DYNAMICAL IRREDUCIBILITY OF PURE POLYNOMIALS OVER THE RATIONAL FIELD

by
MOHAMED OSAMA HAFEZ DARWISH MOHAMED

Submitted to the Graduate School of Engineering and Natural Sciences
in partial fulfilment of
the requirements for the degree of Master of Science

Sabancı University
July 2022

DYNAMICAL IRREDUCIBILITY OF PURE POLYNOMIALS OVER THE RATIONAL FIELD

MOHAMED OSAMA HAFEZ DARWISH MOHAMED

Mathematics, Master Thesis, JULY 2022

Thesis Supervisor: Assoc. Prof. Dr. Mohammad Sadek

Keywords: Arithmetic Dynamical systems, Dynamically Irreducible Polynomials, Eventually Stable Polynomials, Eisenstein Criterion, Dumas Criterion

Abstract

Let f be a polynomial in $\mathbb{Q}[x]$. We say that f is **dynamically irreducible** or stable over $\mathbb{Q}$ if all its iterates $f^n := \underbrace{f \circ f \circ \ldots \circ f}_{n}$ are irreducible over $\mathbb{Q}$. Generally, a polynomial is called **eventually stable** if the number of irreducible factors of any iterate f^n is bounded by some $c \in \mathbb{Z}^+$, in particular, if $c = 1$, then f is dynamically irreducible. A polynomial defined over $\mathbb{Q}$ is said to be **pure** with respect to a prime p if its Newton polygon consists of exactly one line, e.g., p^r-Eisenstein polynomials for some $r \geq 1$.

In 1985, Odoni showed that Eisenstein polynomials are dynamically irreducible over $\mathbb{Q}$. Ali extended this result to include p^r-Eisenstein polynomials for any $r \geq 1$. In this thesis, we present families of pure polynomials that are dynamically irreducible in $\mathbb{Q}[x]$. Under some conditions, we characterize certain families and develop some criteria of dynamically irreducible polynomials that possess a pure iterate. In addition, we describe some iterative techniques to produce irreducible polynomials in $\mathbb{Q}[x]$ from pure polynomials by composition.

Recently, Demark et al. investigated the eventual stability of a quadratic binomial of the form $x^2 - \frac{1}{c} \in \mathbb{Q}[x]$ for some $c \in \mathbb{Z} \backslash \{0, -1\}$. In this work, we prove that pure polynomials are eventually stable in $\mathbb{Q}[x]$. Also, we display a family of eventually stable polynomials that possess a pure iterate.

SAF POLINOMLARIN RASYONEL CISIMLERIN ÜZERINE DINAMIK İNDIRGENEMEZLIĞI

MOHAMED OSAMA HAFEZ DARWISH MOHAMED

Matematik, Yüksek Lisans Tezi, TEMMUZ 2022

Tez Danışmanı: Assoc. Prof. Mohammad Sadek

Anahtar Kelimeler: Aritmetik Dinamik Sistemler, Dinamik İndirgenemez Polinomlar, Zamanla Stabil Polinomlar, Eisenstein Kriteri, Dumas Kriteri

Özet

$f \in \mathbb{Q}[x]$ bir polinom olsun. Eğer f'in tüm iterasyonları $f^n := \underbrace{f \circ f \circ \ldots \circ f}_{n}$ indirgenemez ise f, **dinamik indirgenemez** ya da $\mathbb{Q}$ üzerine stabil denir. Genel olarak, eğer bir polinomun herhangi bir iterasyonunun f^n indirgenemez çarpanlarının sayısı bir $c \in \mathbb{Z}^+$ tamsayısı ile sınırlı ise bu polinoma **zamanla stabil** denir, özel olarak, eğer $c = 1$ ise f dinamik indirgenemezdir. f, $\mathbb{Q}$ üzerine tanımlanmış bir polinom olsun ve p asal olmak üzere eğer Newton poligonu kesin olarak bir doğru içeriyorsa bu polinoma **saf** denir. Örnek olarak p^r-Eisenstein polinomları bazı $r \geq 1$ için verilebilir.

1985'de, Odoni Eisenstein polinomlarının $\mathbb{Q}$ üzerine dinamik indirgenemez olduğunu gösterdi. Ali bu sonucu p^r-Eisenstein polinomlarının her bir $r \geq 1$ için genelleştirdi. Bu tezde, $\mathbb{Q}[x]$ de dinamik indirgenemez olan saf polinom ailelerini tanımlıyoruz. Bazı koşullar altında, belirli aileleri karakterize ediyoruz ve saf bir yinelemeye sahip dinamik olarak indirgenemez polinomların bazı kriterlerini geliştiriyoruz. Ek olarak, bileşimleri saf polinomlardan olan $\mathbb{Q}[x]$ cinsinden indirgenemez polinomlar üretmek için bazı yinelemeli teknikleri açıklıyoruz.

Yakın zamanda, Demark ve diğerleri, $x^2 - \frac{1}{c} \in \mathbb{Q}[x]$ biçimindeki ikinci dereceden bir iki terimlinin nihai kararlılığını bazı $c \in \mathbb{Z} \setminus \{0, -1\}$ için araştırdı. Bu çalışmada, saf polinomların $\mathbb{Q}[x]$ içinde zamanla stabil olduğunu kanıtlıyoruz. Ayrıca, saf yineleme-eye sahip, zamanla stabil polinomların bir ailesini gösteriyoruz.

Acknowledgment

First, I would like to express my deepest appreciation to my supervisor Assoc. Prof. Dr. Mohammad Sadek for his constant support and meticulous care to amend the smallest detail and idea in this thesis. His patience, passion for his work and dedication were always motivating me to progress as a Mathematician and a human. Dr. Mohammad, I will miss working with you!

Second, I would like to thank my jury members Ass. Prof. Dr. Ayesha Asloob Qureshi and Ass Prof. Dr. Wade Hindes for their review of my thesis.

I would like to thank my father for being the first scientist in my life, my mother for being the main source of love, support and encouragement throughout the years and my sister for the unconditional love she showered me with since our childhood. I would like to thank my nephew, Sherif, for being the blessing of our family.

I could not have undertaken this journey without Dr. Mohammad Sadek and Dr. Nermine El Sissi. Their unconditional help and support in Egypt and Turkey changed my life both academically and personally. They are part of many beautiful moments in my life. Thank you for being in my life.

I want to thank my brother Mohamed Wafik for sharing the journey in Egypt and Turkey. His help with Mathematica and comments helped me a lot in writing the thesis. Wafik, it would have been much harder without your help.

Special thanks to my dearest friends Antigona Pajaziti, Beyza Çepni and Tuğba Yesin for their irreplaceable support and help. I can not forget all the beautiful moments we shared together. Antigona, Beyza and Tuğba, I will miss each one of you.

Last but not least, I gratefully acknowledge the support provided by TÜBİTAK program 1001, project number 120F308.

“Know thyself deathless and able to know all things, all arts, sciences, the way of every life. Become higher than the highest height and lower than the lowest depth. Amass in thyself all senses of animals, fire, water, dryness and moistness. Think of thyself in all places at the same time, earth, sea, sky, not yet born, in the womb, young, old, dead, and in the after death state.”
Ancient Egyptian Proverb

Table of Contents

List of Figures

Introduction

Due to their role in Mathematics and other disciplines, irreducible polynomials have always been an attractive research topic for a long time. In *Disquisitiones Arithmeticae*, Gauss gave one of the first examples of a general irreducible polynomial over $\mathbb{Q}$, namely the cyclotomic polynomial of prime degree [6, p.467]. Consequently, irreducibility criteria started to appear; one of the earliest criterion is attributed to Theoder Schönemann in 1846. Later on, a weaker version of Schönemann's criterion appeared in an article by Gotthold Eisenstein[1] in 1850. Further generalizations were contributed by Koenigsberg (1895), Netto (1897), Bauer (1905) and Perron (1905). All these generalizations are explained by Dumas Theorem (1906) which is discussed in Chapter 4 , see [14, Section 1] for a proof. Due to applications in Cryptography, Coding Theory and other disciplines, iterative techniques to construct irreducible polynomials of arbitrary large degrees are being developed. For example, consider the polynomial $f(x) = x^2 + 2 \in \mathbb{Q}[x]$. It is irreducible over $\mathbb{Q}$ as a 2-Eisenstein polynomial. If we define the nth iterate of the polynomial f to be

$$f^n := \underbrace{f \circ f \ldots \circ f}_{n\text{-times}}, \tag{1}$$

we obtain a sequence of polynomials $f, \ldots, f^n, \ldots$. In fact, if the preceding sequence of polynomials are all irreducible in $\mathbb{Q}[x]$, then, we have an infinite tower of irreducible polynomials in $\mathbb{Q}[x]$ and an iterative technique to construct irreducible polynomials of arbitrary large degrees. In fact, for all $n \geq 1$, the polynomials f^n are 2-Eisenstein polynomials. In general, Odoni [28, lemma 2.2] showed that if a polynomial f is a P-Eisenstein polynomial over an integral domain R for some prime ideal P, then, for all $n \geq 1$, the iterates f^n are all P-Eisenstein and thus irreducible over R.

The aforementioned example motivates the following definitions. First, the construction in Equation (1) is an example of a discrete dynamical system. A discrete dynamical system is a pair (S, ϕ) such that ϕ is the self map $\phi : S \to S$ for some set S. In addition, we define the nth iterate of the map ϕ to be

$$\phi^n := \underbrace{\phi \circ \phi \ldots \circ \phi}_{n\text{-times}}$$

In our example, $S = \mathbb{Q}$, ϕ is a polynomial in $\mathbb{Q}[x]$ and $\phi^n(x)$ is the n-fold self-composition of the polynomial ϕ for $n \geq 0$ assuming $\phi^0(x) = x$ as in Equation 1. Second, if all the iterates are irreducible over some field K, in other words, f^n

[1] Some authors call this criterion "Schönemann-Eisenstein" criterion instead as Theodor Schönemann published a more general criterion four years before Gotthold Eisenstein. For a historical and mathematical analysis of this dispute, see [10].

is irreducible over K for all $n \geq 1$, we say f is dynamically irreducible or stable over K. Odoni [28] was the first to establish the concept of dynamical irreducibility (the credit of the term *stable* is attributed to him). In addition to his result about Eisenstein polynomials, he presented the first nontrivial example of a dynamically irreducible polynomial over $\mathbb{Q}$; namely the polynomial $x^2 - x + 1$ (refer to [29, Proposition 4.1]). In 1992, Stoll [31] produced a dynamical irreducibility criteria for quadratic polynomials in $\mathbb{Q}[x]$ of the form $f(x) = x^2 + a$. In fact, Stoll associated the sequence $c_1 = -a$ and $c_{n+1} = {c_n}^2 + a = f^{n+1}(0)$ for all $n \geq 2$ to the iterations of the previous quadratic binomial. He proved that if this sequence has no squares in $\mathbb{Z}$, then, f is dynamically irreducible (refer to [31, Corollary 1.3]). Jones [23] extended this result to any quadratic polynomial over a field K with characteristic different from 2 (see Proposition 1.6). Also, Danielson and Fein [11] extended Stoll's result to produce a dynamical irreducibility criterion for any polynomial in the form $x^n - b$ over some specific rings (see Proposition 1.8). We will introduce new dynamical irreducibility criteria in Chapter 3 and Chapter 4. For example, in one criterion (see Corollary 3.14), we deduce dynamical irreducibility from the 2-adic valuations of coefficients of a polynomial in $\mathbb{Z}[x]$ of the form $x^{2^m} + 1 \pmod 2$.

Since there are different types of irreducible polynomials and many irreducibility tests, characterizing all irreducible polynomials is a hard question. Yet, in 1793 Schubert provided the first algorithm to factorize a polynomial in finitely many steps and thus check irreducibility. Later on, Kronecker [26] in 1882 rediscovered Schubert's algorithm and extended it for any algebraic extension of $\mathbb{Q}$. Another important algorithm was devised by Berlekamp in 1967. He was able to factorize a polynomial of degree n and r irreducible factors over $\mathbb{Z}_p$ for some prime p with a complexity of $\mathcal{O}(n^3 + prn^2)$. In 1969, Zassenhaus proposed the idea of using Hensel's lemma in factorization algorithms over $\mathbb{Z}$. He presented an algorithm to lift the polynomial $f(x) \in \mathbb{Z}[x]$ from $f(x) \pmod p$ to $f(x) \pmod{p^t}$ in just t iterations. Zassenhaus's idea is used to combine factorization algorithms over finite and rational fields (for more details, check [25]). Finally, one of the most important algorithms was discovered in 1982 by Arjen **L**enstra, Hendrik **L**enstra and **L**ászló Lovász. The LLL Algorithm was one of the first algorithms with polynomial complexity to factorize polynomials in $\mathbb{Z}[x]$. Its complexity is

$$\mathcal{O}\left(d^{12} + d^9 (\log h)^3\right)$$

for a primitive polynomial $f(x) = a_d x^d + \ldots + a_0$ in $\mathbb{Z}[x]$ such that $h = \sqrt{{a_d}^2 + \ldots + {a_0}^2}$.

In general, not all irreducible polynomials are dynamically irreducible; consider the polynomial

$$f(x) = x^2 - \frac{4}{3}.$$

It is irreducible over $\mathbb{Q}$, but,

$$f^2(x) = \left(x^2 - 2x + \frac{2}{3}\right)\left(x^2 + 2x + \frac{2}{3}\right)$$

is reducible over $\mathbb{Q}$ [9, Example 2.2]. Inspired by the previous example, one speculates that it might be sufficient to check the first few iterations to test a polynomial for dynamical irreducibility. However, In [19, Section 3], Illig et al. produced families of polynomials whose first two iterates are irreducible but the third is reducible. We also present another example of a polynomial f such that $f, \ldots, f^5$ are irreducible but f^6 is reducible, check Example 1.14. Since there is no known characterization of irreducible polynomials, there is also no known characterization of dynamically irreducible polynomials. In his treatise about Irreducibility criteria, Dorwart [14] classified irreducible polynomials into three types: criteria depending on the divisibility of coefficients, criteria depending on the comparative sizes of the coefficients and criteria depending on integer evaluations of a polynomial. The Eisenstein criterion is the most famous example of the first *type* as it depends on the divisibility of the coefficients by some *prime.* The p^r-Eisenstein criterion is another prime type criterion. Ali [2] proved that p^r-Eisenstein polynomials for some prime p and $r \geq 1$ are dynamically irreducible in $\mathbb{Q}[x]$. We generalize this result in Chapter 4 and prove that p^r-Dumas polynomials are dynamically irreducible, see Corollary 4.17.

In practice, we do not always apply an irreducibility criterion to show a polynomial is irreducible. Consider the following family of irreducible polynomials.

$$f(x) = x^{p^m} + px + 1 \text{ where } p \text{ is an odd prime and } m \geq 1.$$

Note that $f(x-1)$ is p-Eisenstein and thus f is irreducible. We shall show that the preceding family is also dynamically irreducible, see Example 3.27. Dynamically, Bush, Hindes and Looper [7] constructed families of dynamically irreducible polynomials over a number field from Eisenstein polynomials by conjugation. Similarly, Odoni [28] noticed that if one of the iterates is dynamically irreducible then all the iterates are dynamically irreducible. We use Odoni's lemma to produce two dynamically irreducible families in Chapters 3 and 4, namely eventually p-Eisenstein polynomials and specific family of eventually p^r-Dumas polynomials. In order to show such results, we need to characterize polynomials for which one of its iterates is *eventually* of the form $f(x) \equiv ax^d \pmod{p}$ for some $a \in \mathbb{Q}$ with $\nu_p(a) = 0$ and identify the least iteration to reach such a form. In Chapter 2, we introduce p-

type polynomials, characterize eventually p-type polynomials and identify the least iteration of an eventually p-type to become p-type.

If a polynomial is reducible, one is still interested in collecting facts about the number, degree and types of the irreducible factors of the polynomial. Dumas Theorem, see Proposition 4.5, sets an upper bound on the number and degree of irreducible factors just from the Newton polygon of a polynomial. In a similar way, Eisenstein mistakenly claimed that for some polynomial $f(x) = a_d x^d + \ldots + a_0 \in \mathbb{Z}[x]$, if there exists some prime p such that $p \nmid a_d$ and $p | a_i$ for $1 \leq i \leq d-1$, but, $p^2 \nmid a_k$ for some $1 \leq k \leq d-1$, then, f is irreducible over $\mathbb{Q}$. In [32], Weintraub provided a family of counterexamples. He proposed a correction to Eisenstein's claim by letting k_0 to be the smallest value of k such that $p^2 \nmid a_{k_0}$ so that if $f(x) = g(x)h(x)$, then, the minimum degree of both g and h is at most k_0, see Theorem 1 in [32] for a proof.

Dynamically, we say a polynomial f is eventually stable if the number of irreducible factors of any iterate is at most some $c \in \mathbb{Z}^+$. In particular, if $c = 1$, then, f is dynamically irreducible. Most results discuss quadratic eventually stable polynomials (see [24], [13] and [17]) in addition to a discussion in [27] about polynomials of the form $z^d + \frac{1}{c}$ where $c \in \mathbb{Z} \backslash \{0\}$. In Chapter 4, we introduce pure polynomials and use a result by Jakhar [21] to show they are eventually stable, see Theorem 4.26. In Chapter 4 also, we provide a complete characterization of a family of eventually pure polynomials, see Theorem 4.34.

Even if a polynomial is reducible, one may extract an iterative sequence of irreducible polynomials. For example, if $g(x) = x^p + p$ for some prime p and $f(x) = x^2$, then, $g(f^n(x)) = x^{2^n p} + p$ is irreducible for all $n \geq 1$. In such a case we say g is f-stable. In general, if f is eventually stable, the number of irreducible factors of the iterates will not change after some iteration. In other words, there exists an iteration $k \geq 1$ such that f^{n+k} has $s \geq 2$ irreducible factors for all $n \geq 1$. So, if

$$f^k(x) = g_1(x) \cdot \ldots \cdot g_s(x)$$

for some irreducible factors $g_1, \ldots, g_s$, then,

$$f^{k+n}(x) = g_1 \circ f^n \cdot \ldots \cdot g_s \circ f^n.$$

Note that $g_1 \circ f^n, \ldots, g_s \circ f^n$ are irreducible for all $n \geq 1$. This means that, $g_1, \ldots, g_s$ are f-stable. In Chapter 4, we provide some families of f-stable polynomials inspired by the previous argument, see Corollaries 4.20, 4.22 and 4.23. It is worth mentioning that all the computations were performed using Mathematica [20].

Chapter 1

Preliminaries

Definition 1.1. *[4]* ***A (discrete) dynamical system*** (S,ϕ) *is a set S along with a self-map $\phi : S \to S$. The nth-iterate of the map ϕ is defined as:*

$$\phi^n := \underbrace{\phi \circ \phi \ldots \circ \phi}_{n\text{-}times}$$

Conventionally, ϕ^0 is the identity map on S

In this thesis, our main scope is polynomial maps in $\mathbb{Q}[x]$. In particular, we focus on the irreducibility of iterations of a polynomial map. Nevertheless, we first establish the concept of irreducibility.

Definition 1.2. *[30, p.48] Let K be a field. A polynomial $f \in K[x]$ is called* ***reducible over K*** *if $f = gh$, where g and h are polynomials of positive degree in $K[x]$, otherwise, f is called* ***irreducible over K****.*

Given Irreducibility and composition of polynomials are our main focus, it is valid to ask the following question: If f and g are polynomials over a field K, under what conditions is $f \circ g$ irreducible over K? This question is answered by Capelli's Lemma.

Proposition 1.3. *[3, Lemma 1] Let K be a field and f,g be polynomials in $K[x]$. Suppose α is any root of f in the algebraic closure of K. Then, $f \circ g$ is irreducible over K if and only if f is irreducible over K and $g(x) - \alpha$ is irreducible over $K(\alpha)$.*

Dynamically, we are interested in the irreducibility of polynomial iterates. For this purpose, we need the following definition.

Definition 1.4. *[1] Let K be a field. The polynomial f in $K[x]$ is called* ***stable*** *or* ***dynamically irreducible*** *if all the iterates $f, f^2, \ldots, f^n, \ldots$ are irreducible over K.*

An extension of Definition 1.4 is the following.

Definition 1.5. *[23, Definition 2.1] Let K be a field and $f,g \in K[x]$. We say that g is **f-stable** if $g \circ f^n$ is irreducible over K for $n = 0,1,2,\ldots$. In particular, f is dynamically irreducible whenever $g = f$.*

Next, we present a survey of some results on dynamically irreducible polynomials in $\mathbb{Q}[x]$. For further elaboration, We shall apply these results to the polynomial x^2+1.

Proposition 1.6. *[23, Proposition 2.3] Let K be a field with characteristic not equal to 2. Suppose the polynomial $f(x) = ax^2+bx+c \in K[x]$ has a critical point $\gamma = \frac{-b}{2a}$. Then, f is dynamically irreducible over K if $af^2(\gamma), af^3(\gamma), \ldots, af^n(\gamma), \ldots$ and $-af(\gamma)$ are all nonsquares in K.*

Example 1.7. *For x^2+1 in $\mathbb{Q}[x]$, the critical point is $\gamma = 0$ and for all $n > 1$, it is obvious that $f^n(0)$ and $-f(0) = -1$ are all nonsquares in $\mathbb{Q}$. Hence, it is dynamically irreducible over $\mathbb{Q}$.*

Proposition 1.8. *[11, Corollary 5] Let R be either $\mathbb{Z}$, $\mathbb{Z}[t]$ or $K[t]$ where K is an algebraically closed field. If $f(x) = x^n - b \in R[x]$ is irreducible over R, then, it is dynamically irreducible.*

Example 1.9. *Note that x^2+1 is irreducible over $\mathbb{Z}$ and by the previous proposition it is dynamically irreducible over $\mathbb{Z}$. By Gauss's lemma, we conclude that x^2+1 is dynamically irreducible over $\mathbb{Q}$.*

Proposition 1.10. *[22, Theorem 4.5] Let $f(x) = (x-\gamma)^2+\gamma+m \in \mathbb{Z}[x]$ be irreducible and suppose that $|m| > 6+3\sqrt{|\gamma|+1}$ (if $\gamma \in \mathbb{Z}$ then $|m| > 1+\sqrt{|\gamma|+1}$ is sufficient), and that*

$$\frac{-m \pm \sqrt{f^2(\gamma)}}{2} \notin \mathbb{Q}^{*2}.$$

Then, f is dynamically irreducible.

Example 1.11. *We can not use Proposition 1.10 to prove that $f(x) = x^2+1$ is dynamically irreducible as $\gamma = 0 \in \mathbb{Z}$, $m = 1$ and $|1| < 6+3 = 9$. Yet, for the irreducible polynomial $g(x) = x^2+4x+5 = (x+2)^2-2+3$ with $\gamma = -2$ and $m = 3$, we notice that*

$$|3| > 1+1 = 2$$

and

$$\frac{-3 \pm \sqrt{50}}{2} \notin \mathbb{Q}^{*2}.$$

So, g is dynamically irreducible.

Given Proposition 1.3, one should not expect each irreducible polynomial to be dynamically irreducible. For instance, consider the following example.

Example 1.12. *[19, Introduction] The polynomial $g(x) = x^2 - x - 1$ is irreducible but*

$$g^3(x) = (x^4 - 3x^3 + 4x - 1)(x^4 - x^3 - 3x^2 + x + 1) \text{ is reducible.}$$

In light of the previous example, we introduce the following definition.

Definition 1.13. *[19] Let K be a field. The polynomial f in $K[x]$ is called **n-newly reducible** if $f, \dots, f^{n-1}$ are irreducible over K, but, f^n is reducible for some iteration n.*

For a discussion on newly reducible polynomials, refer to [19] and [9]. Unlike testing for irreducibility, it is unknown if dynamical irreducibility over a field can be tested in finitely many steps as the degrees of the iterates grow exponentially. Also, the first few irreducible iterates of a polynomial do not always imply its dynamical irreducibility. For instance, consider the following example.

Example 1.14. *Consider $f(x) = x^2 + 1$ over $\mathbb{F}_{43}$. The iterates f^2, f^3, f^4 and f^5 are irreducible. However, the iterate f^6 is reducible. In other words, f is 6-newly reducible. In conclusion, the irreducibility of the first 5 iterates does not imply that f is dynamically irreducible.*

Moving on to newly reducible polynomials, one is interested to find an upper bound for the number of irreducible factors of the reducible iterates. To be a dynamical property, the bound should not depend on the iteration. For this purpose, we have the following extension of Definition 1.4

Definition 1.15. *[13, Definition 1.1] Let K be a field, f be a polynomial in $K[x]$, and $\alpha \in K$. We say (f, α) is eventually stable over K if there exists a constant $C(f, \alpha)$ such that the number of irreducible factors over K of $f^n(x) - \alpha$ is at most $C(f, \alpha)$ for all $n \geq 1$. In particular, we say that f is **eventually stable over K** if $(f, 0)$ is eventually stable.*

In fact, not all polynomials in $\mathbb{Q}[x]$ are eventually stable; consider the following family.

Example 1.16. *[22] The polynomial $f_k(x) = x^2 + kx - (k+1) \in \mathbb{Z}[x]$ is not eventually stable because $f_k^2(x) = x(x+k)(x^2 + kx - k - 2)$. Thus, x divides f_k^{2n} for all $n \geq 1$ and the number of irreducible factors is unbounded. The preceding condition can be rephrased as 0 being periodic under f, i.e., $0 \in \{f_k^n(0) : n \geq 1\}$.*

The previous example motivates the following conjecture.

Conjecture 1.17. *[22, Conjecture 4.9] If $f \in \mathbb{Z}[x]$ is monic, quadratic and 0 is not periodic under f, then, f is eventually stable.*

A test for eventually stable polynomials like Proposition 1.6 is the following.

Proposition 1.18. *[22, Proposition 4.2] Let K be a field and $f(x) = ax^2 + bx + c \in K[x]$ with critical point γ. Suppose there is a polynomial $g \in K[x]$ such that $g \circ f^{n-1}$ is irreducible over K for some $n \geq 2$. Then, $g \circ f^n$ is irreducible over K if $g(f^n(\gamma))$ is not a square in K.*

For polynomials of the form $x^d + c \in \mathbb{Q}[x]$, we mention the following result.

Proposition 1.19. *[17, Corollary 1.7] Let $f(x) = x^d + c \in \mathbb{Q}[x]$ such that c is non-zero and not the reciprocal of an integer. Then, f is eventually stable over $\mathbb{Q}$.*

A thorough discussion of the quadratic case of Proposition 1.19 can be found in [13].

Chapter 2

p-Type and Eventually p-Type Polynomials

In this chapter, we introduce some properties of p-type and eventually p-type polynomials. These properties will be used frequently throughout the thesis.

Definition 2.1. *Let $a \in \mathbb{Z}$ and p be a rational prime. The* ***p-adic valuation*** *of a is the function $\nu_p : \mathbb{Z} \to \mathbb{Z}_{\geq 0} \cup \{\infty\}$ such that*

$$\nu_p(a) := \begin{cases} r & \text{if } p^r | a \text{ but } p^{r+1} \nmid a \text{ for } a \neq 0 \\ \infty & a = 0 \end{cases}$$

The p-adic valuation can be extend to rational numbers by defining $\nu_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ such that $\nu_p(\frac{a}{b}) = \nu_p(a) - \nu_p(b)$

The previous definition can be extended further to the following.

Definition 2.2. *[5, Introduction] Let $f(x) = a_d x^d + \ldots + a_0 \in \mathbb{Q}[x]$ and p be a prime.* ***The Gaussian valuation*** *of f with respect to p is defined as.*

$$\nu_p(f) := \min_{0 \leq i \leq d} \nu_p(a_i).$$

We shall use ν_p to denote both the p-adic and Gaussian valuation as an element in $\mathbb{Q}$ can be considered as a constant polynomial in $\mathbb{Q}[x]$.

Definition 2.3. *A polynomial $f(x) = a_d x^d + \ldots + a_0 \in \mathbb{Q}[x]$ is said to be* ***p-type*** *if $\nu_p(a_d) = 0$ and $f(x) \equiv a_d x^d \pmod p$. In other words, $\nu_p(a_0), \ldots, \nu_p(a_{d-1}) \geq 1$.*

Proposition 2.4. *If f is p-type, then, for some $a \in \mathbb{Q}$ with $\nu_p(a) = 0$, the polynomial $f(ax^d)$ is p-type. Moreover, f^n is p-type for all iterations $n \geq 1$.*

Proof. The statement follows from Definition 2.3. □

Example 2.5. *The polynomial*

$$f(x) = x^7 + \frac{3}{5}x + \frac{18}{7}$$

is 3*-type because* $\nu_3(1) = 0$, $\nu_3\left(\frac{3}{5}\right) = 1$ *and* $\nu_3\left(\frac{18}{7}\right) = 2$.

Furthermore, one can find a polynomial f which is not p-type for some prime p, yet, one of its iterates is p-type; consider the following example.

Example 2.6. *The polynomial*

$$f(x) = x^3 + 3x^2 + \frac{9}{2}x + \frac{11}{2}$$

is not 3*-type because* $\nu_3\left(\frac{11}{2}\right) = 0$ *and the second iterate*

$$f^2(x) = x^9 + 9x^8 + \frac{81x^7}{2} + \frac{255x^6}{2} + \frac{1197x^5}{4} + \frac{2133x^4}{4} + \frac{5967x^3}{8} + \frac{6237x^2}{8} + \frac{4617x}{8} + \frac{2299}{8}$$

is again not 3*-type because* $\nu_3\left(\frac{2299}{8}\right) = 0$, *yet, the third iterate*

$$\begin{aligned} f^3(x) = {} & x^{27} + 27x^{26} + \frac{729x^{25}}{2} + \frac{6597x^{24}}{2} + 22545x^{23} + 124011x^{22} + 570510x^{21} + 2251476x^{20} \\ & + \frac{62057097x^{19}}{8} + \frac{189021339x^{18}}{8} + \frac{1027333125x^{17}}{16} + \frac{2507352489x^{16}}{16} + \frac{2761048809x^{15}}{8} \\ & + \frac{5504594355x^{14}}{8} + \frac{19905289839x^{13}}{16} + \frac{32659896843x^{12}}{16} + \frac{777625553637x^{11}}{256} \\ & + \frac{1047643321527x^{10}}{256} + \frac{2547482271141x^{9}}{512} + \frac{2781671553585x^{8}}{512} + \frac{1354537004751x^{7}}{256} \\ & + \frac{1165197294621x^{6}}{256} + \frac{218300122899x^{5}}{64} + \frac{279385323201x^{4}}{128} + \frac{74036338389x^{3}}{64} \\ & + \frac{30889750545x^{2}}{64} + \frac{73718914131x}{512} + \frac{12278651451}{512} \end{aligned}$$

is 3*-type as* $f^3(x) \equiv x^{27} \pmod 3$.

The previous example motivates the following definition.

Definition 2.7. *Let* $f \in \mathbb{Q}[x]$ *and* p *be a prime. We say* f *is* ***eventually p-type*** *if an iterate* f^n *is* p*-type for some* $n \geq 1$.

Trivially, a p-type polynomial is also eventually p-type. However, for a polynomial that is not p-type but eventually p-type, it is valid to ask the following question.

Question 2.8. *If a polynomial* f *is not* p*-type, yet, it is eventually* p*-type. Is there any restriction on the degree of* f*? Is there an exhaustive classification of such* *polynomials?*

Indeed, this question is answered in Theorem 2.10, yet, a lemma is needed.

Lemma 2.9. *Suppose f and g are polynomials in $\mathbb{Q}[x]$ such that $f \circ g$ is p-type. Then, $f(x+g(0))$ and $g(x)-g(0)$ are p-type.*

Proof. Assume f and g are polynomials in $\mathbb{Q}[x]$ such that $f \circ g$ is p-type for some prime p. Define the following polynomials:

$$F(x) := f(x+g(0)) = ax^e + a_{e-1}x^{e-1} + \ldots + a_0$$

$$G(x) := g(x) - g(0) = bx^f + b_{f-1}x^{f-1} + \ldots + b_1 x$$

First, note that $F \circ G = f \circ g$ and $\nu_p(a) = \nu_p(b) = 0$. Second, observe that G divides the polynomial $F \circ G - F(0)$. As, $\nu_p(F \circ G - F(0)) = 0$, then,

$$\nu_p(G) + \nu_p\left(\frac{F \circ G - F(0)}{G}\right) = 0$$

Given $\nu_p(b) = 0$, thus, $\nu_p(G) = 0$. Otherwise, $\nu_p(G) < 0$ and $\nu_p\left(\frac{F \circ G - F(0)}{G}\right) > 0$. Nonetheless, this assumption shall yield the contradiction:

$$0 < \nu_p\left(\frac{F \circ G - F(0)}{G}\right) = \nu_p\left(aG^{e-1} + \ldots + a_1\right) \leq \nu_p\left(ab^{e-1}x^{(e-1)f}\right) = 0$$

Hence, $G(x) = g(x) - g(0) \equiv bx^f \pmod{p}$ and it is p-type. Finally, $F(G(x)) \equiv F\left(bx^f\right) \pmod{p}$, so, $F(x) = f(x+g(0))$ is p-type too. □

We are now ready to prove the characterization theorem of eventually p-type polynomials.

Theorem 2.10. *If $f \in \mathbb{Q}[x]$ is not p-type but eventually p-type, then, $f(x) \equiv ax^{p^m} + b \pmod{p}$ for some $a, b \in \mathbb{Q}$ such that $\nu_p(a) = \nu_p(b) = 0$.*

Proof. Assume $f(x) = a_d x^d + \ldots + a_0$ so that f^n is p-type for some $n > 1$. Considering Lemma 2.9, the polynomials $f(x) - f(0)$ and $f(x + f^{n-1}(0))$ are p-type, hence, $\nu_p(a_d) = 0$. Moreover, $\nu_p(f(0)) \leq 0$ else f is p-type. In fact, we should show that $\nu_p(f(0)) = 0$. To achieve this, we shall use an argument analogous to that in the proof of Lemma 2.9. The polynomial $f^n - f^n(0)$ is p-type and if $\nu_p(f(0)) < 0$, then, $\nu_p(f) < 0$. Given f divides $f^n - f^n(0)$ and $\nu_p\left(\frac{f^n - f^n(0)}{f}\right) \leq 0$ as the p-adic valuation of its leading coefficient is 0, we shall reach the following contradiction:

$$0 = \nu_p\left(f^n - f^n(0)\right) = \nu_p(f) + \nu_p\left(\frac{f^n - f^n(0)}{f}\right) < 0$$

Then, for $f(x) = a_d x^d + \ldots + a_0$, one concludes that $\nu_p(a_d) = 0$, $\nu_p(a_{d-1}), \ldots, \nu_p(a_1) \geq 1$ and $\nu_p(a_0) = 0$

In other words, $f(x) \equiv a_d x^d + a_0 \pmod{p}$. Note that the same conclusion applies to f^{n-1} by interchanging f and f^{n-1} in the previous proof; in particular, $\nu_p(f^{n-1}(0)) = 0$. Next, from Lemma 2.9, we know $f(x + f^{n-1}(0))$ is p-type, so, $f\left(x + f^{n-1}(0)\right) \equiv a_d\left(x + f^{n-1}(0)\right)^d + a_0 \equiv a_d x^d \pmod{p}$. Finally, we must have

$$\nu_p\left(\binom{d}{k}\right) \geq 1 \text{ for all } 0 < k < d.$$

It follows from Kummer theorem [8, Definition 1.2] that $d = p^m$ for some $m \geq 1$. In conclusion, if f is not p-type but eventually p-type, then, $f(x) \equiv ax^{p^m} + b \pmod{p}$ such that $\nu_p(a) = \nu_p(b) = 0$ as desired. □

We shall use eventually p-type polynomials to mean the particular family $f(x) \equiv ax^{p^m} + b \pmod{p}$ with $\nu_p(a) = \nu_p(b) = 0$. Next, if f is an eventually p-type polynomial, can we identify the smallest iteration $n > 1$ such that f^n is p-type? This question is addressed in Theorem 2.11

Theorem 2.11. *Suppose $f(x) \equiv ax^{p^m} + b \pmod{p}$ is an eventually p-type polynomial with $\nu_p(a) = \nu_p(b) = 0$ and $k = \mathrm{ord}_p(a)$. Then, the **least** integer $n > 1$ such that f^n is p-type is:*

(a) $n = p$ if $a \equiv 1 \pmod{p}$

(b) $n = k$ otherwise.

We need the following Lemma to prove Theorem 2.11.

Lemma 2.12. *Suppose $f(x) \equiv ax^{p^m} + b \pmod{p}$ is an eventually p-type polynomial. Then, the iterate $f^n(x) \equiv a^n x^{p^{nm}} + \sum_{i=0}^{n-1} a^i b \pmod{p}$ for any $n \geq 2$. In particular, $f^n(0) \equiv \sum_{i=0}^{n-1} a^i b \pmod{p}$*

Proof. Assume $f(x) \equiv ax^{p^m} + b \pmod{p}$ with $\nu_p(a) = \nu_p(b) = 0$ for some prime p.

We have:

$$f^{n+1}(x) = f\left(f^n(x)\right) = a\left(a^n x^{p^{nm}} + \sum_{i=0}^{n-1} a^i b\right)^{p^m} + b \equiv a^{n+1} x^{p^{(n+1)m}} + \sum_{i=0}^{n} a^i b \pmod{p}$$

So, in particular, $f^n(0) \equiv \sum_{i=0}^{n-1} a^i b \pmod{p}$ □

We are now ready to prove Theorem 2.11.

Proof of Theorem 2.11. By Lemma 2.12, if $a \equiv 1 \pmod{p}$, then,

$$f^p(0) \equiv \sum_{i=0}^{p-1} b \equiv pb \equiv 0 \pmod{p};$$

$$\text{otherwise, } f^k(0) \equiv \sum_{i=0}^{k-1} a^i b \equiv b\left(\frac{a^k - 1}{a-1}\right) \equiv 0 \pmod{p}$$

Example 2.13. *Consider*

$$f(x) = 2x^5 + \frac{5x}{3} + 7$$

Note that $\mathrm{ord}_5(2) = 4$*, so, we expect* f^4 *to be first* 5*-type iterate. Indeed, we get:*

$$\begin{aligned} f(x) \equiv& 2x^5 + 2 \pmod{5} \\ f^2(x) \equiv& 4x^{25} + 1 \pmod{5} \\ f^3(x) \equiv& 3x^{125} + 4 \pmod{5} \\ f^4(x) \equiv& x^{625} \pmod{5} \end{aligned}$$

□

Chapter 3

Eventually Eisenstein Polynomials

An interesting example of p-type polynomials is p-Eisenstein polynomials. In general, p-type polynomials are not necessarily dynamically irreducible. In this chapter, our goal is to prove that the family of eventually p-Eisenstein polynomials are dynamically irreducible. To motivate the aforementioned goal, we discuss eventually 2-Eisenstein polynomials in the first section.

3.1 Eventually 2-Eisenstein Polynomials

Recall the definition of a p-Eisenstein polynomial.

Definition 3.1. *[16, p.310] Let* $f(x) = a_d x^d + \ldots + a_0 \in \mathbb{Q}[x]$. *Suppose there exists a rational prime* p *such that:*

(a) $\nu_p(a_d) = 0$

(b) $\nu_p(a_i) \geq 1$ *for all* $i \in \{1, \ldots, d-1\}$

(c) $\nu_p(a_0) = 1$

then, f *is irreducible over* $\mathbb{Q}$ *and is called* p*-Eisenstein.*

Odoni [28] showed that p-Eisenstein polynomials are not only irreducible but also dynamically irreducible over $\mathbb{Q}$. Moreover, he also presented the following simple test.

Proposition 3.2. *[28, Lemma 1.2] Let* $f(x) \in \mathbb{Q}[x]$. *If there exists a positive integer* n *such that* $f^n(x)$ *is dynamically irreducible over* $\mathbb{Q}$*, then,* $f(x)$ *is dynamically* *irreducible over $\mathbb{Q}$*

Consider the following example:

Example 3.3. *Let*

$$f(x) = x^4 + 2x^3 + 2x^2 + 2x + 3.$$

we know $f(x)$ is not p-Eisenstein for any prime p. Nevertheless,

$$\begin{aligned} f^2(x) = x^{16} &+ 8x^{14} + 16x^{13} + 36x^{12} + 96x^{11} + 200x^{10} + 336x^9 + 600x^8 + 960x^7 \\ &+ 1280x^6 + 1536x^5 + 1756x^4 + 1664x^3 + 1144x^2 + 496x + 114 \end{aligned}$$

is 2-Eisenstein and hence dynamically irreducible. By Proposition 3.2, f is also dynamically irreducible over $\mathbb{Q}$.

In light of the previous example, we introduce the following definition:

Definition 3.4. *A polynomial $f \in \mathbb{Q}[x]$ is* ***eventually 2-Eisenstein*** *if f^n is 2-Eisenstein for some $n \geq 1$.*

Corollary 3.5. *Eventually 2-Eisenstein polynomials are dynamically irreducible over $\mathbb{Q}$*

Proof. The result follows immediately from Proposition 3.2 and the dynamical irreducibility of p-Eisenstein polynomials. □

A 2-Eisenstein polynomial is also eventually 2-Eisesntein. Yet, we are more interested in polynomials that are not 2-Eisenstein but eventually 2-Eisenstein. Definition 3.4 and Example 3.3 motivate the following question:

Question 3.6. *Is there a complete characterization of eventually 2-Eisenstein polynomials? Can we determine the smallest $n > 1$ for the nth iterate to be 2-Eisenstein?*

The following theorem answers this question.

Theorem 3.7. *Let $f(x) = a_d x^d + \ldots + a_0 \in \mathbb{Q}[x]$ such that f is not 2-Eisenstein.*

Some iterate f^n is 2-Eisenstein if and only if the following conditions hold

(a) $d = 2^m$ *for some* $m \geq 1$

(b) $f(x) \equiv x^{2^m} + 1 \pmod{2}$

(c) $f(x+c)$ *is 2-Eisenstein for some* $c \in \mathbb{Q}$

Moreover, the least integer n such that f^n is 2-Eisenstein is exactly $n = 2$

Before proving the theorem, we need the following Lemma

Lemma 3.8. *Let p be a prime. Suppose $f \in \mathbb{Q}[x]$ is a p-Eisenstein polynomial of degree $d > 1$ and $c \in \mathbb{Q}$. If $\nu_p(c) \geq 1$, then, $\nu_p(f(c)) = 1$*

Proof. Assume $f(x) = a_d x^d + \ldots + a_0$ is p-Eisenstein polynomial of degree $d > 1$ and c is a rational number with $\nu_p(c) \geq 1$. Then,

$$f(c) = a_d c^d + \sum_{i \neq 0,d} a_i c^i + a_0$$

By Definition 3.1, $\nu_p(a_d) = 0$, $\nu_p(a_i) \geq 1$ for $i = 1, \ldots, d-1$ and $\nu_p(a_0) = 1$. It follows that $\nu_p(a_i c^i) > 1$ for all $i \neq 0$ and so $\nu_p(f(c)) = \nu_p(a_0) = 1$ □

Next, we prove the theorem.

Proof of Theorem 3.7. Assume $f(x) \equiv a_d x^d + \ldots + a_0$ is not 2-Eisenstein, yet, f^n is 2-Eisenstein for some minimal $n > 1$. By Definition 2.7, Since $a_d \equiv 1 \pmod 2$, then, f^2 is 2-type. Also, as f is eventually 2-type, then, $d = 2^m$ for some $m \geq 1$ and $f(x) \equiv x^{2^m} + 1 \pmod 2$. For simplicity, let $c = f(0)$. We just need to show that $g(x) = f(x+c)$ is 2-Eisenstein. Observe that $g(x) = f(x+c) \equiv (x+c)^{2^m} + 1 \equiv x^{2^m} \pmod 2$ and $\nu_2(g(0)) = \nu_2(f^2(0)) = 1$ as f^2 is 2-Eisenstein. For the other direction, if $f(x) \equiv x^{2^m} + 1 \pmod 2$ and $g(x) = f(x+c)$ is 2-Eisenstein for some c, then f^2 is 2-Eisenstein. First, note that $\nu_2(c) = 0$ else g will not be 2-Eisenstein. Second, we observe that $f(f(x))$ is 2-type by Theorem 2.11, so, we just need to show that $\nu_2(f^2(0)) = 1$. since, $f(f(0)) = g(f(0) - c)$ and $\nu_2(f(0) - c) \geq 1$, then, by Lemma 3.8 and given g is 2-Eisenstein, $\nu_2(f^2(0)) = 1$ and f^2 is 2-Eisenstein. □

Based on the previous theorem, we can conclude the following corollary.

Corollary 3.9. *Let f be a 2-Eisenstein polynomial of degree 2^m. The polynomial $f(x+c)$ is dynamically irreducible over $\mathbb{Q}$ for all $c \in \mathbb{Q}$ with $\nu_2(c) \geq 0$*

Proof. Assume f is 2-Eisenstein. By Lemma 3.8, if $\nu_2(c) \geq 1$, $f(x+c)$ is 2-Eisenstein. Moreover, if $\nu_2(c) = 0$, then, $f(x+c)$ is eventually 2-Eisenstein by Theorem 3.7. □

Since shifts over $\mathbb{Q}$ were mentioned, it is valid to ask the following question:

Question 3.10. *Let $f \in \mathbb{Z}[x]$ and $c \in \mathbb{Z}$. If f is dynamically irreducible over $\mathbb{Q}$, is $f(x+c)$ always dynamically irreducible too?*

The answer is No. Consider the following example.

Example 3.11. *The polynomial*

$$f(x) = x^2 + 5x + 5$$

is 5*-Eisenstein and thus dynamically irreducible over* $\mathbb{Q}$*. But,* $g(x) = f(x-3) = x^2 - x - 1$ *is* 3*-newly reducible as discussed in Example 1.12*

However, the following property is a consequence of Theorem 3.7 .

Corollary 3.12. *If* $f \in \mathbb{Z}[x]$ *is* 2*-Eisenstein of degree* 2^m*, then,* $f(x+c)$ *is dynamically irreducible for all* $c \in \mathbb{Z}$

Next, we can conclude two dynamical irreducibility criteria for polynomials of the form $x^{2^m} + 1 \pmod 2$.

Corollary 3.13. *Let* $f(x) \equiv x^{2^m} + 1 \pmod 2$ *be a polynomial in* $\mathbb{Q}[x]$*. If* $\nu_2(f(1)) = 1$*, then,* f *is dynamically irreducible over* $\mathbb{Q}$

Proof. If $\nu_2(f(1)) = 1$, then, by Theorem 3.7, $f(x+1)$ and f^2 are 2-Eisenstein. It follows from Proposition 3.2 that f is dynamically irreducible over $\mathbb{Q}$ □

Corollary 3.14. *Let* $f(x) = a_{2^m} x^{2^m} + \ldots + a_0 \in \mathbb{Q}[x]$ *such that* $f(x) \equiv x^{2^m} + 1 \pmod 2$*. Define*

$$\delta(f) := \#\{i : \nu_2(a_i) = 1\}$$

Then, f *is dynamically irreducible over* $\mathbb{Q}$ *if one of the following conditions hold:*

(a) $\delta(f)$ *is even and* $a_{2^m} + a_0 \equiv 2 \pmod 4$

(b) $\delta(f)$ *is odd and* $a_{2^m} + a_0 \equiv 0 \pmod 4$

Proof. Let $f(x) \equiv a_{2^m} x^{2^m} + \ldots + a_0 \in \mathbb{Q}[x]$ such that $f(x) \equiv a_{2^m} x^{2^m} + g(x) + a_0 \pmod 4$ where $g(x)$ represents the coefficients of f with 2-adic valuation equal to 1. If $\delta(f)$ is even and $a_{2^m} + a_0 \equiv 2 \pmod 4$. Then, $\nu_2(g(1)) \geq 2$ and $f(1) \equiv a_{2^m} + a_0 \equiv 2 \pmod 4$. Thus, $\nu_2(f(1)) = 1$ and by Corollary 3.13, f is dynamically irreducible. On the other hand, if $\delta(f)$ is odd and $a_{2^m} + a_0 \equiv 0 \pmod 4$, then, $\nu_2(g(1)) = 1$ and $f(1) \equiv a_{2^m} + 2 + a_0 \equiv 2 \pmod 4$. So, again $\nu_2(f(1)) = 1$ and f is dynamically irreducible. □

Finally, we end this section with some examples.

Example 3.15. *Consider the polynomial*

$$f(x) = x^8 - 8x^7 + 28x^6 - 56x^5 + 70x^4 - 56x^3 + 28x^2 - 8x + 7$$

Since gcd$(-8,7)=1$, we can't use the Eisenstein criterion for any prime. As $\nu_2(f(1))=\nu_2(6)=1$, therefore, we expect $f(x+1)$ and f^2 to be 2-Eisenstein. As a check,

$$f(x+1)=x^8+6$$

$$f^2(x)\equiv x^{64}+2 \textit{ mod } 4$$

As f^2 is 2-Eisenstein then f is dynamically irreducible over $\mathbb{Q}$ by Corollary 3.13. Using Corollary 3.14, we notice that

$$f(x)\equiv x^8+2x^4+3 \textit{ mod } 4$$

which means that $\delta(f)=1$ and $1+3\equiv 0 \pmod 4$, so, dynamical irreducibility still holds.

Example 3.16. *Consider the polynomial*

$$f(x)=(x+a)^{2^m}+b \text{ such that } \nu_2(a)\geq 0 \text{ and } \nu_2(b)=1$$

If $\nu_2(a)\geq 1$, then, f is 2-Eisenstein, else, $f(x-a)$ is 2-Eisenstein and thus f is dynamically irreducible by Theorem 3.7.

Example 3.17. *Consider the polynomial*

$$f(x)=\frac{x^4}{7}+\frac{12x^3}{7}+\frac{54x^2}{7}+\frac{582x}{35}+\frac{1943}{105}$$

Note that gcd$(12,1943)=1$, *so, we can not use the Eisesntein Criterion for any prime. Nevertheless,*

$$\begin{aligned}f^2(x)=&\frac{x^{16}}{16807}+\frac{48x^{15}}{16807}+\frac{1080x^{14}}{16807}+\frac{10824x^{13}}{12005}+\frac{6512x^{12}}{735}+\frac{779568x^{11}}{12005}+\frac{22153752x^{10}}{60025}\\&+\frac{140178768x^9}{84035}+\frac{307086776x^8}{50421}+\frac{38054968352x^7}{2100875}+\frac{13193004576x^6}{300125}\\&+\frac{530372576x^5}{6125}+\frac{5532951143206x^4}{40516875}+\frac{2268156195544x^3}{13505625}+\frac{1611936869204x^2}{10504375}\\&+\frac{8935631095012x}{94539375}+\frac{26020147948246}{850854375}\end{aligned}$$

is 2-Eisenstein because

$$f^2(x)\equiv 3x^{16}+2x^4+2 \pmod 4$$

Indeed, f^2 is 2-Eisenstein because

$$f(x+1)=\frac{x^4}{7}+\frac{16x^3}{7}+\frac{96x^2}{7}+\frac{1322x}{35}+\frac{4694}{105}\equiv 3x^4+2x+2 \pmod 4$$

is 2-Eisenstein too. Thus, f is dynamically irreducible over $\mathbb{Q}$ by Theorem 3.7.

Example 3.18. *Consider the polynomial*

$$f(x)=a(x+c)^{2^m}+b(x+c)+d\in\mathbb{Q}[x]$$

such that $\nu_2(a)=0$, $\nu_2(b)\geq 1$, $\nu_2(d)=1$ and $\nu_2(c)\geq 0$ for some $m\geq 1$. Note that $f(x-c)$ is 2-Eisenstein and by Corollary 3.9, the polynomial f is dynamically irreducible over $\mathbb{Q}$.

3.2 Eventually p-Eisenstein Polynomials

In this section, we shall extend the results of the previous section for all primes. Throughout the section, we assume p is a rational prime and $d=p^m$ for some $m\geq 1$. First, we generalize Definition 3.4.

Definition 3.19. *A polynomial $f\in\mathbb{Q}[x]$ is **eventually p-Eisenstein** if f^n is p-Eisenstein for some $n\geq 1$.*

Corollary 3.20. *Eventually p-Eisenstein polynomials are dynamically irreducible over $\mathbb{Q}$.*

Proof. The result follows immediately from Proposition 3.2 and the dynamical irreducibility of p-Eisenstein polynomials. □

Consider the following example.

Example 3.21. *Let*

$$f(x)=x^3+3x^2+3x+4$$

Note that f is not p-Eisenstein for any prime p. Moreover, f^2 is not p-Eisenstein as gcd $(9,128)=1$ as seen below.

$$f^2(x)=x^9+9x^8+36x^7+96x^6+198x^5+306x^4+372x^3+360x^2+225x+128$$

Yet, f^3 is 3-Eisenstein because

$$f^3(x) \equiv x^{27} + 3 \pmod 9$$

By Corollary 3.20, f is dynamically irreducible over $\mathbb{Q}$

Unlike eventually 2-Eisenstein, if a polynomial is eventually p-Eisenstein, the second iterate f^2 is not always p-Eisenstein. Yet, we can determine the smallest such iterate using Theorem 2.11 as an eventually p-Eisenstein is also eventually p-type. Next, we introduce the second major theorem in this thesis.

Theorem 3.22. *Let $f(x) = a_d x^d + \ldots + a_0 \in \mathbb{Q}[x]$ such that f is not p-Eisenstein. Then, some iterate f^n is p-Eisenstein if and only if the all following hold:*

(a) $d = p^m$ for some prime p and $m \in \mathbb{Z}^+$,

(b) $f(x) \equiv a_d x^d + a_0 \pmod p$ such that $\nu_p(a_d) = \nu_p(a_0) = 0$,

(c) $f(x+c)$ is p-Eisenstein for some $c \in \mathbb{Q}$.

Moreover, the least integer n such that f^n is p-Eisenstein is determined by Theorem 2.11.

Proof. Assume that $f(x) = a_d x^d + \ldots + a_0$ is not p-Eisenstein but some iterate f^n is p-Eisenstein for some minimal $n > 1$. Note that f is eventually p-type and by Theorem 2.10, we can conclude that $d = p^m$, $f(x) \equiv a_d x^d + a_0 \pmod p$ with $\nu_p(a_d) = \nu_p(a_0) = 0$ and also $g(x) = f(x + f^{n-1}(0))$ is p-type. In fact, we should prove that $g(x)$ is p-Eisenstein also. Observe that $\nu_p(g(0)) = \nu_p(f^n(0)) = 1$. Moreover, by Theorem 2.11, we know that $n = \mathrm{ord_p}(a_d)$ and using Lemma 2.12, $\nu_p(f^{n-1}(0)) = 0$ as $n-1 <\mathrm{ord}_p(a_d)$. Therefore, g is indeed p-Eisenstein. For the other direction, assume $f(x) \equiv a_d x^d + a_0 \pmod p$ for some $a, b \in \mathbb{Q}$ such that $\nu_p(a) = \nu_p(b) = 0$, $d = p^m$ and there exists a $c \in \mathbb{Q}$ such that $g(x) = f(x+c)$ is p-Eisenstein. We need to show that f^n is p-Eisenstein for some iteration n. Again, we know that $n = \mathrm{ord}_p(a)$ is the minimal iteration. Let $c \equiv -{a_d}^{-1} a_0 \pmod p$; using Lemma 2.12, we get

$$\begin{aligned} f^n(x) &\equiv g\left(f^{n-1}(x) - c\right) \equiv g\left({a_d}^{n-1} x^{d^{n-1}} + \sum_{i=0}^{n-2} {a_d}^i a_0 + {a_d}^{-1} a_0\right) \pmod p \\ &\equiv g\left({a_d}^{n-1} x^{d^{n-1}} + a_0 {a_d}^{-1}(1 + a_d + \ldots + {a_d}^{n-1})\right) \pmod p \end{aligned}$$

If $a_d \equiv 1 \pmod p$, then, $n = p$ and

$$f^p(x) \equiv g\left({a_d}^{p-1}x^{d^{p-1}} + a_0 p\right) \equiv g\left({a_d}^{p-1}x^{d^{p-1}}\right) \pmod p$$

Otherwise, $a_d \not\equiv 1 \pmod p$ and $n = \mathrm{ord}_p(a_d)$. In this case, again,

$$\begin{aligned} f^n(x) &\equiv g\left({a_d}^{n-1}x^{d^{n-1}} + a_0{a_d}^{-1}(1 + a_d + \ldots + {a_d}^{n-1})\right) \pmod p \\ &\equiv g\left({a_d}^{n-1}x^{d^{n-1}} + a_0{a_d}^{-1}(\frac{a_d^n - 1}{a_d - 1})\right) \pmod p \\ &\equiv g\left({a_d}^{n-1}x^{d^{n-1}}\right) \pmod p \end{aligned}$$

Since g is p-type, then, f^n is p-type too. As $\nu_p(f^n(0)) = 1$, we conclude that f^n is p-Eisenstein. □

An extension of Corollary 3.9 is the following corollary.

Corollary 3.23. *Let f be a p-Eisenstein polynomial of degree p^m. The polynomial $f(x+c)$ is dynamically irreducible over $\mathbb{Q}$ for all $c \in \mathbb{Q}$ with $\nu_p(c) \geq 0$*

Proof. Assume f is p-Eisenstein. By Lemma 3.8, if $\nu_p(c) \geq 1$, $f(x+c)$ is p-Eisenstein. Moreover, if $\nu_p(c) = 0$, then, $f(x+c)$ is eventually p-Eisenstein by Theorem 3.22 □

Next, we also extend Corollary 3.12 to the following corollary.

Corollary 3.24. *If $f \in \mathbb{Z}[x]$ is p-Eisenstein of degree p^m for some positive integer m, then, $f(x+c)$ is dynamically irreducible for all $c \in \mathbb{Z}$.*

Finally, we extend the criterion in Corollary 3.13 to the following.

Corollary 3.25. *Let $f(x) \equiv ax^{p^m} + b \pmod p$ such that $\nu_p(a) = \nu_p(b) = 0$ and $c \equiv -a^{-1}b \pmod p$. If $\nu_p(f(c)) = 1$, then, $f(x)$ is dynamically irreducible over $\mathbb{Q}$.*

Proof. Suppose $f(x) \equiv ax^{p^m} + b \pmod p$ such that $\nu_p(a) = \nu_p(b) = 0$. If $c = \frac{a}{b} \in \mathbb{Q}$ is in the simplest form and $\nu_p(c) = 0$, then, $c \equiv -a^{-1}b \pmod p$. Whenever $\nu_p(f(c)) = 1$, then, $f(x+c)$ is p-Eisenstein and, by Corollary 3.23, the polynomial f is dynamically irreducible over $\mathbb{Q}$. □

Finally, we conclude this section with some examples.

Example 3.26. *Consider any polynomial f in $\mathbb{Z}[x]$ such that*

$$f(x) \equiv 2x^{25} + 10x^3 + 3 \pmod{25}$$

Using Corollary 3.23, we have $c \equiv -2^{-1} \times 3 \equiv 1 \pmod 5$ *and* $\nu_5(f(1)) = \nu_5(15) = 1$*. Note that* $\mathrm{ord}_5(2) = 4$*. Thus, we expect* $f^4(x)$ *to be* 5*-Eisenstein. As a check,* $f^2(0) \equiv 9 \pmod{25}$*,* $f^3(0) \equiv 16 \pmod{25}$ *and* $f^4(0) \equiv 15 \pmod{25}$*. So,* $f^4(x)$ *is indeed* 5*-Eisenstein and* f *is dynamically irreducible over* $\mathbb{Q}$*.*

Example 3.27. *Consider the following trinomial in* $\mathbb{Z}[x]$:

$$f(x) = x^{p^m} + px + 1 \text{ where } p \text{ is an odd prime and } m \geq 1.$$

Observe that $c \equiv -(1)^{-1} \cdot 1 \equiv -1 \pmod p$ *and* $\nu_p(f(c)) = 1$ *because* $f(c) = f(-1) \equiv -1 - p + 1 \equiv -p \pmod{p^2}$*. So,* $f(x-1)$ *and* $f^p(x)$ *are* p*-Eisenstein. By Corollary 3.23,* f *is dynamically irreducible over* $\mathbb{Q}$*.*

Example 3.28. *Consider the polynomial*

$$\begin{aligned} f(x) = {} & \frac{x^{11}}{2} + \frac{11x^{10}}{2} + \frac{55x^9}{2} + \frac{165x^8}{2} + 165x^7 + 231x^6 + 231x^5 + 165x^4 \\ & + \frac{165x^3}{2} + \frac{55x^2}{2} + \frac{297x}{10} + \frac{851}{30} \equiv 6x^{11} + 6 \pmod{11}. \end{aligned}$$

Note that $c \equiv -(2^{-1})^{-1}(\frac{851}{30}) \equiv -\frac{851}{15} \equiv -851(15)^{-1} \equiv -1 \pmod{11}$*. So, we expect* $f(x-1)$ *to be* 11*-Eisenstein. Indeed,*

$$f(x-1) = \frac{x^{11}}{2} + \frac{121x}{5} + \frac{11}{3}$$

is 11*-Eisenstein. Next,* $\mathrm{ord}_{11}(\frac{1}{2}) = \mathrm{ord}_{11}(2) = 10$*. Thus, we expect* f^{10} *to be the least* 11*-Eisenstein iterate. To check, we calculate the following.*

$$\begin{aligned} f^2(0) &\equiv 64 \pmod{121} \\ f^3(0) &\equiv 104 \pmod{121} \\ f^4(0) &\equiv 91 \pmod{121} \\ f^5(0) &\equiv 24 \pmod{121} \\ f^6(0) &\equiv 106 \pmod{121} \\ f^7(0) &\equiv 103 \pmod{121} \\ f^8(0) &\equiv 118 \pmod{121} \\ f^9(0) &\equiv 109 \pmod{121} \\ f^{10}(0) &\equiv 44 \equiv 4 \cdot 11 \pmod{121} \end{aligned}$$

From the previous list, f^{10} *is* 11*-Eisenstein and* f *is dynamically irreducible over* $\mathbb{Q}$*.*

Example 3.29. *Consider the following polynomial in* $\mathbb{Q}[x]$:

$f(x) = a(x+c)^{p^m} + b$ *where* p *is a prime,* $m \geq 1$, $\nu_p(a) = 0$, $\nu_p(b) = 1$ *and* $\nu_p(c) \geq 0$

Note that $f(x-c)$ *is* p*-Eisenstein and, by Corollary 3.23,* f *is dynamically irreducible over* $\mathbb{Q}$.

Chapter 4

Pure Polynomials

4.1 Pure Polynomials

Throughout this Chapter, we use p to denote a rational prime. In general, a p-Eisenstein polynomial is an example of a p^r-pure polynomial. In this chapter, we study the dynamical behavior of p^r-pure polynomials. To do so, we first introduce the concept of Newton polygons.

Definition 4.1. *[12, Section 1.1] A subset S of a plane is called convex if and only if for any points $P, Q \in S$, the line segment $\overline{PQ}$ is totally contained in S. The* ***convex hull*** *of a set S is the smallest convex set that contains S. In other words, it is the intersection of all convex sets containing S.*

Assuming a 2-dimensional space, we can partition the convex hull to an upper and lower convex hulls defined as follows:

Definition 4.2. *[12, p.6] Let $P_1 = (x_1, y_1), \dots, P_k = (x_k, y_k)$ be the convex hull of some set S such that $x_1 \leq \dots \leq x_k$. Extend a line from P_1 and rotate it counterclockwise (clockwise) until it passes through another point in the convex hull. Call this second point P_{i_2}. Repeat the same process with P_{i_2} until you reach P_k. The subset of the convex hull $P_1, P_{i_2}, \dots, P_{i_j} = P_k$ is the lower (upper) convex hull of S.*

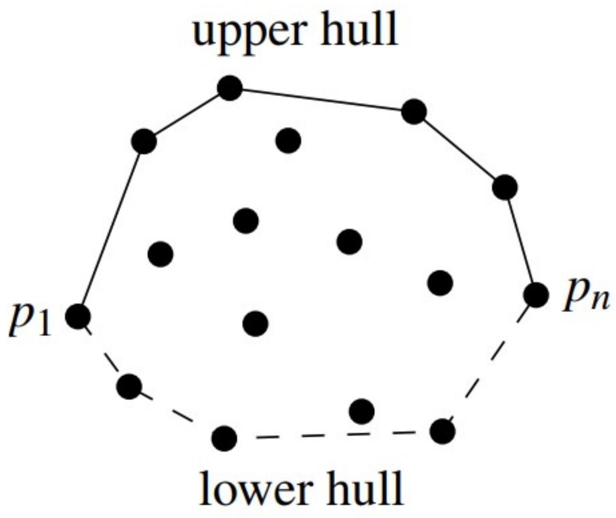


Figure 4.1 The upper and lower convex hull [12, p.6]

Definition 4.3. *[30, Section 2.2.1] Let $f(x) = a_d x^d + \ldots + a_0 \in \mathbb{Q}[x]$ with $a_d a_0 \neq 0$. For a prime p, suppose $\alpha_i = \nu_p(a_i)$. The **Newton Polygon of f with respect to p** is constructed as follows:*

(a) Define $S := \{(0, \alpha_d), \ldots, (d-i, \alpha_i), \ldots, (d, \alpha_0)\}$.

(b) Consider the lower convex hull of S to be $P_0 = (0, \alpha_d), \ldots, P_r = (d, \alpha_0)$.

(c) Construct a set of broken lines $P_0P_1, \ldots, P_{r-1}P_r$.

(d) Mark the lattice points (points with integer coordinates) on the broken lines $P_0 = Q_0, \ldots, P_r = Q_{r+s}$. They are called the vertices of the Newton polygon.

(e) The broken lines joining the vertices $Q_0Q_1, \ldots, Q_{r+s-1}Q_{r+s}$ are the sides of the Newton polygon.

Consider the following example:

Example 4.4. *Let*

$$f(x) = x^5 + 6x^4 + 2x^3 - 4x^2 + 40x + 32$$

If we consider the Newton polygon of f with respect to 2, we should write the 2-adic valuations of the coefficients. Thus, we write f as

$$f(x) = \mathbf{2^0} x^5 + \mathbf{2^1} 3x^4 + \mathbf{2^1} x^3 - \mathbf{2^2} x^2 + \mathbf{2^3} \cdot 5x + \mathbf{2^5}$$

First, we should construct the set S from the coefficients of f

$$S = \{(0,0),(1,1),(1,2),(2,3),(3,4),(5,5)\}$$

Finally, we should plot the set S and sketch the Newton polygon of f

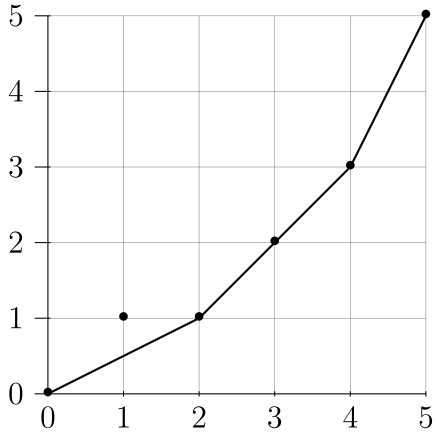
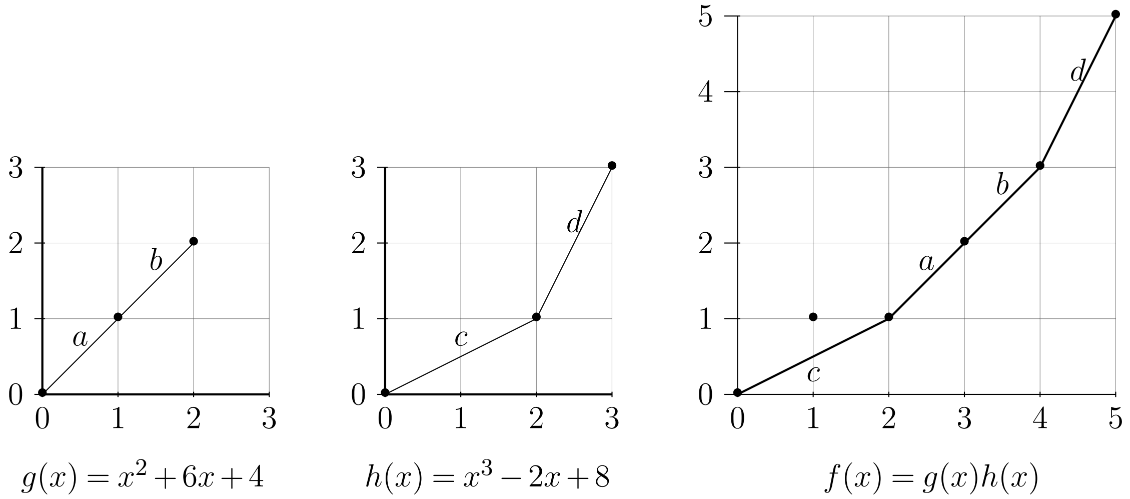


Figure 4.2 Newton Polygon of $f(x)$

Notice that f is reducible as

$$x^5 + 6x^4 + 2x^3 - 4x^2 + 40x + 32 = (x^2 + 6x + 4)(x^3 - 2x + 8)$$

Call $g(x) = x^2 + 6x + 4$ and $h(x) = x^3 - 2x + 8$. If we consider the Newton polygons of g and h with respect to 2 and mark the sides, we notice the sides of the Newton polygon of f are composed of the sides of g and h ordered ascendingly by slope.



$g(x) = x^2 + 6x + 4$ $h(x) = x^3 - 2x + 8$ $f(x) = g(x)h(x)$

Figure 4.3 Newton polygons of $g(x)$ and $h(x)$ compared to $g(x)h(x)$

In fact, the previous example is an application of Dumas theorem [15] which is presented below.

Proposition 4.5. *[14] Let f, g and h be polynomials in $\mathbb{Z}[x]$ such that $f = g \times h$ and $g(0)h(0) \neq 0$. The Newton polygon of f is composed of the polygons of g and h in such way that the sides are ordered according to increasing slopes.*

Proof. Refer to [30, Theorem 2.2.1]. □

Similar to the case of the polynomial g in Example 4.4, we shall focus on polynomials whose Newton polygon is one line.

Definition 4.6. *Let $f(x) = a_d x^d + a_{d-1}x^{d-1} + \ldots + a_0 \in \mathbb{Q}[x]$. Suppose there exists a prime p and a positive integer r such that:*

(a) $\nu_p(a_d) = 0$

(b) $\nu_p(a_0) = r$

(c) the Newton polygon of f with respect to p is exactly one line joining $(0,0)$ and (d,r)

Then, f is said to be ***p^r-pure****.*

Let $f(x) = a_d x^d + \ldots + a_0$ be a p^r-pure polynomial of degree d. By the previous Definition, the Newton polygon of f is precisely the line ℓ joining $(0,0)$ and (d,r). Now, consider a point $P = (d-i, \nu_p(a_i))$ for some $0 < i < d$. If P lies on ℓ, then, $\frac{\nu_p(a_i)}{d-i} = \frac{r}{d}$. By Definition 4.3, if P is not on ℓ, then, it has to be above it else ℓ does not include the lower convex hull of the set S in Definition 4.3. Geometrically, if we choose a point $Q = (d-i, y_0)$ on the line ℓ, then, $\nu_p(a_i) \geq y_0$ which implies

$$\frac{\nu_p(a_i)}{d-i} \geq \frac{y_0}{d-i} = \frac{r}{d}$$

In fact, the previous inequality is an alternative to condition (c) in Definition 4.6.

Definition 4.7. *[21] If $f(x) = a_d x^d + a_{d-1}x^{d-1} + \ldots + a_0 \in \mathbb{Q}[x]$ is* ***p^r-pure*** *for some prime p and some $r > 0$, then, it satisfies the following:*

(a) $\nu_p(a_d) = 0$

(b) $\nu_p(a_0) = r$

(c) $\frac{\nu_p(a_i)}{d-i} \geq \frac{r}{d}$ *for all* $1 \leq i \leq d-1$

Despite the fact that a p-Eisenstein polynomial is an example of a pure polynomial, pure polynomials are not necessarily irreducible; consider the following example.

Example 4.8. *The polynomial $f(x) = x^4 + 4 = (x^2 - 2x + 2)(x^2 + 2x + 2)$ is 2^2-pure but reducible over $\mathbb{Q}$.*

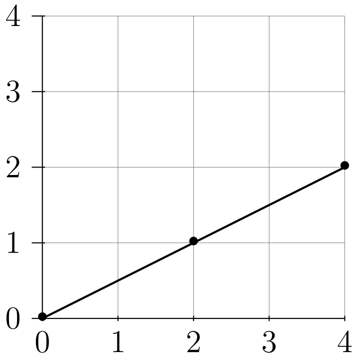


Figure 4.4 The polynomial $f(x)$ is 2^2-pure but reducible over $\mathbb{Q}$.

Nevertheless, a pure polynomial in $\mathbb{Q}[x]$ satisfying the Dumas criterion is irreducible over $\mathbb{Q}$.

Definition 4.9. *[15] Let $f(x) = a_d x^d + a_{d-1}x^{d-1} + \ldots + a_0 \in \mathbb{Q}[x]$ is called **p^r-Dumas** if there exists a prime p and a positive integer r such that:*

(a) $\nu_p(a_d) = 0$*,*

(b) $\nu_p(a_0) = r$*,*

(c) $\frac{\nu_p(a_i)}{d-i} \geq \frac{r}{d}$ *for* $1 \leq i \leq d-1$*,*

(d) $\gcd(r,d) = 1$*.*

Moreover, $f(x)$ is irreducible over $\mathbb{Q}$.

In some sources, condition (c) in the previous definition is written as a strict inequality. Nevertheless, if $\frac{\nu_p(a_i)}{d-i} = \frac{r}{d}$ for some $1 \leq i \leq d-1$, then, $\gcd(r,d) > 1$. Thus, the equality in the condition is superfluous but it was included to tone with Definition 4.7. Next, observe that the Eisenstein criterion is a special case of the Dumas criterion with $r = 1$. For p-Eisenstein polynomials, one can notice that all the iterates of a p-Eisenstein polynomial are p-Eisenstein. In addition, one has following property:

Proposition 4.10. *Let $g, f \in \mathbb{Q}[x]$. If g is p-Eisenstein for some prime p and f is p-type, then, $g \circ f$ is p-Eisenstein.*

Proof. Let g be a p-Eisenstein and f be a p-type polynomial. Since both f and g are both p-type polynomials, then, $f \circ g$ is p-type. It is enought to show that

$\nu_p(f(g(0))) = 1$ to conclude that $f \circ g$ is p-Eisenstein. By Lemma 3.8, it follows that $\nu_p(f(g(0))) = 1$ and $f \circ g$ is p-Eisenstein. □

Next, we generalize these two facts for p^r-pure polynomials. Nevertheless, some preparation is needed. The following Lemma is a generalization of Lemma 3.8.

Lemma 4.11. *Suppose f is a p^r-pure polynomial of degree d and let $c \in \mathbb{Q}$ such that $\nu_p(c) = s > \frac{r}{d}$, then, $\nu_p(f(0)) = r$.*

Proof. Suppose $f(x) = a_d x^d + \ldots + a_0$ is a p^r-pure polynomial. Assume that $\nu_p(c) = s > \frac{r}{d}$. Moreover, $f(c) = a_d (c)^d + \ldots + a_i (c)^i + \ldots + a_0$ for some $0 < i < d$. We have $\nu_p(a_d c^d) = ds > d(\frac{r}{d}) = r$. Also, $\nu_p(a_i c^i) = \nu_p(a_i) + is$. Since, f is p^r-pure, then, $\nu_p(a_i) + is > (d-i)\frac{r}{d} + i\frac{r}{d} = r$. Given, $\nu_p(a_0) = r$, it follows that $\nu_p(f(c)) = r$ □

Next, we extend Proposition 4.10 to p^r-pure polynomials in the following theorem.

Theorem 4.12. *Let $f, g \in \mathbb{Q}[x]$. Suppose f is a p^r-pure polynomial of degree $d > 1$ and $g(x) \equiv bx^e \bmod p^s$ for some $e \geq 1$ such that $\nu_p(b) = 0$ and $s > \frac{r}{d}$. Then, $f \circ g$ is p^r-pure.*

Proof. Let $f(x) = a_d x^d + \ldots + a_i x^i + \ldots + a_0$ be p^r-pure and $g(x) = bx^e + p^s h(x)$ such that $\nu_p(h) \geq 0$, it degree is less than e and $s\frac{r}{d}$. To show $f \circ g$ is p^r-pure, we first need to show that all the monomials in the expansion of $a_i(bx^e + p^s h(x))^i$ for all $0 \leq i \leq d$ satisfy Definition 4.9. First, we prove that condition (c) in Definition 4.9 is satisfied; neglecting the coefficients with zero p-adic valuation, a monomial in the expansion of $a_d(bx^e + p^s(h(x))^d$ is of the form

$$a_d (x^e)^{d-k} (p^s h(x))^k = cx^{e(d-k)+k\alpha} = cx^{de-ek+k\alpha}$$

such that $\nu_p(c) \geq ks > k\frac{r}{d}$ and $0 \leq \alpha \leq e-1$ for some $0 < k \leq d$. If the monomial doesn't satisfy the condition then,

$$\frac{s}{e-\alpha} = \frac{ks}{de-de+ek-k\alpha} \leq \frac{\nu_p(c)}{de-de+ek-k\alpha} < \frac{r}{de}$$

Given $s > \frac{r}{d}$, we deduce the following inequality.

$$\frac{\frac{r}{d}}{e-\alpha} < \frac{s}{e-\alpha} < \frac{r}{de}$$

Simplifying, we conclude the following inequality.

$$\frac{1}{e-\alpha} < \frac{1}{e}$$

Yet, this implies that $\alpha < 0$ which is a contradiction. For the second type namely $a_i(bx^e + p^s h(x))^i$ for $0 < i < d$, a monomial in the expansion is of the form

$$(bx^e)^{i-k}(p^s h(x))^k = a_i t x^{e(i-k)+k\alpha} = a_i t x^{ei-ek+k\alpha}$$

such that $\nu_p(a_i t) = \nu_p(a_i) + \nu_p(t) \geq \nu_p(a_i) + ks$ for some $0 \leq k \leq i < d$ and $0 \leq \alpha \leq e-1$. Again, if the monomial doesn't satisfy the condition, then,

$$\frac{\nu_p(a_i) + \nu_p(t)}{de - ei + ek - k\alpha} < \frac{r}{de}.$$

Since f is p^r-pure, i.e., $\frac{\nu_p(a_i)}{d-i} \geq \frac{r}{d}$ and $s > \frac{r}{d}$, we get the following inequality:

$$\frac{(d-i)\frac{r}{d} + k\frac{r}{d}}{de - ei + ek - k\alpha} < \frac{\nu_p(a_i) + ks}{de - ei + ek - k\alpha} \leq \frac{\nu_p(a_i) + \nu_p(t)}{de - ei + ek - k\alpha} < \frac{r}{de}$$

Simplifying, we get

$$\frac{(d-i) + k}{de - ei + ek - k\alpha} < \frac{1}{e}$$

Cross multiplication and simplification yield the same contradiction

$$de - ei + ek < de - ei + ek - k\alpha \text{ which implies } \alpha < 0$$

Next, it is obvious to see that the leading coefficient of $f \circ g$ has zero p-adic valuation. Finally, by Lemma 4.11, as $\nu_p(g(0)) \geq s > \frac{r}{d}$, then $\nu_p(f(g(0)) = r$ and thus $f \circ g$ is p^r-pure. □

In particular, If $d > r$ in the previous Theorem, we get the following interesting corollary:

Corollary 4.13. *Let f be a p^r-pure polynomial of degree $d > r$, If g is a p-type polynomial, then, $f \circ g$ is p^r-pure.*

Proof. This is a special case of Theorem 4.12 with $s \geq 1 > \frac{r}{d}$. □

In fact, if g in Theorem 4.12 is p^r-pure, we conclude the following.

Theorem 4.14. *If $f, g \in \mathbb{Q}[x]$ are p^r-pure of positive degrees, then, $f \circ g$ is p^r-pure.*

Proof. Let $f(x) = a_d x^d + a_{d-1}x^{d-1} + \ldots + a_0$ and $g(x) = b_e x^e + b_{e-1}x^{e-1} + \ldots + b_0$ be two p^r-pure polynomials for some positive integers d, e, r and a prime p. We should show that

$$f(g(x)) = a_d(b_e x^e + b_{e-1}x^{e-1} + \ldots + b_0)^d + \ldots + a_i(b_e x^e + b_{e-1}x^{e-1} + \ldots + b_0)^i + \ldots + a_0$$

is p^r-pure, in other words, $f \circ g$ should satisfy Definition 4.7. To check condition (c) in the Definition, we classify the monomials of $f \circ g$ into two types: monomials from the expansion of $a_d(b_e x^e + b_{e-1}x^{e-1} + \ldots + b_0)^d$ and $a_t(b_e x^e + b_{e-1}x^{e-1} + \ldots + b_0)^t$ for any $0 \le t \le d$. For the first type, suppose

$$\prod_{i=1}^{e} \left(b_i x^i\right)^{q_i}$$

is a monomial in the expansion of $a_d\left(b_e x^e + b_{e-1}x^{e-1} + \ldots + b_0\right)^d$ such that: its degree is $d \le \sum q_i i < de$, the sum of the exponents is $\sum q_i = d$, the p-adic valuation of the coefficients $\nu_p(b_i) = \alpha_i \ge \frac{r(e-i)}{e}$ for every $0 < i < e$ and the p-adic valuation of the coefficient of the monomial is $\nu_p\left(\prod_{i=1}^{e} {b_i}^{q_i}\right) = \sum q_i \alpha_i$. Note that we are excluding the exponents of b_0 else the p-adic valuation of the monomial will be at least r and it will trivially satisfy the condition (c) in Definition 4.7. We should show that

$$\frac{\sum q_i \alpha_i}{de - \sum q_i i} \ge \frac{r}{de}.$$

Indeed, consider the following inequality:

$$\sum q_i \alpha_i \ge \frac{r}{e} \sum q_i (e-i) = \frac{r}{e}(e \sum q_i - \sum q_i i) = \frac{r}{d}(de - \sum q_i i) > \frac{r}{de}(de - \sum q_i i)$$

For the second type, any monomial in the expansion of $a_t(b_e x^e + b_{e-1}x^{e-1} + \ldots + b_0)^t$ is of the form

$$a_t \prod_{i=1}^{e} (b_i x^i)^{q_i}$$

such that the degree is $t \le \sum q_i i \le et$, the sum of the exponents $\sum q_i = t$, the p-adic valuation of the coefficient is $\nu_p(a_t) + \sum q_i \alpha_i$ given $\nu_p(a_t) \ge \frac{r}{d}(d-t)$ and $\alpha_i \ge \frac{r}{e}(e-i)$. Again, we need to show that

$$\frac{\nu_p(a_t) + \sum q_i \alpha_i}{de - \sum q_i i} \ge \frac{r}{de}.$$

Which implies that

$$\nu_p(a_t) + \sum q_i \alpha_i \ge \frac{r}{d}(d-t) + \frac{r}{e} \sum q_i (e-i) = \frac{r}{d}(d-t) + \frac{r}{e}(e \sum q_i - \sum q_i i).$$

If this monomial does not satisfy condition (c), then,

$$\frac{r}{d}(d-t) + rt - \frac{r}{e}(\sum q_i i) = \frac{r}{d}(d-t) + \frac{r}{e}(e \sum q_i - \sum q_i i) \le \nu_p(a_t) + \sum q_i \alpha_i < \frac{r}{de}(de - \sum q_i i).$$

Taking the leftmost and rightmost part of the inequality, we have

$$\frac{r}{d}(d-t)+rt-\frac{r}{e}(\sum q_i i) < \frac{r}{de}(de-\sum q_i i).$$

Dividing by r, the inequality becomes

$$\frac{1}{d}(d-t)+t-\frac{1}{e}(\sum q_i i) < \frac{1}{de}(de-\sum q_i i).$$

After expansion, we conclude

$$1-\frac{t}{d}+t-\frac{1}{e}\sum q_i i < 1-\frac{1}{de}\sum q_i i \text{ which implies } -\frac{t}{d}+t < (\frac{1}{e}-\frac{1}{de})\sum q_i i.$$

Finally, we reach the following contradiction:

$$t(1-\frac{1}{d}) < \frac{1}{e}(1-\frac{1}{d})\sum q_i i \text{ which means that } et < \sum q_i i.$$

So, $f \circ g$ satisfies condition (c). Finally, given g is p^r-pure, then, $\nu_p(g(0)) = r$. By Lemma 4.11, as $r > \frac{r}{d}$, then, $\nu_p(f(g(0))) = r$ and the statement follows. □

To understand the difference between Theorem 4.12 and Theorem 4.14, consider the following example.

Example 4.15. *The following polynomials:*

$$f(x) = x^2+32,$$
$$g(x) = x^4+4x^3+32.$$

are both 2^5*-Dumas and*

$$f(g(x)) = x^8+8x^7+16x^6+64x^4+256x^3+1056. \equiv x^8+8x^7+16x^6 \pmod{2^5}$$

is 2^5*-Dumas too as* $\frac{\nu_2(8)}{8-7} = 3 > \frac{\nu_2(1056)}{8} = \frac{5}{8}$ *and* $\frac{\nu_2(16)}{8-6} = 2 > \frac{5}{8}$*. This is a direct application of Theorem 4.14. However, if we try to apply Theorem 4.12, then,* $d = \deg(f) = 2$*,* $r = 5$*, so,* $s \geq 3 = \left\lceil \frac{5}{2} \right\rceil$*. But,* $g(x) \equiv x^4+4x^3 \not\equiv x^4 \pmod{2^3}$*. Thus, Theorem 4.12 fails to prove* $f \circ g$ *is* 2^5*-pure in this case. Now, if we introduce the polynomial*

$$h(x) = x^4+8.$$

We have $h(x) \equiv x^4 \pmod{2^3}$ *and, by Theorem 4.12,* $f \circ h$ *is* 2^5*-Dumas. To check, we have*

$$f(h(x)) = x^4+16x^2+96$$

and $\nu_2(f(h(0))) = \nu_2(96) = 5$ *and* $\frac{\nu_2(16)}{4-2} = 2 > \frac{5}{4}$*. Nevertheless, h is not* 2^5*-pure and Theorem 4.14 can not be applied.*

The following corollary follows from Theorem 4.14 by restricting $f = g$.

Corollary 4.16. *If* f *is a* p^r*-pure polynomial, then,* f^n *is* p^r*-pure for all* $n \geq 1$.

4.2 Applications of Theorems 4.12 and 4.14

In this section, we will discuss several applications of Theorems 4.12 and 4.14. In the previous section, we introduced Dumas polynomials as a class of irreducible pure polynomials. Given Theorem 4.14, we deduce the following fact.

Corollary 4.17. *Let* f *and* g *be* p^r*-Dumas polynomials in* $\mathbb{Q}[x]$ *for some prime* p*, then,* $f \circ g$ *is* p^r*-Dumas. Moreover, a* p^r*-Dumas polynomial is dynamically irreducible over* $\mathbb{Q}$.

Proof. If f and g are p^r-pure, then by Theorem 4.14, $f \circ g$ is p^r-pure. Let the degrees of f and g be d and e respectively. If f and g are p^r-Dumas, then, $\gcd(r,d) = \gcd(r,e) = \gcd(r,de) = 1$. This implies that $f \circ g$ is p^r-Dumas. Inductively, it follows that f^n is p^r-Dumas for all $n \geq 1$ and hence dynamically irreducible by Definition 4.9 □

In what follows, we introduce a subclass of Dumas polynomials.

Definition 4.18. *[2, Definition 5] Let* $f(x) = a_d x^d + \ldots + a_0 \in \mathbb{Q}[x]$*. We say* f *is* ***p^r-Eisenstein*** *if there is a prime* p *and an integer* $r \geq 1$ *such that*

(a) $\nu_p(a_d) = 0$

(b) $\nu_p(a_i) \geq r$ *for all* $1 \leq i \leq d-1$

(c) $\nu_p(a_0) = r$

(d) $\gcd(r,d) = 1$

Note that a p-Eisenstein polynomial is a p^r-Eisenstein with $r = 1$. Ali [2, Corollary 1] proved that p^r-Eisenstein polynomials are dynamically irreducible over $\mathbb{Q}$. In fact, Corollary 4.17 is a generalization of this result.

Example 4.19. *Consider the following trinomial in* $\mathbb{Q}[x]$

$$f(x) = x^d + ax^{d-1} + p^{2^k}; \ d \text{ is odd, } k \geq 0 \text{ and } \nu_p(a) > \frac{2^k}{d}$$

Note that $\frac{\nu_p(a)}{d-(d-1)} = \nu_p(a) > \frac{2^k}{d}$ *and* $\gcd(2^k, d) = 1$. *In this case,* f *is* p^{2^k}*-Dumas and thus dynamically irreducible over* $\mathbb{Q}$.

Corollary 4.20. *Let* g *be a* p^r*-Dumas of degree* d *and* $f(x) \equiv ax^e \pmod{p^s}$ *be a* p*-type polynomial for some* $s > \frac{r}{d}$. *If* $\gcd(r,e) = 1$, *then,* $g^n \circ f^m$ *is irreducible for all* $n, m \geq 1$. *In particular,* g^n *is* f*-stable for any* $n \geq 1$.

Proof. By Theorem 4.17, g^n is p^r-Dumas for any $n \geq 1$. Also, $f^m(x) \equiv bx^{e^m} \pmod{p^s}$ is p-type for some b with $\nu_p(b) = 0$. Since $\gcd(r,e) = 1$, therefore, $f^n \circ g^m$ is p^r-Dumas by Theorem 4.12. □

Consider the following example.

Example 4.21. *Let*

$$\begin{aligned} f(x) &= x^{17} + 27x^{12} + 27x^{10} + 162x^7 + 729x^5 + 4374. \\ &= (x^7 + 27)(x^5 + 9)(x^5 + 18) \end{aligned}$$

Note that $g_1(x) = x^7 + 27$ *is* 3^3*-Dumas with* $\frac{r_1}{d_1} = \frac{3}{7} < 1$, $g_2(x) = x^5 + 9$ *is* 3^2*-Dumas with* $\frac{r_2}{d_2} = \frac{2}{5} < 1$ *and* $g_3(x) = x^5 + 18$ *is* 3^2*-Dumas with* $\frac{r_3}{d_3} = \frac{2}{5} < 1$. *This implies that* $s_1, s_2, s_3 \geq 1$. *Since* $f(x) \equiv x^{17} \pmod{3^1}$ *and* $\gcd(17,7) = \gcd(17,5) = 1$. *By the previous Corollary,* g_1, g_2 *and* g_3 *are* f*-stable. In other words, for any* $n \geq 1$, *the number of irreducible factors of* f^n *is exactly* 3.

The previous example motivates the following corollary.

Corollary 4.22. *Let* $f(x) \equiv ax^e \pmod{p^s}$ *be a* p*-type polynomial of degree* e, $s \geq 1$. *Suppose for any* $n \geq 1$ *and some* $t \geq 2$, *the iterate* $f^n(x) = g_1(x)g_2(x) \cdot \ldots \cdot g_t(x)$ *of degrees* $d_1, d_2 \ldots, d_t \geq 1$. *If for all* $2 \leq i \leq t$, *the following conditions apply:*

(a) g_i *is* p^{r_i}*-Dumas for some* $r_i \geq 1$,

(b) gcd$(d_i, e) = 1$,

(c) $s > \frac{r_i}{d_i}$.

Then, $g_1, g_2, \ldots, g_t$ *are all* f*-stable. In fact, for any* $N \geq n$, *the number of irreducible factors of* f^N *is exactly* t. *Moreover, the irreducible factors of* f^N *are all Dumas polynomials.*

Proof. Let $f(x) \equiv a_e x^e \pmod{p}$ be a p-type polynomial. Assume $g = g_1$ with degree $d = d_1$ is a p^r-Dumas polynomial such that it is an irreducible factor of an iterate f^n with $\gcd(d,e) = 1$ and $s > \frac{r}{d}$. By Corollary 4.17, $g \circ f^k$ is p^r-Dumas for any $k \geq 1$. In general, if $f^n(x) = g_1(x) \cdot g_2(x) \cdot \ldots \cdot g_t(x)$ and every g_i for $1 \leq i \leq t$ is p^{r_i}-Dumas, then, for any $N \geq n$, we conclude $f^N = f^n(f^{N-n}) = g_1\left(f^{N-n}\right) \cdot g_2\left(f^{N-n}\right) \cdot \ldots \cdot g_t\left(f^{N-n}\right)$. By the previous argument, the polynomials $g_1\left(f^{N-n}\right), g_2\left(f^{N-n}\right), \ldots, g_t\left(f^{N-n}\right)$ are p^{r_i}-Dumas and the result follows. □

If the condition "$s > \frac{r}{d}$" in Corollary 4.20 is dropped, we deduce a more general corollary.

Corollary 4.23. *Let g be a p^r-Dumas polynomial of degree d and $f(x) \equiv ax^e \pmod{p^s}$ be a p-type polynomial of degree e such that $\gcd(r,e) = 1$. Then, there exists an integer $n \geq 1$ such that for all $N \geq n$ it is true that $g^N \circ f^k$ is irreducible for all $k \geq 1$. In particular, g^n is f-stable for all $N \geq n$.*

Proof. Let $N = \min\{n : s > \frac{r}{d^n}\}$. For any $n \geq N$, g^n is p^r-Dumas of degree d^n by Corollary 4.17 and $s > \frac{r}{d^N} \geq \frac{r}{d^n}$ and also $\nu_p(g^k(x) - b_k x^{e^k}) \geq s$ where b_k is the leading coefficient of g^k. So, by Corollary 4.12, $g^n \circ f^m$ is p^r-Dumas for all $n \geq N$. □

In the previous corollary, one can not be sure of the irreducibility of $g^n \circ f$ whenever $n < N$. Consider the following example:

Example 4.24. *Consider the following polynomials*

$$g(x) = x^2 + 27 \text{ is } 3^3\text{-Dumas}$$
$$f(x) = x^2 + 3x + 3 \text{ is } 3\text{-type}$$

Based on corollary 4.20, $r = 3$ and $d = 2$ thus $\frac{r}{d} = \frac{3}{2}$. Then, $s \geq 2 > \frac{3}{2}$ but $f(x) \not\equiv x^2 \pmod{3^2}$. So, we need to use Corollary 4.23 with $s = 1$ to find $N = \min\{n : 1 > \frac{3}{2^n}\} = 2$. So, we expect $g^n \circ f$ to be 3^3-Dumas for all $n \geq 2$. Indeed,

$$(g^2 \circ f)(x) = x^8 + 12x^7 + 66x^6 + 54x^5 + 27x^4 + 27x^2 + 27$$

is 27-Dumas and by Corollary 4.17, $g^n \circ f$ is 27-Dumas. Yet,

$$g \circ f = \left(x^2 + 3\right)\left(x^2 + 6x + 12\right) \text{ is reducible}$$

So far, we have discussed the applications of Theorems 4.12 and 4.14 to Dumas polynomials. We have already mentioned that pure polynomials are not always irreducible, yet, can we find an upper bound for the number of irreducible factors of a pure polynomial? In fact, the answer is in the following proposition.

Proposition 4.25. *[21, Theorem 1.2] Let f be a p^r-pure polynomial of degree d in $\mathbb{Q}[x]$. Then, f has at most $\gcd(d,r)$ irreducible factors over $\mathbb{Q}$ and each irreducible factor has degree which is at least $\frac{d}{\gcd(d,r)}$*

Dynamically, we can conclude the following about the iterations of a pure polynomial.

Theorem 4.26. *Suppose f is a p^r-pure. Then, for any $n \geq 1$, the iterate f^n has most $\gcd(d^n,r)$ irreducible factors over $\mathbb{Q}$ and each irreducible factor has degree which is at least $\frac{d^n}{\gcd(d^n,r)}$. Moreover, f is eventually stable over $\mathbb{Q}$.*

Proof. Let f be a p^r-pure polynomial of degree d. For some $n \geq 1$, consider an iterate f^n of degree d^n. By Corollary 4.16, the iterate f^n is p^r-pure and by Proposition 4.25, has most $\gcd(d^n,r)$ irreducible factors over $\mathbb{Q}$ and each irreducible factor has degree which is at least $\frac{d^n}{\gcd(d^n,r)}$. Moreover, let $c_n = \gcd(d^n,r)$ and define k_n to be the number of irreducible factors of f^n. Obseve that the set $\{c_1,\ldots,c_n,\ldots\}$ is finite as there must exist an $N \geq 1$ such that for all $n \geq N$, it is true that $\gcd(d^n,r) = c_n = c_N = \gcd(d^N,r)$. In this case, $k_n \leq c_n \leq c_N$ for all $n \geq 1$ and thus f is eventually stable. □

In [18], Brown and Micheli introduced a set S of irreducible quadratic polynomials over a finite field. This set S induced another set C composed of arbitrary compositions of polynomials in S. If all the elements of C are irreducible, then S is said to be dynamically irreducible. In $\mathbb{Q}[x]$, one can deduce the following definition.

Definition 4.27. *Let I be a set of polynomials in $\mathbb{Q}[x]$ with positive degrees. We say I is **a dynamically irreducible set** in $\mathbb{Q}[x]$ if any polynomial formed by composition of polynomials in I is irreducible over $\mathbb{Q}$.*

So far, we are focusing on the dynamically irreducible set of the form $I(f) = \{f,\ldots,f^n,\ldots\}$. The set p-Eisenstein polynomials for a particular prime p is another example of a dynamically irreducible set. In light of our results, we display the following example.

Example 4.28. *Let p be a prime. Define*

$$E(p) := \{f \in \mathbb{Q}[x] : \ f \text{ is } p\text{-Eisenstein and } p \nmid \deg(f)\}.$$

The set $E(p)$ is dynamically irreducible over $\mathbb{Q}$. Also, define

$$D(p,q) := \{f \in \mathbb{Q}[x] : f \text{ is } p^{q^k}\text{-Dumas such that } \deg(f) > q^k \text{ for a prime } q \text{ and } k \geq 1\}$$

In fact, $D(p,q)$ is a dynamically irreducible set because if f and g are p^{q^k}-Dumas and p^{q^m}-Dumas respectively, Corollary 4.13 ensures that the composition $f \circ g$ $(g \circ f)$ is of degree not divisible by q and is p^{q^k} (p^{q^m})-Dumas. Moreover, the set $E(p) \cup D(p,q)$ is also dynamically irreducible because if $f \in D(p,q)$ $(E(p))$ and $g \in E(p)$ $(D(p,q))$, then, $f \circ g \in D(p,q)$ $(E(p))$ by Corollary 4.13 (Proposition 4.10).

4.3 Eventually Pure Polynomials

In this section, we focus on eventually p-type polynomials, In particular, a polynomial which is not p-type but one of its iterates is p-type. In Chapter 3, we discussed Eventually p-Eisenstein polynomials. In this section, our aim is to extend this discussion to include p^r-pure polynomials. First, Consider the following example.

Example 4.29. *The polynomial*

$$f(x) = -x^3 - \frac{39x^2}{7} - \frac{72x}{7} - \frac{31}{35}$$

is not p-type for any prime p. Yet,

$$\begin{aligned} f^2(x) = x^9 + \frac{54x^8}{7} + \frac{1287x^7}{49} + \frac{56607x^6}{1715} - \frac{53919x^5}{1715} - \frac{36864x^4}{245} \\ - \frac{696429x^3}{8575} + \frac{1465479x^2}{8575} + \frac{356184x}{1715} - \frac{1090557}{6125} \end{aligned}$$

is 3^3-pure. As $\nu_p\left(\frac{1090557}{6125}\right) = 3$ and $\frac{r}{d} = \frac{3}{9} = \frac{1}{3}$. To check condition (c) in Definition 4.7, we notice that

$$f^2(x) \equiv x^9 + 18x^7 + 3x^6 + 9x^4 + 9x^3 \pmod{3^3}$$

In fact, it is enough to check the condition for the coefficients with a 3-adic valuation less than 3. We have $\frac{\nu_3(18)}{9-7} = 1 \geq \frac{1}{3}$, $\frac{\nu_3(3)}{9-6} = \frac{1}{3} \geq \frac{1}{3}$, $\frac{\nu_3(9)}{9-4} = \frac{2}{5} \geq \frac{1}{3}$, $\frac{\nu_3(9)}{9-3} = \frac{1}{3} \geq \frac{1}{3}$. and thus f^2 is 3^3-pure.

The previous example motivates the following definition.

Definition 4.30. *Let p be a prime and r be a positive integer. A polynomial $f \in \mathbb{Q}[x]$ of degree d is said to be* ***eventually $\mathbf{p^r}$-pure*** *if f^n is p^r-pure for some iteration n. In particular, f is eventually p^r-Dumas if f^n is p^r-Dumas.*

Corollary 4.31. *An eventually p^r-pure polynomial is eventually stable. In particular, an eventually p^r-Dumas polynomial is dynamically irreducible.*

Proof. Suppose f is eventually p^r-pure for some prime and $r \geq 1$. In other words, f^n is p^r-pure for some $n \geq 1$. If $n = 1$, the result follows from Theorem 4.26. Whenever $n > 1$, the iterates f^{tn} are p^r-pure for all $t \geq 1$ by Corollary. 4.16. Thus by Theorem 4.26, the number of irreducible factors for the iterates f^{nt} is less than some $c \geq 1$ for any $t \geq 1$. Thus f is eventually stable. In particular, if f^n is p^r-Dumas, then, $c = 1$ and f is dynamically irreducible over $\mathbb{Q}$. □

A p^r-pure is also p-type, so, an eventually p^r-pure should satisfy Theorem 2.10. Furthermore, an eventually p-Eisenstein polynomial is exactly eventually p-pure. As a generalization of Theorem 3.22, one predicts a polynomial f to be eventually p^r-pure whenever its degree is p^m and $f(x+c)$ is p^r-pure for some $c \in \mathbb{Q}$ such that $\nu_2(c) \geq 1$. However, the following example shows that the previous guess is not always true.

Example 4.32. *For a polynomial*

$$f(x) = x^2 + 10x + 17,$$

its shift,

$$f(x-1) = x^2 + 8x + 8,$$

is 2^3-Dumas, but,

$$f^2(x) = (x^2 + 8x + 14)(x^2 + 12x + 34)$$

is not 2^3-Dumas because it is reducible.

In the previous example, the degree of f is $d = 2$, the prime is $p = 2$ and $r = 3$. In particular, $d = p^m \leq r$ for some $m \geq 1$. Nevertheless, we assume $d > r$ for the rest of this section. Our aim is to provide a complete characterization of eventually p^r-pure polynomials of degree $d > r$. First, we introduce the following proposition.

Proposition 4.33. *Let r be a positive integer and p be a prime. Suppose f, g are polynomials in $\mathbb{Q}[x]$ with degrees d and e respectively. If $f \circ g$ is p^r-pure polynomials for some $d < r$ and g is p-type, then, $f(x + g(0))$ is p^r-pure.*

Proof. Suppose $f \circ g$ is p^r-pure and g is p-type. Assume that $\deg(f) = d > r$. Let

$h(x) = f(x+g(0))$. By Lemma 2.9, h is p-type and $\nu_p(h(0)) = \nu_p(f(g(0)) = r$. So, we need to show that h satisfies condition (c) in Definition 4.7. Suppose $h(x) = a_d x^d + \ldots + a_0$ and $g(x) - g(0) = b_e x^e + \ldots + b_1 x$. First, assume that some $0 < k < d$ is the maximum positive integer such that a_k doesn't satisfy condition (c), i.e., $\frac{\nu_p(a_k)}{d-k} < \frac{r}{d}$. Given

$$h\left(g(x) - g(0)\right) = a_d(b_e x^e + \ldots + b_1 x)^d + \ldots + a_k(b_e x^e + \ldots + b_1 x)^k + \ldots + a_0,$$

the monomial $a_k x^{ek}$ doesn't satisfy condition (c) as $\frac{\nu_p(a_k)}{de-ek} < \frac{r}{de}$. Yet, when added with monomials of the same degree, the sum should satisfy the condition as $f \circ g$ is p^r-pure. Thus, there has to be other monomials in the expansion of $h(g(x) - g(0))$ of degree ek whose coefficients have p-adic valuation less than $\frac{(d-k)r}{d}$. For some $0 < j < k$, the monomials in the expansion of $a_j(b_e x^e + \ldots + b_1 x)^j$ have degree strictly less than ek. If $k < j < d$, then, a_j satisfies the condition (c). By Corollary 4.13 and since $g(x) - g(0)$ is p-type, all the monomials in the expansion of $a_j(b_e x^e + \ldots + b_1 x)^j$ should satisfy condition (c). Finally, for $j = d$ and given $\nu_p(a_d) = 0$, the monomials in the expansion of $a_d(b_e x^e + \ldots + b_1 x)^d$ satisfy the condition as outlined in the proof of Theorem 4.12 and stated in Corollary 4.13, so, $f(x+g(0))$ is p^r-pure. □

We are now ready to state and prove the main theorem of this section.

Theorem 4.34. *Let r be a positive integer and p be a prime. Suppose $f(x) = a_d x^d + \ldots + a_0 \in \mathbb{Q}[x]$ is not p^r-pure and $d > r$. Then, $f(x)$ is eventually p^r-pure if and only if the following conditions hold.*

(a) $d = p^m$ for some $m \geq 1$,

(b) $f(x) \equiv a_d x^d + a_0 \pmod{p}$ such that $\nu_p(a_d) = \nu_p(a_0) = 0$,

(c) $f(x+c)$ is p^r-pure for some $c \in \mathbb{Q}$.

Moreover, the least integer $n > 1$ such that f^n is p^r-pure is determined by Theorem 2.10.

Proof. Suppose $f(x) = a_d x^d + \ldots + a_0$ is not p^r-pure but f^n is p^r-pure for some $n > 1$ and $d > r$. Then f satisfies Theorem 2.10, in other words, $d = p^m$ for some $m \geq 1$ and $f(x) \equiv a_d x^d + a_0 \pmod{p}$ such that $\nu_p(a_d) = \nu_p(a_0) = 0$. Since $f^n(x) = f\left(f^{n-1}(x)\right)$ is p^r-pure, therefore by Proposition 4.33, $f\left(x + f^{n-1}(0)\right)$ is p^r-pure. Conversely, suppose f satisfies conditions (a),(b) and (c) in the previous Theorem. Let $g(x) = f(x+c)$ be p^r-pure for some $c \in \mathbb{Q}$. By Theorem 2.10, there exists an iteration $n > 1$ such that f^n is p-type. Moreover, $f^n(x) = f\left(f^{n-1}(x)\right) = g\left(f^{n-1}(x) - c\right)$, so, $f^{n-1}(x) - c$ must be p-type as $g\left(f^{n-1}(x) - c\right)$ is p-type. By Proposition 4.13

as $d > r$, then, $f^n(x) = g\left(f^{n-1}(x) - c\right)$ is p^r-pure, in other words, f is eventually p^r-pure. □

Consider the following examples.

Example 4.35. *The polynomial*

$$\begin{aligned} f(x) &= x^8 + 8x^7 + 28x^6 + 56x^5 + 70x^4 + 56x^3 + 28x^2 + 8x + 5. \\ &= \left(x^4 + 4x^3 + 4x^2 + 1\right)\left(x^4 + 4x^3 + 8x^2 + 8x + 5\right). \end{aligned}$$

is reducible but not p^r-pure for any prime p as $\gcd(5, 8) = 1$. *However,*

$$f^2(x) \equiv x^{64} + 4 \pmod 8$$

Indeed, f^2 is 2^2-pure because

$$f(x-1) = x^8 + 4$$

is 2^2-pure too by Theorem 4.34. Moreover, as $\gcd(8, \nu_2(4)) = 2$, *the factors of f, namely $g(x) = x^4 + 4x^3 + 4x^2 + 1$ and $h(x) = x^4 + 4x^3 + 8x^2 + 8x + 5$ are f-stable by Theorem 4.26.*

Example 4.36. *The family of polynomials*

$$f(x) = (x + a)^{p^m} + b \in \mathbb{Q}[x];\ \nu_p(a) \geq 0 \textit{ and } 1 \leq \nu_p(b) \leq p^m \textit{ for some prime } p.$$

is eventually stable over $\mathbb{Q}$. If $\gcd(p^m, \nu_p(b)) = 1$, *then, f is dynamically irreducible. Otherwise, the number of irreducible factors of any iterate is at most* $\max\{\gcd(p^{nm}, \nu_p(b)) : n \geq 1\}$.

We extend Question 3.24 to the following.

Question 4.37. *If $f \in \mathbb{Z}[x]$ is eventually stable polynomial, then, is $f(x + c)$ eventually stable for all $c \in \mathbb{Z}$?*

The answer is No. Consider the following example.

Example 4.38. *The polynomial*

$$f(x) = x^2 + 8x + 12$$

is 2^2-pure as $\nu_2(12) = 2$ and $\frac{\nu_2(8)}{2-1} = 3 > 1$. By Proposition 4.25, If the number of irreducible factors of f^n is k_n, then, $k_n \leq 2$ for all $n \geq 1$. Thus, f is eventually *stable over $\mathbb{Q}$. However,*

$$f(x-3) = x^2 + 2x - 3$$

is not eventually stable by Example 1.16.

In the previous example, the degree d of f is equal to the 2-adic valuation of its constant coefficient, r. However, if $d > r$, we conclude the following corollary.

Corollary 4.39. *Let $f \in \mathbb{Z}[x]$ be a p^r-pure polynomial of degree p^m. The polynomial $f(x+c)$ is eventually stable for all $c \in \mathbb{Z}$. In particular, if f is p^r-Dumas, then, $f(x+c)$ is dynamically irreducible.*

Proof. The proof follows from Theorem 4.30. □

The previous corollary is an extension of Corollary 3.24. In addition, an extension of Corollary 3.23 is the following.

Corollary 4.40. *Let $f \in \mathbb{Q}[x]$ be a p^r-pure polynomial of degree p^m. The polynomial $f(x+c)$ is dynamically irreducible for all $c \in \mathbb{Q}$ with $\nu_p(c) \geq 0$. In particular, if f is p^r-Dumas, then, $f(x+c)$ is dynamically irreducible given $\nu_p(c) \geq 0$.*

Proof. The proof follows from Theorem 4.34. □

Next, An application of Theorem 4.30 and Corollary 4.17 is the following.

Corollary 4.41. *Let p be a prime. Suppose f, g are monic polynomials in $\mathbb{Q}[x]$ such that $\overline{g}$ is the reduction of g modulo p and $\deg(g) = \deg(\overline{g}) = e$. If f is eventually p^r-Dumas for some iteration $n \geq 1$, $\overline{g}$ is irreducible in $\mathbb{F}_p[x]$ and $\gcd(e, r) = 1$, then, $f^{kn} \circ g$ is irreducible in $\mathbb{Q}[x]$ for all $k \geq 1$. In addition, if $\overline{g}$ is dynamically irreducible in $\mathbb{F}_p[x]$, then, $f^{kn} \circ g^m$ is irreducible in $\mathbb{Q}[x]$ for all $k, m \geq 1$ and f^{kn} is g-stable for all $k \geq 1$ in $\mathbb{Q}[x]$.*

The proof of the previous Corollary depends on a special case of the generalized Schönemann polynomial discussed in [5]. We present this special case as a lemma.

Lemma 4.42. *Let A and g be polynomials in $\mathbb{Q}[x]$. Assume that the g-expansion of the polynomial A in $\mathbb{Q}[x]$ is given by*

$$A = a_d g^d + \ldots + a_1 g + a_0.$$

for some $a_0, \ldots, a_d \in \mathbb{Q}[x]$. Suppose there exists a prime p such that:

(a) The reduction of g modulo p is irreducible over $\mathbb{F}_p$,

(b) $a_d(x) = 1$,

(c) $\frac{\nu_p(a_i)}{d-i} \geq \frac{\nu_p(a_0)}{d} > 0$ *for all* $1 \leq i \leq d-1$,

(d) $\gcd(\nu_p(a_0), d) = 1$.

Then, A *is irreducible in* $\mathbb{Q}[x]$.

We remark that if we force $a_0, \ldots, a_d$ to be constant polynomials and $g(x) = x$, we deduce the monic case of Definition 4.9

Proof of Corollary 4.41. Let f be a polynomial in $\mathbb{Q}[x]$ such that $f^n(x) = x^d + \ldots + a_0$ is p^r-Dumas for some prime p and some iteration $n \geq 1$. Suppose g is a polynomial in $\mathbb{Q}[x]$ of degree e such that $\overline{g}$ is irreducible in $\mathbb{F}_p[x]$. If $\gcd(e, r) = 1$, then

$$A(x) = f^n(g(x)) = a_d g^d + \ldots + a_0.$$

By assumption, the polynomial $f^n \circ g$ satisfies the conditions in Lemma 4.42 and thus irreducible in $\mathbb{Q}[x]$. □

Another lemma that combines irreducibility over a finite field, number field and the Rational field is the following.

Corollary 4.43. *let* $f, g \in \mathbb{Q}[x]$ *and* p *be a rational prime such that* $\overline{g}$ *is the reduction of* g *modulo* p*. Assume that* f *is a* p^r*-Dumas polynomial for some* $r \geq 1$ *and* α *is a root of* f*. If* $\overline{g}$ *is irreducible over* $\mathbb{F}_p$*, then,* $g(x) - \alpha$ *is irreducible over the number field* $\mathbb{Q}(\alpha)$*.*

Proof. Assume $f, g \in \mathbb{Q}[x]$ satisfy the conditions in the Lemma for some rational prime p. By Lemma 4.42, $f \circ g$ is irreducible over $\mathbb{Q}$. By Proposition 1.3, if α is a root of f, the polynomial $g(x) - \alpha$ must be irreducible over $\mathbb{Q}(\alpha)$. □

We end this section with the following example.

Example 4.44. *Consider the polynomial*

$$g(x) = x^2 + 1 \in \mathbb{Q}[x].$$

If we consider $\overline{g}$ *in* $\mathbb{F}_3[x]$ *and using the condition in Proposition 1.6, we get* $\gamma = 0$, $-a\overline{g}(\gamma) = 2 = a\overline{g^n}(\gamma)$ *for all* $n \geq 2$*. Since* 2 *is a nonsquare in* $\mathbb{F}_3$*, so,* $\overline{g}$ *is dynamically irreducible over* $\mathbb{F}_3$*. If* $f \in \mathbb{Q}[x]$ *is a monic* 3^r*-Dumas polynomial for some* $r \geq 1$*, then,* $f^n \circ g^m \in \mathbb{Q}[x]$ *is irreducible for all* $n, m \geq 1$ *by the previous corollary. Moreover, if* f *is eventually* 3^r*-Dumas, then, by Theorem 2.10, the iterates* f^{kp}

are 3^r*-Dumas for all* $k \geq 1$*. It follows by the previous corollary that* $f^{kp} \circ g^m$ *is irreducible over* $\mathbb{Q}$*.*

Bibliography

[1] O. Ahmadi, F. Luca, A. Ostafe, and I. E. Shparlinski. On stable quadratic polynomials. *Glasgow Mathematical Journal*, 54(2):359–369, 2012. doi: 10.1017/S001708951200002X.

[2] N. Ali. Stabilité des polynômes. *Acta Arithmetica*, 119(1):53–63, 2005. URL http://eudml.org/doc/278202.

[3] M. Ayad and D. McQuillan. Irreducibility of the iterates of a quadratic polynomial over a field. *Acta Arithmetica*, 93(1):87–97, 2000. doi: 10.4064/aa-93-1-87-97. URL https://doi.org/10.4064/aa-93-1-87-97.

[4] R. Benedetto, P. Ingram, R. Jones, M. Manes, J. Silverman, and T. Tucker. Current trends and open problems in arithmetic dynamics. *Bulletin of the American Mathematical Society*, 56(4):611–685, Mar. 2019. doi: 10.1090/bull/1665. URL https://doi.org/10.1090/bull/1665.

[5] A. Bishnoi and S. K. Khanduja. On generalized schönemann polynomials. *Communications in Algebra*, 41(7):2417–2426, May 2013. ISSN 0092-7872, 1532-4125. doi: 10.1080/00927872.2012.658534. URL http://www.tandfonline.com/doi/abs/10.1080/00927872.2012.658534.

[6] C. B. Boyer and U. C. Merzbach. *A history of mathematics*. Jossey Bass Wiley, Chichester, England, 3 edition, Dec. 2010.

[7] M. R. Bush, W. Hindes, and N. R. Looper. Galois groups of iterates of some unicritical polynomials. *arXiv: Number Theory*, 2016.

[8] S. Casacubertan. On The Divisibility Of Binomial coefficients. *Ars Mathematica Contemporanea*, 19(20):297–309, 2020. doi: https://doi.org/10.26493/1855-3974.2103.e84.

[9] K. Chamberlin, E. Colbert, S. Frechette, P. Hefferman, R. Jones, and S. Orchard. Newly reducible iterates in families of quadratic polynomials. *Involve, a Journal of Mathematics*, 5(4):481–495, Dec. 2012. doi: 10.2140/involve.2012.5.481. URL https://doi.org/10.2140/involve.2012.5.481.

[10] D. A. Cox. Why eisenstein proved the eisenstein criterion and why schönemann discovered it first. *The American Mathematical Monthly*, 118(1):3, 2011. doi: 10.4169/amer.math.monthly.118.01.003. URL https://doi.org/10.4169/amer.math.monthly.118.01.003.

[11] L. Danielson and B. Fein. On the irreducibility of the iterates of $x^n - b$. *Proceedings of the American Mathematical Society*, 130(6):1589–1596, Oct. 2001. doi: 10.1090/s0002-9939-01-06258-x. URL https://doi.org/10.1090/s0002-9939-01-06258-x.

[12] M. de Berg, O. Cheong, M. van Kreveld, and M. Overmars. *Computational Geometry*. Springer Berlin Heidelberg, 2008. doi: 10.1007/978-3-540-77974-2. URL https://doi.org/10.1007/978-3-540-77974-2.

[13] D. DeMark, W. Hindes, R. Jones, M. Misplon, M. Stoll, and M. Stoneman. Eventually stable quadratic polynomials over $\mathbb{Q}$. *New York Journal of Mathematics*, 26:526–561, 2020. URL https://eref.uni-bayreuth.de/58380/.

[14] H. L. Dorwart. Irreducibility of polynomials. *The American Mathematical Monthly*, 42(6):369–381, June 1935. doi: 10.1080/00029890.1935.11987732. URL https://doi.org/10.1080/00029890.1935.11987732.

[15] G. Dumas. Sur quelques cas d'irréductibilité des polynomes à coefficients rationnels. *Journal de Mathématiques Pures et Appliquées*, 2:191–258, 1906. URL http://eudml.org/doc/233912.

[16] D. S. Dummit and R. M. Foote. *Abstract algebra*. Wiley, 3rd ed edition, 2004.

[17] S. Hamblen, R. Jones, and K. Madhu. The Density of Primes in Orbits of zd+c. *International Mathematics Research Notices*, 2015(7):1924–1958, 01 2014. ISSN 1073-7928. doi: 10.1093/imrn/rnt349. URL https://doi.org/10.1093/imrn/rnt349.

[18] D. R. Heath-Brown and G. Micheli. Irreducible polynomials over finite fields produced by composition of quadratics. *Revista Matemática Iberoamericana*, 35 (3):847–855, Apr. 2019. doi: 10.4171/rmi/1072. URL https://doi.org/10.4171/rmi/1072.

[19] P. Illig, R. Jones, E. Orvis, Y. Segawa, and N. Spinale. Newly reducible polynomial iterates. *International Journal of Number Theory*, 17(06):1405–1427, Feb. 2021. doi: 10.1142/s1793042121500433. URL https://doi.org/10.1142/s1793042121500433.

[20] W. R. Inc. Mathematica, Version 12.2. Champaign, IL, 2020.

[21] A. Jakhar. On the factors of a polynomial. *Bulletin of the London Mathematical Society*, 52(1):158–160, 2020. doi: https://doi.org/10.1112/blms.12315. URL https://londmathsoc.onlinelibrary.wiley.com/doi/abs/10.1112/blms.12315.

[22] R. Jones. The density of prime divisors in the arithmetic dynamics of quadratic polynomials. *Journal of the London Mathematical Society*, 78(2):523–544, July 2008. doi: 10.1112/jlms/jdn034. URL https://doi.org/10.1112/jlms/jdn034.

[23] R. Jones and N. Boston. Settled polynomials over finite fields. *Proceedings of the American Mathematical Society*, 140(6):1849–1863, Oct. 2011. doi: 10.1090/s0002-9939-2011-11054-2. URL https://doi.org/10.1090/s0002-9939-2011-11054-2.

[24] R. Jones and A. Levy. Eventually stable rational functions. *International Journal of Number Theory*, 13(09):2299–2318, Sept. 2017. doi: 10.1142/s1793042117501263. URL https://doi.org/10.1142/s1793042117501263.

[25] E. Kaltofen. Factorization of polynomials. In *Computing Supplementa*, pages 95–113. Springer Vienna, 1983. doi: 10.1007/978-3-7091-7551-4_8. URL https://doi.org/10.1007/978-3-7091-7551-4_8.

[26] L. Kronecker. Grundzüge einer arithmetischen theorie der algebraische grössen. *crll*, 1882(92):1–122, 1882. doi: 10.1515/crll.1882.92.1. URL https://doi.org/10.1515/crll.1882.92.1.

[27] S. Laishram, R. Sarma, and H. Sharma. Stability of certain higher degree polynomials, 2022. URL https://arxiv.org/abs/2206.04290.

[28] R. W. K. Odoni. The galois theory of iterates and composites of polynomials. *Proceedings of The London Mathematical Society*, pages 385–414, 1985.

[29] R. W. K. Odoni. On the Prime Divisors of the Sequence Wn+1 = 1 + W1. . . Wn. *Journal of the London Mathematical Society*, s2-32(1):1–11, 08 1985. ISSN 0024-6107. doi: 10.1112/jlms/s2-32.1.1. URL https://doi.org/10.1112/jlms/s2-32.1.1.

[30] V. V. Prasolov. *Polynomials*, volume 11 of *Algorithms and Computation in Mathematics*. Springer Berlin Heidelberg, Berlin, Heidelberg, 2004. ISBN 9783642039799 9783642039805. doi: 10.1007/978-3-642-03980-5. URL http://link.springer.com/10.1007/978-3-642-03980-5.

[31] M. Stoll. Galois groups over $\mathbb{Q}$ of some iterated polynomials. *Archiv der Mathematik*, 59(3):239–244, Sept. 1992. doi: 10.1007/bf01197321. URL https://doi.org/10.1007/bf01197321.

[32] S. Weintraub. A mild generalization of eisenstein's criterion. *Proceedings of the American Mathematical Society*, 141(4):1159–1160, Aug. 2012. doi: 10.1090/s0002-9939-2012-10880-9. URL https://doi.org/10.1090/s0002-9939-2012-10880-9.