrew Odlyzko and Bjorn Poonen. *Zeros of polynomials with* $0, 1$ *coefficients*. Enseign. Math. (2) **39** (1993), 317–348.

[40] Hiroyuki Osada. *The Galois groups of the polynomials* $X^n + aX^l + b$. J. Number Theory **25** (1987), 230–238.

[41] Bjorn Poonen. *Answer to problem "Irreducible polynomials with constrained coefficients"*. Posted by user "some guy on the street" on Math Overflow, https://mathoverflow.net/questions/7969/. 2009.

[42] Griffith Baley Price. *On the completeness of a certain metric space with an application to Blaschke's selection theorem*. Bull. Amer. Math. Soc. **46** (1940), 278–280.

[43] Michael P. Saclolo. *How a medieval troubadour became a mathematical figure*. Notices Amer. Math. Soc. **58** (2011), 682–687.

[44] Ernst S. Selmer. *On the irreducibility of certain trinomials*. Math. Scand. **4** (1956), 287–302.

[45] Jean-Pierre Serre. *Local fields*. Vol. 67. Graduate Texts in Mathematics. Translated from the French by Marvin Jay Greenberg. Springer-Verlag, New York-Berlin, 1979, viii+241.

[46] Chris J. Smyth. *On the product of the conjugates outside the unit circle of an algebraic integer*. Bull. London Math. Soc. **3** (1971), 169–175.

[47] Andrew Taylor and Roxana Preda. *The Cantos Project*. A digital research environment dedicated to The Cantos of Ezra Pound. United Kingdom, 2016.

[48] Paulo Viana and Paula Murgel Veloso. *Galois theory of reciprocal polynomials*. Amer. Math. Monthly **109** (2002), 466–471.

[49] Bartel L. van der Waerden. *Die Seltenheit der Gleichungen mit Affekt*. Math. Ann. **109** (1934), 13–16.

[50] Bartel L. van der Waerden. *Die Seltenheit der reduziblen Gleichungen und der Gleichungen mit Affekt*. Monatsh. Math. Phys. **43** (1936), 133–147.

[51] Bartel L. van der Waerden. *Modern Algebra. Vol. I*. Translated from the second revised German edition by Fred Blum, With revisions and additions by the author. Frederick Ungar Publishing Co., New York, N. Y., 1949, xii+264.

[52] Lawrence C. Washington. *Introduction to cyclotomic fields*. Second. Vol. 83. Graduate Texts in Mathematics. Springer-Verlag, New York, 1997, xiv+487.