Galois Theory and Polynomial Orbits

by

Kalyani K. Madhu

Submitted in Partial Fulfillment
of the
Requirements for the Degree
Doctor of Philosophy

Supervised by
Professor Thomas J. Tucker

Department of Mathematics
Arts, Sciences and Engineering
School of Arts and Sciences

University of Rochester
Rochester, New York

2011
Kalyani Madhu was born in Seattle, Washington in 1962. She earned her Bachelor of Arts in English with Distinction at Cornell University in 1984. She received a Masters of Arts in Mathematics at the State University of New York College at Brockport in 2005. She received a Master of Arts in Mathematics at the University of Rochester in 2008. She began her graduate studies in Mathematics at the University of Rochester in 2006. There she pursued her interest in Algebraic Number Theory and Arithmetic Dynamics under the guidance of her doctoral advisor, Thomas J. Tucker.
Acknowledgments

I would like to thank all the good people of the Math department at the University of Rochester for creating a warm, supportive environment. In particular I would like to thank Jonathan Pakianathan, Nick Rogers, and Shannon Starr for their help. I would like to thank Adam Towsley for working with me, helping me, and for his friendship. I would like to thank Joan Robinson for her knowledge and friendly interest. Without her our department would be a much colder place. And I would like to thank my advisor, Tom Tucker, a true mensch.

I would like to thank my parents for their endless childcare help, for their enthusiastic support of my studies, and for forgetting to mention to me when I was little that girls are not analytical thinkers. I would like to thank my children, Noah, Hannah, Jo and Susi, for their patience and love, and my daughters for their proofreading. I would like to thank my husband, Ashwani, for his enduring, unequivocal support.
Abstract

We address two questions arising from the iteration of the polynomial $f(x) = x^m + c$. The first question concerns orbits of points in finite fields. Let $E_m$ be the set of rational primes congruent to 1 modulo $m$. Let $p \in E_m$ and $f(x) \in \mathbb{F}_p[x]$. We show that, with some restrictions on $c$, the proportion of points in $\mathbb{F}_p$ that are periodic points of $f$ goes to zero as $p \in E_m$ goes to infinity. The second question concerns orbits of rational numbers. Let $f(x) \in \mathbb{Q}[x]$, and $\alpha \in \mathbb{Q}$. We show that, with some restrictions on $c$, the subset of primes of $E_m$ that divide the orbit of $\alpha$ has natural density zero.

We use Galois theoretic methods developed by R.W.K. Odoni for both questions. Odoni showed that, in general, prime divisors of the orbits of polynomials in $\mathbb{Z}[x]$ are a sparse set in spec $\mathbb{Z}$ [18, Theorem III(Colloquial version)]. Rafe Jones [12] showed that sets of primes dividing the orbits of certain quadratic maps have density zero. We continue this process of uncovering specific maps for which Odoni’s generalization holds.
# Table of Contents

Curriculum Vitae ........................................... ii

Acknowledgments ........................................... iii

Abstract ..................................................... iv

1 Introduction .............................................. 1
   1.1 Galois Groups and Wreath Products .................... 3
   1.2 Stability and Reducibility of Iterates .................. 5
   1.3 Frobenius Automorphisms and Chebotarev’s Density Theorem . 7

2 Periodic Points in Finite Fields ......................... 9
   2.1 Periodicity and Roots .................................. 9
   2.2 Maximality ............................................ 14
   2.3 Proof of Theorem 2.3 .................................. 18

3 Primes Dividing the Orbits of Rational Numbers ......... 22
   3.1 Roots and Galois Groups ............................... 23
   3.2 Proof of Theorem 3.2 ................................. 42
   3.3 Quadratics ............................................ 43
4 Conclusion 49

Appendices 52

Bibliography 59
1 Introduction

A dynamical system is a pair \((S, \phi)\) where \(S\) is a set and \(\phi\) is a map from \(S\) to \(S\). As \(\phi\) is a self-map, we may compose \(\phi\) with itself and consider iterates of \(\phi\). By \(\phi^n\) we mean \(n\) such compositions \(\phi \circ \phi \circ \cdots \circ \phi\). The notion of an orbit naturally arises. Suppose \(s \in S\); the forward orbit of \(s\) under \(\phi\) is the set \(O_\phi(s) := \{s, \phi(s), \ldots, \phi^n(s), \ldots\}\). Arithmetic dynamics concerns the study of such orbits in sets that are of arithmetic interest.

**Definition 1.1.** The orbit of a point \(\alpha\) is periodic if, for some \(n > 0\), \(f^n(\alpha) = \alpha\). A point is preperiodic if it has finite orbit. Hence, periodic points are always preperiodic. A point is strictly preperiodic if it is preperiodic, but not periodic. A point is called wandering if it is not preperiodic.

We will fix our map to be always \(f(x) = x^m + c\), a polynomial map, and address two questions.

Let \(p\) be a rational prime not dividing \(m\) or \(c\), and let \(f(x) = x^m + c \in \mathbb{F}_p[x]\). As \(\mathbb{F}_p\) is a finite set, all orbits are also finite, and so the interesting distinction is between periodic and strictly preperiodic points. Several natural questions regarding periodicity arise. For example, one might ask whether or not a particular point in \(\mathbb{F}_p\) is \(f\)-periodic, or for what kinds of maps a particular point is periodic. We are able to answer a similar question in the finite field setting. We show that
for the map \( f \) and large \( p \) in the class of primes congruent to 1 modulo \( m \), we may expect very few points in \( \mathbb{F}_p \) to be periodic for \( p \). That is, if we take the limit as \( p \) goes to infinity of primes \( p \equiv 1 \pmod{m} \), we will find that the proportion of periodic points in \( \mathbb{F}_p \) goes to zero. This is Theorem 2.3, which we prove in chapter 2.

For the second question we regard \( f(x) = x^m + c \) as a polynomial over the rational numbers. Let \( \alpha \in \mathbb{Q} \) and consider \( O_f(\alpha) \). This is a sequence of rational numbers. We will consider the set of rational primes that divide the numerator of some element in \( O_f(\alpha) \).

**Definition 1.2.** Let \( K \) be a field. Let \( a_n = f^n(\alpha) \) for some \( \alpha \in K \). Let \( p \) be a prime of \( \mathcal{O}_K \). We say \( p \) divides the orbit of \( \alpha \) if \( v_p(a_n) > 0 \) for some \( n \in \mathbb{Z}_{\geq 0} \).

Note that our definition does not consider primes at which elements of the orbit have negative valuation. This is because our map is a polynomial, and so there are only finitely-many such primes.

**Definition 1.3.** The natural density of a set \( P \) of primes of \( \mathbb{Z} \), denoted \( D(P) \), is given by

\[
D(P) = \lim_{n \to \infty} \frac{\# \{ \text{primes in } P \cap \mathbb{Z}_{\leq n} \}}{\# \{ \text{primes in } \mathbb{Z}_{\leq n} \}}.
\]

Let \( E_m = \{ p \in \mathbb{Z} \mid p \text{ is prime and } p \equiv 1 \pmod{m} \} \). We consider the set of primes dividing the orbit under \( f \) of a rational number \( \alpha \). We will show that, with some restrictions on \( m \) and \( c \), the set of primes in \( E_m \) that divide \( O_f(\alpha) \) has natural density zero. This is Theorem 3.2, which we prove in Chapter 3.

The link between these two questions has largely to do with the method of proof. We consider the successive Galois groups of the iterated polynomials, and make use of the correspondence between primes dividing orbits and the cycle type of the elements in the Frobenius conjugacy classes of those primes in the Galois group of a polynomial. This technique was introduced by R.K.S. Odoni [18].
Odoni considered generic polynomial maps $\mathcal{F}$ over fields of characteristic zero. He shows that the Galois group of the $n$th iterate of $\mathcal{F}$ [18, Theorem 1] is the $n$-fold wreath product of the symmetric group $S_k$ with itself, where $k$ is the degree of $\mathcal{F}$. He also shows that the proportion of elements in this group whose action on the roots of $\mathcal{F}^n$ fixes at least one root goes to zero as $n$ increases.

Rafe Jones showed via properties of Galois groups that the set of primes dividing the orbit under certain quadratic polynomials of any fixed integer point has natural density zero [12, Theorem 1.2]. Our second result shows that Jones’ result may be extended, with some restrictions, to maps of the form $f := x \mapsto x^m + c$. As in the quadratic case, it is more difficult to determine the Galois groups here than it is in the generic case, as one must deal with the issue of stability of iterates, which we define in Section 1.2. We find that if there exists a prime $q \in \mathbb{Z}$ such that $v_q(c) > 0$, then $f$ is eventually stable. This is Proposition 3.7.

### 1.1 Galois Groups and Wreath Products

We would like to establish some properties of iterated polynomials and their Galois groups. We begin with notation that will be used with minor modifications throughout this paper. Let $K$ be a field and $f(x) \in K[x]$ a polynomial. Let $x = f^0(x)$ and $f^n(x) = f \circ f^{n-1}(x)$. Let $K_n$ be the splitting field of $f^n$ over $K$. Let $G_n = \text{Gal}(K_n/K)$ and $H_n \subset G_n$ the Galois group of $K_n$ over $K_{n-1}$.

If $\alpha$ is a root of $f^n$ in $\bar{K}$, then $\alpha \in K_n$, and so $f(\alpha) \in K_n$ as well. As $\alpha$ is a root of $f^n$, $f(\alpha)$ is a root of $f^{n-1}$. Hence, we have containments $K_{n-1} \subset K_n$, and restriction maps $\psi_{n-j,n}$ from $G_n$ to $G_{n-j}$, where $j \geq 1$. That is, let $\sigma \in G_n$. Then $\psi_{n-j,n}(\sigma)$ is the restriction of $\sigma$ to $K_{n-j}$. If $\sigma$ fixes $\alpha$, then $\sigma$ fixes $f(\alpha)$, because $\sigma \circ f = f \circ \sigma$. Contrapositively, if $f(\alpha) = \beta$, and $\sigma(\beta) \neq \beta$, then $\sigma(\alpha) \neq \alpha$.

We may create a tree graph whose vertices are the roots of successive iterates of $f$ and whose edges connect roots and their images and inverse images under
As \( \sigma \circ f = f \circ \sigma \), adjacency in the graph is preserved under the action of the Galois groups of successive iterates. Hence \( G_n \) is a subgroup of the group of automorphisms of the tree (see [2]).

Suppose that \( f^{n-1} \) is separable of degree \( r \) and that \( \{ \beta_1, \ldots, \beta_r \} \) is the set of roots of \( f^{n-1} \). A useful fact to note is that

\[
f^n(x) = \prod_{i=1}^{r} (f(x) - \beta_i).
\]

Let \( L_i \) be the splitting field of \( f(x) - \beta_i \) over \( K_{n-1} \). Then \( K_n \) is the compositum of the \( L_i \).

**Definition 1.4.** Let \( \mathcal{G}, \mathcal{H} \) be two permutation groups and \( r \) the degree of \( G \). Then the wreath product of \( \mathcal{G} \) by \( \mathcal{H} \), which we denote \( \mathcal{G}[\mathcal{H}] \) is the semidirect product of the Cartesian product of \( r \) copies of \( H \) by \( \mathcal{G} \) in which \( \mathcal{G} \) acts on \( \mathcal{H}^r \) by permuting the indices.

**Remark 1.5.** The wreath product can be defined much more generally, and enjoys a wide variety of notation in the literature. This definition works well in the context of iterated Galois groups.

The wreath product is associative in the sense that \( \mathcal{G}[\mathcal{H}[K]] \cong \mathcal{G}[\mathcal{H}][K] \), so we may refer to wreath powers \( [\mathcal{G}]^n \), where \( [\mathcal{G}]^1 = \mathcal{G} \), and \( [\mathcal{G}]^n = [\mathcal{G}]^{n-1}[\mathcal{G}] \). We will make extensive use of a Lemma of Odoni [18, Lemma 4.1].

**Lemma 1.6.** Let \( K \) be any field and \( f, g \) monic polynomials in \( K[x] \). Let \( f \circ g(x) \) be separable over \( K \), and let the degree of \( f \) be \( k \) and the degree of \( g \) be \( \ell \), \( k, \ell \geq 1 \). Then \( f(x) \) is also separable over \( K \). Let \( \mathcal{F} \) be the Galois group of \( f \) over \( K \). Then the Galois group of \( f \circ g \) over \( K \) can be embedded in \( \mathcal{F}[S_\ell] \), where \( S_\ell \) is the symmetric group on \( \ell \) letters.

This tells us that, if \( f^n \) is separable for all \( n \) and the degree of \( f = m \), then \( G_n \subseteq G_{n-1}[S_m] \).
We can write an element of the wreath product $\mathcal{F}[\mathcal{G}]$ as $(\tau; \pi_1, \cdots, \pi_r)$ where $\tau \in \mathcal{F}$, $r$ is the degree of $\mathcal{F}$ considered as a permutation group, and $(\pi_1, \cdots, \pi_r)$ is an element of $\mathcal{G}^r$. Consider the iteration of a polynomial $f$ of degree $m$ in $K[x]$, and suppose that iterates of $f$ never factor, so that $f^{n-1}$ is irreducible of degree $r := m^{n-1}$. We may write the roots of $f^n$ as $\{\alpha_{i,j}\}$ where $f(\alpha_{i,j}) = \beta_i$, a root of $f^{n-1}$. Then the $i$ range between 1 and $r$, and the $j$ range between 1 and $m$. If $\sigma = (\tau; \pi_1, \cdots, \pi_d) \in G_n \subseteq G_{n-1}[S_m]$, then $\sigma(\alpha_{i,j}) = \alpha_{\tau(i), \pi(i)(j)}$.

Example 1.7. Let $f(x) = x^2 - 3$. Then $\text{Gal}(f^2/\mathbb{Q}) \cong \mathcal{D}_4 \cong [S_2]^2$.

\[
\begin{array}{c|ccc|ccc}
\sqrt{3} + \sqrt{3} & -\sqrt{3} + \sqrt{3} & \sqrt{3} - \sqrt{3} & -\sqrt{3} - \sqrt{3} \\
\sqrt{3} & -\sqrt{3} & 0 & 0 \\
\end{array}
\]

$\alpha_{1,1} = 1 \quad \alpha_{1,2} = 3 \quad \alpha_{2,1} = 2 \quad \alpha_{2,2} = 4$

We compare permutation and wreath notation for the same group.

<table>
<thead>
<tr>
<th>Permutation</th>
<th>Wreath</th>
</tr>
</thead>
<tbody>
<tr>
<td>$e \leftrightarrow (e; e, e)$</td>
<td>$(1432) \leftrightarrow ((12); (12), e)$</td>
</tr>
<tr>
<td>$(14)(23) \leftrightarrow ((12); (12), (12))$</td>
<td>$(13)(24) \leftrightarrow (e; (12), (12))$</td>
</tr>
<tr>
<td>$(12)(34) \leftrightarrow ((12); e, e)$</td>
<td>$(1234) \leftrightarrow ((12); e, (12))$</td>
</tr>
</tbody>
</table>

Lemma 1.8. Let $P_n$ be the proportion of elements of $G_n$ that fix at least one root. If $G_n \cong [G]^n$, then

$$\lim_{n \to \infty} P_n = 0.$$ 

Proof. This is Odoni’s [18, Lemma 4.3], which we prove in Section 2.2. \qed

1.2 Stability and Reducibility of Iterates

Iterates of irreducible polynomials are not necessarily irreducible. This issue becomes important in the identification of the Galois groups of iterates. We will
discuss irreducibility of iterates in Chapter III, but we give the basic definitions here.

**Definition 1.9.** A polynomial over a field $K$ is called **stable** if all of its iterates are irreducible.

A polynomial is called **eventually stable** if there are integers $k, \ell$ such that

$$f^\ell(x) = \prod_{i=1}^{k} g_i \circ f^{n_i}(x)$$

and $g_i \circ f^n(x)$ is irreducible for all $n \geq 0$.

**Example 1.10.** Let $f(x) = x^2 - \frac{16}{9}$.

$$f(x) = \left(x - \frac{4}{3}\right) \left(x + \frac{4}{3}\right)$$

$$= g_1(x) g_2(x)$$

$$f^2(x) = \left(x^2 - \frac{16}{9} - \frac{4}{3}\right) \left(x^2 - \frac{16}{9} + \frac{4}{3}\right)$$

$$= g_1(f(x)) g_2(f(x))$$

$$= g_1(x) \left(x - \frac{2}{3}\right) \left(x + \frac{2}{3}\right)$$

$$= g_1(f(x)) g_{1,1}(x) g_{2,2}(x)$$

$$f^3(x) = g_1(f^2(x)) \left(x^2 - \frac{16}{9} - \frac{2}{3}\right) \left(x^2 - \frac{16}{9} + \frac{2}{3}\right)$$

$$= \left(x^4 - \frac{32}{9} x^2 + \frac{4}{81}\right) \left(x^2 - \frac{22}{9}\right) \left(x^2 - \frac{10}{9}\right)$$

$$= \left(x^2 - 2x + \frac{2}{9}\right) \left(x^2 + 2x + \frac{2}{9}\right) \left(x^2 - \frac{22}{9}\right) \left(x^2 - \frac{10}{9}\right)$$

$$= g_{1,1}(x) g_{1,2}(x) g_{2,1}(f(x)) g_{2,2}(f(x))$$

In Chapter III we will show that $f$ factors no further and so is eventually stable. By contrast $f(x) = x^2 - 1$ is not eventually stable.
1.3 Frobenius Automorphisms and Chebotarev’s Density Theorem

Definition 1.11. Let $K$ be a field and $p$ a prime of $\mathcal{O}_K$, and suppose that $\mathcal{O}_K/p$ is the finite field of $q$ elements. Suppose that $L$ is a finite Galois extension of $K$ with Galois group $G := \text{Gal}(L/K)$, and that $p$ is unramified in $L$. Let $\mathfrak{P}$ be a prime of $\mathcal{O}_L$, with $\mathfrak{P} \cap \mathcal{O}_K = p$. Then the extension $\mathcal{O}_L/\mathfrak{P}$ over $\mathcal{O}_K/p$ is Galois with generator $\sigma_{\mathfrak{P}}$ called the Frobenius automorphism at $\mathfrak{P}$. For $x \in \mathcal{O}_L/\mathfrak{P}$, $\sigma_{\mathfrak{P}}(x) = x^q$.

We have defined the Frobenius automorphism as generating the Galois group of $\mathcal{O}_L/\mathfrak{P}$ over $\mathcal{O}_K/p$, a definition that specifies $\mathfrak{P}$. However, we can also define it from below. The decomposition groups of each of the $\mathfrak{P}_i$ extending $p$ contain (as long as $p$ is unramified) a unique element $\sigma$ that satisfies $\sigma(x) \equiv x^q \mod \mathfrak{P}_i$. The unique elements for each $i$ coming from primes that extend a single $p$ are conjugate, and so we may refer to $\text{Frob}(p)$, the conjugacy class of $\sigma_{\mathfrak{P}_i}$ for each $i$ (see, for example, [10, III.2,p.125]).

Suppose that $f$ is a polynomial in $K[x]$ and $E$ a simple extension obtained by adjoining to $K$ a root of $f$. Let $L$ be the Galois closure of $E$ over $K$. Let $G = \text{Gal}(L/K)$. Suppose that a prime $p$ of $\mathcal{O}_K$ is unramified in $L$. The factoring of a prime $p$ of $\mathcal{O}_K$ in $\mathcal{O}_E$ corresponds exactly to the cycle type of the elements in $\text{Frob}(p) \subset G$. That is, if

$$p\mathcal{O}_E = \prod_{i=1}^{s} \mathfrak{P}_i,$$

then the elements of $\text{Frob}(p)$ will be composed of $s$ disjoint cycles each of length $f_i$, where $f_i$ is the residue degree of $\mathfrak{P}_i$. Hence, if the reduction of $f \mod p$ has a linear factor, elements of $\text{Frob}(p)$ will have a cycle of length one. In particular, if $f$ has a root modulo $p$, then the elements of $\text{Frob}(p)$ will fix a root of $f$. 
We are able to relate the density of primes with certain cycle types to the size of their Frobenius conjugacy classes via the Chebotarev Density Theorem. (We use the statement given by Lenstra in [23, p.18].)

**Theorem 1.12.** Let $K$ be a number field and $L$ a finite Galois extension of $K$ with Galois group $G$. Then, for any conjugacy class $C$ of $G$, the density of the set of primes $p$ of $K$ for which $\text{Frob}(p) = C$ exists and equals $\#C/\#G$.

There are analogous theorems in the function field setting, (see for example [19, Theorems 9.13a,b]), but we will be using an effective version of the Theorem instead, which we will state in context in Chapter 2.
2 Periodic Points in Finite Fields

Let $f := x \mapsto x^m + c$ be a map over $\mathbb{F}_p$. Let $E_m := \{\text{primes } p \mid p \equiv 1 \mod m\}$. We show that, if $p \in E_m$, then, with some restriction on $c$, the proportion of periodic points of $\mathbb{F}_p$ under $f$ goes to zero as $p$ goes to infinity if $p \in E_m$.

2.1 Periodicity and Roots

For some prime $p \in \mathbb{Z}$ and $m \geq 2$, let $f(x) = x^m + c \in \mathbb{F}_p[x]$. Let $\alpha \in \mathbb{F}_p$. As $\mathbb{F}_p$ is finite, so is the orbit of $\alpha$ under $f$. Thus $\alpha$ is at least preperiodic, so the important distinction is between whether $\alpha$ is periodic or strictly preperiodic.

We begin with two examples of orbits. In both examples the map is the same, but the congruence classes of $p$ modulo $m$ are different. We see that $x \mapsto x^m + c$ will be a permutation on $\mathbb{F}_p$ for primes $p$ that are congruent to 2 modulo 3, and not for primes congruent to 1 modulo 3, because if $p \equiv 1 \mod 3$, then $\mathbb{F}_p$ contains the primitive cube roots of unity.
Example 2.1. Orbit graph of $f(x) = x^3 + 2$ over $\mathbb{F}_{43}$

```
Example 2.1. Orbit graph of $f(x) = x^3 + 2$ over $\mathbb{F}_{43}$

In Example 2.1, $f$ has five periodic points out of forty-three.

Example 2.2. Orbit graph of $f(x) = x^3 + 2$ over $\mathbb{F}_{17}$

In Example 2.2, all points are periodic.

We wish to consider the primes modulo which $f$ is not a permutation, so that we have a combination of periodic and strictly preperiodic points. We limit ourselves to primes $p$ such that $\mathbb{F}_p$ contains a primitive $m$th root of unity. This will guarantee that our map is $m$-to-one except over $c$, where the map ramifies.

In the example of $\mathbb{F}_{43}$, the number of periodic points is fairly small. This agrees with our intuition about the matter. Picking the points in the orbit of $\alpha$, where
\( \alpha \in \mathbb{F}_p \) and \( p \equiv 1 \mod m \), is like picking with replacement from a set of \( p \) items. Just as in the birthday problem, if we pick about \( \sqrt{p} \) items, the probability that we have picked some item twice approaches 0.50. Thus we would expect orbits in \( \mathbb{F}_p \) to be about \( \sqrt{p} \) in size. Each of the \( \sqrt{p} \) possibilities for a duplicate point is equally likely, so we would not expect to return to the beginning and re-pick the initial point. Thus we would expect the orbit of a periodic point to be shorter than \( \sqrt{p} \), and we should expect to see preperiodic orbits.

Further, as our maps are \( m \)-to-one, we experience branching as we move backward through the orbit. That is, if a point has a pre-image under \( f \), then it has \( m \) pre-images. All the pre-images of strictly preperiodic points are themselves strictly preperiodic, and exactly one of the pre-images of a periodic point is periodic. So heuristically we would expect to have few periodic points, and many strictly preperiodic ones.

In the case \( f(x) = x^m + c \) and \( p \equiv 1 \mod m \), we are able to prove that this heuristic is correct.

**Theorem 2.3.** Let \( f(x) = x^m + c \), with \( m, c \in \mathbb{Z} \) and \( m \geq 2 \). Suppose that \( m, c \) are such that 0 is not a preperiodic point of \( f \) over \( \mathbb{Z} \). Let \( E_m := \{ \text{primes } p \mid p \equiv 1 \mod m \} \). Let \( P_{f,p} \) refer to the proportion of points in \( \mathbb{F}_p \) that are periodic points of \( f \). Then,

\[
\lim_{p \to \infty} \lim_{p \in E_m} P_{f,p} = 0.
\]

The proof of Theorem 2.3 follows from a Proposition and its Corollary given in the next two Sections. Here we will reformulate the question of periodicity in finite fields as one about primes in function fields so that we may apply techniques from Galois theory.

We begin by noticing that a point \( \alpha \in \mathbb{F}_p \) is periodic if and only if \( \alpha \) appears in the set of images of \( f^n \) for every \( n \). This is not hard to see, as, if \( \alpha \) is periodic,
then we can find its $n$th preimage for every $n$ by moving backward through the periodic cycle of which $\alpha$ is a member.

**Definition 2.4.** A point $\alpha$ has exact period $k$ under $f$ if $f^k(\alpha) = \alpha$, but $f^j(\alpha) \neq \alpha$ if $j < k$.

Suppose that $\alpha$ has exact period $k$. For any $n \in \mathbb{N}$, let $j$ be the least integer such that $jk \geq n$. Then $f^n(f^{jk-n}\alpha)) = \alpha$.

Consider the function field $\mathbb{F}_p(t)$. For every $n$, the polynomial $f_n := f^n(x) - t$ is an element of the ring $\mathbb{F}_p(t)[x]$. We will be working with the Galois group of $f_n$ over $\mathbb{F}_p(t)$. Let $\mathfrak{p}_\alpha := (t - \alpha)$, a principal prime ideal of $\mathbb{F}_p[t]$. We see that $f_n$ has a root modulo $\mathfrak{p}_\alpha$ for every $n$ if and only if $\alpha$ is periodic under $f$, so we may productively rephrase the question about periodic points in finite fields as a question about prime ideals in function fields.

Suppose that $\alpha$ is periodic under $f$. When we factor $f_n$ modulo $\mathfrak{p}_\alpha$ for successive $n$, we will find that the reduced polynomial has a linear factor for each $n$. If $F \in K[x]$, and $F \mod \mathfrak{p} = \prod_{i=1}^{s} g_i(x)$, where the $g_i$ are distinct, irreducible over $O_K/\mathfrak{p}$, and each $g_i$ has degree $f_i$, then the elements in $\text{Frob}(\mathfrak{p})$, acting as permutations on the roots of $f_n$, will be composed of $s$ disjoint cycles, each of length $f_i$.

If $K = \mathbb{F}_p(t)$ and $F = f_n$, and $\alpha$ is periodic under $f$, then elements in $\text{Frob}(\mathfrak{p}_\alpha)$ in $G_n := \text{Gal}(f_n/K)$ will have at least one cycle of length one corresponding to the linear factor coming from the root of $f_n \mod \mathfrak{p}_\alpha$, and so each will fix at least one root of $f_n$.

Murty and Scherk [13] provide an effective Chebotarev Density Theorem in the function field case. We have modified it somewhat to fit our circumstances. Let $K_n$ be the splitting field of $f_n$ over $\mathbb{F}_p(t)$ and $G_n := \text{Gal}(K_n/\mathbb{F}_p(t))$. Let $g_n$ be the genus of the curve given by $f_n$, which is equal to the genus of the function field $K_n$. We think of $\mathbb{P}^1(\mathbb{F}_p)$ as $\mathbb{F}_p \cup \infty$. 
**Theorem 2.5.** Let $\psi$ be the points of $\mathbb{P}^1(\mathbb{F}_p)$ that are unramified in $K_n$, and $\psi_C = \{ \beta \in \psi \mid \text{Frob}(\beta) = C \}$ where $C$ is a conjugacy class in $G_n$. Let $D$ be the set of points of $\mathbb{P}^1(\mathbb{F}_p)$ ramifying in $K_n$. Then

$$\left| \frac{\# \psi_C}{\# G_n} - \frac{\# C}{\# G_n} \right| < 2g_n \frac{\# C}{\# G_n} \sqrt{p} + \# D.$$

We wish to consider the union of all conjugacy classes of $G_n$ that have fixed points. Suppose that there are $N$ conjugacy classes $C_i \subset G_n$ whose elements have at least one fixed point. Let $C = \bigcup_{i=1}^N C_i$. By the triangle inequality

$$\left| \frac{\# \psi_C}{\# G_n} - \frac{\# C}{\# G_n} \right| < \sum_{i=1}^N \left| \frac{\# \psi_{C_i}}{\# G_n} - \frac{\# C_i}{\# G_n} \right| < 2g_n \frac{\# C}{\# G_n} \sqrt{p} + N \# D.$$

We require that zero is not a preperiodic point of $f$ if considered as a map on $\mathbb{Z}$. This allows us to choose, for sufficiently large $p$, an $M$ such that $f^i(0)$ and $f^j(0)$ are distinct if $i, j < M$ and $i \neq j$. We will show in Section 2.2 that, given such an $M$ and $p$, $G_n \cong [C_m]^n$, as in Definition 1.4. By Lemma 2.6, we see that for every $\epsilon > 0$ there is an $n$ such that $\frac{\# C}{\# G_n} < \epsilon$. We choose such an $n$ and note that there is a sufficiently large $p_0$ to ensure that there exists $M \in \mathbb{F}_{p_0}$, $M > n$, such that, if $i \neq j$, $i, j < M$, then $f^i(0) \not\equiv f^j(0) \mod p_0$. Then for any $p > p_0$, we will still have that the Galois group of $f_n$ over $\mathbb{F}_p(t)$ is $[C_m]^n$. In Section 2.3 we will show that, for sufficiently large $p$, $N, D$, and $g_n$ depend on $f_n$, and not on $p$. Then, for fixed $n$, dividing by $\# \psi$ in the inequality allows us to make the bound arbitrarily small. Thus the proportion of points in $\mathbb{F}_p$ that are periodic for $f$ approximates the proportion of elements in the Galois group of $f_n$ that fix at least one root, and we may take this approximation to be as close as we like.

Then we need only consider the Galois groups that arise from successive iterations of $f$ and identify the proportion of elements of each Galois group that have fixed points. In the following Section, we will show in Proposition 2.9 and its Corollary that $G_n \cong [C_m]^n$. We stated in Chapter 1 that the proportion of elements of $[C_m]^n$ that fix one or more points approaches zero as $n$ approaches...
infinity. We prove it here for completeness, and because the indicatrix function defined in the proof is of intrinsic interest. The proof is due to Odoni [18, Lemma 4.3].

**Lemma 2.6.** Let \( K \) be a field, and let \( f(x) \in K[x] \), with \( \deg(f(x)) \geq 2 \). Let \( G = \text{Gal}(f/K) \) and suppose \( G_n := \text{Gal}(f^n/K) \cong [G]^n \). Let \( F_n \) be the proportion of elements of \( G_n \) that fix at least one root of \( f^n \). Then \( \lim_{n \to \infty} F_n = 0 \).

**Proof.** Let \( \Phi_G(X) = \frac{1}{\#G} \sum_{\sigma \in G} X^{r_{\sigma}} \) where \( r_\sigma \) is the number of points fixed by \( \sigma \). This polynomial in \( \mathbb{Q}[X] \) is called the indicatrix and is attributed by Odoni to Pólya. It has the property that, if \( F \) and \( G \) are two finite groups, then \( \Phi_{F[G]} = \Phi_F \circ \Phi_G \). Clearly \( F_n = 1 - \Phi_{G_n}(0) = 1 - \Phi_G^n(0) \). Note that \( \Phi_G(1) = 1 \). From Burnside’s Lemma ([7, Theorem 17.1]) we have that \( \Phi_G'(1) = 1 \), because \( G \) acts transitively. So we have a polynomial on the interval \((0,1]\) whose first and second derivatives are positive, and whose graph is tangent to the line \( x = y \) at \( x = 1 \). Thus the graph of \( \Phi_G \) lies entirely above the line \( x = y \) on \([0,1)\), so \( \Phi_G(x) > x \). Then for all points \( a \in [0,1) \) and all \( n \in \mathbb{N} \), \( \Phi_G^n(a) > \Phi_G^{n-1}(a) \). As \( \Phi_G^n(a) \leq 1 \) for all \( n \), it must be that the the sequences \( \{\Phi_G^n(a)\}_{n \geq 1} \) converge for every \( a \in [0,1] \). Since \( \Phi_G \) is continuous, each sequence, including \( \{\Phi_G^n(0)\}_{n \geq 1} \), converges to a fixed point of \( \Phi_G \) in \([0,1] \), that is, to 1. \( \square \)

### 2.2 Maximality

We recall the notation of Section 2.1. That is, let \( f, m, \) and \( c \) be as in Theorem 2.3. Consider \( f_n := f^n(x) - t \) as a polynomial in \( \mathbb{F}_p(t)[x] \) where \( p \in E_m \). Let \( K_n \) refer to the splitting field of \( f_n \) over \( \mathbb{F}_p(t) \). Let \( G_n = \text{Gal}(K_n/\mathbb{F}_p(t)) \), and \( H_n = \text{Gal}(K_n/K_{n-1}) \). Let \( r = \deg(f^{n-1}) \). Let \( \beta_1, \beta_2, \ldots, \beta_r \) be the roots of \( f^{n-1}(x) - t \). We use this notation throughout the following section.

**Claim 2.7.** The polynomial \( f^n(x) - t \) is separable over \( \mathbb{F}_p(t) \) for each \( n \).
Proof. As $f_n$ generates a prime ideal of $\mathbb{F}_p(t)[x]$, it is irreducible. The roots
\[ \sqrt[n]{t - c}, \zeta_m \sqrt[n]{t - c}, \ldots, \zeta_m^{m-1} \sqrt[n]{t - c} \]
of $f_1$ are distinct, as $t \neq c$. Suppose that $f_{n-1}$ is separable with distinct roots $\beta_1, \ldots, \beta_r$. Then each root of $f_n$ has the form $\zeta_m^j \sqrt[n]{\beta_i - c}$. Each is distinct, as the $\beta_i$ are distinct, $c \in \mathbb{F}_p$, and $\beta_i$ is transcendental over $\mathbb{F}_p$, so $\beta_i - c$ is non-zero. \hfill \square

We may write
\[ f^n(x) - t = \prod_{i=1}^r (f(x) - \beta_i). \]
For each $i$, we choose one of the $m$ elements of the set $f^{-1}(\beta_i)$ and name it $\alpha_i$. Then $f(x) - \beta_i$ splits in $K_{n-1}(\alpha_i) := L_i$. Thus $K_n$ is the compositum of the $L_i$.

Definition 2.8. Let $H_n = \text{Gal}(K_n/K_{n-1})$. Let $J_i = \text{Gal}(L_i/K_{n-1})$. Note $J_i \cong J_k$ for all $i, k$. Then we say $H_n$ is maximal if $\#H_n = \#J_i$.

Proposition 2.9 and its Corollary show that, given our conditions, $H_n$ is maximal for each $n$.

Proposition 2.9. Let $N \in \mathbb{N}$ such that for $i, j < N$, $i \neq j$, we have $f^i(0) \not\equiv f^j(0) \mod p$. Let $n < N$. Then:

(i) There is a prime $p$ of $\mathbb{F}_p[t]$ that is unramified in $K_{n-1}$ and ramifies in $K_n$.

(ii) Let $\mathfrak{P} \subseteq \mathcal{O}_{K_{n-1}}$ such that $\mathfrak{P} \cap \mathbb{F}_p[t] = p$. Then $\mathfrak{P}$ ramifies in $\mathcal{O}_{L_i}$ to degree $m$ for exactly one $i \in \{1, \ldots, r\}$, and is unramified in $OL_j$ if $j \neq i$.

Proof. We will begin by showing that $p_n := (t - f^n(0))$ ramifies in $K_n$ and is unramified in $K_{n-1}$. This will prove (i). Let $f(\alpha_i) = \beta_i$. Let $C_{f,n} = \mathbb{F}_p[t, x]/(f^n(x) - t)$. Then $\mathbb{F}_p[t][\alpha_i] \cong C_{f,n}$. As $L_i$ contains all of $K_{n-1}$, it is not necessarily true that $\mathcal{O}_{L_i} \cong \mathbb{F}_p[t][\alpha_i]$. However, $K_n$ is also the compositum of the $\mathbb{F}_p(t)(\alpha_i)$, so a prime ramifies in $\mathbb{F}_p(t)(\alpha_i)$ for some $i$ if and only if it ramifies in $K_n$. As
\[ \mathbb{F}_p[t, x]/(f^n(x) - t) \cong \mathbb{F}_p[x], \mathbb{F}_p[t][\alpha_i] \text{ is a principal ideal domain, thus a Dedekind domain, and so we may consider the unique factorization of its ideals.} \]

We may write \( f^n(x) - t = f^n(0) - t + \prod_{j=1}^d g_j(x)^{\epsilon_j} \), where \( g_j(x) \) is irreducible over \( \mathbb{F}_p(t) \). Thus the maximal ideals of \( C_{f,n} \) containing \( p_n \) are generated by \( g_j(x) \) for some \( j \in \{1, \ldots, d\} \), and \( p_n \) ramifies in \( C_{f,n} \) if and only if \( e_j > 1 \) for some \( j \). Let \( M_j = (g_j(\alpha_i)) \), the image of one of the maximal ideals extending \( p_n \) under the isomorphism between \( C_{f,n} \) and \( \mathbb{F}_p[t][\alpha_i] \).

We will show that \( p_n \) ramifies in \( \mathbb{F}_p[t][\alpha_i] \) if and only if \( \frac{d}{dx}(f^n)(\alpha_i) \in M_j \), because \( (f^n)'(\alpha_i) = \sum_{j=1}^d e_j g_j(\alpha_i)^{\epsilon_j - 1} g_j'(\alpha_i) \prod_{k \neq j} g_k(\alpha_i)^{\epsilon_k} \). If \( j \neq k \), \( g_k(\alpha_i) \notin M_j \), because \( g_k(\alpha_i) \) generates the ideal \( M_k \). As \( \mathbb{F}_p[t][\alpha_i]/M_j \) is a finite extension of the perfect field \( \mathbb{F}_p[t]/p_n \), and \( g_j(x) \) is irreducible in \( \mathbb{F}_p[t]/p_n \), we have that \( g_j(\alpha_i) \notin M_j \). Hence \( (f^n)'(\alpha_i) \in M_j \) for some \( j \) if and only if \( e_j > 1 \) if and only if \( M_j \) is ramified over \( K_{n-1} \).

We have \( \frac{d}{dx}(f^n(x) - t) = m^n \prod_{i=1}^n (f^{n-i}(x))^{m-1} \), so \( (f^n)'(\alpha_i) = m^n \prod_{j=1}^n \beta_j^{m-1} \), where \( f^2(\beta_j) = t \). \( M_j \) ramifies if and only if it contains \( \beta_k \) for some \( k \), so if and only if it contains the product of all the roots of \( f^k(x) - t \), which is \( f^k(0) - t \).

Suppose a maximal ideal \( M \) of \( C_{f,n} \) contains \( \beta_j \). Then \( M \cap \mathbb{F}_p[t] = p_j \). Then if \( M \) is ramified over \( \mathbb{F}_p[t] \), \( M \cap \mathbb{F}_p[t] \) is one of the \( p_i \) for \( i \in \{1, \ldots, n\} \). As \( n < N \), these primes are distinct. In particular, \( p_n = (t - f^n(0)) \) ramifies in \( \mathcal{O}_{K_n} \) and is unramified in \( \mathcal{O}_{K_{n-1}} \). This concludes the proof of part (i).

For part (ii), let \( \mathfrak{P}_i \) be a prime of \( \mathcal{O}_{K_{n-1}} \) extending \( p_n \) and containing \( f(0) - \beta_i \). Let \( f(\alpha_i) = \beta_i \). We will show that \( \mathfrak{P}_i \) ramifies in \( L_i = K_{n-1}(\alpha_i) \) and not in \( L_j \) if \( j \neq i \). Recall that \( f^n(0) - t = \prod_{j=1}^d (f(0) - \beta_j) \), so any prime extending \( p_n \) contains \( f(0) - \beta_i \) for some \( i \).

As \( \mathfrak{P}_i \) is unramified over \( \mathbb{F}_p[t] \), \( v_{\mathfrak{P}_i}(f(0) - \beta_i) = 1 \). Thus \( \mathfrak{P}_i(\mathcal{O}_{K_{n-1}})_{\mathfrak{P}_i} \) can be generated by \( f(0) - \beta_i \). Then any element of \( \mathfrak{P}_i(\mathcal{O}_{K_{n-1}})_{\mathfrak{P}_i} \) has the form \( u(f(0) - \beta_i)^k \) for some \( k \geq 1 \) and unit \( u \). Any prime ideal \( M \) of \( \mathcal{O}_{L_i} \) extending
\( \mathfrak{P}_i \) must contain \( \alpha_i \). Hence any element of \( \mathfrak{P}_i (\mathcal{O}_{L_i})_M \) has the form \( u\alpha_i^{kn} \). Then \( \mathfrak{P}_i (\mathcal{O}_{L_i})_M \subset M^m (\mathcal{O}_{L_i})_M \), so \( \mathfrak{P}_i \) ramifies to degree \( m \) in \( L_i \).

We must show that \( \mathfrak{P}_i \) is unramified in \( \mathcal{O}_{L_j} \) if \( j \neq i \). We write \( f(x) - \beta_j = h(x) + \prod_{k=1}^{s} g_k(x)^{e_k} \) where \( h(x) \), hence \( h'(x) \), is in \( \mathfrak{P}_i \mathcal{O}_{K_{n-1}}[x] \). Then

\[
f'(\alpha_j) = h'(\alpha_j) + \sum_{k=1}^{s} e_k(g_k(\alpha_j))^{e_k-1}g'_k(\alpha_j) \prod_{k \neq \ell} g_\ell(\alpha_j).
\]

So a prime \( M \) of \( \mathcal{O}_{L_j} \) extending \( \mathfrak{P}_i \) ramifies over \( \mathcal{O}_{K_{n-1}} \) if and only if it contains \( f'(\alpha_j) \). If \( M \) ramifies over \( \mathcal{O}_{K_{n-1}} \), then \( \alpha_j \in M \), so \( f(0) - \beta_j \in M \cap \mathcal{O}_{K_{n-1}} \). As \( \mathfrak{P}_i \) contains \( f(0) - \beta_i \) and is unramified in \( K_{n-1} \), \( f(0) - \beta_j \notin \mathfrak{P}_i \). Hence \( \mathfrak{P}_i \) is unramified in \( \mathcal{O}_{L_j} \).

\[ \square \]

**Corollary 2.10.** With the suppositions of Proposition 2.9, \( H_n \) is maximal for each \( n \).

**Proof.** By Proposition 2.9, we have that \( K_n \) is the compositum of extensions of \( K_{n-1} \) none of which is unramified, and in each of which a prime ramifies to degree \( m \) that doesn’t ramify in any other. It is clear that \( \text{Gal}(L_i/K_{n-1}) \cong C_m \).

So \( [L_i : K_{n-1}] = m \) for each \( i \). Fix \( L_r \) arbitrarily. Let \( L = \prod_{k=1}^{r-1} L_k \). Then \( [K_n : L] = m \), because any prime of \( \mathcal{O}_{K_{n-1}} \) containing \( f(0) - \beta_r \) is unramified in \( L \), but ramifies to degree \( m \) in \( K_n \). As \( r \) was arbitrarily chosen, we have that \( [K_n : K_{n-1}] = m^r \).

\[ \square \]

**The Galois Group of \( G_n \)**

We will show that, if \( H_n \) is maximal, then \( G_n \cong G_{n-1}[C_m] \).

Even if \( H_n \) is maximal, it does not follow immediately that \( G_n \cong G_{n-1}[C_m] \). For example, let \( f(x) = x^3 + 2 \) over \( \mathbb{F}_p(t) \) where \( p \equiv 2 \mod 3 \) and \( p > 11 \). Then \( \#G_2 = \#S_3[C_3] \), but \( G_2 \not\cong S_3[C_3] \). This is because the field \( K_1 \) contains an extension of the constant field \( \mathbb{F}_p \), so \( \zeta_3 \) is not fixed by \( G_1 \). Thus we can get
automorphisms of the form \(((12); (12), (12)) \notin S_3[C_3]\), but not, for example \(((12); e, e, e) \in S_3[C_3]\).

**Lemma 2.11.** With the notation and conditions of Theorem 2.3 and Proposition 2.9, if \(H_n\) is maximal, then \(G_n \cong G_{n-1}[C_m]\).

**Proof.** Let \(\zeta_m\) be a fixed primitive \(m\)th root of unity, and let \(\{\beta_1, \ldots, \beta_r\}\) be the roots of \(f_{n-1}\). We will refer to \(\sqrt[m]{\beta_i} - c\) as \(\alpha_{i,1}\). Then \(\alpha_{i,2} = \zeta_m \alpha_{i,1}, \alpha_{i,3} = \zeta_m^2 \alpha_{i,1}, \ldots, \alpha_{i,m} = \zeta_m^{m-1} \alpha_{i,1}\).

We know that \(G_n \subseteq G_{n-1}[S_m]\). We will show that an arbitrary element \(\sigma\) of \(G_n\) has the form \(\sigma = (\tau; \pi_1, \ldots, \pi_d)\), where each \(\pi_i \in C_m\). This would imply that \(G_n \subseteq G_{n-1}[C_m]\), and by counting our proof would be complete.

As \(\zeta_m\) must be fixed by \(\sigma\), we know

\[
\sigma (\alpha_{i,j}) = \sigma (\zeta_m^{j-1} \alpha_{i,1}) = \zeta_m^{j-1} \sigma (\alpha_{i,1})
\]

Suppose \(\sigma(\alpha_{i,1}) = \alpha_{\tau(i),k+1} = \zeta_m^k \alpha_{\tau(i),1}\). Then \(\sigma(\alpha_{i,j}) = \zeta_m^{j-1+k} \alpha_{\tau(i),1}\) for each \(j\). That is, we could write \(\pi_i\) in permutation notation as

\[
(1, k+1, 2k+1, \ldots, (m-1)k+1)
\]

where each term is reduced modulo \(m\). So \(\pi_i = (123 \cdots m)^k \in C_m\).

\[
\square
\]

### 2.3 Proof of Theorem 2.3

**Proof.** From Proposition 2.9 and Corollary 2.11, we know that for each \(n\), \(G_n \cong G_{n-1}[C_m]\). As \(G_1 \cong C_m\), we may conclude by induction that \(G_n \cong [C_m]^n\). From Lemma 2.6, we know that, if \(F_n\) refers to the proportion of elements of \(G_n\) that fix at least one root of \(f_n\), then \(\lim_{n \to \infty} F_n = 0\). For any fixed \(p\), we can not take this limit, as we must have that \(f^i(0) \neq f^j(0)\) in \(\mathbb{F}_p\) if \(i, j < n\), and for sufficiently large \(n\) in a fixed \(\mathbb{F}_p\), this condition will not hold. However, as we are taking \(p\) in
the infinite class $E_m$, then, for very large $n$ we will always find a $p$ such that the condition does hold.

Let $C_i = \text{Frob}(p_i)$ where $p_i = (t - c_i)$, $p_i$ is unramified, and $c_i \in \mathbb{F}_p$ is $f$-periodic. Let $C = \bigcup_{i=1}^{N} C_i$. Then, with the notation of Theorem 2.5, $\psi_C$ is the set of unramified periodic points in $\mathbb{F}_p$. We see that $P_{f,p} \leq \frac{\#\psi_C + n + 1}{p + 1}.$

\[
\left| \frac{\#\psi_C + n + 1}{p + 1} - \frac{\#C}{\#G_n} \right| < \left| \frac{\#\psi_C + n + 1}{p + 1} - \frac{\#\psi_C}{p - n} \right| + \left| \frac{\#\psi_C}{p - n} - \frac{\#C}{\#G_n} \right|
\]

\[
< \left| \frac{\#\psi_C + n + 1}{p + 1} - \frac{\#\psi_C}{p - n} \right| + 2g_n \frac{\#C}{\#G_n} \frac{\sqrt{p}}{p - n} + \frac{N \#D}{p - n}.
\]

Let $\epsilon > 0$ and fix $n$ large enough so that $\frac{\#C}{\#G_n} < \frac{\epsilon}{4}$. We know that there exists a prime $p_0 \in E_m$ such that

(i) $p_0 > m$, and

(ii) if $i, j < n, i \neq j$, then $f^i(0) \not\equiv f^j(0) \mod p_0$.

Let $P_m = \{p \in E_m \mid p \geq p_0\}$. Any prime of $P_m$ will also have both properties.

It is clear that $N$ depends only on $G_n$. Let us consider $\#\psi$ and $D$. The only critical number of $f$ is zero, and so the only primes of $\mathbb{F}_p[t]$ ramifying in $\mathcal{O}_{K_n}$ are the $p_{f_k(0)}$ for each $k \in \{1, \ldots, n\}$, and the point at infinity. (This fact is shown in the proof of Proposition 2.9.) Thus $\#\psi = p - n$ and $\#D = n + 1$.

The genus $g_n$ also depends only on $f_n$ and can be bounded for each $n$ independent of choice of $p$ as long as $p \in P_m$. (The following theorem is [24, III.5.6 Corollary], and Abhyankar’s lemma is [24, III.8.9].)

Let $F/K$ be an algebraic function field over $K$. That is, $F/K$ is a finite, algebraic extension of $K(t)$ where $t \in F$ is transcendental over $K$. Let $P \in \mathbb{P}_F$ denote a maximal ideal of some valuation ring $\mathcal{O}_P$ of $F/K$. 


Theorem 2.12. Suppose that $F'/F$ is a finite separable extension of function fields having the same constant field $K$. Let $g$ (resp. $g'$) denote the genus of $F/K$ (resp. $F'/K$). Then

$$2g' - 2 \geq [F' : F] \cdot (2g - 2) + \sum_{P \in \mathbb{P}_F} \sum_{P' | P} (e(P' | P) - 1) \cdot \deg P'$$

Equality holds if and only if $F'/F$ is tame.

Lemma 2.13 (Abhyankar’s Lemma). Let $F'/F$ be a finite separable extension of functions fields. Suppose that $F' = F_1F_2$ is the compositum of two intermediate fields $F \subseteq F_1, F_2 \subseteq F'$. Let $P' \in \mathbb{P}_{F'}$ be an extension of $P \in \mathbb{P}_F$, and set $P_i := P' \cap F_i$. Assume that at least one of the extensions $P_i | P$ is tame. Then

$$e(P' | P) = \text{lcm}\{e(P_1 | P), e(P_2 | P)\}.$$

We have that $K_n/\mathbb{F}_p(t)$ is a finite separable extension of function fields with constant field $\mathbb{F}_p$, and we assume $p \in P_m$. Then $\gcd(p, m) = 1$, so the the extension is tamely ramified.

We have that $K_n$ is the compositum of the fields $L_i$. From Proposition 2.9 we know that the finite primes of $\mathbb{F}_p(t)$ either ramify to degree $m$ in $L_i$ or are unramified, and that there are $n$ such primes. By Abhyankar’s lemma we see that $p_i$ ramifies to degree $m$ in $K_i$, as it ramifies to degree $m$ in each subfield $L_i$. By Propostion 2.9, no further ramification occurs, and each ramifies to degree $m$ in $K_n$. Hence there are $\frac{\#G_n}{m \deg p}$ primes of $K_n$ extending each one. The prime at infinity ramifies to the degree of $f_n$ and have degree 1, so there are $\#G_n/m^n$ of them. The genus of $\mathbb{F}_p(t) = 0$. This gives us

$$2g_n - 2 = -2\#G_n + n \frac{\#G_n}{m}(m - 1) + \frac{\#G_n}{m^n}(m^n - 1),$$

which is independent of $p$.

Then we may select $p \in P_m$ so that both

$$\left| \frac{\#\psi_C + n + 1}{p + 1} - \frac{\#\psi_C}{p - n} \right|$$
and
\[
2g_n \frac{\#C}{\#G_n} \frac{\sqrt{p}}{p - n} + \frac{N\#D}{p - n}
\]
are less than \( \frac{\epsilon}{4} \).

Then \( \left| \frac{\#C_{p+1}}{p+1} - \frac{\#C}{\#G_n} \right| < \frac{\epsilon}{2} \), so \( \frac{\#C_{p+1}}{p+1} < \epsilon \).

Work in this Section was done in collaboration with T. Tucker and P. Kurlberg.
3 Primes Dividing the Orbits of Rational Numbers

In this Chapter we will consider the orbits of rational numbers under the polynomial map \( f(x) = x^m + c \in \mathbb{Q}[x], m \geq 2 \). Let \( a \in \mathbb{Q} \). We will show that the set of primes that both divide \( \mathcal{O}_f(\alpha) \) and are elements of \( E_m \) has natural density zero. This is Theorem 3.2.

This question can be related to periodic points in finite fields. For example, suppose a prime \( p \in \mathbb{Z} \) divides the orbit of \( a \) exactly once. Suppose that \( v_p(a_{n_0}) > 0 \). Then if we considered \( f \) as a map over \( \mathbb{F}_p \), we would see that \( \bar{a}_n = 0 \) in \( \mathbb{F}_p \), where \( \bar{a}_n \) is the reduction of \( a_n \) modulo \( p \). If we know that \( p \) does not divide the orbit of \( a \) again, we know that \( 0 \in \mathbb{F}_p \) is strictly preperiodic under \( f \).

The linkage between the two questions of periodicity of points in finite fields and the density of primes dividing rational orbits extends to the manner of proof. That is, we can relate the question of primes dividing rational orbits to fixed points in Galois groups. We will show that the factorization in the splitting field of \( f^n \) of some primes coming from the critical orbit (that is, \( \mathcal{O}_f(0) \),) forces the Galois group of \( f^n \) to be large, just as in the function field case. The Galois groups that arise can be shown to have few fixed points; this in turn controls the density of primes dividing any orbit.

Iteration of \( f \) in \( \mathbb{Q}[x] \) gives rise to some complications that are not present
in the function field case. The polynomial $f^n(x) - t$ is always irreducible over $\mathbb{F}_p(t)$, whereas $f^n(x)$ is not necessarily irreducible over $\mathbb{Q}$. So we must address the stability of $f$. Further, $(f^n(0) - t)$ is always a prime of $\mathbb{F}_p[t]$, and for large enough $p$, the primes $(f^i(0) - t)$ and $(f^j(0) - t)$ are distinct primes. In the rational case, the numerator of $f^n(0)$ may be composite, so it may be divisible by a power of a prime. Further, it is possible that $f^n(0)$ has positive valuation only at primes that also divided $f^j(0)$ for some $j < n$. Both of these possibilities will affect the ramification of primes in the splitting field $K_n$, and so the maximality of the Galois group $G_n$.

In Section 3.1 we present the theorem and set up notation and the basic idea behind the proof. In Section 3.1.2 we show that, under certain very general circumstances, the factoring of iterates of $f$ is controlled. That is, we show that $f$ is eventually stable. In Section 3.1.3 we discuss the Galois groups of successive iterates of $f$ and show that they are maximal for infinitely many $n$. In Section 3.1.4 we make a counting argument concerning the proportion of elements of the Galois groups that fix at least one root, and, in Section 3.2, we assemble this information and prove the Theorem.

To obtain the result concerning eventual stability, we are required to restrict our choice of constant $c$. We require that there be a prime $q$ of $\mathbb{Z}$ such that $v_q(c) > 0$. In the case that $m = 2$, we are able to relax this condition somewhat, which we do in Section 3.3.

### 3.1 Roots and Galois Groups

Let $f(x) = x^m + c \in \mathbb{Q}[x]$, $m \geq 2$, and suppose that $c = \frac{r}{s}$ with $r, s$ relatively prime integers. Let $\alpha \in \mathbb{Q}$, and consider $O_f(\alpha)$. Although this orbit is a set of rational numbers, we see that the only denominators in the orbit are products of $s$ and primes dividing the denominator of $\alpha$. 

Definition 3.1. Let $K$ be a number field and $R$ its ring of integers. Let $S$ be a finite set of primes of $K$ including the infinite primes. Then the set

$$R_S := \{ a \in K \mid v_p(a) \geq 0 \text{ for all primes } p \notin S \}$$

is called the set of $S$-integers of $K$.

We may consider $\mathcal{O}_f(\alpha)$ as a set of $S$-integers with

$$S = \{ p \in \mathbb{Z} \mid p \text{ is prime and } v_p(c) < 0 \text{ or } v_p(\alpha) < 0 \} \cup M_\infty.$$

Thus our orbit is contained in a ring, rather than a field, and we can discuss prime ideals containing elements in the orbit without ambiguity.

Theorem 3.2. Let $f(x) = x^m + c \in \mathbb{Q}[x]$, with $m \geq 2$, the numerator of $c$ is not $\pm 1$, and $\mathcal{O}_f(0)$ is infinite. Let $E_m = \{ p \in \mathbb{Z} \mid p \text{ is prime, and } p \equiv 1 \pmod{m} \}$. Let $\alpha \in \mathbb{Q}$, and $\mathcal{O}_f(\alpha)$ the forward orbit of $\alpha$ under $f$. Let $a_n = f^n(\alpha)$. Let $S = \{ p \in M_\mathbb{Q} \mid v_p(c) < 0 \text{ or } v_p(\alpha) < 0 \} \cup M_\infty$, and $R_S$ the ring of $S$-integers of $\mathbb{Q}$. Let $P_{f,m,\alpha} = \{ p \in \mathbb{Z} \mid p \in E_m \text{ and } a_n \in (p)R_S \text{ for some } n \}$. Then the natural density of $P_{f,m,\alpha}$ equals 0.

The proof of the theorem follows from the correspondence between primes dividing orbits and their Frobenius classes.

Remark 3.3. Suppose $a_n \in \mathcal{O}_f(\alpha)$ is contained in $(p)R_S$, where $p \in E_m$. Suppose $f^n(x)$ is irreducible for all $n \geq 1$. Then $f^n(x)$ has a root modulo $(p)R_S$. Unless $p$ ramifies in $K_n$, automorphisms in $\text{Frob}(p) \subset G_n$ will fix at least one root of $f^n$.

In Section 3.1.2, we will address the possibility that there is a $k \in \mathbb{N}$ such that $f^k$ is not irreducible. Then we will consider polynomials of the form $g \circ f^n(x)$, where $g \circ f^i(x)$ is irreducible for all $i \geq 0$. We note that if $K_n$ is the splitting field of $g \circ f^n(x)$ over $\mathbb{Q}$, and $G_n = \text{Gal}(K_n/\mathbb{Q})$, then, unless $p$ ramifies in $K_n$, automorphisms in $\text{Frob}(p) \subset G_n$ will fix at least one root of $g \circ f^n$. 
Therefore we may relate the density of primes dividing an orbit via Chebotarev’s Density Theorem to the proportion of automorphisms in $G_n$ that have fixed points. Let $F_n$ be the proportion of automorphisms in $G_n$ that fix at least one root of $g \circ f^n$. We will show in Section 3.1.4 

$$\lim_{n \to \infty} F_n = 0.$$ 

We will make some adjustments to our notation. We will show that $f$ is eventually stable as in definition 1.9. That is, we show that there is a fixed integer $N$, depending only on $f$, such that further iteration of $f$ after $f^N$ causes no further factorization. We will then consider maps of the form $g \circ f^n$ where $g$ is a polynomial divisor of $f^k$ for some $k$, and $g \circ f^n$ is irreducible for all $n \geq 0$. If a prime $p \in E_m$, then $\mathbb{F}_p$ contains a primitive $m$th root of unity. The factorization of $g \circ f^n$ modulo $p$, and thus the permutation group cycle type of the elements in $\text{Frob}(p)$, will reflect the presence of the $m$th roots of unity in $\mathbb{F}_p$. Then automorphisms of the Galois group of $g \circ f^n$ that are in the Frobenius class of a prime belonging to $E_m$ are contained in the subgroup that fixes $\mathbb{Q}(\zeta_m)$, so we will be considering only that subgroup. We will adjust our notation accordingly. Let $K = \mathbb{Q}(\zeta_m)$ where $\zeta_m$ is a primitive $m$th root of unity. Let $K_n$ be the splitting field of $g \circ f^n$ over $K$. Let $G_n = \text{Gal}(K_n/K)$. Let $H_n := \text{Gal}(K_n/K_{n-1})$.

### 3.1.1 Rigid Divisibility

**Definition 3.4. Rigid Divisibility Sequence**

Let $A = \{a_i\}_{i \in \mathbb{N}} \subset K$ be a sequence in a number field $K$. Then $A$ is a rigid divisibility sequence if it has two properties:

(i) For any prime $p$ of $\mathcal{O}_K$ and natural numbers $k, n$, if $v_p(a_n) = e_n > 0$, then $v_p(a_n) = v_p(a_{kn})$.

(ii) If $v_p(a_n) = e_n > 0$ and $v_p(a_k) = e_k > 0$, then $v_p(a_{\text{gcd}(k, n)}) > 0$. 

A consequence of the second condition is that if \( v_p(a_n) = e_n > 0 \) and \( v_p(a_k) = e_k > 0 \), then \( e_k = e_n \).

**Lemma 3.5.** Let \( K \) be a number field, and let \( f(x) = x^n + c \in K[x] \), and suppose that \( O_f(0) \) is infinite. Let \( a_n = f^n(0) \). Then the sequence \( a_1, a_2, a_3, \ldots \) is a rigid divisibility sequence.

**Proof.** Proof of property (i):
Suppose that for some \( n \) and some prime \( p \), we have that \( v_p(a_n) = e > 0 \). We wish to show that for every \( k \in \mathbb{N} \), \( v_p(a_{kn}) = e \). We proceed by induction.
If \( k = 1 \), then \( a_n = a_{kn} \). Suppose the condition holds for \( t \leq k - 1 \). Then \( f^{kn}(0) = f^n \circ f^{(k-1)n}(0) \). We may write \( f^n(x) = f^n(0) + \sum_{i=1}^{m^{n-1}} a_i x^{mi} \). Since \( v_p(\sum_{i=1}^{m^{n-1}} a_i (f^{(k-1)n}(0))^{mi}) \geq em \), then it must be that
\[
v_p\left(f^{kn}(0)\right) = v_p\left(f^n(0) + \sum_{i=1}^{m^{n-1}} a_i (f^{(k-1)n}(0))^{mi}\right) = v_p(f^n(0)) = e.
\]

Proof of property (ii)
By property(i), if \( v_p(a_d) > 0 \) for some \( d \), and the \( d \)th is the first term of the sequence contained in \( p \), then \( 0 \) has exact period \( d \) under \( f \) in \( \mathbb{F}_p \), where \( p = \mathbb{Q} \cap p \).
For any \( k = \ell d + r \), \( a_k \mod p \) will be zero if and only if \( r = 0 \). So if both \( a_k \) and \( a_n \) are in \( p \), then \( d \mid \gcd(k, n) \).

We wish to allow the possibility the \( f \) is not stable. Then we will be considering properties of the translation of iterates of \( f \) by a polynomial divisor \( g \) of \( f^k \) for some \( k \), where \( g \circ f^n \) is irreducible for all \( n \). Thus we wish to extend the rigid divisibility property to a translated orbit of zero. While \( \{g \circ f^n(0)\}_{n \geq 1} \) is not a rigid divisibility sequence, \( \{g \circ f^{kn}(0)\}_{n \geq 0} \) is. (See Example 1.10.)

**Lemma 3.6.** Let \( \{f^n(0)\}_{n \geq 1} \) be a rigid divisibility sequence. Suppose that \( g \) is a polynomial divisor of \( f^k \). Then the sequence \( a_1, a_2, \ldots, a_n, \ldots \), where \( a_n = g \circ f^{kn}(0) \), is a rigid divisibility sequence.
Proof. Proof of property (i)
Suppose that for some prime \( p \), \( v_p(a_n) = e > 0 \). As \( g \) divides \( f^k \), \( v_p(f^k \circ f^{k(n-1)}(0) = v_p(f^{kn}(0)) \geq e \). As \( \{f^n(0)\}_{n \geq 1} \) is a rigid divisibility sequence, \( v_p(f^{knr}(0)) \geq e \) for all \( r \in \mathbb{N} \). Consider \( v_p(a_{n\ell}) \) for any natural number \( \ell \). Suppose that the degree of \( g \circ f^{k(n-1)} = md \). Write

\[
g \circ f^{k(n-1)}(x) = g \circ f^{k(n-1)}(0) + \sum_{i=1}^{d} b_i x^{mi}.
\]

Then

\[
a_{n\ell} = g \circ f^{k(n\ell-1)}(0) = g \circ f^{k(n-1)}(f^{k(n\ell-n)}(0)) = g \circ f^{k(n-1)}(0) + \sum_{i=1}^{md-1} b_i (f^{kn(\ell-1)}(0))^{mi}.
\]

Then, by the ultrametric property, \( v_p(a_{n\ell}) = v_p(g \circ f^{k(n-1)}(0)) = e \). Property (ii) follows immediately.

3.1.2 Eventual Stability

Proposition 3.7. Let \( c \in \mathbb{Q} \), and suppose that there exists a prime \( q \) of \( \mathbb{Z} \) such that \( v_q(c) > 0 \). Then, for any \( m \in \mathbb{Z}_{\geq 2} \), \( f(x) = x^m + c \) is eventually stable over \( \mathbb{Q} \).

Recall from Chapter 1 that a polynomial is eventually stable if there is a finite number of iterates with new factorization. That is, for some \( N \in \mathbb{N} \), if \( n > N \), then

\[
f^n(x) = \prod_{i=1}^{s} g_i \circ f^{n_i}(x)
\]

where \( g_i \circ f^k(x) \) is irreducible for all \( k \geq 0 \). Hence, the maximum number of factors of \( f^n \) for any \( n \) is \( s \).

We will devote Section 3.1.2 to the proof of Proposition 3.7. We take the quadratic case separately, because its proof provides a simpler example of the proof for \( m > 2 \). The proof for \( m > 2 \) follows.

We begin with a Lemma given by Stoll [25].
Lemma 3.8. Let $f(x) = x^2 + c$ where $c \in \mathbb{Q}$. Suppose $f$ is irreducible and $n$ is the least integer greater than one such that $f^n$ is reducible. Then $f^n(x) = g(x)g(-x)$ where $g(x)$ is irreducible over $\mathbb{Q}$.

Proof. Let 

$$f^n(x) = (x - \alpha_1)(x + \alpha_1) \cdots (x - \alpha_{2^{n-1}})(x + \alpha_{2^{n-1}})$$

with $\alpha_i \in \overline{\mathbb{Q}}$. If $f^n$ has a proper, even divisor, $g$, then we may write it as follows, renumbering as necessary:

$$g(x) = (x - \alpha_1)(x + \alpha_1) \cdots (x - \alpha_d)(x + \alpha_d) = (x^2 - \alpha^2_1) \cdots (x^2 - \alpha^2_d)$$

Here $d < 2^{n-1}$. We know that if $\alpha$ is a root of $f^n$, then $f(\alpha)$ is a root of $f^{n-1}$. So we could write

$$f^{n-1}(x + c) = (x + c - f(\alpha_1)) \cdots (x + c - f(\alpha_{2^{n-1}})) = \prod_{i=1}^{2^{n-1}} (x - \alpha^2_i).$$

Then $f^{n-1}(x + c)$ has proper divisor $\hat{g}(x) = \prod_{i=1}^{d} (x - \alpha^2_i)$. We know that $\hat{g}$ is a polynomial in $\mathbb{Q}[x]$, because it has the same coefficients as $g$. Thus $f^{n-1}$ is not irreducible, contrary to our supposition. So $f^n$ can have no proper, even divisor.

Suppose that $g(x)$ is a non-constant, proper divisor of $f^n$. Then so is $g(-x)$, as $f^n$ is even. Let $h(x)$ be a polynomial divisor of both $g(x)$ and $g(-x)$ of minimal positive degree. Then $h(x) \neq h(-x)$, as $h(x)$ divides $f^n$, so it can’t be even. Hence, $h(x)$ and $h(-x)$ are relatively prime, as any common divisor would be a divisor of $g$ of degree less than that of $h$. As $h(x)$ divides both $g(x)$ and $g(-x)$, it must be that $h(-x)$ divides both $g(-x)$ and $g(x)$. Then $h(x)h(-x)$ divides $g(x)$, meaning that $f^n$ has a proper even divisor. So no such $h$ exists. Then $g(x)$ and $g(-x)$ have no common polynomial divisor, so $g(x)g(-x)$ divides $f^n(x)$. As $g(x)g(-x)$ is even, it must be that $g(x)g(-x) = f^n(x)$.
Corollary 3.9. Let $f$ be quadratic and $g$ an irreducible polynomial divisor of $f^k$ for some $k$. If $n \geq 1$ is the least integer such that $g \circ f^n$ is reducible, then $g \circ f^n(x) = h(x)h(-x)$ where $h$ is irreducible.

Proof. As in the proof of the preceding Lemma, noting that $g \circ f^n$ is even for all $n \geq 1$, and letting $r := \deg(g \circ f^n)$, we write $g \circ f^n$ as

$$g \circ f^n(x) = (x - \alpha_1)(x + \alpha_1) \cdots (x - \alpha_r)(x + \alpha_r)$$

with $\alpha_i \in \overline{\mathbb{Q}}$. If $\alpha$ is a root of $g \circ f^n$, then $f(\alpha)$ is a root of $g \circ f^{n-1}$. Hence

$$g \circ f^{n-1}(x + c) = \prod_{i=1}^{r/2} (x + c - f(\alpha_i)) = \prod_{i=1}^{r/2} (x - \alpha_i^2).$$

If $g \circ f^n$ has a proper even divisor, then, as above, $g \circ f^{n-1}$ factors. The remainder of the proof is the same as that of 3.8. \qed

We prove Proposition 3.7 for quadratics.

Proof. We may build a sequence of polynomials $g_1, g_2, \ldots$ with the following properties. Let $g_1$ be a divisor of $f^k$ where $k \geq 1$ and $f^{k-1}$ is irreducible. (Recall that $f^0(x) = x$.) For each subsequent $i$, let $g_i$ be a divisor of $g_{i-1} \circ f^k$ where $k \geq 1$ and $g_{i-1} \circ f^{k-1}$ is irreducible. Such a sequence will be finite if and only if $f$ is eventually stable. We show that this sequence is necessarily finite.

Let $q$ be a prime of $\mathbb{Z}$ such that $v_q(c) = e$. We begin by showing that $v_q(g_1(0)) = \frac{e}{2}$. Suppose first that $f$ is reducible. Then $f(x) = -g(x)g(-x)$, where $g(x) = x - \sqrt{-c}$. Then $f(0) = -g(0)^2$, so $v_q(g(0)) = \frac{1}{2}v_q(f(0))$. If $f$ is irreducible, we apply Lemma 3.8. If $k$ is the least integer so that $f^k$ factors, then $g_1(0)^2 = f^k(0)$, so $v_q(g_1(0)) = \frac{1}{2}f^k(0) = \frac{e}{2}$, by the rigid divisibility property. By Corollary 3.9, $v_q(g_i(0)) = \frac{1}{2}v_q(g_{i-1}(0))$. Thus $v_q(g_k(0)) = 2^{-ke}$. There is a $k_0$ such that $2^{-k_0e}$ will not be divisible by 2, and $g_{k_0} \circ f^n(0)$ can not be a square for $n \geq 0$. Then $g_{k_0} \circ f^n$ will be irreducible for $n \geq 0$, so the sequence will terminate with $g_{k_0}$. \qed
In the proof of the quadratic case, the set of roots of $g \circ f^n$ occurred in pairs $\pm \alpha$. The idea was that if $\alpha$ and $-\alpha$ are Galois conjugates, then a previous iterate must have factored. So our sets of Galois conjugates consisted of exactly one root from each $\pm$ pair. In the case $m > 2$, the same idea applies. We outline it here.

Suppose that $g \circ f^{n-1}$ is irreducible and $g \circ f^n$ factors. Roots of $g \circ f^n$ are naturally partitioned into sets of the form $R_i := \{f^{-1}(\beta_i)\}$ where $\beta_i$ is a root of $g \circ f^{n-1}$. They are also partitioned into sets whose members are all Galois conjugates. That is, let $g \circ f^n = \prod_{j=1}^{d} h_j$ where the $h_j$ are irreducible. Let $C_j = \{\alpha \in \bar{\mathbb{Q}} \mid h_j(\alpha) = 0\}$. The sets $C_j$ form another partition of the roots of $g \circ f^n$.

If $m$ is prime, we will pick exactly one element from each $R_i$ to assemble any particular $C_j$. This is because if $m$ is prime and $\alpha, \zeta_m^j \alpha$ are two distinct roots of $h_j$ then the element $\sigma$ in the Galois group of $h_j$ that maps $\alpha$ to $\zeta_m^j \alpha$ will generate $C_m$. So, if two elements of $R_i$ are Galois conjugates, then $R_i$ is a subset of some $C_j$. Then by the transitivity of $G_{n-1}$, there is only one set $C_j$, so $g \circ f^n$ is not reducible.

If $m$ is not prime, different elements of one $R_i$ could be contained in the same $C_j$, but the way we partition $R_i$ into various $C_j$ has to match a possible cycle type of an element of $C_m$ that is not a generator of $C_m$.

We prove Proposition 3.7 for $m \geq 3$.

Proof. The following lemma is an analogue of Lemma 3.8 for $m \geq 3$.

**Lemma 3.10.** Let $f(x) = x^m + c$ for $m \geq 3$, and let $g(x)$ be an irreducible polynomial divisor of $f^k$ for some $k$. We allow the possibility that $g(x) = x$. Let $g \circ f^{n-1}$ be irreducible over $\mathbb{Q}(\zeta_m)$ for some $n \in \mathbb{N}$, and suppose that $g \circ f^n$ factors. Let $\beta$ be a root of $g \circ f^{n-1}$ in $\bar{\mathbb{Q}}$. Then $f(x) - \beta$ factors over $\mathbb{Q}(\zeta_m, \beta)$, and $f(x) - \beta = \prod_{i=0}^{d-1} h(\zeta_m^i x)$ where $d$ is a divisor of $m$, and $h(x)$ is irreducible over $\mathbb{Q}(\zeta_m, \beta)$. 
Proof. We make use of a classical result, Capelli’s Lemma (see [6] for a proof).

Lemma 3.11. Let \( u(x), v(x) \) be polynomials over a field \( K \), and suppose \( \beta \) is any root of \( u(x) \) in \( \bar{K} \). Then \((u \circ v)(x)\) is irreducible over \( K \) if and only if \( u(x) \) is irreducible over \( K \) and \( v(x) - \beta \) is irreducible over \( K(\beta) \).

Since we assume that \( g \circ f^n \) factors and \( g \circ f^{n-1} \) does not, Capelli’s Lemma tells us that we may consider the factorization of \( f(x) - \beta \) in \( \mathbb{Q}(\zeta_m, \beta) \). Let 
\[
\alpha = \sqrt[\frac{m}{k}]{\beta - c}. \text{ Let } k \text{ be the least positive integer such that } \alpha^k \in \mathbb{Q}(\zeta_m, \beta).
\]

We claim that \( k \) is a divisor of \( m \). Let \( d \in \mathbb{Z} \) be such that \( 0 \leq m - dk < k \). Then, as \( \alpha^m = \alpha^{dk} \alpha^{m-dk} \), it must be that \( m - dk = 0 \), because \( \alpha^{m-dk} \in \mathbb{Q}(\zeta_m, \beta) \), but \( m - dk < k \).

Let \( d = \frac{m}{k} \). We see that \( h(x) = x^k - \alpha^k \) is the minimal polynomial of \( \alpha \) over \( \mathbb{Q}(\zeta_m, \beta) \). Note that 
\[
f(x) - \beta = (x^k - \alpha^k)(x^k - \zeta_d \alpha^k)(x^k - \zeta_{d^2} \alpha^k) \cdots (x^k - \zeta_{d^{d-1}} \alpha^k),
\]
and
\[
x^k - \zeta_d^{j} \alpha^k = \zeta_d^{j} \left( \zeta_d^{d-j} x^k - \alpha^k \right) = \zeta_d^{j} \left( \zeta_{d^j}^k x^k - \alpha^k \right) = \zeta_d^{j} h(\zeta_{d^j} x).
\]

Then
\[
f(x) - \beta = \prod_{j=0}^{d-1} (x^k - \zeta_d^{j} \alpha^k) = \prod_{j=0}^{d-1} \zeta_d^{j} \prod_{j=0}^{d-1} h(\zeta_{d^j} x) = \prod_{j=0}^{d-1} h(\zeta_{d^j} x).
\]

This concludes the proof of Lemma 3.10 \( \square \)

Corollary 3.12. Let \( f(x) = x^m + c \) where \( m \geq 3 \). Let \( g(x) \) be an irreducible polynomial divisor of \( f^n \) for some \( n \). Let \( g \circ f^n \) be irreducible over \( \mathbb{Q}(\zeta_m) \) and suppose that \( g \circ f^n \) factors. Then \( g \circ f^n(x) = \prod_{j=0}^{d-1} h(\zeta_{m^j} x) \) where \( d \) is a divisor of \( m \).
Proof. Let the degree of $g \circ f^{n-1} = r$. If we consider the factorization given in Lemma 3.10, as $\beta$ was arbitrarily chosen, it must be that $f(x) - \beta_i$ has the above factorization over $\mathbb{Q}(\zeta_m, \beta_i)$ for some divisor $k_i$ of $m$ for each $i \in \{1, \ldots, r\}$. For each $i$, we fix $\alpha_i$, where $f(\alpha_i) = \beta_i$, and let $d_i = \frac{m}{k_i}$. Then we have $f(x) - \beta_i = \prod_{j=0}^{d_i-1} h_i(\zeta_m^j x)$, where $h_i(x) = x^{k_i} - \alpha_i^{k_i}$. Let $R_{i,j}$ refer to the set of roots of $h_i(\zeta_m^{-1} x)$. Then $\alpha_1 \in R_{1,1}$. There are $d_i$ such sets of order $k_i$ for each $i$. (It turns out that $d_i = d_k, \forall i, k$, but we haven’t used this fact.)

As we assume that $g \circ f^n$ is not irreducible, we let $g \circ f^n(x) = \prod_{s=1}^{t} \hat{h}_s(x)$ with $\hat{h}_s \in K$ for each $s$. Let $H_s$ refer to the Galois group of $\hat{h}_s$ over $K$. Let $G_{n-1}$ be the Galois group of $g \circ f^{n-1}$ over $K$. Then $G_{n-1}$ acts transitively on the $\beta_i$. Further $G_{n-1}$ is a subgroup of $H_s$ for each $s$, so $H_s$ also acts transitively on the $\beta_i$.

We may select a set of $r - 1$ automorphisms $\{\tau_i \mid 2 \leq i \leq r\}$ from $H_1$ in such a way that $\tau_i$ maps $R_{1,1}$ into $\{f^{-1}(\beta_i)\}$, exactly one $\tau_i$ for each $i$. Let $C_1 := R_{1,1} \cup \tau_2(R_{1,1}) \cup \cdots \cup \tau_r(R_{1,1})$.

Without loss of generality, we may number the $\hat{h}_s$ so that $\hat{h}_1(\alpha_1) = 0$. We claim that $C_1$ is the complete set of Galois conjugates of $\alpha_1$. Then we would have that $\hat{h}_1(x) = h(x) \prod_{i=2}^{r}(x^k - \tau_i(\alpha_1)^k)$. Clearly, for each $i$, every element of $\tau_i(R_{1,1})$ is conjugate to $\alpha_1$. If there were $\gamma \in \{f^{-1}(\beta_i)\} - \tau_i(R_{1,1})$ such that $\gamma$ is a root of $\hat{h}_1(x)$, then there must be an automorphism of $H_1$ mapping $\tau_i(R_{1,1})$ to $\{f^{-1}(\beta_i)\}$ such that the image includes some $\hat{\gamma} \in \{f^{-1}(\beta_1)\} - (R_{1,1})$. But then $\hat{\gamma}$ is conjugate to $\alpha_1$ by transitivity. This is not possible, as the conjugates of $\alpha_1$ that are in $\{f^{-1}(\beta_1)\}$ must be in $R_{1,1}$. Then we must have that $C_1$ is the complete set of Galois conjugates of $\alpha_1$.

We let $C_j := \zeta_m^{-1} C_1$. There are $d_1$ such sets, each of order $rk_1$. The $C_j$ partition the set of roots of $g \circ f$ into sets of Galois conjugates, giving us the desired factorization: $g \circ f^n = \prod_{j=0}^{d-1} \hat{h}(\zeta_m^j x)$ where $d := d_1$ and $\hat{h} := \hat{h}_1$. \qed

Proof. Proof of Proposition 3.7
Consider the sequence of polynomials in $Q(\zeta_m)[x]$, \{g_1, g_2, \ldots \} with the following properties. First, $g_1$ is a divisor of $f^n$ for some $n \geq 1$, where $f^{n-1}$ is irreducible. For subsequent terms in the sequence, $g_i$ is a divisor of $g_{i-1} \circ f^k$ for some $k \geq 1$ where $g_{i-1} \circ f^{k-1}$ is irreducible. We will show that any such sequence must be finite. This will be equivalent to the eventual stability of $f$ over $Q(\zeta_m)$, for if $f$ were not eventually stable, we could build an infinite sequence of this form. If $f$ is eventually stable over $Q(\zeta_m)$, then it is eventually stable over $Q$.

We have assumed that there is a rational prime $q$ such that $v_q(c) > 0$. We select a prime $q$, of $Q(\zeta_m)$ extending $q$, and note that $v_q(c) = e > 0$. Let $D := \{d_1, d_2, \ldots, d_k\}$ be all the positive divisors of $m$ including $m$, but excluding 1. We claim that $v_q(g_1(0)) = \frac{1}{d_1}v_q(f(0))$, for some $d_1 \in D$, and, for $i \geq 2$, $v_q(g_i(0)) = \frac{1}{d_{j_2}}v_q(g_{i-1}(0))$ for some $d_{j_2} \in D$. We do not claim that $d_{j_1} \neq d_{j_2}$. We proceed by induction.

Suppose that the $n$th is the least iterate of $f$ that is reducible. By Corollary 3.12, $f^n(x) = \prod_{\ell=0}^{d_{j_0}-1} g_1(x_m^\ell x)$, where $d_{j_0} \in D$. Then $f^n(0) = (g_1(0))^{d_{j_0}}$, so $v_q(g_1(0)) = \frac{1}{d_{j_0}}v_q(f^n(0))$. Now consider $v_q(g_i(0))$ and $v_q(g_{i-1}(0))$. We write $g_i(x) = g_i(0) + \sum_{k=1}^t a_kx^k$. Now $\sum_{k=1}^d a_k(f^n(0))^k = f^n(0)\sum_{k=1}^d a_k f^n(0)^{k-1}$.

In Section 3.1.1 we showed that the orbit of 0 under $f$ forms a rigid divisibility sequence. Hence $v_q(f^n(0)) = v_q(c) = e$. Then $v_q(\sum_{k=1}^d a_k(f^n(0))^k) \geq e$, whereas $v_q(g_i(0)) \leq v_q(g_1(0)) = \frac{1}{d_{j_2}}v_q(f^n(0)) < e$. By the ultrametric property, $v_q(g_i \circ f^n(0)) = v_q(g_i(0))$.

From 3.12 we know that if $k$ is the least integer such that $g_{i-1} \circ f^k$ factors, then $g_{i-1} \circ f^k(x) = \prod_{\ell=0}^{d_{j_0}} g_i(x_m^\ell x)$. Thus $g_{i-1}(0) = (g_i(0))^{d_{j_i}}$, and $v_q(g_i(0)) = \frac{1}{d_{j_i}}v_q(g_{i-1}(0)) = es_i^{-1}$, where $s_i$ is a product of elements of $D$. We see that $s_i = d_{j_i}s_{i-1}$. By the pigeonhole principle, there will eventually be an $i_0$ such that $es^{-i_0} = v_q(g_{i_0} \circ f^n(0))$ will fail to be divisible by any member of $D$. \(\Box\)

From 3.12, $g_{i_0} \circ f^n$ can only factor if $g_{i_0} \circ f^n(0)$ is a $d_i$th power for some $d_i \in D$. 
so only if there is a $d_{j_0} \in D$ such that $es^{-i_0}$ is divisible by $d_{j_0}$. Then $g_{i_0} \circ f^n(x)$ will be irreducible for all $n$, so the sequence $\{g_1, g_2, \ldots\}$ will terminate with $g_{i_0}$. As this sequence is finite, all such sequences must be finite, and $f$ is eventually stable over $\mathbb{Q}(\zeta_m)$, and therefore over $\mathbb{Q}$.

\[\square\]

3.1.3 Maximality

Let $K_n$ be the splitting field of $g \circ f^n(x)$ over $K := \mathbb{Q}(\zeta_m)$, and $G_n := \text{Gal}(K_n/K)$. Let $H_n$ be the subgroup of $G_n$ fixing $K_n - 1$. We wish to define what it means for $H_n$ to be maximal in this context. Let $\beta_1, \ldots, \beta_r$ be the roots of $g \circ f^n - 1$. These roots are distinct, as $g \circ f^n - 1$ is irreducible. We obtain $K_n$ from $K_n - 1$ by adjoining to $K_n - 1$ the roots of $f(x) - \beta_i$ for each $i$. Let $L_i$ be the splitting field of $f(x) - \beta_i$ over $K_n - 1$, and $J_i := \text{Gal}(L_i/K_n - 1)$. Note that $J_i \cong J_j$ for all $i, j$.

**Definition 3.13.** With the above notation, $H_n$ is maximal if $\#H_n = \#J^r$.

**Lemma 3.14.** Let $K = \mathbb{Q}(\zeta_m)$ and $f(x) = x^m + c$. Suppose that $g \mid f^k$ for some $k \geq 0$ and $g \circ f^n$ is irreducible for all $n \geq 0$. Suppose further that the translated orbit of zero, $\{g(0), g \circ f(0), \ldots\}$, is infinite. Then $H_n$ is maximal for infinitely many $n$.

**Proof.** Let $D := \{d \in \mathbb{Z} \mid d \text{ divides } m \text{ and } d \neq 1\}$ as in the proof of Proposition 3.7. Let $\{p_n\}_{n \geq 1}$ be an infinite sequence of primes of $\mathbb{Z}$. Let $g(0) = \frac{r}{s}$ with $r, s \in \mathbb{Z}$ and $\gcd(r, s) = 1$. Let $c_n = g \circ f^k(0)$, so $c_{p_n} = g \circ f^{p_n}(0)$. Let $\frac{1}{r}c_{p_n} = b_n$.

Let $S = \{p \in M_K \mid v_p(c) < 0\} \cup M_\infty$. Then $b_n$ is an $S$-integer for each $n$.

Let $d_i \in D$ and $\phi_{d_i}$ be the curve given by $g \circ f^2(x) = ry^{d_i}$. If $b_n$ is a $d_i$th power, then $(f^{k(p_n - 1)}(0), \sqrt[d_i]{b_n})$ will be an $S$-integer point on $\phi_{d_i}$. Let $\pi_x : \phi_{d_i} \to \mathbb{P}^1(\mathbb{C})$ be projection on the $x$-coordinate. By the Riemann Hurwitz formula, the genus $g$ of $\phi_{d_i}$ satisfies

$$g = -1 + \frac{1}{2} \sum_{\begin{array}{c} P \text{ramifies} \\ P \end{array}} (e_P - 1).$$
As \( g \circ f^2(x) \) is irreducible over \( \mathbb{Q} \), it is separable. The degree of \( g \circ f^2(x) \) is at least \( m^2 \geq 4 \), so there are at least \( m^2 \) points ramifying to degree 2. Hence, \( \phi_{d_i} \) has positive genus.

Suppose that \( b_n \) is an \( S \)-unit. By Dirichlet’s Unit Theorem, the unit group \( U \) of \( R_S \) is finitely generated. Thus there are finitely many cosets \( u_i U^m \) comprising \( U \). Consider the curve \( \psi_i \) given by \( u_i g \circ f^2(x) = ry^m \) where \( u_i \) is a coset representative. Suppose that \( b_n \) lies in the coset \( u_j U^m \) and that \( u_i = u_j^{-1} \). Then \( (f^{k(p_n-1)-2}(0), \sqrt{u_i b_n}) \) is an \( S \)-integer point on \( \psi_i \). As with \( \phi_{d_i} \), \( \psi_i \) has positive genus.

By Siegel’s Theorem, (see, for example [1, Theorem 7.3.9, Remark 7.3.10]), a curve of positive genus can only contain a finite number of \( S \)-integer points.

Two facts follow. First, \( b_n \) can not be an \( S \)-unit for infinitely many \( n \). Second, there is only a finite number of \( n \) such that \( b_n \) is a \( d_i \)th power.

**Definition 3.15.** Let \( \{a_n\}_{n \geq 1} \) be a sequence in a number field \( K \). If there is a prime \( q \) of \( \mathcal{O}_K \) such that, for some index \( k \), \( v_q(a_k) = e > 0 \), but \( v_q(a_j) = 0 \) for all \( j < k \), then we call \( q \) a primitive prime divisor of \( a_k \).

As the \( c_n \) form a rigid divisibility sequence and \( p_n \) is prime, any prime \( q \) such that \( q \) divides the numerator of \( b_n \) is a primitive prime divisor of \( c_{p_n} \). We know there exists \( N \) such that \( b_n \) is not an \( S \)-unit or a \( d_i \)th power for \( n > N \). Hence, for \( n > N \), \( c_{p_n} \) has a primitive prime divisor \( q \). Further \( v_q(b_n) \neq d_i \) for any \( d_i \) in \( D \). Thus there infinitely many \( n \) such that the sequence \( \{g \circ f^n(0)\}_{n \geq 0} = \{a_n\}_{n \geq 1} \supset c_n \supset c_{p_n} \) has a primitive prime divisor whose exponent in \( a_n \) is not \( d_i \) for any \( d_i \) in \( D \).

Suppose that \( q \in \mathbb{Z} \) is a primitive prime divisor of \( a_n = g \circ f^n(0) \) Let \( g \circ f^n(0) = q^k s_q \) where \( s_q \in \mathbb{Q} \) and both the numerator and denominator of \( b_q \) are relatively prime to \( q \). Suppose further that \( k \neq d_i \) for any \( d_i \) in \( D \) and that \( p \nmid m \), and, for any root \( \theta \) of \( g \) and any extension \( q \) of \( q \) in \( \mathbb{Q}(\zeta_m) \), \( g'(\theta) \notin q \). We have only
ruled out finitely many primes of $\mathcal{O}_K$, so there are infinitely many $n$ for which such $q$ exists. Let $t$ equal the degree of $G_{n-1}$ acting as a permutation group. Let $\beta_1, \ldots, \beta_t$ be the roots of $g \circ f^{n-1}$.

The field $K_n$ is obtained from $K_{n-1}$ by adjoining $\sqrt[\frac{1}{m}]{f(0) - \beta_i}$ for each $i$. Thus

$$\left( \prod_{i=1}^{t} (f(0) - \beta_i) \right)^{\frac{1}{m}} = q^k s_{\frac{1}{m}} \in K_n.$$ 

As $\gcd(k, m) = 1$, we have that $\sqrt[q]{q} \in K_n$. Thus $q$ ramifies to degree $m$ in $K_n$. Let $q_i$ be extensions of $q$ in $\mathbb{Q}(\zeta_m)$. Then each $q_i$ ramifies to degree $m$ in $K_n$, because only primes dividing $m$ ramify in $\mathbb{Q}(\zeta_m)$.

We show that $q$ is unramified in $K_{n-1}$. As in the function field case, if a prime $q$ of $K$ ramifies in $K_{n-1}$, it ramifies in one of the $K(\alpha) \cong K[x]/\theta_i f^{n-1}(x)$ where $\alpha$ is a root of $g \circ f^{n-1}$. Suppose $\mathfrak{P}$ of $\mathcal{O}_K(\alpha)$ is ramified over $K$. Then it contains

$$(g \circ f^{n-1})'(\alpha) = g'(f^{n-1}(\alpha)) \prod_{j=2}^{n} f'(f^{n-j}(\alpha)),$$

because $\mathcal{O}_K(\alpha)/\mathfrak{P}$ must be a separable extension of $K/(\mathfrak{P} \cap K)$. For any $j$, $f^{n-j}(\alpha) \in \{(g \circ f^{j-1})^{-1}(0)\}$. If $\mathfrak{P}$ contains $f^{n-j}(\alpha)$, then $\mathfrak{P}$ contains $g \circ f^{j-1}(0)$. As $j$ ranges between 2 and $n$, primes containing $\prod_{j=2}^{n} f'(f^{n-j}(\alpha))$ are those whose intersections with $K$ contain one of $g \circ f(0), \ldots, g \circ f^{n-1}(0)$. As $q$ is a primitive prime divisor of $g \circ f^{n}(0)$, $g \circ f^{n-j}(0) \notin q$ for any $j > 0$. We have assumed that $g'(f^{n-1}(\alpha)) = g'(\theta)$ where $\theta$ is a root of $g$ is not in $q$ for any extension of $q$ in $\mathcal{O}_{K_0}$. Hence $q$ is unramified in $K_{n-1}$.

Let $\mathfrak{P}_i$ be an extension in $\mathcal{O}_{K_{n-1}}$ of $q$, and suppose without loss of generality that $f(0) - \beta_i \in \mathfrak{P}_i$. We know that $G_{n-1}$ acts transitively on the $\beta_j$, so it must be that, for each $j \in \{1, \ldots, s\}$, $f(0) - \beta_j \in \mathfrak{P}_j$ where $\mathfrak{P}_j$ also extends $q$.

Let $L_i = K_{n-1}(\alpha_i)$ where $\alpha_i = \sqrt[\frac{1}{m}]{f(0) - \beta_i}$. If a prime $M$ of $L_i$ ramifies over $K_{n-1}$, then it contains $f'(\alpha_i) = ma_i^{m-1}$, so its intersection with $K_{n-1}$ contains $f(0) - \beta_i$. Hence, $\mathfrak{P}_i$ ramifies in $L_i$, but not in $L_j$ for $j \neq i$, as $f(0) - \beta_j \notin \mathfrak{P}_i$. 

If \( f(0) - \alpha_j \in \mathfrak{P}_i \), then \( \sqrt[k]{\prod_{i=1}^{l} (f(0) - \beta_i)} \in \mathfrak{P}_i^2 \), in which case \( q \) would ramify in \( K_{n-1} \).

For each \( i \), \( \mathfrak{P}_i \) ramifies to degree \( m \) in \( L_i \), as \( q \) ramifies to degree \( m \) in \( K_n \), and \( K_n \) is a Galois extension. We see that \( [L_i : K_{n-1}] = m \), as \( \mathfrak{P}_i \) ramifies to degree \( m \), and \( [L_i : \mathcal{O}_{K_{n-1}}] \) is at most \( m \). Let \( L = \prod_{j \neq i} L_j \), the compositum. As \( \mathfrak{P}_i \) is unramified in \( L \), \( [K_n : L] = m \), as \( [K_n : L] \) is at most \( m \). As this is true for all \( i \), \( [K_n : K_{n-1}] = m^r \). \( \square \)

### 3.1.4 Probability

Jones [11] uses probability theory to measure the proportion of elements in successive Galois groups of iterated quadratics that fix a root. We use his technique with some adjustments for the different degree of our polynomial, and show that this proportion approaches zero as \( n \) increases.

As before, we will let \( f(x) = x^m + c \). Let \( g \) be a polynomial divisor of \( f^k \) for some \( k \geq 0 \), and suppose further that \( g \circ f^n \) is irreducible over \( K := \mathbb{Q}(\zeta_m) \) for all \( n \geq 0 \). Let \( K_n \) be the splitting field of \( g \circ f^n \) over \( K \) and \( G_n \) the Galois group of \( K_n \) over \( K \). Recall \( K_n \subset K_{n+1} \). This subset relation gives an inverse system of groups with restriction maps. That is, let \( \sigma_j \in G_j \), and suppose \( j > i \). Then let \( \psi_{i,j} \) be the restriction of \( g_j \in G_j \) to \( K_i \). Let

\[
G(f,g) = \lim_{\leftarrow n \in \mathbb{N}} G_n
\]

equipped with the profinite topology.

Then \( G(f,g) \) is a compact, Hausdorff topological group, and so it has a Haar measure. Let \( \mathcal{P} \) be the normalized Haar measure on \( G(f,g) \), so \( \mathcal{P}(G(f,g)) = 1 \). Let \( \Psi_n \) be the projection on \( n \)th coordinate of \( \bar{\sigma} \in G(f,g) \) and \( \mathcal{B} \) be the Borel \( \sigma \)-algebra on \( G(f,g) \). Then the triple \( (G(f,g), \mathcal{B}, \mathcal{P}) \) is a probability space. We
assign to it a set of random variables, \( X_n \), where, for \( \sigma \in G(f, g) \), \( X_n(\sigma) = t \) if \( \Psi_n(\sigma) \) fixes exactly \( t \) roots of \( g \circ f^n \). Then
\[
P(X_n = t) = \frac{\# \{ \sigma \in G_n \mid \sigma \text{ fixes } t \text{ roots of } g \circ f^n \}}{\# G_n}.
\]
The sequence of random variables gives a stochastic process Jones calls the Galois process, and labels \( GP(f, g) \).

**Definition 3.16.** [3, Definitions 3.4,3.5] A stochastic process \( X_1, X_2, \ldots \) is a martingale with respect to a filtration \( F_1, F_2, \ldots \) if

(i) \( X_n \) is integrable for each \( n = 1, 2 \ldots \);

(ii) \( X_1, X_2, \ldots \) is adapted to \( F_1, F_2, \ldots \);

(iii) \( E(X_{n+1} \mid F_n) = X_n \) for each \( n = 1, 2 \ldots \); The process is a supermartingale if the third condition reads \( E(X_{n+1} \mid F_n) \leq X_n \) for each \( n = 1, 2 \ldots \).

The sequence of \( \sigma \)-fields generated by \( X_n \), denoted \( \sigma(X_n) \) gives a filtration, and the sequence \( X_n \) is adapted to it [3, Example 3.3]. As each \( G_n \) is finite, \( X_n \) is integrable. Here we show that the third criterion also holds.

**Theorem 3.17.** [12, Theorem 2.5] Let \( f, g \in K[x] \) be such that \( g \circ f^n \) is separable for all \( n \geq 0 \). Suppose that for \( n \geq 1 \) and every root \( \beta \) of \( g \circ f^{n-1} \), the polynomial \( f(x) - \beta \) is irreducible over \( K_{n-1} \). Then \( GP(f, g) \) is a Martingale.

We refer the reader to [12, p.6] for the proof.

**Claim 3.18.** With \( g, f, \) and \( K \) as in Theorem 3.2, \( GP(f, g) \) is a martingale.

**Proof.** We have assumed that \( g \circ f^n \) is irreducible over \( \mathbb{Q} \) for all \( n \). Hence \( g \circ f^n \) is separable. By Capelli’s Lemma, we know that for each \( \beta_i, f(x) - \beta_i \) is irreducible over \( K(\beta_i) \). For each \( \beta_i := \beta \) and \( \alpha \) where \( f(\alpha) = \beta \), we have the following diagram of field extensions.
By Capelli’s Lemma, as \( g \circ f^{n-1} \) and \( g \circ f^n \) are irreducible, so is \( f(x) - \beta \) over \( K(\beta) \). So \([K(\beta)(\alpha) : K(\beta)] = m\). Let \([K_{n-1} : K(\beta)] = d_1\). Then

\[K_{n-1} = K(\beta)(x_1, \ldots, x_{d_1})\]

Then \(K_{n-1}(\alpha) \subseteq K(\beta)(\alpha)(x_1, \ldots, x_{d_1})\), so \([K_{n-1}(\alpha) : K(\beta)(\alpha)] = d_2 \leq d_1\). Hence \([K_{n-1}(\alpha) : K_{n-1}] = m\). As \([K_{n-1}(\alpha) : K_{n-1}]\) is at most \(m\), it must be that \(f(x) - \beta\) is irreducible over \(K_{n-1}\).

Martingales are of interest to us, because they converge almost surely. Note that a martingale is always a supermartingale.

**Theorem 3.19.** [3, Theorem 4.2, Doob’s Martingale Convergence Theorem] Suppose that \(X_1, X_2, \ldots\) is a supermartingale (with respect to a filtration \(\mathcal{F}_1, \mathcal{F}_2, \ldots\)) such that

\[
sup_n E(|X_n|) < \infty.
\]

Then there is an integrable random variable \(X\) such that

\[
\lim_{n \to \infty} X_n = X \text{ almost surely.}
\]

We have that \(|X_n| = X_n\), and, as \(\{X_n\}_{n \geq 1}\) is a martingale, \(E(X_n) = E(X_1) < \infty\) [3, p.50]. Thus \(\sup_n E(|X_n|) < \infty\). Let \(X = \lim_{n \to \infty} X_n\). Let \(t \in \mathbb{N}\) and suppose that \(Pr\{X = t\} > 0\). As the \(X_n\) are integer-valued, it must be that there exists \(m \in \mathbb{N}\) such that

\[
Pr\left(\bigcap_{i \geq m}\{X_i = t\}\right) = r > 0
\]
for some fixed $r \in \mathbb{Q}_{>0}$. We will show that, if $t > 0$ and $H_n$ is maximal for infinitely-many $n$, then $Pr(\cap_{i \geq m} \{X_i = t\}) < r$ for any fixed $r > 0$.

We make a counting argument to adjust for the difference between the degree of our polynomial and a quadratic one. Of course, our argument reduces to the quadratic case if $m = 2$.

**Lemma 3.20.** Suppose that $H_n$ is maximal. Let $t \in \mathbb{N}$. Then $Pr(X_n = t \mid X_{n-1} = t, X_{n-2} = t, \ldots, X_{n-k} = t) \leq \frac{1}{2}$.

**Proof.** Let the degree of $G_{n-1}$ acting as a permutation group be $r$ and $\beta_1, \ldots, \beta_r$ the roots of $g \circ f^{n-1}$. Thus $\#H_n = m^r$, and $\#G_n = m^r \cdot \#G_{n-1}$. Just as in the proof of Lemma 2.11, we know that $G_n \subseteq G_{n-1}[S_m]$, and as $\zeta_m \in K$, and $\sigma \in G_n$ fixes $\zeta_m$. The rest follows immediately as in Lemma 2.11, and we may assume that $G_n \cong G_{n-1}[C_m]^r$. Let

$$P(X_{n-1} = t, \ldots, X_{n-k} = t) = \frac{k}{\#G_{n-1}}.$$

As, for $n \geq 1, t$ is a multiple of $m$, we may replace $t$ with $mt$; this substitution serves to ease the notation in the calculations below. As always, we assume $m \geq 2$.

Suppose that $X_{n-1}(\sigma) = mt$. The elements $\tau$ of $G_n$ such that $\psi_{n-1,n}(\tau) = \sigma$ have the form $\tau = (\sigma; \pi_1, \ldots, \pi_r)$ with $\pi_i \in C_m$. If $\sigma(\beta_i) \neq \beta_i$, then $\tau$ will not fix any inverse image of $\beta_i$, so $\pi_i$ may be any of the $m$ elements of $C_m$. Thus we have remaining $r - mt$ coordinates. We choose $t$ of these, and place the identity in those positions. The other $mt - t$ positions have $m - 1$ possibilities for $\pi_j$, as we may not place the identity at those positions. This gives us

$$\binom{mt}{t}(m - 1)^{mt-t}m^{r-mt}$$

automorphisms $\tau$ of $G_n$ that restrict to any particular automorphism of $G_{n-1}$ fixing $mt$ roots.

We consider the conditional probability:
\[ P(X_n = mt \mid X_{n-1} = mt, \ldots, X_{n-k} = mt) \]
\[ = \frac{\Pr[(X_n = mt) \cap (X_{n-1} = mt, \ldots, X_{n-k} = mt)]}{\Pr(X_{n-1} = mt, \ldots, X_{n-k} = mt)} \]
\[ = \left( \frac{k^{mt}(m-1)^{mt-t}m^{r-mt}}{#G_n} \right) \left( \frac{#G_{n-1}}{k} \right) \]
\[ = \left( \frac{mt}{t} \right) \frac{(m-1)^{mt}}{m} (m-1)^{-t} \]
\[ = \left( \frac{mt}{t} \right) \frac{mt-1}{t(m-1)} \left( \frac{mt-t-1}{t-1} \right) \left( \frac{m-1}{m} \right)^{mt} \]

For fixed \( k < t \), let \( R(m, t) = \frac{mt-k}{t-k(m-1)} \). Both \( \frac{\partial R}{\partial m} \) and \( \frac{\partial R}{\partial t} \) are negative, and \( (\frac{m-1}{m})^{mt} \) is also decreasing as \( m, t \) increase. Thus \( \left( \frac{mt}{t} \right) \left( \frac{m-1}{m} \right)^{mt} (m-1)^{-t} \) takes its maximum at the minimum values for \( m, t \), that is \( m = 2 \) and \( t = 1 \). Hence,
\[ \left( \frac{mt}{t} \right) \left( \frac{m-1}{m} \right)^{mt} (m-1)^{-t} \leq \left( \frac{2}{1} \right) \left( \frac{2-1}{2} \right)^2 (2-1)^{-1} = \frac{1}{2}. \]
\[ \square \]

**Lemma 3.21.** If \( H_n \) is maximal infinitely often, then
\[ \lim_{n \to \infty} P(X_n > 0) = 0. \]

**Proof.** Let \( X = \lim_{n \to \infty} X_n \). Let \( t \in \mathbb{N} \) and suppose that \( P\{X = t\} > 0 \). There exists \( m \in \mathbb{N} \) and \( r \in \mathbb{Q}_{>0} \) such that
\[ P(\cap_{i \geq m} \{ X_i = t \}) = r > 0, \]
because the \( X_n \) are integer-valued. We fix \( t \in \mathbb{N} \). Let \( C_i = \{ X_i = t \} \).
\[ r \leq P(\cap_{i \geq m} C_i) \leq P(\cap_{i = m}^k C_i) \]
for any integer \( k > m \).
\[ P(\cap_{i = m}^k C_i) = P(C_k \mid \cap_{i = k-1}^m C_i) \cdot P(C_{k-1} \mid \cap_{i = k-2}^m C_i) \ldots P(C_m) \]
Suppose that \( H_n \) is maximal for \( s \) of the iterates between the \( m \)th and \( k \)th. Then
\[ r < P(\cap_{i = m}^k X_i = t) \leq \frac{1}{2^s}. \]
We let \( k \) go to infinity, and, since \( H_n \) is maximal for infinitely-many \( n \), \( s \) goes to infinity as well. Then
\[ r < \lim_{s \to \infty} \left( \frac{1}{2} \right)^s. \]
This conclusion is clearly false, therefore \( P\{X = t\} = 0 \) for all \( t > 0 \). \( \square \)
\section{Proof of Theorem 3.2}

\textit{Proof.} Let $P_{f,m,a} := \{ p \in E_m \mid f^n(a) \in (p)R_S \text{ for some } n \in \mathbb{N}\}$. By Proposition 3.7, we know that there is an $N \in \mathbb{N}$ such that, for all $n \geq N$ we have

$$f^n(x) = \prod_{i=1}^{s} g_i \circ f^{n_i}(x)$$

and $g_i \circ f$ is irreducible for all $n \geq 0$.

We fix $g_i$ and let $a_n = g_i \circ f^n(a)$ for some rational starting point $a$. Let $\mathcal{P}_{i,a} = \{ p \in E_m \mid a_n \in (p)R_S \text{ for some } n \in \mathbb{N}\}$, and $\mathcal{P}_{i,a,N} = \{ p \in \mathcal{P}_{i,a} \mid a_n \in (p)R_S \text{ for some } n \geq N\}$. Let $G_N = \text{Gal}(K_N/Q)$ and $G'_N = \text{Gal}(K_N/Q(\zeta_m))$. Let $C_N = \{ \sigma \in G'_N \mid \sigma \text{ fixes at least one root of } g \circ f^N\}$. Let Frob$_N(p)$ be the Frobenius class of $p$ in $G_N$. Let $P_N = \{ \text{primes } p \mid \text{Frob}(p) \subset C_N\}$.

Let $D(S)$ be the natural density of set $S$.

Let $\sigma \in C_N$, and $\tau = \gamma \sigma \gamma^{-1}$ for some $\gamma \in G_N$. Then $\tau(\zeta_m) = \zeta_m$, and, if $\sigma$ fixes $\alpha$, $\tau$ fixes $\gamma(\alpha)$. Hence, $\tau \in C_N$, so $C_N$ is a union of conjugacy classes in $G_N$. Then, with the triangle inequality, me may apply Chebotarev’s Density Theorem to show that $D(P_N) = \#C_N/\#G_N$.

We claim that $\mathcal{P}_{i,a,N} \subset P_N$. If $q \in E_m$, but $q \notin P_N$, then elements in Frob($q$) have no fixed point is $K_N$. The restriction $\psi_{N,N+\ell}$ maps Frob$_{N+\ell}(q)$ to Frob$_N(q)$. If Frob$_N(q)$ has no fixed points in $K_N$, then Frob$_{N+\ell}(q)$ has none in $K_{N+\ell}$. But $q \in \mathcal{P}_{i,a,N}$ contains $a_{N+\ell}$ for some $\ell$, so if $q \in \mathcal{P}_{i,a,N}$, then $q \in P_N$.

Then $D(\mathcal{P}_{i,a,N}) < D(P_N)$. Further, there is a finite number of primes in $\mathcal{P}_{i,a}$ that ramify in $K_N$ or contain $a_n$ for some $n < N$. Therefore, $D(\mathcal{P}_{i,a,N}) = D(\mathcal{P}_{i,a}) < D(P_N)$.

By Lemma 3.21 there is $N \in \mathbb{N}$ so

$$D(P_{i,a}) < D(P_N) = \#C_N/\#G_N < \#C_N/\#G'_N < \frac{\epsilon}{s}$$

for any $\epsilon > 0$. 

As
\[ P_{f,m,a} = \bigcup_{i=1}^{n} P_{i,a} \]
we know that \( D(P_{f,m,a}) = 0. \)

\[ \square \]

### 3.3 Quadratics

We have shown that, if \( f(x) = x^2 + c \) where \( c \in \mathbb{Q}, \mathcal{O}_f(0) \) is infinite, and where some prime of \( \mathbb{Z} \) divides the numerator of \( c \), then \( f \) is eventually stable. We would like to be able to say something about when this is not the case, that is, when \( c = \frac{1}{s} \) for some \( s \in \mathbb{Z} \). It turns out that there are large classes of \( s \) where we may assert that \( f \) is in fact stable. We hope that some of the techniques illustrated here may be of use in showing that \( f \) is stable under wider conditions.

**Theorem 3.22.** Let \( f(x) = x^2 + \frac{1}{s} \) where \( s \in \mathbb{Z} \). Suppose that \( s < -1 \) or that \( s \geq 4 \) and \( s \) is odd or a power of 2. Suppose further that \( f \) is irreducible. Then \( f \) is stable.

**Proof.** Suppose that \( s < -1 \), and \( f \) is irreducible. Then \( f^n(0) < 0 \) for \( n \geq 2 \), so \( f^n(0) \) is not a positive square. By Lemma 3.8, we know that \( f^n \) is then irreducible. Thus we need only concern ourselves with positive \( s \).

Suppose for the remainder of this Section that \( s > 0 \). Let \( \{a_n\}_{n \in \mathbb{N}} \) be the sequence of numerators of \( f^n(0) \). We note that
\[ a_n = a_{n-1}^2 + s^{2^{n-1}-1}. \]

We would like to establish that, under certain conditions, \( a_n \) is non-square. The denominator of \( f^n(0) \) is always an even power of \( s \) for \( n \geq 2 \). Thus the squareness of \( f^n(0) \), and so the reducibility of iterates of \( f \), depends only on the \( a_n \).

We begin with a few useful facts.
Claim 3.23. When \( s > 1 \), the second iterate of \( f(x) = x^2 + \frac{1}{s} \) factors if and only if \( s \) has the form \( 4t^2(t^2 - 1) \) where \( t \in \mathbb{Z} \) and \( t > 1 \).

Proof. From Lemma 3.8, we know that if \( f^2 \) is not irreducible over \( \mathbb{Q} \), then

\[
f^2(x) = x^4 + \frac{2}{s} x^2 + \frac{s + 1}{s^2} = (x^2 + ax + b)(x^2 - ax + b)
\]

where \( a, b \in \mathbb{Q} \), \( b = \frac{\sqrt{s+1}}{s} \), and \( 2b - a^2 = \frac{2}{s} \). Using the fact that \( s = (\sqrt{s+1} - 1)(\sqrt{s+1} + 1) \), we find that \( a^2 = \frac{2}{\sqrt{s+1}+1} \), so \( \frac{2}{a^2} \in \mathbb{Z} \). Let \( \frac{1}{a^2} = t^2 \). We know that \( t \in \mathbb{Z} \), as the numerator of \( a^2 \) divides 2. Then \( 2t^2 = \sqrt{s+1} + 1 \), so \( s = 4t^2(t^2 - 1) \).

Conversely, we see that if \( s = 4t^2(t^2 - 1) \), then

\[
f^2(x) = (x^2 + \frac{1}{t} x + \frac{2t^2 - 1}{4t^2(t^2 - 1)}) \cdot (x^2 - \frac{1}{t} x + \frac{2t^2 - 1}{4t^2(t^2 - 1)}).
\]

Note that Fact 3.23 implies that \( f^2 \) is irreducible if \( s \) is odd or a power of 2.

We include an example of what such factorization might look like.

Example 3.24. Let \( f(x) = x^2 + \frac{1}{48} \)

\[
f^2(x) = x^4 + \frac{1}{24} x^2 + \frac{49}{2304} = \left( x^2 + \frac{1}{2} x + \frac{7}{48} \right) \left( x^2 - \frac{1}{2} x + \frac{7}{48} \right)
\]

\[
h_1(x)g_2(x)
\]

\[
f^3(x) = x^8 + \frac{1}{12} x^6 + \frac{17}{384} x^4 + \frac{49}{27648} x^2 + \frac{112993}{5308416}
\]

\[
= \left( x^2 - \frac{1}{2} x + \frac{19}{48} \right) \left( x^2 + \frac{1}{2} x + \frac{19}{48} \right) \left( x^4 - \frac{11}{24} x^2 + \frac{313}{2304} \right)
\]

\[
h_{1,1}(x)h_{1,2}(x)g_2(f(x))
\]

\[
f^4(x) = \left( x^4 - \frac{11}{24} x^2 + \frac{7 \cdot 127}{48^2} \right) \left( x^4 + \frac{13}{24} x^2 + \frac{937}{48^2} \right) \cdot \left( x^8 + \frac{1}{12} x^6 - \frac{175}{384} x^4 - \frac{527}{27648} x^2 + \frac{7 \cdot 102871}{48^4} \right)
\]

\[
h_{1,1}(f(x))h_{1,2}(f(x))g_2(f^2(x))
\]
This example serves to illustrate the difficulties that arise once factoring begins if \( f(0) \) has no prime of positive valuation. We see that if \( g_t(x) = (x^2 \pm \frac{1}{2}x + \frac{7}{48}) \), then \( g_t \circ f^{2n}(0) \) is non-square for every \( n \), because \( v_7(g_t \circ f^{2n}(0)) = 1 \). However, this gives us no control outside the rigid divisibility sequence \( \{g \circ f^{2n}(0)\}_{n \geq 0} \), as we can see by the factorization of \( f^4 \). At \( f^4 \) we have begun a rigid divisibility sequence \( \{h_{1,2} \circ f^{3n}(0)\}_{n \geq 0} \) in which 7 will never appear.

**Claim 3.25.** If \( f \) and \( f^2 \) are irreducible, then so is \( f^3 \).

**Proof.** Suppose there are integers \( s \) and \( y \) so that \( f^3(0) = y^2 \). Then we get an integer point on the elliptic curve given by \( x^3 + x^2 + 2x + 1 = y^2 \). The only rational points on this curve are \((0,1)\) and \((0,-1)\) and the point at infinity. 

**Claim 3.26.** If \( s \geq 4 \), then \( f^n(0) < \frac{s-2}{s(s-3)} \).

**Proof.** Note that \( f(0) = \frac{1}{s} < \frac{(s-2)}{s(s-3)} \) as \( \frac{s-2}{s-3} > 1 \). If \( f^{n-1}(0) < \frac{s-2}{s(s-3)} \), then

\[
\frac{f^n(0)}{s^2(s-3)^2} + \frac{1}{s} = \frac{s-2}{s(s-3)} \cdot \frac{s^2 - 3s - 1 + \frac{2}{s-2}}{s(s-3)} < \frac{s-2}{s(s-3)}
\]
as \( \frac{2}{s-2} - 1 < 0 \). 

From the above fact, we see that \( a_n \leq \frac{(s-2)}{(s-3)} s^{2n-1} \). Suppose that \( a_n \) is a square in \( \mathbb{Z} \). Then \( s^{2n-1} = (\sqrt{a_n} - a_{n-1})(\sqrt{a_n} + a_{n-1}) \). It turns out that, if \( s^{2n-1} \) has such a factorization in integers, and \( s \geq 4 \) is odd or a power of 2, then we can show that \( a_n > \frac{(s-2)}{(s-3)} s^{2n-1} \).

**Claim 3.27.** If \( \gcd((\sqrt{a_n} - a_{n-1}), (\sqrt{a_n} + a_{n-1})) = 1 \) if \( s \) is odd, and 2 if \( s \) is even.

**Proof.** We show by induction that for all \( n \geq 1 \), \( \gcd(s, a_n) = 1 \). We see that \( a_1 = 1 \). Suppose that \( \gcd(a_{n-1}, s) = 1 \). If \( r = \gcd(s, a_n) \), then \( r \mid (a_n - s^{2n-1}) = a_{n-1}^2 \). So \( r = 1 \). This means that \( a_n, a_{n-1}, \) and \( s \) are pair-wise relatively prime. Suppose \( d = \gcd((\sqrt{a_n} - a_{n-1}), (\sqrt{a_n} + a_{n-1})) \). Then \( d \mid 2\sqrt{a_n} \) and \( d \mid 2a_{n-1} \). So \( d = 1 \) or
\(d = 2\). If \(s\) is even, then both \(\sqrt{a_n}\) and \(a_{n-1}\) are odd, so their sum and difference is even. Then \(d = 2\). If \(s\) is odd, then, as \(d \mid s\), \(d=1\).

**Claim 3.28.** Suppose that \(s\) is odd. Then, if \(a_n\) is a square,

\[
a_n = \left(\frac{r^{2^{n-1}-1}}{2}\right)^2 + \left(\frac{k^{2^{n-1}-1}}{2}\right)^2 + \frac{s^{2^{n-1}-1}}{2}
\]

where \(k, r\) are relatively prime integers with \(k > r\).

**Proof.** By Fact 3.27, \(s^{2^{n-1}-1}\) has a factorization into relatively prime integers:

\[
s^{2^{n-1}-1} = (\sqrt{a_n} - a_{n-1})(\sqrt{a_n} + a_{n-1}).
\]

Let \(s = rk\) where \(\gcd(r, k) = 1\), \(r^{2^{n-1}-1} = (\sqrt{a_n} - a_{n-1})\), and 
\(k^{2^{n-1}-1} = (\sqrt{a_n} + a_{n-1})\). We allow the possibility that \(r = 1\).

Then \(\sqrt{a_n} = \frac{r^{2^{n-1}-1} + k^{2^{n-1}-1}}{2}\) and

\[
a_n = \left(\frac{r^{2^{n-1}-1}}{2}\right)^2 + \left(\frac{k^{2^{n-1}-1}}{2}\right)^2 + \frac{s^{2^{n-1}-1}}{2}.
\]

With these facts in hand we will continue with the proof of 3.22.

**Case 1:**

Suppose that \(s\) is odd and \(s > 4\). Then we know \(f\) is irreducible, and by Fact 3.23, we know that \(f^2\) is as well. From Fact 3.28, we know that if \(a_n\) is a square, there are relatively prime integers \(r, k\) so that

\[
a_n = \left(\frac{r^{2^{n-1}-1}}{2}\right)^2 + \left(\frac{k^{2^{n-1}-1}}{2}\right)^2 + \frac{s^{2^{n-1}-1}}{2}.
\]

From Fact 3.26, we know that

\[
\left(\frac{r^{2^{n-1}-1}}{2}\right)^2 + \left(\frac{k^{2^{n-1}-1}}{2}\right)^2 + \frac{s^{2^{n-1}-1}}{2} \leq \frac{(s - 2)}{(s - 3)} \cdot s^{2^{n-1}-1}.
\]

Dividing by \(s^{2^{n-1}-1}\) we find that

\[
\frac{1}{4} \left(\frac{r}{k}\right)^{2^{n-1}-1} + \left(\frac{k}{r}\right)^{2^{n-1}-1} + \frac{1}{2} < \frac{s - 2}{s - 3}
\]
Thus
\[
\left( \frac{r}{k} \right)^{2^{n-1}-1} + \left( \frac{k}{r} \right)^{2^{n-1}-1} < \frac{2(s - 1)}{(s - 3)} \quad (3.28.1)
\]

Let \( g(x, y, n) = \left( \frac{x+y}{x} \right)^{2^{n-1}-1} + \left( \frac{x}{x+y} \right)^{2^{n-1}-1} - \frac{2(x^2 + xy - 1)}{(x^2 + xy - 3)}. \) We will show that \( g \) is non-negative for \( x, y \geq 1 \) and \( n \geq 3. \) That would show that \( a_n \) is non-square, for if \( a_n \) were a square, there would be integers \( x \) and \( y, \) with \( r = x \) and \( k = x + y \) and \( s = rk, \) such that \( g \) would be less than zero.

As \( n \) increases, \( \left( \frac{x+y}{x} \right)^{2^{n-1}-1} + \left( \frac{x}{x+y} \right)^{2^{n-1}-1} \) increases. Since \( n > 3, \)
\[
\left( \frac{x+y}{x} \right)^3 + \left( \frac{x}{x+y} \right)^3 - \frac{2(x^2 + xy - 1)}{x^2 + xy - 3} = g(x, y, 3) \leq g(x, y, n)
\]
for all \( n. \)

Suppose that \( y > x. \) Then \( \left( \frac{x+y}{x} \right)^3 > 2^3, \) whereas, for \( s \geq 5, \) \( \frac{2(s-1)}{s-3} \leq 4. \) Then, if \( y > x, \) \( g(x, y, 3) > 0. \) Suppose \( x > y. \) We consider partials. We find that \( \partial g(x,y,3) \) is negative for \( s \geq 5 \) in the cases where it is possible to factor \( s \) as \( x(x+y) \) with \( x > y. \) For any fixed \( y, \) we also see that the limit as \( x \) goes to infinity of \( g(x, y, 3) \) is zero. Thus, for fixed \( y, \) \( g \) decreases toward zero as \( x \) increases, and so \( g(x, y, 3) \) is always non-negative, which implies that \( g(x, y, n) \) is also.

**Case 2:**

Suppose that \( s = 2^k \) for some integer \( k \geq 2. \) Then, if \( a_n \) is a square, \( s^{2^{n-1}-1} = 2^{k(2^{n-1}-1)} = (\sqrt{a_n} - a_{n-1})(\sqrt{a_n} + a_{n-1}) = 2 \cdot 2^{k(2^{n-1}-1)-1}. \) Thus \( \sqrt{a_n} = 1 + 2^{k(2^{n-1}-1)-2}, \) and
\[
a_n = 1 + 2^{2k(2^{n-1}-1)-4} + 2^{k(2^{n-1}-1)-1} \quad (3.28.2)
\]
Dividing by \( s^{2^{n-1}-1} \) as before, and subtracting \( \frac{1}{2} \) from both sides as before, we find that
\[
2^{k(2^{n-1}-1)-4} < \frac{2(s-1)}{s-3} \leq 6 \text{ if } a_n \text{ is a square. Then we would have that } k(2^{n-1} - 1) - 4 < 3. \text{ But } k \text{ is at least 2, and } n \text{ is at least 4.}
\]

We might name other classes of positive integers \( s \) such that we may show \( f(x) = x^2 + \frac{1}{s} \) is stable by using the same techniques. For example, if \( s = 2p \)
where $p$ is an odd prime, then, if $a_n$ were a square, we would have that $\left( \frac{p}{2} \right)^{2^{n-1} - 1} < \frac{2(s-1)}{s-3} < 4$, which is clearly false, as $\left( \frac{p}{2} \right)^{2^{n-1} - 1} > (\frac{3}{2})^7$. However, our goal is to show that $f$ is stable where $s$ is any integer except $-1$, and excepting the cases where $f$ or $f^2$ factors, which we conjecture is true. Thus eliminating specific classes of $s$ in an ad hoc manner does not seem useful.

Work in rational orbits comes from research originally done in collaboration with Adam Towsley.
4 Conclusion

We answered two questions about periodicity and orbits under the same map in different arithmetically interesting sets. The link between these two questions has been the method of proof. We use the fact that large Galois groups coming from wreath products have few elements that fix points.

Odoni showed that the iteration of generic polynomials gives rise to Galois groups that are wreath powers of the full symmetric groups on the degree of the polynomial. This is the most general case, and shows what ”should” happen. We have shown that field extensions that arise from the iteration of certain polynomials can at least contain subgroups that grow in a way that is similar enough to the growth of wreath powers. Below we consider areas where similar techniques to Odoni’s might be applied, and also questions that naturally arise, not from the proof technique, but from our research.

Opportunities for Further Research

Graph Components and Fixed Characteristic

In examples 2.2 and 2.1 one might ask about the components of the orbit graph. The permutation has two, and the three-to-one map has only one. We could
provide example with several components in both settings; multiple components
simply come from multiple periodic cycles. Experimenting in a haphazard way,
one might be led to think that the occurrence of large numbers of components is
very rare. For example, \( x \mapsto x^5 + 2 \) over \( \mathbb{F}_{101} \) has exactly one periodic cycle with
four elements in it.

Suppose that a reasonable heuristic for why orbit graphs for maps with a lot of
preperiodic points appear to have few components is that, as we move backward
through the graph away from periodic cycles, we must experience branching due
to the fact that the map is \( m \)-to-one. Would it then be reasonable to suppose
that over a field where the same map is a permutation we may expect to see more
components than over fields where it is not a permutation?

In the function field setting, we fixed the polynomial \( f \) and varied the char-
acteristic of the fields, \( p \), while keeping our constant field as \( \mathbb{F}_p \). One might ask
what would happen if, rather than change the characteristic to larger and larger
primes, we instead took larger and larger extensions of \( \mathbb{F}_p \).

This is a different question from the one we proved, and one wonders to what
extent Galois theoretic methods will help. For example, suppose we considered a
the cubic map \( x \mapsto x^3 + 2 \). If \( p \equiv 1 \mod 3 \), then we conjecture that the Galois
method would work, as there will be no constant field extension. However in
characteristic 5, we get a constant field extension. That is, over \( \mathbb{F}_5 \), our map is a
permutation, but in \( \mathbb{F}_{25} \) it is not a permutation. Yet, when we move from \( \mathbb{F}_5 \) to
\( \mathbb{F}_{25} \), we keep the permutation of \( \mathbb{F}_5 \), as \( \mathbb{F}_5 \subset \mathbb{F}_{25} \).

*Example 4.1.* Let \( f(x) = x^3 + 2 \) and consider first \( \mathbb{F}_5 \), then \( \mathbb{F}_{25} \). Initially we get
two periodic cycles.

![Diagram](image)
The same map over $\mathbb{F}_{25}$ is 3-to-1, except at 2, where the map ramifies. That dictates where eight of the new points must go—they must fill in the additional two pre-images for every point except 2.

However, can we provide a reasonable heuristic to justify the eventual picture?

**Eventual Stability and Finite Critical Orbit**

In the rational case, our proof depended on two properties of our map. We required that our map have infinite critical orbit and that it be eventually stable.

The Galois groups of iterations of the stable polynomial $f(x) = x^2 - 2$ are never maximal, as the map has finite critical orbit. An even more difficult example is $f(x) = x^2 - 1$. Here $f$ enjoys neither infinite critical orbit nor eventual stability. Work has been done studying this map in the context of iterated monodromy groups (see, for example [17]). The Galois group of the infinite binary tree graph given by the splitting fields of iterations of $x \mapsto x^2 - 1$ is called the basilica group. This group is generated by a finite automaton. These two examples provide a fruitful area for continued research (see for example [2]).
If a map has the property that all of its critical orbits are finite, such as \( x \mapsto x^2 - 1 \), it is called post-critically finite. Post-critically finite rational maps are a subject of study in themselves. Ingram [9] shows that the set of conjugacy classes of post-critically finite polynomials of degree \( d \) with coefficients of algebraic degree less than any fixed integer is a finite and effectively computable set.

**More General Maps**

In our work we considered a map, \( x \mapsto x^m + c \), whose critical orbit furnished a sufficient number of primitive primes. Suppose we consider more general polynomial maps, in particular ones with multiple critical orbits. If the orbits had non-zero intersection, then, even if we had a primitive prime in one critical orbit, it may have appeared in another critical orbit at an earlier iterate. Hence, a primitive in a critical orbit would not guarantee that we get enough new ramification from critical points.

Suppose a map has at least one infinite critical orbit that does not intersect the others and this critical orbit provides an infinite list of primitive primes. Suppose further that the splitting fields of iterations of this map do not have extensions of the constant field. Then is seems reasonable to conjecture that the Galois groups of successive iterations of the map will end up being wreath products, and therefore will have few elements with fixed points. It seems likely that Galois theoretic methods would apply to this problem.
Glossary

This glossary is intended as an aid to readers from outside mathematics, so we have organized it by page number rather than alphabetically. For the same reason, we have omitted definitions of notation if that notation is defined in the text.

• p.1

\( \mathbb{F}_p \): the finite field of \( p \) elements. This is the set \{0, 1, \ldots, p - 1\} with operations addition and multiplication modulo \( p \).

• p.2

\( \mathcal{O}_K \): the ring of integers of the field \( K \). Unfortunately, this coincides with the traditional orbit notation. The ring of integers of a number field is the set of algebraic integers in that field. Such a ring is Dedekind–its ideals have unique factorization, and primes are maximal. (See [10].)

\( v_p(a_{w_0}) \): \( v_p(c) \), where \( c \) is a rational number, means the power to which \( p \) appears in the factorization of the number:

\[ v_5(10) = 1, \quad v_5(50) = 2, \quad v_5(11) = 0, \quad v_5\left(\frac{2}{5}\right) = -1. \]

We can extend this definition to primes in other rings, by saying \( v_p(c) = e \) if \( c \in p^e \) and \( c \notin p^{e+1} \). This gives us a valuation, \( | \cdot |_p \), where

\[ | x |_p = e^{v_p(x)} \]

for some \( e \in (0, 1) \).
Gal\((L/K)\): The Galois group of a field \(L\) over a field \(K\).

\(\bar{K}\): the algebraic closure of a field \(K\).

separable polynomial: A separable polynomial \(f(x)\) is irreducible, and all its roots are distinct.

degree of a permutation group: When a group is considered as acting on a set, the number of elements in the set is the degree of the group as a permutation group. The Galois group of a separable polynomial acts by permuting the roots of the polynomial, so its degree as a group is the degree of the polynomial.

semi-direct product: A product of two groups, one of which acts on the other. Suppose \(H\) acts on \(G\), and denote the action of an element of \(H\) on an element of \(G\) by \(g^h\). Then we could form the product of the two groups with the following multiplication:

\[
(g_1, h_1)(g_2, h_2) = (g_1 g_2^{h_2^{-1}}, h_1 h_2)
\]

unramified: Let \(L\) over \(K\) be a finite extension of fields. Then primes of the ring of integers of \(K\) might factor in \(L\) as a product of primes. Suppose

\[
p\mathcal{O}_L = \prod_{i=1}^{d} \mathfrak{p}_i^{e_i}.
\]

If one of the \(e_i > 1\), we say \(p\) is ramified in \(L\), and that \(\mathfrak{p}_i\) ramifies over \(K\).
extension of a prime: In the above factorization, the primes $\mathfrak{P}$ are said to extend $p$. They all have the property that $\mathfrak{P} \cap O_K = p$.

decomposition group: If $G = \text{Gal}(L/K)$, and $p$ is a prime of $O_K$, then $G$ permutes the primes extending $p$. The subgroup of elements $\sigma \in G$ such that $\sigma(\mathfrak{P}) = \mathfrak{P}$ is the decomposition group of $\mathfrak{P}$. Note that $\sigma$ may not fix $\mathfrak{P}$ element-wise, it just maps the set $\mathfrak{P}$ onto the set $\mathfrak{P}$.

conjugate: Two elements of a group $\gamma, \tau$ are conjugate if $\gamma = \sigma \tau \sigma^{-1}$ for some $\sigma$ in the group. Of extreme importance here is that conjugate elements of a permutation group have the same cycle types. So if a permutation has a fixed point, so do all its conjugates.

• p.8

conjugacy class: Conjugacy partitions a group. The sets in the partition are conjugacy classes.

primitive $m$th root of unity: A number $\zeta_m$ such that $\zeta_m^m = 1$, and $\zeta_m^k \neq 1$ for any integer $k < m$.

where the map ramifies: This means that a map that we would expect to be $k$-to-1 is not $k$-to-1 over some point. It coincides with other notions of ramification.

• p.12

$\mathbb{F}_p(t)$: The field of rational functions with coefficients on $\mathbb{F}_p$. That is, ratios of elements of $\mathbb{F}_p[t]$.

$p_{\alpha} = (t - \alpha)$: The ideal generated by the polynomial $t - \alpha$. This ideal is prime, because $t - \alpha$ is irreducible.

$$p_{\alpha} = \{(t - \alpha)g(t) \mid g(t) \in \mathbb{F}_p[t]\}$$
**principal**: A principal ideal is generated by one element.

**genus**: The genus of a curve is an important invariant. For a topologist, the genus of a surface is the number of handles it has. A donut has genus one, hence the famous joke about the donut, the coffee cup, and the topologist.

- p.15

**compositum**: The compositum of two field $K, L$, is the smallest field containing both.

- p.16

$\left( O_{K_{n-1}} \right)_{p_1}^+$: The localization of a ring $R$ at a maximal ideal $m$, denoted $R_m$ is the subset of the field of fraction of $R$ whose denominators are NOT in $m$. Such a ring is local--it has only one maximal ideal. However, whenever we name a multiplicative subset of $R$, say $S$, and allow elements of $S$ to be denominators, we call that localization as well, although it doesn’t necessarily create a local ring. It is hopefully clear from context which is meant. If a ring is Dedekind, all its localizations at maximal ideals are discrete valuation rings. These have the property that their maximal ideals are principal, and anything in the ring can be written as a power of the generator times a unit, like $u\alpha_i^k$, where $\alpha_i$ generates the maximal ideal of the local ring.

- p.20

$e(P' \mid P)$: This is the ramification index of $P'$ over $P$.

**critical orbit**: The orbit of a critical number.

**tame ramification**: Ramification is tame if it does not divide the characteristic of the field.

- p.23
\( M_\infty \): \( M_K \) refers to the set of equivalent valuations, or primes or places of a number field \( K \). There are two kinds, the finite, which are extensions of the \( p \)-adic valuations on \( \mathbb{Q} \), and infinite, which come from embeddings of \( K \) in \( \mathbb{C} \), one for each real embedding and one for each conjugate pair of complex embeddings. The latter are referred to as \( M_\infty \).

- p.25

**ultrametric property**: We have that \( v_p(\cdot) \) satisfies a stronger version of the triangle inequality. That is, \( v_p(a + b) \geq \min \{ v_p(a), v_p(b) \} \). If \( v_p(a) > v_p(b) \), then \( v_p(a + b) = v_p(b) \).

- p.27

\( \bar{\mathbb{Q}} \): The algebraic closure of \( \mathbb{Q} \). That is, \( \mathbb{C} \) without the transcendentalss.

- p.30

**Galois conjugates**: Roots of the same irreducible polynomial.

- p.32

**S-integer**: defined p.22

- p.34

**unit group** A number field may have infinitely-many units, but Dirichlet showed that the group of units is finitely generated. Then, if you take a quotient of the group by the subgroup of units that are \( m \)th powers, the number of cosets will be finite.

- p. 36 Probability Section

**inverse system**: A set of groups and homomorphisms as described. An element in the inverse limit of this system will be a sequence \( \{ \alpha_i \}_{i \geq 1} \) with
the property that for any $\alpha_j$ in the sequence, $\psi_{i,j}(\alpha_j) = \alpha_i$. Then we can think of $G_n$ as a truncation of every sequence in $G(f,g)$ at the $n$th place.

**compact, Hausdorff topological group:** A topological group is one that is also a space. The group operation and the map sending an element to its inverse are continuous. The important fact here is that a compact, Hausdorff space has a Haar measure.

See [3], Chapter 2 for a discussion of martingales.

- p. 40

$D(S)$: **Natural density** defined on p.2.
Bibliography


