AN ABSTRACT OF THE THESIS OF

Lynda Major Danielson for the degree of Doctor of Philosophy in Mathematics presented on April 27, 1995. Title: The Galois Theory of Iterated Binomials

Redacted for Privacy

Abstract approved: _____

Burton I. Fein

Let K be a field and let $f(x) = x^n - b$ be a binomial in $K[x]$. The iterates of $f(x)$ are the polynomials $f_1(x), f_2(x), \ldots$ in $K[x]$ defined by $f_1(x) = f(x)$, and $f_{m+1}(x) = f(f_m(x))$ for $m \geq 1$. In this dissertation we determine conditions under which the iterates of an irreducible binomial remain irreducible, and if so, we investigate the corresponding Galois groups Ω_m for $m \geq 1$.

Let R be a unique factorization domain with quotient field K. Let $f(x) = x^n - b \in R[x]$ with $0 \neq b \in R$, b a non-unit, and $n > 1$. Assume either

(i) if u is a unit in R, then $u \in R^p$ for all primes p dividing n, or

(ii) if u is a unit in R, then $u \in \{\pm 1\}$.

We show under these conditions that if $f(x)$ is irreducible in $K[x]$, then $f_m(x)$, the m^{th} iterate of $f(x)$, is irreducible in $K[x]$ for all $m \geq 1$. If we assume further that $n = p^t$, for p an odd prime, and $\epsilon_p \notin K$ with ϵ_p a primitive p^{th} root of unity, then we are able to show for a given $m \geq 1$, if none of $c_1, \ldots, c_m$ is in K^p, then $G_m \cong [C_n]^m$, where G_m is the Galois group of $f_m(x)$ over $K(\epsilon_n)$ and $c_k = \prod_{d|k} f_d(0)^{\mu(k/d)}$, for $1 \leq k \leq m$. Restricting our arguments to $R = \mathbb{Z}$ (the integers) and thus $K = \mathbb{Q}$

(the rationals), we show $G_m \cong [C_{p^t}]^m$ except for at most finitely many $b \in K$. We also show if $f(x) = x^p - b$ is irreducible in $\mathbb{Z}[x]$, then $G_2 \cong [C_p]^2$.

The Galois Theory of Iterated Binomials

by

Lynda Major Danielson

A Thesis

submitted to

Oregon State University

in partial fulfillment of
the requirements for the
degree of

Doctor of Philosophy

Completed April 27, 1995
Commencement June 1995

Doctor of Philosophy thesis of Lynda Major Danielson presented on April 27, 1995

APPROVED:

Redacted for Privacy

Major Professor, representing Mathematics

Redacted for Privacy

Head of Department of Mathematics

Redacted for Privacy

Dean of Graduate School

I understand that my thesis will become part of the permanent collection of Oregon State University libraries. My signature below authorizes release of my thesis to any reader upon request.

Redacted for Privacy

Lynda Major Danielson, Author

ACKNOWLEDGEMENTS

I wish to thank first and foremost my advisor, Professor Burton Fein, for all his guidance, help, support, and above all patience.

Christie Gilliland and Troy Warwick are also due special thanks for encouraging me and helping me to finish my first year of graduate school. I am especially grateful to Christie for her steadfast faith in my ability these past six years. I would not have reached this stage in my mathematical career without both of them.

I would also like to thank several of the wonderful teachers I have had along the way. I am especially appreciative of my fifth grade teacher, Tom Briten, for not only spending extra time with me after school to get me caught-up on "long division," but also giving me my first dose of Algebra. I am grateful to my marvelous high-school mathematics teachers, Carol McCloy and Bob Bowman. And thanks to Professors Roger Higdem, Ralph Applebee, and Les Tanner of my undergraduate days. I would also like to thank all of the faculty at Oregon State who assisted me along the way, especially Dennis Garity, Ron Guenther, Juha Pohjanpelto, Bob Burton, Tom Dick, and Gary Musser.

And last, but certainly not least, I wish to thank my husband, Mike, for all of his support and love through this struggle!

TABLE OF CONTENTS

THE GALOIS THEORY OF ITERATED BINOMIALS

1. INTRODUCTION

1.1. STATEMENT OF THE PROBLEM

Let K be a field and let $f(x)$ be a polynomial in $K[x]$, that is

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

with $a_n, \ldots, a_0 \in K$ and $a_n \neq 0$. A nonzero polynomial $f(x)$ is said to be irreducible over K if $f(x)$ is not a constant, and if, whenever $f(x)$ is expressed as a product $f(x) = g(x)h(x)$ with $g(x), h(x) \in K[x]$, then $g(x)$ or $h(x)$ is a constant in K. The iterates of $f(x)$ are the polynomials $f_1(x), f_2(x), \ldots$ in $K[x]$ defined by $f_1(x) = f(x)$, and $f_{m+1}(x) = f(f_m(x))$ for $m \geq 1$. For simplicity, we shall work with monic polynomials, i.e. the leading coefficient a_n is equal to one. A binomial is a polynomial of the form $f(x) = x^n - b$.

This dissertation deals with the problem of determining whether the iterates $f_m(x)$ of an irreducible binomial remain irreducible, and if so, determining the corresponding Galois groups Ω_m for $m \geq 1$.

1.2. HISTORY OF THE PROBLEM

Computing the Galois group for a specific polynomial over the rationals can be difficult. Describing the Galois group for a whole class of polynomials can pose an even bigger problem. In fact, there are few classes of polynomials for which an

explicit description of the Galois group is known. R.W.K. Odoni [12] calculated the Galois groups for the iterates of the polynomial $f(x) = x^2 - x + 1$ over the rationals. He, along with others, also investigated the Galois groups of the iterates of the binomial $x^2 + 1$. We give a brief history of this problem.

In the early 1980's, J. McKay (Concordia, Montreal) posed the following problem.

Let $f_m(x)$ be the m^{th} iterate of $f(x) = x^2+1$ over $\mathbb{Q}$. What is Ω_m, the Galois group of $f_m(x)$ over $\mathbb{Q}$?

This is the natural first step in the study of the Galois groups of iterated binomials, since for linear binomials, Ω_m is trivial for $m \geq 1$.

In 1988, R. W. K. Odoni [14] offered a partial solution to the above question. It is easy to see that all iterates of $x^2 + 1$ are irreducible over the rationals. Odoni was able to prove that the Galois group Ω_m is $[C_2]^m$ for $m \leq 750$, where $[C_2]^m$ denotes the m-fold wreath product of C_2 (the cyclic group of order 2) with itself. He gave an algorithm for testing $\Omega_m \cong [C_2]^m$ for any given m. Odoni was, however, unable to offer a general solution to the problem.

In 1989, J. E. Cremona [3] carried out the algorithm of Odoni up to $m = 5 \cdot 10^7$. He conjectured that $\Omega_m \cong [C_2]^m$ for all m.

In 1992, M. Stoll [18] considered a more general problem with $f(x) = x^2+a \in \mathbb{Z}[x]$, where $-a$ is not a square in $\mathbb{Z}$. With considerably more difficulty, he was able to show that the iterates of $f(x)$ remain irreducible over the rationals. Stoll was also able to compute Ω_m $(m \geq 1)$ for certain a, including the case $a = 1$ of McKay (proving Odoni and Cremona's conjecture). He showed there exist infinitely many $a \in \mathbb{Z}$ with $\Omega_m \ncong [C_2]^m$, for all $m \geq 2$. He also showed there is one special case

(with $a = -2$) yielding $\Omega_m \cong C_{2^m}$, the cyclic group of order 2^m, for all $m \geq 1$. His results still left open the general problem of determining the groups Ω_m, when $a \in \mathbb{Z}$ is given.

1.3. DISSERTATION SUMMARY

We now give a brief outline of the paper.

Chapter 2 begins with notation and standard definitions and results to be used throughout the thesis. Included is a brief review of basic field theory and finite Galois theory. Section 2.2 contains two standard theorems fundamental to the thesis; the first describes the conditions necessary and sufficient for irreducibility of a binomial and the second concerns irreducibility and composition of functions.

Chapter 3 contains a discussion of the irreducibility of the iterates of an irreducible binomial. We investigate the irreducibility of iterates of $x^n - b$, with b an element of a unique factorization domain, including the case b an integer. We are able to show that the iterates of an irreducible binomial over the integers remain irreducible. Section 3.2 demonstrates conditions under which the second iterate of an irreducible binomial of degree 2 is reducible. Concerning the irreducibility of iterates of a binomial over the rationals, two separate approaches are given. The first uses results from diophantine equations. The second employs valuation theory. Both yield conditions which will give rise to irreducible iterates. In the final section we show that for polynomials of degree $n = p^t$, for p an odd prime, if $f_m(x)$ is irreducible in $K[x]$ for all iterates of $f(x) = x^n - b$, and K does not contain any primitive p^{th} roots of unity for all p dividing n, then $f_m(x)$ is irreducible in $K(\epsilon_n)$, where ϵ_n is a primitive n^{th} root of unity. This result is needed for our investigation of the Galois groups of the iterates in Chapter 4.

In Chapter 4, with n still equal to p^t for some odd prime p, we investigate the Galois groups G_m of the iterates $f_m(x)$ over $K(\epsilon_n)$, where K is the quotient field of a unique factorization domain R, and K does not contain a primitive p^{th} root of unity. We also assume the characteristic of K is zero. We begin with a brief discussion of permutation groups and the wreath product of two groups. The second section is an investigation of the Galois groups G_m. We let $b_m = f_m(0)$ and suppose $f_k(x)$ is irreducible in $K(\epsilon_n)[x]$. Using Kummer theory, we show $b_1, \ldots, b_m$ are p-independent in $K(\epsilon_n)$ if and only if $G_m \cong [C_n]^m$, where $[C_n]^m$ is the m^{th} wreath power of the cyclic group of order n. In 4.3 we construct a sequence $\{c_m\}$ of pairwise coprime elements related to the $\{b_m = f_m(0)\}$ generated by the iterated binomials. We add the hypothesis that the units of K are either all p^{th} powers in K or are ± 1. Then we show if none of $c_1, \ldots, c_m$ is in K^p, then $G_m \cong [C_n]^m$. In the final section we restrict our arguments to the case $R = \mathbb{Z}$, hence $K = \mathbb{Q}$, and show $G_m \cong [C_n]^m$ except for possibly finitely many $b \in \mathbb{Z}$. We show specifically that if $f(x) = x^p - b$ is irreducible in $\mathbb{Z}[x]$, then $G_2 \cong [C_p]^2$. Finally, as a consequence of the Schur-Zassenhaus Theorem from group theory, if $f(x) = x^p - b$ is irreducible in $\mathbb{Z}[x]$, then for the Galois group, Ω_m, of f_m over $\mathbb{Q}$, we have $\Omega_m = G_m S$, for some subgroup S of Ω_m with $G_m \cap S = \{1\}$.

2. PRELIMINARIES

2.1. NOTATION AND TERMINOLOGY

We will establish notation and terminology to be used throughout the thesis.

Let K be a field, and let K^* denote the nonzero elements of K. Let $f(x) \in K[x]$, that is

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

with $a_n, \ldots, a_0 \in K$ and $a_n \neq 0$. The sequence $f_1(x), f_2(x), \ldots$ of polynomials in $K[x]$ defined by $f_1(x) = f(x)$, and $f_{m+1}(x) = f(f_m(x))$ will be called the iterates of $f(x)$, with $f_m(x)$ the m^{th} iterate of $f(x)$ for $m \geq 1$. We are concerned with polynomials of the form $f(x) = x^n - b$. We note here for future reference that the m^{th} iterate $f_m(x)$ has degree n^m.

We now review standard terminology and results necessary for our discussion of the irreducibility of $f(x)$ and Galois group of $f(x)$, which can be found in various references, such as [8] or [10].

Let D be an integral domain and let $a, b \in D$. We say that b **divides** a, or that b is a **divisor** of a, denoted $b \mid a$, if there is an element $c \in D$ such that $a = bc$. An element $u \in D$ is called a **unit** of D if u divides 1. We call a and b **associates** if there is a unit $u \in D$ such that $a = ub$; this is the case if and only if a and b divide each other. An element of D is called a **prime** if it is not zero or a unit, and if it has no divisors other than its associates and units.

An integral domain R is called a **unique factorization domain (UFD)** if

(1) every element of R which is not zero or a unit can be written as a product of a finite number of primes, and

(2) the factorization given in (1) is unique except for the order in which the factors are written and the replacement of prime factors by their associates.

Examples. The ring of integers, $\mathbb{Z}$, and $\mathbb{Z}[x]$ are both UFD's. In fact, for any field F, $F[x]$ is a UFD.

Definition 2.1.1 *Let R be a UFD. A set $\mathcal{P}_R$ of primes of R is called a* **complete set of representatives for the primes of** R *if*

(a) $\pi_1,\ \pi_2 \in \mathcal{P}_R,\ \pi_1 \neq \pi_2 \Rightarrow \pi_1$ *and* π_2 *are not associates, and*

(b) π *a prime of* $R \Rightarrow$ *there exists a* $\pi' \in \mathcal{P}_R$ *such that* π *is an associate of* π'.

Examples. $\mathcal{P}_{\mathbb{Z}} = \{2, 3, 5, 7, \ldots\}$ is a complete set of representatives for the primes of $\mathbb{Z}$. $\mathcal{P}_{F[x]} = \{f(x) \mid f(x) \text{ is monic irreducible}\}$ is a complete set of representatives for the primes of $F[x]$.

Throughout the remainder of the thesis, we assume R is a UFD and we have fixed $\mathcal{P}_R$. Then define uniquely for a non-unit $a \in R$, **the prime factorization of** a by $a = u\pi_1^{a_1} \cdots \pi_r^{a_r}$, for u a unit in R, $\pi_1, \ldots, \pi_r \in \mathcal{P}_R$, and $a_1, \ldots, a_r > 0$.

In a UFD any pair of non-zero elements a, b has a **greatest common divisor**, $\gcd(a, b) = (a, b) = \pi_1^{min(a_1,b_1)} \cdots \pi_s^{min(a_s,b_s)}$, where $\{\pi_1, \ldots, \pi_s\}$ is the complete set of primes from $\mathcal{P}_R$ dividing both a and b (allowing some $a_i, b_j = 0$). We note this may be extended to the notion of the $\gcd(c_1, \ldots, c_k)$, for $c_i \in R$ and $k \geq 2$. If $(a, b) = 1$ then a and b are said to be **relatively prime.**

Let R and S be integral domains with $R \subset S$. An element $\alpha \in S$ is **integral over** R if there exists a monic polynomial $f(x) \in R[x]$ with $f(\alpha) = 0$. The set of all elements of S which are integral over R is the **integral closure of** R **in** S. R is **integrally closed in** S when the integral closure of R in S is equal to R. For future reference, we note the following fact about UFD's.

Fact 2.1.2 *Any UFD is integrally closed in its quotient field.*

Let E be an extension of K and let $\alpha \in E$. Recall that α is **algebraic** over K if there is a nonzero polynomial $f(x) \in K[x]$ such that $f(\alpha) = 0$. The extension E of K is an **algebraic extension** of K if each element of E is algebraic over K. The polynomial $f(x) \in K[x]$ **splits completely** in $E[x]$ if

$$f(x) = \prod_{i=1}^{r} (x - \beta_i)^{e_i},$$

for some $\beta_1, \ldots, \beta_r \in E$. E is a **splitting field** for $f(x)$ if $f(x)$ splits completely in $E[x]$ and E is generated over K by the roots in E of $f(x)$. E is **algebraically closed** if every $f(x) \in E[x]$ splits completely in $E[x]$, and E is an **algebraic closure** of K if E/K is algebraic and E is algebraically closed. Recall also that the polynomial $f(x) \in K[x]$ is **irreducible in** $K[x]$ if $f(x) = g(x)h(x)$ for polynomials $g(x), h(x) \in K[x]$ implies one of $g(x), h(x)$ is a unit in K. Also, if the leading coefficient of $f(x)$ is 1, then $f(x)$ is called **monic**.

Suppose $\alpha \in E$ is algebraic over K. Then there is a unique monic irreducible polynomial, $\mathrm{Irr}(\alpha, K)$, in $K[x]$ having α as a root.

We will repeatedly use the following basic fact from field theory.

Fact 2.1.3 *If $\alpha \in \bar{K}$, the algebraic closure of K, then the degree of the irreducible polynomial* $\mathrm{Irr}(\alpha, K)$ *is equal to the degree of the extension $K(\alpha)$ over K; that is,*

$$[K(\alpha) : K] = \textit{ the degree of } \mathrm{Irr}(\alpha, K).$$

Throughout this paper, we only deal with separable algebraic extensions E of K; i.e., if $\alpha \in E$, then α is a simple root of $\mathrm{Irr}(\alpha, K)$. For example, this holds if K has characteristic zero, e.g. $K = \mathbb{Q}$ or any finite extension of $\mathbb{Q}$.

Recall that for α an element of E, the **norm** of α from E to K is defined by

$$N_{E \to K}(\alpha) = \prod_{\sigma} \sigma(\alpha),$$

where the product is taken over the distinct embeddings of E in $\bar{K}$ over K.

We list some of the basic properties of the norm.

Fact 2.1.4 *Let $\alpha \in E$ and let*

$$p(x) = \mathrm{Irr}(\alpha, K) = x^r + c_{r-1}x^{r-1} + \cdots c_0.$$

(i) $N_{E\to K}(\alpha) = ((-1)^r c_0)^{[E:K(\alpha)]} = ((-1)^r p(0))^{[E:K(\alpha)]}$,

(ii) $N_{E\to K}(\alpha)$ *is an element of* K,

(iii) $N_{E\to K}(\alpha\beta) = N_{E\to K}(\alpha)N_{E\to K}(\beta)$ *for all* $\alpha, \beta \in E$,

(iv) if $\alpha \in K$ *then* $N_{E\to K}(\alpha) = \alpha^{[E:K]}$,

(v) if L *is a finite extension of* E *and if* $\alpha \in L$, *then* $N_{L\to K}(\alpha) = N_{E\to K}(N_{L\to E}(\alpha))$,

(vi) if R *is a UFD with quotient field* K *and* $\beta \in E$ *is integral over* R, *then* $N_{E\to K}(\beta) \in R$.

Let E be an algebraic extension of the field K. Let $\mathrm{Aut}(E)$ be the group of automorphisms of E. Define

$$\mathrm{Aut}_K(E) = \{\sigma | \sigma \in \mathrm{Aut}(E) \text{ and } \sigma(a) = a, \ \ \forall a \in K\}.$$

Then $\mathrm{Aut}_K(E)$ is called the **Galois group of** E/K. Suppose H is a subgroup of $\mathrm{Aut}_K(E)$. Define

$$E^H = \{e \in E | \sigma(e) = e, \ \ \forall \sigma \in H\}.$$

Example. Let $E = \mathbb{Q}(\sqrt{2})$, $K = \mathbb{Q}$. Then $\mathrm{Aut}_K(E) = \{id, \sigma\}$, where $\sigma(a + b\sqrt{2}) = a - b\sqrt{2}$, and $E^{\mathrm{Aut}_K(E)} = \mathbb{Q}$.

An algebraic extension E of a field K is called **Galois** if $E^{\mathrm{Aut}_K(E)} = K$. The extension E/K is **finite Galois** if E/K is Galois and $[E : K] < \infty$. We recall that E/K is finite Galois if and only if E is the splitting field of a separable polynomial $f(x) \in K[x]$. A Galois extension E/K is **abelian** if its Galois group G is abelian. A Galois extension E/K is of **exponent** k if $g^k = 1$ for all $g \in G$, the Galois group.

We will invoke the following main result of finite Galois theory.

Theorem 2.1.5 (The Fundamental Theorem of Finite Galois Theory) *If E is a finite dimensional Galois extension of K, then there is a one–to–one correspondence between the set of all intermediate fields of the extension and the set of all subgroups of the Galois group $Aut_K(E)$ (given by $F \mapsto F' = Aut_F(E)$) such that:*

(i) the relative dimension of two intermediate fields is equal to the relative index of the corresponding subgroups; in particular, $Aut_K(E)$ has order $[E : K]$;

(ii) E is Galois over every intermediate field F, but F is Galois over K if and only if the corresponding subgroup $F' = Aut_F(E)$ is normal in $G = Aut_K(E)$; in this case G/F' is (isomorphic to) the Galois group $Aut_K(F)$ of F over K.

For a proof, the reader is referred to [6].

2.2. IRREDUCIBILITY AND COMPOSITION OF FUNCTIONS

The following theorem allows us to determine when the first iterate is irreducible. The case $K = \mathbb{Q}$ and $n = p$, a prime number, is due to Abel.

Theorem 2.2.1 *Let $b \in K$, $b \neq 0$. Then $x^n - b$ is irreducible in $K[x]$ if and only if*

(i) for all prime numbers p such that $p|n$ we have $b \notin K^p = \{a^p \mid a \in K\}$, and

(ii) if $4|n$, *then* $b \notin -4K^4 = \{-4a^4 \mid a \in K\}$.

For a proof, see [8]. The following lemma (see [19]), due to Capelli, establishes a relationship between the irreducibility of consecutive iterates.

Lemma 2.2.2 ("Capelli's Lemma") *Let* $f(x), g(x) \in K[x]$.

(1) Let β *be a root of* $f(x)$. *Then every root of* $g(x) - \beta$ *is a root of* $f(g(x))$. *Conversely, if* α *is a root of* $f(g(x))$, *then* $g(\alpha)$ *is a root of* $f(x)$.

(2) Let E *and* L *be, respectively, the splitting fields for* $f(g(x))$ *and* $f(x)$ *over* K. *Then* $L \subseteq E$.

(3) $f(g(x))$ *is irreducible in* $K[x]$ *if and only if both* $f(x)$ *is irreducible in* $K[x]$ *and* $g(x) - \beta$ *is irreducible in* $K(\beta)[x]$ *for every root* β *of* $f(x)$.

For the convenience of the reader, we include the following elementary proof taken from [5].

Proof. (1) Let α be a root of $g(x)-\beta$. Then $g(\alpha) = \beta$ so $f(g(\alpha)) = f(\beta) = 0$, showing that α is a root of $f(g(x))$. The converse is equally clear. (2) is immediate from (1). Now suppose that β is any root of $f(x)$ and α is a root of $g(x) - \beta$. Then $g(\alpha) = \beta$, so $\beta \in K(\alpha)$ and $f(g(\alpha)) = f(\beta) = 0$. So α is a root of $f(g(x))$. Let m and n be, respectively, the degrees of $g(x)$ and $f(x)$. Then $f(g(x))$ has degree mn and $f(g(x))$ is irreducible in $K[x]$ if and only if $[K(\alpha) : K] = mn$. But $[K(\alpha) : K] = [K(\alpha) : K(\beta)][K(\beta) : K]$. Since β is a root of $f(x)$, $[K(\beta) : K] \leq n$. Since α is a root of $g(x) - \beta \in K(\beta)[x]$, $[K(\alpha) : K(\beta)] \leq m$. Thus $f(g(x))$ is irreducible in $K[x]$ if and only if both $[K(\beta) : K] = n$ and $[K(\alpha) : K(\beta)] = m$, which is equivalent to if $f(x)$ is irreducible in $K[x]$ and $g(x) - \beta$ is irreducible in $K(\beta)[x]$. □

We have now established enough preliminaries to move on to a discussion of the irreducibility of the iterates of an irreducible binomial.

3. THE IRREDUCIBILITY OF THE ITERATES

3.1. OVER CERTAIN UFD'S

In this section, we shall determine sufficient conditions for irreducibility of iterates of binomials over certain UFD's. We shall make use of the properties of the norm. We begin with some general lemmas which will be used repeatedly in what follows.

Lemma 3.1.1 *Let K be a field and let $f(x) = x^n - b \in K[x]$. Assume that $f_m(x)$ is irreducible in $K[x]$ for some m and let $\alpha_m \in \bar{K}$ be a root of $f_m(x)$. Then*

$$N_{K(\alpha_m)\to K}(b + \alpha_m) = (-1)^{n^m} f_m(-b).$$

Proof: Let $\delta_m = b + \alpha_m$. This implies δ_m is a root of $f_m(x - b)$, which is irreducible in $K[x]$ since $f_m(x)$ is irreducible by assumption. (Suppose $f_m(x - b) = g(x)h(x) \in K[x]$. Then set $y = x - b$ so $x = y + b$. Then $f(y) = g(y + b)h(y + b) = G(y)H(y) \in K[y]$.) Since $K(\delta_m) = K(b + \alpha_m) = K(\alpha_m)$, we have $[K(\delta_m) : K] = [K(\alpha_m) : K]$ = the degree of $f_m(x) = n^m$. But the degree of $f_m(x - b)$ equals the degree of $f_m(x)$, implying $f_m(x - b) = \mathrm{Irr}(\delta_m, K)$. And again since $K(\alpha_m) = K(\delta_m)$ we have the norm

$$\begin{aligned} N_{K(\alpha_m)\to K}(\delta_m) &= [(-1)^{n^m} f_m(0 - b)]^{[K(\alpha_m):K(\delta_m)]} \\ &= (-1)^{n^m} f_m(-b). \end{aligned}$$

□

Context: Throughout the remainder of this section, let R be a UFD with quotient field K.

Lemma 3.1.2 *Let $z_1, z_2 \in R$ be non-zero, with z_1 and z_2 relatively prime. Let $n \geq 2$ and $f_1(x) = f(x) = x^n - \frac{z_1}{z_2}$. Let $d_m = z_2^{n^m} f_m(-\frac{z_1}{z_2})$. Then z_2 is relatively prime to d_m, and z_1 divides d_m.*

Proof: Proceed by induction on m.

Suppose first that $m = 1$. We have

$$\begin{aligned} d_1 = z_2^n f_1(-\frac{z_1}{z_2}) &= z_2^n[(-\frac{z_1}{z_2})^n - \frac{z_1}{z_2}] \\ &= (-z_1)^n - z_1 z_2^{n-1} \in R. \end{aligned}$$

Clearly $z_1 | d_1$. Also, since $(z_1, z_2) = 1$, if q is a prime of R dividing z_2, then q does not divide z_1, showing $(z_2, d_1) = 1$.

Now suppose inductively that $d_k = z_2^{n^k} f_k(-\frac{z_1}{z_2}) \in R$, $(z_2, d_k) = 1$, and $z_1 | d_k$, for all $k \leq m$. Then

$$\begin{aligned} d_{m+1} = z_2^{n^{m+1}} f_{m+1}(-\frac{z_1}{z_2}) &= z_2^{n^{m+1}}([f_m(-\frac{z_1}{z_2})]^n - \frac{z_1}{z_2}) \\ &= [z_2^{n^m} f_m(-\frac{z_1}{z_2})]^n - z_1 z_2^{n^{m+1}-1} \\ &= (d_m)^n - z_1 z_2^{n^{m+1}-1} \in R. \end{aligned}$$

By the inductive hypotheses we have $(z_2, d_m) = 1$ which implies if q is a prime of R dividing z_2, then q does not divide d_{m+1}, showing $(z_2, d_{m+1}) = 1$. And since $z_1 | d_m$ by the inductive hypotheses, $z_1 | d_{m+1}$. Thus, by induction we are done. □

We will now suppose $f(x) = x^n - b \in R[x]$. Let α_i be a root of f_i and let $K_i = K(\alpha_i)$ for $i \geq 1$. Then we have the following results.

Corollary 3.1.3 *For all $m \geq 1$, b divides $f_m(-b)$.*

Proof: Applying Lemma 3.1.2 with $z_1 = b$ and $z_2 = 1$, we get the result. □

Before moving on, we require a simple result about UFD's.

Lemma 3.1.4 *Suppose R is a UFD with quotient field K, with α, β non-zero elements of R. Suppose $(\alpha, \beta) = 1$ and $\alpha^k \beta^j = \gamma^p$ for some prime number p, integers k and j, and $\gamma^p \in K$. Then $\alpha^k = u\delta^p$ for some $\delta \in K$ and u a unit in R. Further, if $k \geq 0$, then $\delta \in R$.*

Proof: Let $p_1, \ldots, p_s \in \mathcal{P}_R$ be the set of distinct primes dividing γ. Then $\gamma = u_\gamma p_1^{\gamma_1} \cdots p_s^{\gamma_s}$, for u_γ a unit in R, and $\gamma_i \neq 0$ for $i = 1, \ldots, s$. Thus $\alpha^k \beta^j = \gamma^p = u_\gamma^p p_1^{\gamma_1 p} \cdots p_s^{\gamma_s p}$. Suppose p_i is a prime dividing α^k. Then p_i does not divide β^j since $(\alpha, \beta) = 1$. Therefore, since $p_i^{\gamma_i p}$ divides γ^p, we must have $p_i^{\gamma_i p}$ divides α^k. Since $p_i^{\gamma_i p+1} \nmid \gamma^p$, then $p_i^{\gamma_i p+1} \nmid \alpha^k$. Also note $q|\alpha$, q a prime, implies q is an associate of p_i for some i. Thus, $\alpha^k = u_\alpha (p_{i_1}^{\gamma_{i_1}} \cdots p_{i_t}^{\gamma_{i_t}})^p$, where u_α is a unit in R and $i_j \in \{1, \ldots, s\}$. Clearly, if $k \geq 0$ then $\delta = p_{i_1}^{\gamma_{i_1}} \cdots p_{i_t}^{\gamma_{i_t}} \in R$. □

The next lemma will be used to derive a contradiction in the proof of Theorem 3.1.6.

Lemma 3.1.5 *Let α_m be a root of the m^{th} iterate, $f_m(x)$. Suppose $g(x) = x^n - b - \alpha_m$ is reducible in $K_m[x]$, with $b \in K^*$ and $[K_m : K] = n^m$ (i.e. $f_m(x)$ is irreducible in $K[x]$). Then there is a prime p dividing n, an element $e \in R^*$, and a unit $u \in R$ such that $b = ue^p$.*

Proof: Since $g(x)$ is reducible in $K_m[x]$, by Theorem 2.2.1 there are two possibilities. Either

(i) there is a prime p dividing n such that $b + \alpha_m \in K_m^p$, or

(ii) $4|n$ and $b + \alpha_m \in -4K_m^4$.

In case (i), $b + \alpha_m = \beta^p$ for some prime $p|n$ and some $\beta \in K_m$. We have

$$N_{K_m \to K}(b + \alpha_m) = N_{K_m \to K}(\beta^p) = [N_{K_m \to K}(\beta)]^p.$$

Let $c = N_{K_m \to K}(\beta)$. Then $c \in K$ (see Fact 2.1.4). By Corollary 3.1.3 we have $f_{m-1}(-b) = br$ for some $0 \neq r \in R$ and so by Lemma 3.1.1,

$$\begin{aligned} N_{K_m \to K}(b + \alpha_m) &= (-1)^{n^m} f_m(-b) \\ &= (-1)^{n^m} f_1(f_{m-1}(-b)) \\ &= (-1)^{n^m} f_1(br) \\ &= (-1)^{n^m} [(br)^n - b] \\ &= (-1)^{n^m} b[b^{n-1} r^n - 1] \end{aligned}$$

It follows that

$$(-1)^{n^m} b[b^{n-1} r^n - 1] = c^p. \tag{3.1}$$

Thus $c^p \in R$ since $b, r \in R$. Since c is a root of $x^p - c^p \in R[x]$, then c is integral over the UFD R, implying $c \in R$ (see Fact 2.1.2). Now if p is odd, equation (3.1) becomes

$$b[b^{n-1} r^n - 1] = \pm c^p = (\pm c)^p = c_1^p,$$

for some $c_1 \in R$. Likewise, if $p = 2$, then n is even and equation (3.1) becomes

$$b[b^{n-1} r^n - 1] = c^2.$$

Therefore, case (i) results in the relationship

$$b[b^{n-1} r^n - 1] = c^p,$$

for some prime p dividing n and some $r, c \in R$.

Similarly, in case (ii), there exists $\gamma \in K$ such that $b + \alpha_m = -4\gamma^4 = -(2\gamma^2)^2 = -\beta^2$ for some $\beta \in K_m$. Again, let $c = N_{K_m \to K}(\beta)$. Then $c \in K$, and we have

$$\begin{aligned} N_{K_m \to K}(b + \alpha_m) &= N_{K_m \to K}(-\beta^2) \\ &= N_{K_m \to K}(-1)[N_{K_m \to K}(\beta)]^2 \\ &= (-1)^{[K_m:K]} c^2 \\ &= c^2 \end{aligned}$$

since by assumption $[K_m : K] = n^m$, and in this case, $4|n$, and so n is even. As before, we have

$$\begin{aligned} N_{K_m \to K}(b + \alpha_m) &= (-1)^{n^m} b[b^{n-1} r^n - 1] \text{ for some r} \in R, \\ &= b[b^{n-1} r^n - 1] \end{aligned}$$

since n is even, yielding

$$b[b^{n-1} r^n - 1] = c^2.$$

Thus, in either case (i) or case (ii), we have

$$b[b^{n-1} r^n - 1] = c^p \tag{3.2}$$

for some $p|n$, and some $r, c \in R$.

Since R is a UFD, if q is a prime dividing b, q does not divide $[b^{n-1} r^n - 1]$. Thus b and $b^{n-1} r^n - 1$ are relatively prime. But then by Lemma 3.1.4 we have $b = ue^p$ for some $e \in R$, with u a unit in R. □

We are now in a position to prove the main result of this section concerning the irreducibility of the iterates of a binomial with coefficients from a UFD under certain hypotheses on the units.

Theorem 3.1.6 *Let R be a UFD with quotient field K. Let $f(x) = x^n - b \in R[x]$ with $0 \neq b$, b a non-unit, and $n > 1$. Assume either*

(i) if u is a unit in R, then $u \in R^p$ for all primes p dividing n, or

(ii) if u is a unit in R, then $u \in \{\pm 1\}$.

If $f_1(x) = f(x)$ is irreducible in $K[x]$ then $f_m(x)$ is irreducible in $K[x]$ for all $m \geq 1$.

Proof: We proceed by induction on m. By hypothesis, $f_1(x) = f(x)$ is irreducible in $K[x]$, implying by Theorem 2.2.1 that $b \notin R^p$ for all primes p dividing n. Assume inductively that for some $m \geq 1$ $f_m(x)$ is irreducible in $K[x]$. Let α_{m+1} be a root of $f_{m+1}(x)$. Since $f_{m+1}(x) = f_m(f(x))$, $0 = f_{m+1}(\alpha_{m+1}) = f_m(\alpha_{m+1}^n - b)$ and $\alpha_m = \alpha_{m+1}^n - b$ is a root of $f_m(x)$. Let $K_m = K(\alpha_m)$ and $K_{m+1} = K(\alpha_{m+1})$. Then $f_{m+1}(x)$ is irreducible in $K[x]$ if and only if $[K_{m+1} : K] = \deg(f_{m+1}) = n^{m+1}$. Since $f_m(x)$ is irreducible in $K[x]$ by our inductive assumption, $[K_m : K] = \deg(f_m) = n^m$. Thus it suffices to show that $[K_{m+1} : K_m] = n$. Since α_{m+1} is a root of

$$g(x) = x^n - b - \alpha_m \in K_m[x], \tag{3.3}$$

it suffices to prove that $g(x)$ is irreducible in $K_m[x]$.

Assume by way of contradiction that $g(x)$ is reducible in $K_m[x]$. Therefore, by Lemma 3.1.5 there is a prime p dividing n and an element $e \in R$ such that $b = ue^p$ for some u a unit of R. If p is odd, then by our assumptions (i) and (ii) we have $u = v^p$ for some unit $v \in R$ (either u is a p^{th} power by (i), or $u = 1 = 1^p$ or $u = -1 = (-1)^p$ by (ii)). Then we have $b = ue^p = (ve)^p \in R^p$. But this contradicts Theorem 2.2.1 and the irreducibility of $f_1(x)$. So we have $p = 2$, n is even, say $n = 2k$, and by the previous argument, R is as in case (ii); that is, $u \in \{\pm 1\}$. If $u = 1$, then $b = ue^2 = e^2$ which contradicts the fact that $f_1(x)$ is irreducible. Therefore, we must have $b = ue^2 = -e^2$, and equation (3.2) becomes

$$-e^2[(-e^2)^{2k-1}r^{2k} - 1] = c^2$$

yielding

$$e^2[(e^2)^{2k-1}r^{2k}+1] = c^2. \tag{3.4}$$

If q is a prime of R dividing e^2, then q does not divide $[(e^2)^{2k-1}r^{2k}+1]$, which implies e^2 and $[(e^2)^{2k-1}r^{2k}+1]$ are relatively prime.

Let $p_1,\ldots,p_s \in \mathcal{P}_R$ be the distinct set of primes dividing e. Then $e = u_e p_1^{e_1}\cdots p_s^{e_s}$ so $e^2 = p_1^{2e_1}\cdots p_s^{2e_s}$ since u_e is a unit in R implying $u_e^2 = 1$. Similarly if $q_1,\ldots,q_t$ are the primes dividing $(e^2)^{2k-1}r^{2k}+1 = \gamma$, then $\gamma = u_\gamma q_1^{\gamma_1}\cdots q_t^{\gamma_t}$. $c = u_c p_1^{c_1}\cdots p_s^{c_s} q_1^{d_1}\cdots q_t^{d_t}$, where u_c a unit in R. Since $u_c^2 = 1$, we have $c^2 = p_1^{2c_1}\cdots p_s^{2c_s} q_1^{2d_1}\cdots q_t^{2d_t} = e^2\gamma = p_1^{2e_1}\cdots p_s^{2e_s} u_\gamma q_1^{\gamma_1}\cdots q_t^{\gamma_t}$. Therefore $u_\gamma = 1$ and $\gamma_i = 2d_i$ (using the fact that e and γ are relatively prime). Thus, $\gamma = (e^2)^{2k-1}r^{2k}+1 = q_1^{2d_1}\cdots q_t^{2d_t} = (q_1^{d_1}\cdots q_t^{d_t})^2 = w^2$. But then we have

$$(e^{2k-1}r^k)^2 - w^2 = -1,$$

that is,

$$(e^{2k-1}r^k - w)(e^{2k-1}r^k + w) = -1. \tag{3.5}$$

Now e, r, and w are in R, and we are considering case (ii). Thus, equation (3.5) implies either $e^{2k-1}r^k + w = 1$ and $e^{2k-1}r^k - w = -1$, or $e^{2k-1}r^k + w = -1$ and $e^{2k-1}r^k - w = 1$. In either case, adding the equations yields $2e^{2k-1}r^k = 0$, which leads to the contradiction that either $e = 0$ ($b = -e^2 \neq 0$) or $r = 0$ ($r \neq 0$ by Lemma 3.1.2).

Thus $g(x)$ is irreducible in $K_m[x]$, completing the proof that f_{m+1} is irreducible in $K[x]$. □

The following two corollaries indicate particular UFD's satisfying the hypotheses of Theorem 3.1.6.

Corollary 3.1.7 *Suppose $R = \mathbb{Z}$ or $R = F[T]$ where T is an indeterminate and either $F = \mathbb{Z}$ or F is an algebraically closed field. Let K be the quotient field of R and $f_1(x) = f(x) = x^n - b$ with $0 \neq b \in R$, b a non-unit, and $n > 1$. If $f_1(x)$ is irreducible in $K[x]$, then $f_m(x)$ is irreducible in $K[x]$ for all $m \geq 1$.*

Proof: First note that the units of $F[T]$ are the units of F. Suppose $R = F[T]$ with F an algebraically closed field. Then R is a UFD with every unit a p^{th} power, for all primes p. (This is true since if $u \in F^*$, then $g(x) = x^p - u$ splits completely in $F[x]$, implying there exists some $\alpha \in F$ with $u = \alpha^p$.) If $R = \mathbb{Z}$ or $R = \mathbb{Z}[T]$, then R is a UFD with (the only) units ± 1. Therefore, since R satisfies the hypotheses of Theorem 3.1.6, the corollary is proved. □

Corollary 3.1.8 *Suppose $R = \mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[i]$. Let K be the quotient field of R and $f_1(x) = f(x) = x^n - b$ with $0 \neq b \in R$, b a non-unit, and $n > 1$ odd. If $f_1(x)$ is irreducible in $K[x]$, then $f_m(x)$ is irreducible in $K[x]$ for all $m \geq 1$.*

Proof: The only units of R are ± 1 and $\pm i$. Since n is odd, every prime dividing n is odd. We show all units are in R^p, for all p dividing n. If $p = 2k + 1$ is a prime dividing n, for some integer k, then $1 = 1^p$ and $-1 = (-1)^p$. Now either k is even or k is odd. If k is even, then $k = 2k_1$ for some integer k_1 and $p = 4k_1 + 1$. Thus $i = (1)i = (i^4)^{k-1}i = i^p$ and $-i = (-1)^p i^p = (-i)^p$. Similarly, if k is odd, then $k = 2k_1 + 1$ for some integer k_1 and $p = 4k_1 + 3$. Thus $i = (-i)^p$ and $(-i) = i^p$. Therefore, R satisfies condition (i) of Theorem 3.1.6 and the corollary is proved. □

In the next section we show that the conclusion of Theorem 3.1.6 is false in general. In fact, Theorem 3.2.2 gives some sufficient conditions under which the second iterate of an irreducible polynomial is reducible.

3.2. REDUCIBLE SECOND ITERATES

Context: Throughout this section, let $R \neq (0)$ be a unique factorization domain (of characteristic zero) with field of quotients K. A Pythagorean triple in R is a triple (x, y, z) of elements of R satisfying

$$x^2 + y^2 = z^2 \tag{3.6}$$

The following theorem of Kubota [7] characterizes the Pythagorean triples in R.

Theorem 3.2.1 *If $R \neq (0)$ is a unique factorization domain of characteristic zero, then every Pythagorean triple is of the form*

$$x = \frac{s(u^2 - v^2)}{t}, \quad y = \frac{2suv}{t}, \quad \text{and } z = \frac{s(u^2 + v^2)}{t}, \tag{3.7}$$

with s, u, and v arbitrary elements of R, and t is a factor of 2 relatively prime to s such that $t \mid u^2 \pm v^2$. If, in addition, the element 2 of R is either prime or invertible in R, then every Pythagorean triple is of the form

$$x = w(u^2 - v^2), \quad y = 2wuv, \quad \text{and } z = w(u^2 + v^2), \tag{3.8}$$

with $u, v, w \in R$.

Context: Throughout the remainder of this section, suppose $\sqrt{-1}$ is not an element of K. Then for $z_1, z_2 \in R$ with $(z_1, z_2) = 1$, the polynomial

$$f_1(x) = x^2 + \frac{z_1^2}{z_2^2},$$

is irreducible in $K[x]$ by Theorem 2.2.1. By Lemma 2.2.2(c) with $g(x) = f(x) = f_1(x)$,

$$f_2(x) = f_1(f_1(x)) = (x^2 + \frac{z_1^2}{z_2^2})^2 + \frac{z_1^2}{z_2^2}$$

is irreducible in $K[x]$ if and only if

$$f_1(x) - \beta = x^2 + \frac{z_1^2}{z_2^2} - \beta$$

is irreducible in $K(\beta)[x]$, for β a root of f_1. Since

$$f_1(x) = x^2 + \frac{z_1^2}{z_2^2} = (x + i\frac{z_1}{z_2})(x - i\frac{z_1}{z_2})$$

for $i^2 = -1$, $\beta = \pm i\frac{z_1}{z_2}$ implying $K(\beta) = K(i)$. Therefore,

$$\begin{aligned} f_2(x) \text{ is reducible} &\iff x^2 + \frac{z_1^2}{z_2^2} - (\pm\frac{z_1}{z_2}i) \text{ is reducible in } K(i)[x]. \\ &\iff \frac{z_1^2}{z_2^2} - (\pm\frac{z_1}{z_2}i) = -\alpha^2, \text{ for some } \alpha \in K(i). \end{aligned}$$

Hence, f_2 reducible is equivalent to having a solution to

$$\frac{z_1^2}{z_2^2} - (\pm\frac{z_1}{z_2}i) = -\alpha^2 = -(\frac{c}{d} + \frac{e}{f}i)^2 = -(\frac{c^2}{d^2} - \frac{e^2}{f^2} + 2\frac{ec}{df}i)$$

for $c, d, e, f \in R$ with $(c, d) = 1$ and $(e, f) = 1$. Then

$$\frac{z_1^2}{z_2^2} + \frac{c^2}{d^2} - \frac{e^2}{f^2} - (\pm\frac{z_1}{z_2} - 2\frac{ec}{df})i = 0.$$

Since $i \notin K$, we have

$$\frac{z_1^2}{z_2^2} + \frac{c^2}{d^2} - \frac{e^2}{f^2} = 0 \text{ and } \pm\frac{z_1}{z_2} - 2\frac{ec}{df} = 0, \text{ or}$$

$$\frac{z_1^2}{z_2^2} = \frac{e^2}{f^2} - \frac{c^2}{d^2} \text{ and } \pm\frac{z_1}{z_2} = 2\frac{ec}{df}. \tag{3.9}$$

For future reference, this last equation is equivalent to

$$\pm\frac{z_1}{z_2} = 2\frac{(ec)(ec)}{(df)(ec)} = 2\frac{(ec)^2}{cfde}. \tag{3.10}$$

But now equation (3.9) is equivalent to

$$4\frac{e^2c^2}{d^2f^2} = \frac{e^2}{f^2} - \frac{c^2}{d^2}, \text{ so}$$
$$4e^2c^2 = d^2e^2 - c^2f^2, \text{ or}$$
$$(2ec)^2 + (cf)^2 = (de)^2,$$

a Pythagorean triple.

Since the characteristic of R is zero, by equation (3.7) we have two cases.

Case 1:

$$ec = \frac{s(u^2 - v^2)}{2t}, \quad cf = \frac{2suv}{t}, \quad \text{and } de = \frac{s(u^2 + v^2)}{t}.$$

Together with equation (3.10) this yields

$$\begin{aligned}\pm\frac{z_1}{z_2} &= 2\frac{(ec)^2}{cfde} \\ &= 2\left(\frac{s^2(u^2 - v^2)^2}{2^2t^2}\right)\Big/\left[\frac{2suv}{t} \cdot \frac{s(u^2 + v^2)}{t}\right] \\ &= \frac{(u^2 - v^2)^2}{4uv(u^2 + v^2)}.\end{aligned}$$

Case 2:

$$ec = \frac{suv}{t}, \quad cf = \frac{s(u^2 - v^2)}{t}, \quad \text{and } de = \frac{s(u^2 + v^2)}{t}.$$

Together with equation (3.10) this case yields

$$\begin{aligned}\pm\frac{z_1}{z_2} &= 2\frac{(ec)^2}{cfde} \\ &= \frac{2(suv)^2}{t^2}\Big/\left[\frac{s(u^2 - v^2)}{t} \cdot \frac{s(u^2 + v^2)}{t}\right] \\ &= \frac{2u^2v^2}{(u^2 - v^2)(u^2 + v^2)}.\end{aligned}$$

We have proved the following theorem.

Theorem 3.2.2 *Let $R \neq (0)$ be a UFD of characteristic zero. Let K be the quotient field of R. Suppose $f_1(x) = x^2 + z_1^2/z_2^2$ is irreducible in $K[x]$. Then the second iterate, f_2, is reducible in $K[x]$ if and only if either*

(i)

$$\pm\frac{z_1}{z_2} = \frac{(u^2-v^2)^2}{4uv(u^2+v^2)}, \text{ or}$$

(ii)

$$\pm\frac{z_1}{z_2} = \frac{2u^2v^2}{(u^2-v^2)(u^2+v^2)}.$$

Example. Let $f_1(x) = x^2 + \frac{64}{225} = x^2 + (\frac{8}{15})^2$. Then by Theorem 2.2.1, $f_1(x)$ is irreducible over $\mathbb{Q}$. Now

$$\begin{aligned} f_2(x) &= (x^2 + \frac{64}{225})^2 + \frac{64}{225} \\ &= \frac{1}{50625}(225x^2 + 180x + 136)(225x^2 - 180x + 136) \end{aligned}$$

is reducible over $\mathbb{Q}$. We see this is the result of Theorem 3.2.2, case (ii), with $u = 2$ and $v = 1$.

In the next section, we investigate the irreducibility of iterates over $\mathbb{Q}$.

3.3. OVER THE RATIONALS

Our discussion of the irreducibility of iterates over $\mathbb{Q}$ will require some results from diophantine equations. We begin with a definition taken from [4].

Definition 3.3.1 *Let A, B, and C be non-zero integers. The* **generalized Fermat equation** *is $Ax^p + By^q = Cz^r$ where p, q, and r positive integers. An integer solution (x, y, z) to this equation is called* **proper** *if $gcd(x, y, z) = 1$.*

We will use the following theorem of Darmon and Granville [4].

Theorem 3.3.2 *Let A, B, and C be fixed non-zero integers and p, q, r positive integers such that $1/p + 1/q + 1/r < 1$. Then the generalized Fermat equation*

$$Ax^p + By^q = Cz^r,$$

has only finitely many proper solutions.

This leads us to the main result of this section regarding the irreducibility of iterates of binomials over the rationals.

Theorem 3.3.3 *Let n be a fixed odd integer with $n \geq 5$. Then there exists a finite subset S (depending on n) of $\mathbb{Q}$ such that for $b \in \mathbb{Q}$ and $b \notin S$, if $f_1(x) = x^n - b$ is irreducible in $\mathbb{Q}[x]$, then $f_m(x)$ is irreducible in $\mathbb{Q}[x]$ for all $m \geq 1$.*

Proof: We begin by identifying the set S. For p a prime dividing n, let

$$S'_p = \{(x, y) \mid (x, y, z) \text{ is a proper solution to } x^p - y^{n-1} = z^p\}.$$

Now

$$2p < (p-2)n + 2 = pn - 2n + 2$$

(since if $p = 3$, then $p - 2 = 1$, and $n \geq 5$, so $(p-2)n + 2 \geq 7 > 6 = 2p$ and if $p > 3$ then $p - 2 > 2$ and $n \geq p$). Subtracting p from both sides yields

$$p < pn - 2n - p + 1 = (p-2)(n-1),$$

which implies

$$\frac{1}{n-1} < \frac{p-2}{p} = 1 - \frac{2}{p}.$$

Therefore, $1/p + 1/(n-1) + 1/p < 1$, and by Theorem 3.3.2 (with $A = 1, B = -1, C = 1$), there are only finitely many proper solutions to the equation $x^p - y^{n-1} = z^p$, implying S'_p is a finite set. Let

$$S_p = \{\frac{x_1}{y_1} \in \mathbb{Q} \mid (x_1, y_1) = 1,\ x_1^{n-1} d^n = x^p,\ \text{and } y_1^s = y,$$
$$\text{for } (x, y) \in S_p' \text{ and some } d \in \mathbb{Z},\ 0 \leq s \in \mathbb{Z}\}.$$

Then S_p is a finite set since S_p' is finite. Now define S as

$$S = \bigcup_{p|n} S_p.$$

Then S is finite since it is the finite union of finite sets.

Now suppose $f_1(x) = x^n - b \in \mathbb{Q}[x]$ is irreducible with $b \notin S$. Suppose $b = \frac{z_1}{z_2}$ for integers z_1, z_2 with $(z_1, z_2) = 1$. Let α_m be a root of $f_m(x)$. Let $K_m = \mathbb{Q}(\alpha_m)$. Proceed by induction on m. By assumption, $f_1(x)$ is irreducible in $\mathbb{Q}[x]$. Suppose inductively that $f_k(x)$ is irreducible in $\mathbb{Q}[x]$ for all $k \leq m$. We must show that $f_{m+1}(x)$ is irreducible. By Capelli's Lemma (2.2.2(3) and Theorem 2.2.1, since $f_{m+1}(x) = f_m(f_1(x))$ and n is odd,

$$f_{m+1}(x) \text{ is irreducible in } \mathbb{Q}[x] \iff f_1(x) - \alpha_m \text{ is irreducible in } K_m\ \forall \text{roots } \alpha_m \text{ of } f_m(x)$$
$$\iff \forall\ p|n,\ b + \alpha_m \notin K_m^p\ \forall \text{roots } \alpha_m \text{ of } f_m(x).$$

Suppose to the contrary there exists a p dividing n and $\beta_m \in K_m$ such that

$$b + \alpha_m = \beta_m^p.$$

Let $c = N_{K_m \to \mathbb{Q}}(\beta_m)$. Then $c \in \mathbb{Q}$ and

$$\begin{aligned} N_{K_m \to \mathbb{Q}}(b + \alpha_m) &= N_{K_m \to \mathbb{Q}}(\beta_m^p) \\ &= [N_{K_m \to \mathbb{Q}}(\beta_m)]^p \\ &= c^p. \end{aligned}$$

By Lemma 3.1.1 and since n is odd, we have

$$N_{K_m \to \mathbb{Q}}(b + \alpha_m) = (-1)^{n^m} f_m(-b) = -f_m(-b).$$

Together with the above, we have two cases. First, if $m = 1$, then the situation is

$$-f_1(-b) = c^p, \text{ which implies}$$
$$-[(-b)^n - b] = c^p, \text{ or}$$
$$b[(-b)^{n-1} + 1] = c^p.$$

But, b and $[(-b)^{n-1} + 1]$ are relatively prime, implying $b \in \mathbb{Q}^p$ (by Lemma 3.1.4 and using the fact that p is odd), a contradiction to $f_1(x)$ irreducible (by Theorem 2.2.1).

Second, if $m > 1$, we have

$$-f_m(-b) = c^p, \text{ which implies}$$
$$-[(f_{m-1}(-b))^n - b] = c^p, \text{ or}$$
$$-[(f_{m-1}(-b))^n - \frac{z_1}{z_2}] = c^p.$$

Multiplying by $-z_2^{n^m}$ yields

$$[z_2{}^{n^{m-1}} f_{m-1}(-b)]^n - z_2^{n^m}(\frac{z_1}{z_2}) = z_2^{n^m} c^p,$$

or

$$[z_2{}^{n^{m-1}} f_{m-1}(-b)]^n - z_1 z_2{}^{n^m - 1} = z_2^{n^m} c^p. \tag{3.11}$$

By Lemma 3.1.2, $d_{m-1} = z_2^{n^{m-1}} f_{m-1}(-b) \in \mathbb{Z}$, and clearly $z_1 z_2^{n^m - 1} \in \mathbb{Z}$, which implies $z_2^{n^m} c^p \in \mathbb{Z}$. Thus, let $c_1^p = (z_2^{n^m/p} c)^p$ (recall $p|n$). Equation (3.11) becomes

$$d_{m-1}^n - z_1 z_2^{n^m - 1} = c_1^p. \tag{3.12}$$

By Lemma 3.1.2, z_1 divides d_{m-1}, say $d_{m-1} = z_1 d'_{m-1}$. Then equation (3.12) is now

$$z_1[z_1^{n-1}(d'_{m-1})^n - z_2^{n^m - 1}] = c_1^p.$$

But z_1 and $z_1^{n-1}(d'_{m-1})^n - z_2^{n^m-1}$ are relatively prime, so again by Lemma 3.1.4 z_1 is a p^{th} power, and $z_1^{n-1}(d'_{m-1})^n - z_2^{n^m-1}$ is a p^{th} power; that is, $z_1 = (z'_1)^p$ and

$$z_1^{n-1}(d'_{m-1})^n - z_2^{n^m-1} = [(z'_1)^{n-1}(d'_{m-1})^{n/p}]^p - (z_2^{n^{m-1}+n^{m-2}+\cdots+1})^{n-1} = c_2^p, \quad (3.13)$$

for some $z'_1, c_2 \in \mathbb{Z}$. Therefore, we are in the situation

$$x^p - y^{n-1} = z^p \quad (3.14)$$

for some $x, y, z \in \mathbb{Z}$, i.e. $(x, y) \in S'_p$. But we then have $x^p = z_1^{n-1}(d'_{m-1})^n$ and $y = z_2^{n^{m-1}+n^{m-2}+\cdots+1}$ implying $b = \dfrac{z_1}{z_2} \in S_p \subseteq S$, a contradiction. Therefore, f_{m+1} is irreducible in $\mathbb{Q}[x]$, completing the induction. □

Remark 3.3.4 *Let $f(x) = x^n - b \in \mathbb{Q}[x]$ with n odd and $n \geq 5$. Then Theorem 3.3.3 implies that, except for finitely many b, if $f(x)$ is irreducible over $\mathbb{Q}$ then so is $f_m(x)$ for all $m \geq 1$. We note that in this context we have not discovered an example where $f(x)$ is irreducible and $f_m(x)$ is reducible for some $m > 1$.*

Remark 3.3.5 *Theorem 3.2.2 shows Theorem 3.3.3 does not hold for $n = 2$. Also the proof of Theorem 3.3.3 does not go through for n even, since if $p = 2$, then equation (3.14) becomes*

$$x^2 - y^{n-1} = z^2,$$

and we have $1/2 + 1/(n-1) + 1/2 > 1$ for all $n > 1$, and Theorem 3.3.2 doesn't apply. Similarly, if $n = 3$, the argument fails since then $p = 3$ and we have $1/3 + 1/2 + 1/3 > 1$. In this case, infinitely many solutions to equation (3.14) are known (see [4]), but it is not clear if any satisfy equation (3.13). We do note, however, for any given m, $f_m(x)$ is irreducible except for finitely many $b = z_1/z_2$, since equation (3.13) becomes

$$[(z'_1)^{n-1}(d'_{m-1})^{n/p}]^p - (z_2^{n-1})^{(n^{m-1}+n^{m-1}+\cdots+1)} = c_2^p,$$

and $1/p + 1/(n^{m-1} + n^{m-1} + \cdots + 1) + 1/p < 1$ since $m \geq 2$ and $n \geq p$.

3.4. OVER ALGEBRAIC NUMBER FIELDS

For a discussion of the irreducibility of iterates over other number fields, we will need to review some elementary algebraic number theory. A complete treatment of the material can be found in [20].

A **nonarchimedean valuation** of the field F is a function φ from F into the nonnegative reals such that

(i) $\varphi(a) = 0 \iff a = 0$,

(ii) $\varphi(ab) = \varphi(a)\varphi(b)$,

(iii) $\varphi(a+b) \leq \max\{\varphi(a), \varphi(b)\}$.

There is also the notion of an *archimedean valuation.* However, we will only be concerned with nonarchimedean valuations in this section. Let valuation refer to a nonarchimedean valuation.

One example of a valuation is the *trivial valuation* of F defined $\varphi(0) = 0$, $\varphi(a) = 1$ for $a \neq 0 \in F$.

A nonarchimedean valuation φ determines a Hausdorff topology T_φ on F. For each $a \in F$, a fundamental system of neighborhoods of a is given by the set of all

$$U(a, \epsilon) = \{b \in F | \varphi(a - b) < \epsilon\}.$$

We say two valuations φ_1 and φ_2 are **equivalent** (and denote this by $\varphi_1 \sim \varphi_2$) when they determine the same topology on F. The equivalence classes with respect to this equivalence relation are called **prime divisors of** F and will be denoted by P, Q, etc.

Suppose that P is a nonarchimedean prime divisor of F, and choose any $\varphi \in P$. Define

$$\Omega_P = \{a \in F \mid \varphi(a) \leq 1\} = \text{ the } \textbf{ring of integers at P},$$

$$\mathcal{P}_P = \{a \in F \mid \varphi(a) < 1\} = \text{ the } \textbf{maximal ideal at P},$$

$$\mathcal{U}_P = \{a \in F \mid \varphi(a) = 1\} = \text{ the } \textbf{group of units at P}.$$

Define the **residue class field of F at P**

$$\overline{F}_P = \frac{\Omega_P}{\mathcal{P}_P}.$$

For $a \in F$, let

$$\nu(a) = -\log \varphi(a)$$

so that $\varphi(a) = e^{-\nu(a)}$. Then ν is called an **exponential valuation** of F. Note that ν is a function from F into $\mathbb{R} \cup \{\infty\}$ such that

(i) $\nu(a) = \infty \iff a = 0$

(ii) $\nu(ab) = \nu(a) + \nu(b)$

(iii) $\nu(a+b) \geq \min\{\nu(a), \nu(b)\}$.

Example. Let $p \in \mathbb{Z}$ be any prime number. Define a function $\nu_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ by

$$\nu_p(a) = \begin{cases} \infty, & \text{if } a = 0 \\ \text{ord}_p(a), & \text{otherwise,} \end{cases}$$

where $\text{ord}_p(a)$ is the exponent to which p appears in the factorization of a. Then ν_p is an exponential valuation of $\mathbb{Q}$.

Fact 3.4.1 *If ν is an exponential valuation of F, then*

$$\nu(a) < \nu(b) \Rightarrow \nu(a+b) = \nu(a).$$

The image $\nu(F^*)$ is a subgroup of $\mathbb{R}^+$ and is called the **value group of** ν, denoted $G(\nu)$. The prime divisor P is said to be **discrete** or **nondiscrete** according

as $G(\nu)$ (for $\nu \in P$) is discrete or nondiscrete as a subgroup of $\mathbb{R}^+$. If P is a discrete nontrivial prime divisor of F, then there exists in P a unique exponential valuation, ν_P, such that $G(\nu_P) = \mathbb{Z}$. ν_P is called the **normalized exponential valuation** of P. In this situation we have

$$\Omega_P = \{a \in F \mid \nu_P(a) \geq 0\} = \{a \in F \mid \nu_P(a) > -1\}$$
$$\mathcal{P}_P = \{a \in F \mid \nu_P(a) > 0\} = \{a \in F \mid \nu_P(a) \geq 1\}$$
$$\mathcal{U}_P = \{a \in F \mid \nu_P(a) = 0\}.$$

Now suppose that E is an extension of the field F. Then we say φ_Q is an **extension** of φ_P if φ_Q is a valuation of E and $\varphi_Q|_F = \varphi_P$.

We then have $\Omega_Q, \mathcal{P}_Q, \mathcal{U}_Q$, as above and

$$\overline{E}_Q = \frac{\Omega_Q}{\mathcal{P}_Q} = \text{ residue class field of } E \text{ at } Q.v$$

Define the **residue class degree of E over F at Q** by

$$f = f(Q/P) = [\overline{E}_Q : \overline{F}_P],$$

and the **ramification degree of Q over P** by

$$e = e(Q/P) = \text{ the number of left cosets of } \nu_P(F^*) in\ \nu_Q(E^*).$$

An **ordinary arithmetic field (OAF)** is a pair $\{F, \mathcal{S}\}$, where F is a field and $\mathcal{S}$ is a nonempty collection of discrete prime divisors of F such that the following axioms are satisfied:

I. For each $a \in F$, we have $\nu_P(a) = 0$ for all but finitely many $P \in \mathcal{S}$ (where $\nu_P \in P$ is the normalized valuation).

II. Given any $P_1, P_2 \in \mathcal{S}$ with $P_1 \neq P_2$, there exists an element $a \in F$ with

$$\nu_{P_1}(a-1) \geq 1$$

$$\nu_{P_2}(a) \geq 1$$

$$\nu_P(a) \geq 0 \text{ for all other } P \in \mathcal{S}.$$

The **ring of integers** of $\{F, \mathcal{S}\}$ is

$$\Omega = \Omega\{\mathcal{S}\} = \Omega\{F, \mathcal{S}\} = \{a \in F \mid \nu_P(a) \geq 0 \ \forall P \in \mathcal{S}\}.$$

We note the following examples:

1. If $F = \mathbb{Q}$ and $\mathcal{S}$ is the set of all nonarchimedean prime divisors of $\mathbb{Q}$, then $\{\mathbb{Q}, \mathcal{S}\}$ is an OAF with $\Omega = \mathbb{Z}$.

2. If $F = k(x)$ the field of rational functions over the field k and we take $\mathcal{S}$ as the set of all prime divisors which are trivial on k and arise from irreducible polynomials in $k[x]$ (only the prime divisor arising from $1/x$ is excluded), then $\{F, \mathcal{S}\}$ is an OAF whose ring of integers is $k[x]$.

Fact 3.4.2 *Let $\{F, \mathcal{S}\}$ be an* OAF. *If E/F is a finite extension, then $\{E, \mathcal{S}^E\}$ is an* OAF, *where $\mathcal{S}^E$ is the set of all extensions to E of the prime divisors belonging to $\mathcal{S}$.*

We will require the following result from [20].

Theorem 3.4.3 *Suppose that $\{F, \mathcal{S}\}$ is an* OAF, *P is a nonarchimedean prime divisor of $\mathcal{S}$, and that E/F is a finite separable extension of degree n. Then there are only finitely many extensions, $Q_1, \ldots, Q_r$ of P to E, and*

$$\sum_{i=1}^{r} e(Q_i/P) f(Q_i/P) = n.$$

For convenience, we will now state the main result of this section.

Theorem 3.4.4 *Let* $\{F, \mathcal{S}\}$ *be an* OAF. *Suppose* $f(x) = x^n - b \in F[x]$ *and let* $\{P_i\}$, $i = 1\ldots, s$, *be the set of nonarchimedean prime divisors of* $\mathcal{S}$ *such that* $\nu_{P_i}(b) > 0$ *for all* i. *Suppose* $\{P_i\}$ *is nonempty and the* $\gcd(n, \nu_{P_1}(b), \ldots, \nu_{P_s}(b)) = 1$. *Then* $f_m(x)$ *is irreducible over* $F[x]$ *for* $m \geq 1$.

We first prove two preparatory lemmas before beginning the proof of Theorem 3.4.4. Lemma 3.4.5 establishes a relationship between the values of the roots of $f_m(x)$ and b, the (negative of the) constant term of $f(x)$.

Lemma 3.4.5 *In the situation of Theorem 3.4.4, if* α_m *is any root of* $f_m(x)$, *then*

$$\nu_{Q_i}(\alpha_m) = \frac{\nu_{P_i}(b)}{n^m},$$

where ν_{Q_i} *is any extension of* ν_{P_i} *to* $F(\alpha_m)$.

Proof: We proceed by induction on m. For the case $m = 1$, let α_1 be any root of $f_1(x) = f(x) = x^n - b$. Then $\alpha_1^n = b$ and

$$n\nu_{Q_i}(\alpha_1) = \nu_{Q_i}(\alpha_1^n) = \nu_{P_i}(b),$$

showing the lemma true for $m = 1$.

Suppose inductively $\nu_{Q_i}(\alpha_k) = \nu_{P_i}(b)/n^k$, for all k such that $1 \leq k < m$, where α_k is any root of $f_k(x)$. Then, if α_m is a root of $f_m(x)$,

$$0 = f_m(\alpha_m) = f_{m-1}(f_1(\alpha_m)) = f_{m-1}(\alpha_m^n - b),$$

implying $\alpha_m^n - b$ is a root of $f_{m-1}(x)$, say $\alpha_m^n - b = \alpha_{m-1}$. Let ν_{Q_i} be an extension of ν_{P_i} to $F(\alpha_{m-1}, \alpha_m)$. Then

$$n\nu_{Q_i}(\alpha_m) = \nu_{Q_i}(\alpha_m^n) = \nu_{Q_i}(\alpha_{m-1} + b). \tag{3.15}$$

By the inductive hypothesis, we have

$$\nu_{Q_i}(\alpha_{m-1}) = \nu_{P_i}(b)/n^{m-1} < \nu_{P_i}(b)$$

since by assumption, $\nu_{P_i}(b) > 0$. So by Fact 3.4.1

$$\nu_{Q_i}(\alpha_{m-1} + b) = \nu_{Q_i}(\alpha_{m-1}) = \nu_{P_i}(b)/n^{m-1}.$$

Combining this and equation (3.15), we have

$$\nu_{Q_i}(\alpha_m) = \nu_{P_i}(b)/n^m,$$

completing the induction. □

Lemma 3.4.6 gives conditions under which the m^{th} iterate is irreducible.

Lemma 3.4.6 *Assume we have the situation of Theorem 3.4.4. Suppose further there exists an* $i \in \{1, \ldots, s\}$ *such that* $\gcd(n, \nu_{P_i}(b)) = 1$. *Then* $f_m(x)$ *is irreducible over* $F[x]$ *for all* $m \geq 1$.

Proof: Let α_m be a root of $f_m(x)$. Suppose without loss of generality $\gcd(n, \nu_{P_1}(b)) = 1$, say $\nu_{P_1}(b) = a$. Let Q be an extension of P_1 to $F(\alpha_m)$. By Lemma 3.4.5,

$$\nu_Q(\alpha_m) = \frac{\nu_{P_1}(b)}{n^m} = \frac{a}{n^m}.$$

Now $\gcd(n, a) = 1$ and so $\gcd(n^m, a) = 1$ implying the order of $\nu_Q(\alpha_m)$ is n^m, and thus n^m divides $e(Q/P_1)$. But then (using the fact that the degree of $f_m(x)$ is n^m and Theorem 3.4.3)

$$n^m \geq [F(\alpha_m) : F] \geq e(Q/P_1) \geq n^m$$

which yields $[F(\alpha_m) : F] = n^m$, implying $f_m(x)$ is irreducible over $F[x]$. □

We are now ready to prove the theorem.

Proof of Theorem 3.4.4: Fix $m \geq 1$. By assumption, $\gcd(n, \nu_{P_1}(b), \ldots, \nu_{P_s}(b)) = 1$, so $\gcd(n^m, \nu_{P_1}(b), \ldots, \nu_{P_s}(b)) = 1$. If for some $i \in \{1, \ldots, s\}$ we have $\gcd(n, \nu_{P_i}(b)) = 1$, then we are done by Lemma 3.4.6. Thus, assume $\gcd(n, \nu_{P_i}(b)) = d_i > 1$, for all $i = 1, \ldots s$. Write $\nu_{P_i}(b) = d_i a_i$ and $n^m = d_i n_i$, for all i. Then, since $d_i = \gcd(n^m, \nu_{P_i}(b))$, we have $\gcd(a_i, n_i) = 1$. Fix i. Let α_m be a root of $f_m(x)$ and let Q be an extension of P_i to $F(\alpha_m)$. By Lemma 3.4.5

$$\nu_Q(\alpha_m) = \frac{\nu_{P_i}(b)}{n^m} = \frac{d_i a_i}{d_i n_i} = \frac{a_i}{n_i}.$$

Since $\gcd(a_i, n_i) = 1$, we have n_i divides $e(Q/P_i)$ for all extensions Q of P_i to $F(\alpha_m)$.

Now, by Theorem 3.4.3,

$$[F(\alpha_m) : F] = l = \sum_{Q \supset P_i} e(Q/P_i) f(Q/P_i). \tag{3.16}$$

Since n_i divides the right hand side of equation (3.16), n_i divides l. But this is independent of the choice of i, so $\mathrm{lcm}(n_1, \ldots, n_s)$ divides l.

Claim: $\mathrm{lcm}(n_1, \ldots, n_s) = n^m =$ the degree of $f_m(x)$. *Proof of Claim:* n_i divides n^m for all i, so $\mathrm{lcm}(n_1, \ldots, n_s)$ divides n^m. Therefore, it suffices to show n^m divides $\mathrm{lcm}(n_1, \ldots, n_s)$. Suppose to the contrary n^m does not divide $\mathrm{lcm}(n_1, \ldots, n_s)$. Then there exists $1 \neq d \mid n^m$ such that $d \nmid \mathrm{lcm}(n_1, \ldots, n_s)$, which implies $d \nmid n_i$ for all i. But $n^m = d_i n_i$ and $d \mid n^m$, $d \nmid n_i$ implies $d \mid d_i$ for all i. This yields $d \mid d_i a_i = \nu_{P_i}(b)$ for all i. But this is a contradiction to $1 = \gcd(n^m, \nu_{P_1}(b), \ldots, \nu_{P_s}(b))$. Thus, the claim is proved, implying n^m divides $l = [F(\alpha_m) : F] \leq n^m$. Hence, $[F(\alpha_m) : F] = n^m$, showing f_m is irreducible, proving the theorem. □

This immediately yields the following result over the rationals.

Corollary 3.4.7 *Suppose* $f(x) = x^n - b \in \mathbb{Q}[x]$. *Let* $\{p_i\}$ *be the set of primes such that* $\nu_{p_i}(b) > 0$ *for all* i. *Suppose* $\{p_i\}$ *is nonempty and* $\gcd(n, \nu_{p_1(b)}, \ldots, \nu_{p_s}(b)) = 1$. *Then* $f_m(x)$ *is irreducible over* $\mathbb{Q}[x]$ *for* $m \geq 1$.

Remark 3.4.8 *Corollary 3.4.7 gives us infinitely many binomials in* $\mathbb{Q}[x]$ *all of whose iterates are irreducible. Corollary 3.4.7 also yields some information which was not given by Theorem 3.3.3 or Corollary 3.1.7. For instance, using Corollary 3.4.7 we can demonstrate infinitely many cubics* $x^3 - b$ *with* $b \in \mathbb{Q}$, $b \notin \mathbb{Z}$, *all of whose iterates are irreducible.*

3.5. WHEN ADJOINING ROOTS OF UNITY

We will need to investigate the irreducibility of iterates in fields containing certain roots of unity before moving on to the Galois theory.

Definition 3.5.1 *A group* G *is called* **nilpotent** *if* G *can be written*

$$G = P_1 \times \cdots \times P_r,$$

where each P_i *is a* p_i*-group for some prime* p_i, *and* $p_i \neq p_j$ *for* $i \neq j$. *That is,* G *is nilpotent if it is the direct product of its Sylow subgroups. Equivalently,* G *is nilpotent if every Sylow subgroup is normal. An extension* E/K *is called* **nilpotent** *if* E/K *is Galois and the corresponding Galois group is nilpotent.*

Examples: Every finite abelian group is nilpotent. S_3 (see Section 4.1), the symmetric group on 3 letters, is not nilpotent.

Theorem 3.5.2 *Suppose* n *is odd,* $g(x) = x^n - b$ *is irreducible in* $K[x]$, *and* E *is an extension of* K *with* E/K *nilpotent. If for all primes* p *dividing* n, K *does not contain any* p^{th} *roots of unity, then* $g(x)$ *is irreducible in* $E[x]$.

Proof: Suppose to the contrary that $g(x) = x^n - b$ is reducible in $E[x]$. Then by Theorem 2.2.1, there exists a prime p dividing n such that $b = \alpha^p$ for some $\alpha \in E$. This implies $b^{1/p} = \alpha \in E$. Therefore, we have the following extension of fields:

$$K \subseteq K(b^{1/p}) \subseteq E$$

with $[K(b^{1/p}) : K] = p$, since p is prime and $g(x)$ is irreducible in $K[x]$ (so $b^{1/p} \notin K$). By assumption, E/K is nilpotent, say the Galois group of E over K is $\mathrm{Gal}(E/K) = P_1 \times \cdots \times P_r$ where P_1 is the Sylow p-subgroup of $\mathrm{Gal}(E/K)$. Let F be the subfield of E with $\mathrm{Gal}(E/F) = P_2 \times \cdots \times P_r$. Since E/K is nilpotent, $P_2 \times \cdots \times P_r$ is normal in $\mathrm{Gal}(E/K)$, implying F/K is Galois. Now $K(b^{1/p}) \subseteq F$, since $[K(b^{1/p} : K] = p$ and $(p,\ [E, F]) = 1$. Let $H = \mathrm{Gal}(F/K(b^{1/p}))$. Then we have the number of left cosets of H in P_1 is $(P_1 : H) = [K(b^{1/p}) : K] = p$, which implies (by [16], Theorem 6.4.14) that H is normal in P_1. It follows that $K(b^{1/p})/K$ is Galois. But then all roots of $x^p - b$ are in $K(b^{1/p})$. This implies ϵ_p, a primitive p^{th} root of unity, is an element of $K(b^{1/p})$ (because if α is a root of $x^p - b$, then $\epsilon_p\alpha$ is also a root since $(\epsilon_p\alpha)^p = \alpha^p$ implying $\epsilon_p = \dfrac{\epsilon_p\alpha}{\alpha} \in K(b^{1/p})$). Thus, we have $K \subseteq K(\epsilon_p) \subseteq K(b^{1/p})$. But $[K(b^{1/p}) : K] = p$ and so $[K(\epsilon_p) : K]$ divides p. Also $[K(\epsilon_p) : K] \leq p - 1$ so we must have $[K(\epsilon_p) : K] = 1$, implying $\epsilon_p \in K$, a contradiction to our assumption. Therefore, $g(x) = x^n - b$ is irreducible in $E[x]$. □

Corollary 3.5.3 *Suppose n is odd, $g(x) = x^n - b$ is irreducible in $K[x]$. Assume that p is a prime dividing n and that $\epsilon_p \notin K$, where ϵ_p is a primitive p^{th} root of unity. Then $g(x)$ is irreducible in $K(\epsilon_n)[x]$.*

Proof: $K(\epsilon_n)/K$ is abelian and thus nilpotent, so we are in the situation of Theorem 3.5.2. □

Remark 3.5.4 *It is necessary to have n odd, since if n is even, we have the following counterexample. The binomial $f(x) = x^6 + 3$ is irreducible in $\mathbb{Q}[x]$, but factors in $\mathbb{Q}(\epsilon_6) = \mathbb{Q}(\sqrt{-3})$ as $(x^3 + \sqrt{-3})(x^3 - \sqrt{-3})$. In fact, we have if $f(x) = x^{2k} - b$, where $b = (-1)^{(p-1)/2}p$ for some odd prime p dividing k, then $f(x)$ is irreducible in $\mathbb{Q}[x]$, but reducible in $\mathbb{Q}(\epsilon_{2k})[x]$. This follows from the fact that (see [20]), if q is an odd prime and ϵ_q is a primitive q^{th} root of unity, then $\mathbb{Q}(\epsilon_q)$ contains exactly one quadratic field, namely*

$$E = \mathbb{Q}\left(\sqrt{(-1)^{\frac{q-1}{2}}q}\right).$$

We now state the final result of this section, which we use in the next chapter.

Corollary 3.5.5 *Suppose p is an odd prime and $n = p^t$, $f(x) = x^n - b$, and $f_m(x)$ is irreducible in $K[x]$ for all $m \geq 1$. Suppose further that $\epsilon_p \notin K$ where ϵ_p is a primitive p^{th} root of unity. Then $f_m(x)$ is irreducible in $K(\epsilon_n)[x]$.*

Proof: We proceed by induction on m. The case $m = 1$ is true by Corollary 3.5.3, so suppose $f_m(x)$ is irreducible in $K(\epsilon_n)[x]$. We show $f_{m+1}(x)$ is irreducible in $K(\epsilon_n)[x]$.

Let α_i be a root of $f_i(x)$. As in the proof of Theorem 3.1.6, since $f_{m+1}(x) = f_m(f(x))$, $0 = f_{m+1}(\alpha_{m+1}) = f_m(\alpha_{m+1}^n - b)$, and we have $\alpha_m = \alpha_{m+1}^n - b$ is a root of $f_m(x)$. Let $K_m = K(\alpha_m)$ and $K_{m+1} = K(\alpha_{m+1})$. Since $f_{m+1}(x)$ is irreducible in $K[x]$ we have $[K_{m+1} : K]$ = the degree of $f_{m+1}(x) = n^{m+1}$, and similarly $[K_m : K] = n^m$. Thus, $[K_{m+1} : K_m] = n$ = the degree of $g(x)$, where

$$g(x) = x^n - (b + \alpha_m) \in K_m[x],$$

implying $g(x)$ is irreducible in $K_m[x]$. Now $\epsilon_p \notin K_m$, since $1 \neq [K(\epsilon_p) : K] | p - 1$ and $[K_m : K] = n^m = (p^t)^m$ and $(p - 1, p^{tm}) = 1$.

Now by Corollary 3.5.3, $g(x)$ is irreducible in $K_m(\epsilon_n)[x]$. But this shows that $[K_{m+1}(\epsilon_n) : K_m(\epsilon_n)] = n$, and, by our inductive hypothesis $[K_m(\epsilon_n) : K(\epsilon_n)] = n^m$. Therefore $[K_{m+1}(\epsilon_n) : K(\epsilon_n)] = n^{m+1}$ = the degree of f_{m+1} and $f_{m+1}(x)$ is irreducible in $K(\epsilon_n)[x]$. □

This concludes our investigation of the irreducibility of the iterates of an irreducible binomial. We now turn to a study of the Galois groups of the iterates.

4. THE GALOIS THEORY

4.1. BRIEF INTRODUCTION TO WREATH PRODUCTS

Let us begin by defining the notions of a permutation group and a wreath product of two groups. We also note some elementary properties which we will make use of in the proofs of our main results. For reference, the reader is referred to [13] or [15].

A **permutation** of a set A is a bijective mapping (both one-to-one and onto) from A onto itself. We define $\mathbf{Sym}(A)$ to be the set of permutations of A, a group under composition of functions.

Example. If $A = \{1, 2, \ldots, n\}$, then $\mathrm{Sym}(A)$ is called the **symmetric group on n letters**, and is denoted S_n.

A **permutation group** is a subgroup of S_n, and n is defined to be its **degree**.

Let A, B be non-empty disjoint sets with orders $|A| = \alpha$ and $|B| = \beta$. Let G and H be permutation groups on A and B, respectively. Define

$$H^A = \{\lambda | \lambda : A \to H,\ \lambda \text{ a (set-) map}\}.$$

Given $g \in G$, and $\lambda \in H^A$, we define a map $[g; \lambda] : A \times B \to A \times B$ by

$$(a, b) \mapsto (g(a), \lambda(a)(b)).$$

Then $[g; \lambda] \in \mathrm{Sym}(A \times B)$ and the product $[g_1; \lambda_1] \circ [g_2; \lambda_2]$ has the effect

$$(a, b) \mapsto (g_1(g_2(a)), \lambda_1(g_2(a))(\lambda_2(a)(b))).$$

Thus $[g_1; \lambda_1] \circ [g_2; \lambda_2] = [g_3; \lambda_3] \in \mathrm{Sym}(A \times B)$, where $g_3 = g_1 \circ g_2$ and $\lambda_3 \in H^A$ satisfies $\lambda_3(a) = \lambda_1(g_2(a)) \circ \lambda_2(a)$. Also, the inverse of $[g; \lambda]$ in $\mathrm{Sym}(A \times B)$ is

$[g_2; \lambda_2]$, where $g_2 = g^{-1}$ and $\lambda_2(a) = \lambda(g^{-1}(a))^{-1}$ for all $a \in A$. Thus, the $[g; \lambda]$ form a subgroup of $\mathrm{Sym}(A \times B)$. We call this subgroup the **wreath product of G by H**, and denote it by $G[H]$. We note there is a natural isomorphism of $G[H[M]]$ with $(G[H])[M]$, allowing us to discuss wreath powers $[G]^m$, where $[G]^1 = G$ and $[G]^{m+1} = G[[G]^m]$.

Fact 4.1.1 *Let α =deg$G$, β =deg$H$. Then*

$$|G[H]| = |G||H|^{\alpha}, \text{ and} \tag{4.1}$$

$$\begin{aligned} \deg G[H] &= (\deg G)(\deg H). \\ &= \alpha\beta. \end{aligned} \tag{4.2}$$

Our work will require the following lemma, which relates Fact 4.1.1 to our results.

Lemma 4.1.2 *Let C_n be the cyclic group of order n. Then*

$$|[C_n]^m| = n^{n^{m-1}+n^{m-2}+\cdots+n+1}.$$

Proof: Proceed by induction on m. Clearly, the result holds if $m = 1$. Suppose inductively that for $m > 1$ we have

$$|[C_n]^m| = n^{n^{m-1}+n^{m-2}+\cdots+n+1}.$$

Then by Fact 4.1.1 and the inductive hypothesis, we have

$$\begin{aligned} |[C_n]^{m+1}| &= |C_n[[C_n]^m]| \\ &= |C_n||[C_n]^m|^n \\ &= n(n^{n^{m-1}+n^{m-2}+\cdots+n+1})^n \\ &= n(n^{n^m+n^{m-1}+\cdots+n^2+n}) \\ &= n^{n^m+n^{m-1}+\cdots+n+1}. \end{aligned}$$

Thus, by induction we are done. □

4.2. THE GALOIS GROUP OF THE ITERATES

For this section we assume that p is an odd prime, $n = p^t$, K is a field of characteristic 0, and ϵ_n is a primitive n^{th} root of unity over K. Let $f_1(x) = x^n - b \in K(\epsilon_n)[x]$, and $f_{m+1}(x) = f_m(f_1(x))$ for $m \geq 1$. We assume that $f_k(x)$ is irreducible in $K(\epsilon_n)[x]$ for all $1 \leq k \leq m$. Let E_m be the splitting field of f_m over $K(\epsilon_n)$ and let $G_m = \mathrm{Gal}(E_m/K(\epsilon_n))$. We begin with a lemma concerning the constant terms of the iterates. Recall that the degree of $f_m(x)$ is n^m and that the roots of $f_m(x)$ are distinct, since by assumption $f_m(x)$ is irreducible and E_m is separable over K. For the remainder of this chapter, let $b_m = f_m(0)$, the constant term of $f_m(x)$.

Lemma 4.2.1 *Let $b_m = f_m(0)$ for $m \geq 1$, and let β_j $(j = 1, \ldots, n^m)$ be the roots of $f_m(x)$ in E_m. Then*

$$b_{m+1} = -\prod_{j=1}^{n^m}(\beta_j + b).$$

Proof: First note that $f_m(x) = \prod_{j=1}^{n^m}(x - \beta_j) \in E_m[x]$. Since $f_{m+1}(x) = f_m(f_1(x)) = f_m(x^n - b)$ we have

$$\begin{aligned} b_{m+1} = f_{m+1}(0) = f_m(-b) &= \prod_{j=1}^{n^m}(-b - \beta_j) \\ &= \prod_{j=1}^{n^m}(-1)(b + \beta_j) \\ &= (-1)^{n^m}\prod_{j=1}^{n^m}(b + \beta_j) \\ &= -\prod_{j=1}^{n^m}(\beta_j + b), \end{aligned}$$

since $n = p^t$ is odd. □

Next we review the notions of Kummer extensions and modules. For reference, see [8] or [21] for example.

Let G be a group and Ω be a set. We say G **acts transitively** on Ω if for each $\alpha, \beta \in \Omega$ there exists a $g \in G$ with $g\alpha = \beta$. We call G a p-**group** if each element of G has p-power order, for some prime p.

Let F be a field and p prime. Let F^* be the non-zero elements of F. Nonzero elements $d_1, d_2, \ldots, d_k \in F^*$ are called p^u-**independent in** F if $d_1^{a_1} \cdots d_k^{a_k} \in F^{p^u} \Rightarrow p^u | a_i$ for $i = 1, \ldots, k$.

Let F be a field which contains a primitive $(p^u)^{th}$ root of unity. A finite abelian extension of exponent p^u of F is called a p^u-**Kummer extension** of F. The p^u-Kummer extensions of F are the splitting fields over F of polynomials of the form $(x^{p^{r_1}} - d_1) \cdots (x^{p^{r_k}} - d_k)$ where $d_1, \ldots, d_k \in F$ and $r_i \leq u$ for all i. We'll need the following standard fact (see [8]).

Fact 4.2.2 *Let p be a prime, $\epsilon_{p^u} \in F$, $d_1, \ldots, d_r \in F^*$. For each i and some positive integer u, let $\delta_i \in \overline{F}$, an algebraic closure of F, with $\delta_i^{p^u} = d_i$. Then $[F(\delta_1, \ldots, \delta_r) : F] = p^{ru} \iff d_1, \ldots, d_r$ are p^u-independent in F.*

We now prove the following useful result, which we use in the arguments which follow.

Lemma 4.2.3 *Let the context be as in Fact 4.2.2. Then $d_1, \ldots, d_r$ are p-independent in $F \iff d_1, \ldots, d_r$ are p^u-independent in F.*

Proof: First suppose $d_1, \ldots, d_r \in F^*$ are p^u-independent. Then $d_1^{e_1} \cdots d_r^{e_r} = c^p \in F$ implies $d_1^{e_1 p^{u-1}} \cdots d_r^{e_r p^{u-1}} = c^{p^u}$. Since $d_1, \ldots, d_r$ are p^u-independent we have $p^u | e_i p^{u-1}$. Therefore $p | e_i$ for all i, which shows $d_1, \ldots, d_r$ are p-independent. Next, if $d_1, \ldots, d_r$ are p-independent, then if $d_1^{e_1} \cdots d_r^{e_r} = c^{p^u} = (c^{p^{u-1}})^p \in F$, we have $p | e_i$ for all i. Say $e_i = pl_i$. Then $(d_1^{l_1} \cdots d_r^{l_r})^p = (c^{p^{u-1}})^p$, and since (by assumption) $\epsilon_{p^u} \in F$, without loss of generality we have $d_1^{l_1} \cdots d_r^{l_r} = c^{p^{u-1}}$. Continuing in this manner, we

reduce down to $d_1^{s_1} \cdots d_r^{s_r} = c^p$, implying $p|s_i$ for all i. But we have shown $p^u|e_i$ for all i implying $d_1, \ldots, d_r$ are p^u-independent. □

Let A be a ring. A set M is called an **A-module** if

(a) M is an abelian group, and

(b) With every ordered pair (a, x) with $a \in A$ and $x \in M$ there is a unique element $ax \in M$ such that the following relations hold:

(i) $a(x + y) = ax + ay$

(ii) $(a + b)x = ax + bx$

(iii) $(ab)x = a(bx)$,

where $a, b \in A$ and $x, y \in M$.

Examples. A vector space over a field F is an F-module. Any commutative group is a $\mathbb{Z}$-module.

Let $\mathbb{F}_p$ denote the finite field of order p. We denote the group algebra of G over $\mathbb{F}_p$ by $\mathbb{F}_p[G]$, i.e. the group ring $\mathbb{F}_p[G]$ with $\mathbb{F}_p$-module structure given by

$$k(\sum r_i g_i) = \sum (kr_i) g_i$$

for $k, r_i \in \mathbb{F}_p$ and $g_i \in G$.

We begin our work with a lemma about p-groups.

Lemma 4.2.4 *If G is a p-group and $M \neq 0$ is a finite $\mathbb{F}_p[G]$-module, then the submodule M^G of G-invariant elements of M is also nontrivial.*

Proof: Induct on the order of G. Suppose G is a cyclic group of order p, i.e. $G \cong C_p =< \sigma >$. Let $T : M \to M$ be the map $Ty = (\sigma - 1)y$, for $y \in M$. Then T is an $\mathbb{F}_p$-linear transformation from M to M. We must show

$\ker T \neq 0$. Suppose to the contrary that $\ker T = 0$. Then T would be 1-1 and thus bijective, since M is finite. Thus every power of T would be bijective. However, $T^p = (\sigma - 1)^p = \sigma^p - 1 = 1 - 1 = 0$ in $\mathbb{F}_p[G]$, so that T is nilpotent. But this contradicts the fact that all powers of T bijective. Therefore, $\ker T \neq 0$, which implies there exists $0 \neq y \in M^G$.

If $|G| > p$, let H be a nontrivial normal subgroup of G. Then M is an $\mathbb{F}_p[H]$-module, too, so by induction, $M^H \neq 0$. Now, M^H is a finite $\mathbb{F}_p[G/H]$-module under the operation $(gH)x = gx$, for all $gH \in G/H$ and $x \in M^H$. We also have $M^G = (M^H)^{G/H}$. (Clearly if $x \in M^G$ then $x \in (M^H)^{G/H}$. Also if $x \in (M^H)^{G/H}$ we have $h(x) = x$ for all $h \in H$ and $(gH)x = x$ for all $gH \in G/H$. So for $g \in G$, we have $gH \in G/H$, so $x = (gH)x = g(Hx) = g(x)$ implying $x \in M^G$.) But then we are done by induction, since $M^G = (M^H)^{G/H} \neq 0$. □

We use Lemma 4.2.4 in the following proof, and so assume $n = p^t$ for some positive integer t, so that G_m is a p-group. (This is a generalization of Lemma 1.6 from [18].)

Lemma 4.2.5 *Suppose p is an odd prime and $n = p^t$. Then for all $m \geq 1$,*

$$[E_{m+1} : E_m] = n^{n^m} \iff b_{m+1} \notin E_m^p.$$

Proof: Let β_j $(j = 1, \ldots, n^m)$ be the roots of $f_m(x)$ in E_m. Now since $f_{m+1}(x) = f_m(f_1(x))$, if β is a root of $f_{m+1}(x)$ then

$$0 = f_{m+1}(\beta) = f_m(f_1(\beta)) = f_m(\beta^n - b)$$

showing $\beta^n - b = \beta_i$ is a root of $f_m(x)$. But then we have $E_{m+1} = E_m(\{\beta \mid \beta \text{ is a root of } f_{m+1}\}) = E_m(\{(\beta_i + b)^{1/n} \mid \beta_i \text{ is a root of } f_m(x)\})$. Therefore (since E_m contains the n^{th} roots of unity) $E_m \subset E_{m+1}$ is an n-Kummer extension. Also

$$
\begin{aligned}
[E_{m+1} : E_m] &= [E_m((\beta_1 + b)^{1/n}, \ldots, (\beta_{n^m} + b)^{1/n}) : E_m] \\
&= [E_m((\beta_1 + b)^{1/n}) : E_m][E_m((\beta_1 + b)^{1/n}, (\beta_2 + b)^{1/n}) : E_m((\beta_1 + b)^{1/n})] \\
&\cdots [E_m((\beta_1 + b)^{1/n}, \ldots, (\beta_{n^m} + b)^{1/n}) : E_m((\beta_1 + b)^{1/n}, \ldots, (\beta_{n^m-1} + b)^{1/n})] \\
&\leq \underbrace{n \cdots n}_{n^m \text{ times}} = n^{n^m}.
\end{aligned}
$$

Clearly, if $b_{m+1} = -\prod_{j=1}^{n^m}(\beta_j + b) \in E_m^p$ then $[E_{m+1} : E_m] < n^{n^m}$ since E_{m+1} is obtained from E_m by adjoining the n^{th} roots of the $\beta_j + b$.

Now to prove $[E_{m+1} : E_m] = n^{n^m}$ we shall show that in any relation

$$\prod_{j=1}^{n^m}(\beta_j + b)^{\epsilon_j} \in (E_m^*)^n$$

where the ϵ_j are positive integers, each ϵ_j must be a multiple of $n = p^t$ (by Fact 4.2.2). But by Lemma 4.2.3, this is the same as showing that in any relation

$$\prod_{j=1}^{n^m}(\beta_j + b)^{\epsilon_j} \in (E_m^*)^p$$

where the ϵ_j are positive integers, each ϵ_j must be a multiple of p.

Let V be the subspace of $\mathbb{F}_p$ defined by

$$V = \{(\epsilon_1, \ldots, \epsilon_{n^m}) \in \mathbb{F}_p^{n^m} \mid \prod_{j \leq n^m} (\beta_j + b)^{\epsilon_j} \in (E_m^*)^p\}.$$

We need to show the dimension of V is zero, i.e. if $(\delta_1, \ldots, \delta_{n^m}) \in V$ then $(\delta_1, \ldots, \delta_{n^m}) = (0, \ldots, 0)$. We suppose $V \neq \{(0, \ldots, 0)\}$ and derive a contradiction. First we note that G_m, the Galois group of E_m over $K(\epsilon_n)$, operates on V by permuting the components of the elements of V according to its action on the β_j. Extending this action linearly to $\mathbb{F}_p[G_m]$, V becomes an $\mathbb{F}_p[G_m]$-module. So by Lemma 4.2.4, $V^{G_m} \neq \{(0, \ldots, 0)\}$. Let $(\delta_1, \ldots, \delta_i, \ldots, \delta_j, \ldots, \delta_{n^m}) \in V^{G_m}$ with $\delta_i \neq 0$. Since G_m operates transitively on the β_j (f_m is irreducible by assumption), we have for each j there exists some $g_j \in G_m$ with $g_j(\beta_i) = \beta_j$, and so

$g_j(\beta_i + b)^{\delta_i} = (\beta_j + b)^{\delta_i}$. Since $(\delta_1, \ldots, \delta_i, \ldots, \delta_j, \ldots, \delta_{n^m}) \in V^{G_m}$, we must have $\delta_i = \delta_j$. But j was arbitrary, so if v is an element of V^{G_m}, $v = (k, \ldots, k)$ for some $0 \neq k \in \mathbb{F}_p$.

But this implies (using Lemma 4.2.1) that $b_{m+1}^k = (-1)^k(\prod_{j \leq n^m}(\beta_j + b))^k = (-1)^k\beta^p$, for some $0 \neq \beta \in E_m$. If k is even, then $b_{m+1}^k = \beta^p$ and if k is odd $b_{m+1}^k = -\beta^p = (-\beta)^p$, since p is odd. So in either case, $b_{m+1}^k = \beta^p$ for some non-zero $\beta \in E_m$. Then, since $(p, k) = 1$, we have $1 = rp + sk$ for some integers r, s. Therefore,

$$\begin{aligned} b_{m+1} &= b_{m+1}^{rp+sk} \\ &= (b_{m+1})^{rp}(b_{m+1}^k)^s \\ &= (b_{m+1})^{rp}(\beta^p)^s \\ &= (b_{m+1}^r\beta^s)^p \in E_m^p. \end{aligned}$$

Thus we have shown if $[E_{m+1} : E_m] < n^{n^m}$ then $b_{m+1} \in E_m^p$, completing the proof. □

Let G be a group. The subgroup of G generated by the set $\{aba^{-1}b^{-1} | a, b \in G\}$ is called the **commutator subgroup** of G and denoted by G'.

Fact 4.2.6 *G' is a normal subgroup of G and G/G' is abelian. Also, if N is a normal subgroup of G, then G/N is abelian if and only if N contains G'. Thus $G^{ab} = G/G'$ is the largest abelian factor group of G.*

We recall the group G is the **semi-direct product of H and K** if

(1) H is normal in G,

(2) $G = HK$, and

(3) $H \cap K = \{e\}$.

Denote this by $G = H \rtimes K$.

Lemma 4.2.7 *If H and G are permutation groups with G transitive, then $(G[H])^{ab} \cong G^{ab} \times H^{ab}$, where $G[H]$ denotes wreath product and $(G[H])^{ab}$ denotes the largest abelian factor group of $G[H]$.*

Proof: Suppose G is a transitive subgroup of $\mathrm{Sym}(\Gamma)$, with $\Gamma = \{\gamma_1, \ldots, \gamma_n\}$, and suppose H is a subgroup of $\mathrm{Sym}(\Delta)$. Setting $H_{\gamma_i} = H$, then $G[H] = (H_{\gamma_1} \times \cdots \times H_{\gamma_n}) \rtimes G \subseteq \mathrm{Sym}(\Gamma \times \Delta)$. Now G acts on $H_{\gamma_1} \times \cdots \times H_{\gamma_n}$ by

$$g(h_{\gamma_1}, \ldots, h_{\gamma_n})g^{-1} = (h_{\gamma_{i_1}}, \ldots, h_{\gamma_{i_n}}), \tag{4.3}$$

where $g\gamma_j = \gamma_{i_j}$, and

$$g(h_{\gamma_1}, \ldots, h_{\gamma_n})(\gamma_i, \delta) = (g(\gamma_i), h_{\gamma_i}(\delta)). \tag{4.4}$$

Now we claim for all $h \in H, (h, 1, \ldots, 1, h^{-1}, 1, \ldots, 1) \in G[H]'$, where h^{-1} is in any position. *Proof of claim:* Suppose h^{-1} is in the t^{th} position, and consider $(h^{-1}, 1, \ldots, 1) \in G[H]$. Since G is transitive, there exists a $g \in G$ with $g(\gamma_1) = \gamma_t$. So by 4.3, $g(h^{-1}, 1, \ldots, 1)g^{-1} = (1, \ldots, 1, h^{-1}, 1 \ldots, 1)$. Thus, we have $(h, 1, \ldots, 1, h^{-1}, 1, \ldots, 1) = g(h^{-1}, 1, \ldots, 1)g^{-1}(h, 1, \ldots, 1) \in G[H]'$, and the claim is proved.

Define a map $\gamma : G[H] \to G^{\mathrm{ab}} \times H^{\mathrm{ab}}$ by $\gamma(g(h_{\gamma_1}, \ldots, h_{\gamma_n})) = (gG', h_{\gamma_1} \cdots h_{\gamma_n} H')$. Then γ is an onto homomorphism. We now show the kernel of γ, $\ker(\gamma) = G[H]'$. Suppose $g(h_{\gamma_1}, \ldots, h_{\gamma_n}) \in \ker(\gamma)$. This implies $g \in G'$ and $h_{\gamma_1} \cdots h_{\gamma_n} \in H'$. Without loss of generality, $g = 1$ since $g \in G'$, so we need only show $(h_{\gamma_1}, \ldots, h_{\gamma_n}) \in G[H]'$ since then $\ker(\gamma) \subseteq G[H]'$ and $G[H]/\ker(\gamma)$ is abelian so $\ker(\gamma) \supseteq G[H]'$. Now, using the claim above,

$$
\begin{aligned}
&(h_{\gamma_1}, \ldots, h_{\gamma_n})\, G\,[H]' \\
&\qquad = (h_{\gamma_1}, \ldots, h_{\gamma_n})(h_{\gamma_2}, h_{\gamma_2}^{-1}, 1, \ldots, 1) G[H]' \\
&\qquad = (h_{\gamma_1} h_{\gamma_2}, 1, h_{\gamma_3}, \ldots, h_{\gamma_n}) G[H]' \\
&\qquad \vdots \\
&\qquad = (h_{\gamma_1} \cdots h_{\gamma_n}, 1, \ldots, 1) G[H]' \\
&\qquad = G[H]' \text{ since } h_{\gamma_1} \cdots h_{\gamma_n} \in H' \subset G[H]',
\end{aligned}
$$

so $(h_{\gamma_1}, \ldots, h_{\gamma_n}) \in G[H]'$. □

Lemma 4.2.8 *Let C_n be the cyclic group of order n. Then $([C_n]^m)^{ab} \cong C_n^m$, the direct product of m copies of C_n.*

Proof: Induct on m. If $m = 1$, then since C_n is cyclic we have $([C_n]^1)^{\mathrm{ab}} = (C_n)^{\mathrm{ab}} = C_n$. Suppose now $([C_n]^{m-1})^{\mathrm{ab}} \cong C_n^{m-1}$. Then using Lemma 4.2.7 and the inductive hypothesis we have $([C_n]^m)^{\mathrm{ab}} = (C_n[[C_n]^{m-1}])^{\mathrm{ab}} = (C_n)^{\mathrm{ab}} \times ([C_n]^{m-1})^{\mathrm{ab}} = C_n \times C_n^{m-1} = C_n^m$, completing the induction. □

We are now able to generalize Lemma 1.5 from [18]. Recall still that $n = p^t$, for some odd prime p.

Lemma 4.2.9 *If $G_m \cong [C_n]^m$ and $b_1, b_2, \ldots, b_m$ are p-independent in $K(\epsilon_n)$, then for all $c \in K(\epsilon_n)^*$:*

$$c \notin (E_m^*)^p \iff b_1, b_2, \ldots, b_m, c \text{ are } p\text{-independent in } K(\epsilon_n).$$

Proof: By Lemma 4.2.8, $([C_n]^m)^{\mathrm{ab}} \cong C_n^m$. Thus the largest p^t-Kummer extension of $K(\epsilon_n)$ within E_m has degree $n^m = |C_n^m|$. Now, let $1 < k \leq m$ and denote by A the set of zeros of f_{k-1}. We have by Lemma 4.2.1,

$$b_k = f_k(0) = f_{k-1}(-b) = -\prod_{\beta \in A} (\beta + b).$$

But if α is a root of f_k, then $\alpha^n - b$ is a root of f_{k-1}. That is, for each $\beta \in A$, $\beta + b = \alpha^n \in E_k^n = E_k^{p^t}$, which implies $b_k \in E_k^{p^t}$ (since p is odd). But $1 < k \leq m$ was arbitrary, so all of the $b_1, \ldots, b_m$ are in $E_m^{p^t}$ so $T = K(\epsilon_n)(b_1^{1/p^t}, \ldots, b_m^{1/p^t}) \subseteq E_m$. Since $b_1, b_2, \ldots, b_m$ are p-independent in $K(\epsilon_n)$, they are p^t-independent in $K(\epsilon_n)$ and so $[T : K(\epsilon_n)] = p^{mt}$ (by Proposition 4.3.4 and Lemma 4.2.3). But $T/K(\epsilon_n)$ as an abelian extension so $\mathrm{Gal}(E_m/T) \supseteq G_m'$ (by Fact 4.2.6). Since $G_m \cong [C_n]^m$ and $|G_m/G_m'| = p^{mt}$, we have $T = E_m^{G_m'}$ implying T is the maximum Kummer p^t-extension of E_m. Let $c \in K(\epsilon_n)^*$. If $c \in (E_m^*)^p$, then $c^{1/p} \in E_m$. Since $T(c^{1/p})/K(\epsilon_n)$ is abelian, we have $c^{1/p} \in T$ which implies $b_1, \ldots, b_m, c$ are p-dependent (i.e. not p-independent) in $K(\epsilon_n)$. Conversely, if $c \notin (E_m^*)^p$, then $c^{1/p} \notin T$, so $[K(\epsilon_n)(b_1^{1/p}, \ldots, b_m^{1/p}, c^{1/p}) : K(\epsilon_n)] = p^{m+1}$, implying $b_1, \ldots, b_m, c$ are p-independent in $K(\epsilon_n)$. □

We will need the following result. For reference see both [8] and Theorem 2 from [14].

Theorem 4.2.10 *Let F be a field containing all the n^{th} roots of unity, T algebraically independent over F, and $H_1(x,T) = x^n - T \in F(T)[x]$. Then $Gal(H_m(x,T)/F(T)) \cong [C_n]^m$. Moreover if $b \in F$ is such that $H_m(x,b) = f_m(x)$ is defined (no denominator vanishes), $deg(f_m) = deg(H_m)$, and $f_m(x)$ has no multiple roots, then there exists a monomorphism from $Gal(f_m/F) \hookrightarrow [C_n]^m$.*

Now we are ready to show the following lemma which is a generalization of Lemma 1.4 from [18].

Lemma 4.2.11 *G_m can be embedded into $[C_n]^m$. Moreover, we have for all m:*

$$G_{m+1} \cong [C_n]^{m+1} \iff G_m \cong [C_n]^m \text{ and } [E_{m+1} : E_m] = n^{n^m}.$$

Proof: Using Theorem 4.2.10, with $F = K(\epsilon_n)$ we get $G_m = \text{Gal}(f_m/K(\epsilon_n)) \hookrightarrow [C_n]^m$. By Lemma 4.1.2, $|[C_n]^{m+1}|/|[C_n]^m| = n^{n^m}$. But $[E_{m+1} : E_m] \leq n^{n^m}$, which proves the lemma. □

We now include a standard result (see [8] for example) concerning cyclic extensions which we require for our induction in the final theorem of this section.

Fact 4.2.12 *Let F be a field of characteristic zero, $n > 0$ an integer, and assume $\epsilon_n \in F$, where ϵ_n is a primitive n^{th} root of unity. If α is a root of the irreducible binomial $g(x) = x^n - b \in F[x]$, then $F(\alpha)/F$ is cyclic of degree n.*

We summarize our results for this section with the following theorem.

Theorem 4.2.13 *Let $n = p^t$, p an odd prime, $f_1(x) = x^n - b \in K(\epsilon_n)[x]$, for ϵ_n a primitive n^{th} root of unity. Let $m \geq 1$ be given. Assume $f_k(x)$ is irreducible in $K(\epsilon_n)[x]$ for all k such that $1 \leq k \leq m$. Then $G_m \cong [C_n]^m \iff b_1, \ldots, b_m$ are p-independent in $K(\epsilon_n)$.*

Proof: We prove this by induction on k. For $k = 1$, $G_1 = \text{Gal}(x^n - b/K(\epsilon_n)) = C_n$ by Fact 4.2.12. Assume $m > 1$ and for $k < m$, we have $G_k \cong [C_n]^k \iff b_1, \ldots, b_k$ are p-independent in $K(\epsilon_n)$. By Lemma 4.2.11, $G_{k+1} \cong [C_n]^{k+1}$ if and only if $[E_{k+1} : E_k] = n^{n^k}$. By Lemma 4.2.5, this will follow if and only if $b_{k+1} \notin E_k^p$. By Lemma 4.2.9, this will follow if and only if $b_1, \ldots, b_{k+1}$ are p-independent in $K(\epsilon_n)$. Thus, we are done by induction. □

In the next section, we construct a sequence which determines when $b_1, \ldots, b_m$ are p-independent in $K(\epsilon_n)$, under additional hypotheses on K.

4.3. A PAIRWISE COPRIME SEQUENCE

Let the context be as in the previous section with the additional assumption that ϵ_p is not in K for ϵ_p a primitive p^{th} root of unity (recall p is prime). Assume further that K is the quotient field of a UFD R. The main lemma of this section makes use of some elementary number theory. For a complete treatment, the reader is referred to [1] or [17].

The **Möbius function** μ is defined as follows:

$$\mu(1) = 1.$$

For n an integer greater than 1, let $n = p_1^{a_1} \cdots p_k^{a_k}$ be the prime factorization of n. Then

$$\mu(n) = \begin{cases} (-1)^k & \text{if } a_1 = a_2 = \cdots = a_k = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Note that $\mu(n) = 0$ if and only if n has a square factor > 1. Two basic properties of $\mu(n)$ are the following.

Fact 4.3.1

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n > 1. \end{cases}$$

Fact 4.3.2 (Möbius inversion formula) *Suppose F is a field and $f, g : \mathbb{N} \to F^*$. Then*

$$g(n) = \prod_{d|n} f(d)^{\mu(n/d)} \iff f(n) = \prod_{d|n} g(d).$$

We now construct a sequence of pairwise coprime (pairwise relatively prime) elements related to the $\{b_m\}$ generated by the iterated binomials. This is a generalization of Lemma 1.1 from [18].

Lemma 4.3.3 *Let R be a* UFD *with quotient field K. Let $f(x) = x^n - b$ be irreducible in $R[x]$ with b a non-unit and $b \neq 0$. For $m \geq 1$, let $b_m = f_m(0) \in R$. Then there exists a sequence c_m $(m \geq 1)$ of pairwise coprime elements of R such that, for all $m \geq 1$,*

$$b_m = \prod_{d|m} c_d.$$

Proof: First we will show that $b_m = f_m(0) \neq 0$ for all $m \geq 1$. Suppose to the contrary that $b_m = 0$ with m minimal. If $m = 1$, then $0 = b_1 = f_1(0) = -b$ implying $b = 0$, a contradiction to our assumptions. Thus $m > 1$. But then $0 = b_m = f_m(0) = f_1(f_{m-1}(0)) = b_{m-1}^n - b$, and so $b = b_{m-1}^n = (b_{m-1}^{n/p})^p$, implying $b \in R^p$, for all p dividing n. But this contradicts our assumption that $f_1(x) = f(x) = x^n - b$ irreducible in $R[x]$ (using Theorem 2.2.1).

Since all $b_m \neq 0$, we can define a sequence

$$c_m = \prod_{d|m} b_d^{\mu(m/d)} \in K \text{ (where } \mu \text{ is the Möbius function).}$$

So c_m is in K, the quotient field of R. We show $c_m \in R$, for $m \geq 1$. Let p be a prime of R dividing at least one of the b_m (note $b_1 = -b$ is a non-unit). Let $l = \min\{k \geq 1 \mid p|b_k\}$ and let $e = v_p(b_l)$. Then we have $p^e|b_l$ and $p^{e+1} \nmid b_l$. We claim for $m \geq 1$,

$$p|b_m \iff p^e|b_m \iff l|m.$$

Proof of claim: First, suppose $l|m$, say $m = dl$ for some $d \in \mathbb{Z}$. Then we have $b_m = b_{dl} = f_{dl}(0) = f_{(d-1)l}(f_l(0)) = f_{(d-1)l}(b_l) \equiv f_{(d-1)l}(0) \equiv f_{(d-2)l}(0) \equiv \cdots \equiv f_l(0) = b_l \equiv 0 \bmod p^e$. Thus if $l|m$ then $p^e|b_m$. Next suppose $l \nmid m$, say $m = dl + r$ where $0 < r < l$. Then $b_m = b_{dl+r} = f_{dl+r}(0) = f_r(f_{dl}(0)) \equiv f_r(0) \bmod p^e$. By the minimality of l, $f_r(0) = b_r \not\equiv 0 \bmod p$. Thus, if $l \nmid m$ then $p \nmid b_m$, and so $p^e \nmid b_m$. This proves the claim.

So by the claim, we have

$$v_p(b_m) = \begin{cases} e, & \text{if } l|m \\ 0, & \text{otherwise.} \end{cases}$$

This gives us

$$\begin{aligned} v_p(c_m) &= v_p(\prod_{d|m} b_d^{\mu(m/d)}) \\ &= \sum_{d|m} v_p(b_d^{\mu(m/d)}) \\ &= \sum_{d|m} v_p(b_d)\mu(m/d) \\ &= \sum_{dl|m} v_p(b_d l)\mu(m/dl) \\ &= \sum_{dl|m} e\mu(m/dl) \\ &= e\sum_{dl|m} \mu(m/dl) \\ &= e\sum_{d|m/l} \mu(d) = \begin{cases} e, & \text{if } m = l \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

We see from this that c_m must be in R since $v_p(c_m) \geq 0$ for all primes p of R. (For if $c_m \notin R$, then there exists a prime p dividing the denominator of c_m and $v_p(c_m) < 0$ for this p.) We also see that if p divides some b_m, then p divides exactly one of the c_m, namely c_l. Thus, the c_m are pairwise coprime. And by Fact 4.3.2 we see $b_m = \prod_{d|m} c_d$. □

We now isolate the following two results about p-independence to be used in the proof of Theorem 4.3.6.

Proposition 4.3.4 *Let F be a field, p an odd prime with $n = p^t$, and suppose $\epsilon_p \notin F$. Suppose $d_1, \ldots, d_r \in F^*$. Then $d_1, \ldots, d_r$ are p-independent in $F(\epsilon_n)$ $\iff$ $d_1, \ldots, d_r$ are p-independent in F.*

Proof: Clearly, if $d_1, \ldots, d_r$ p-independent in $F(\epsilon_n)$, then we have $d_1, \ldots, d_r$ p-independent in F. We now show the reverse implication. Suppose to the contrary

we have $d_1, \ldots, d_r$ p-independent in F but not in $F(\epsilon_n)$, i.e. there is some $a \in F(\epsilon_n)$ with $d_1^{u_1} \cdots d_r^{u_r} = a^p$ and p does not divide u_i for some i. Then $(d_1^{u_1} \cdots d_r^{u_r})^{1/p} = a \in F(\epsilon_n)$, so we have $F \subseteq F((d_1^{u_1} \cdots d_r^{u_r})^{1/p}) \subseteq F(\epsilon_n)$. Since $F(\epsilon_n)/F$ is abelian, $F((d_1^{u_1} \cdots d_r^{u_r})^{1/p})/F$ is Galois. So if $h(x) = x^p - d_1^{u_1} \cdots d_r^{u_r}$ is irreducible in $F[x]$, then we get $\epsilon_p \in F$ (as in the proof of Theorem 3.5.2), a contradiction to our assumptions. If $h(x)$ is reducible, we have $d_1^{u_1} \cdots d_r^{u_r} \in F^p$. Since $d_1, \ldots, d_r$ p-independent in F, this gives $p | u_j$ for all j, a contradiction (from above, we supposed $p \nmid u_i$). Therefore, the proposition is proved. □

Lemma 4.3.5 *Let $c_1, \ldots, c_m$ be as in Lemma 4.3.3 and assume $c_1, \ldots, c_m$ are p-independent in F. Then $b_1, \ldots, b_m$ are p-independent in F.*

Proof: Suppose (without loss of generality) m is minimal with $b_1, \ldots, b_m$ not p-independent. (We derive a contradiction.) Then for some $d \in F^*$, we have $b_1^{a_1} \cdots b_m^{a_m} = d^p$. If $p | a_m$, we get $b_1^{a_1} \cdots b_{m-1}^{a_{m-1}} = (\frac{d}{b_m^{a_m/p}})^p \in K^p$. By the minimality of m, $b_1, \ldots, b_{m-1}$ are p-independent in F, which implies $p | a_i$, for all i such that $1 \leq i \leq m-1$. But then, $b_1, \ldots, b_m$ are p-independent in F, a contradiction to our supposition. Therefore, $p \nmid a_m$. Now note that $d^p = b_1^{a_1} \cdots b_m^{a_m} = c_m^{a_m} \prod_{d|m,\ d \neq m} c_d^{u_d}$ for some integers u_d. Since $c_1, \ldots, c_m$ are pairwise coprime and p-independent in F, $p | a_m$, a contradiction. Therefore $b_1, \ldots, b_m$ are p-independent. □

We are now able to generalize the main result of [18].

Theorem 4.3.6 *Let R be a UFD with quotient field K. Let p be an odd prime, $n = p^t$, and assume $\epsilon_p \notin K$. Assume further that the units of K are either all p^{th} powers in K or are ± 1. Let $f_1(x) = x^n - b \in R[x]$. Let $c_1, \ldots c_m$ be the sequence defined by $c_m = \prod_{d|m} b_d^{\mu(m/d)}$, where $b_d = f_d(0)$. If none of $c_1, \ldots, c_m$ is in K^p, then $G_m \cong [C_n]^m$, where G_m is the Galois group of $f_m(x)$ over $K(\epsilon_n)$ for ϵ_n a primitive n^{th} root of unity.*

Proof: Suppose none of $c_1, \ldots, c_m$ is in K^p. Since $c_1 = b_1$, $b_1 \notin K^p$. But $b = -f_1(0) = -b_1$, so $b \notin K^p$ (using the fact that p is odd). Thus $f_1(x)$ is irreducible in $K[x]$. By Theorem 3.1.6, $f_m(x)$ is irreducible in $K[x]$ for all m. By Corollary 3.5.5, $f_m(x)$ is irreducible in $K(\epsilon_n)[x]$.

Recall $b_m = \prod_{d|m} c_d$ with the c_i's pairwise coprime in R (see Lemma 4.3.3). We show $c_1, \ldots, c_m$ are p-independent in K. Suppose $c_1^{a_1} \cdots c_m^{a_m} = d^p$ for some $d \in K^*$. Then by Lemma 3.1.4 we have $c_i^{a_i} = u_i e_i^p = (u_i e_i)^p$ for some unit u_i a unit and $e_i \in K$ (since either u_i is a p^{th} power, or $u_i = \pm 1 = (\pm 1)^p$ since p odd). Since c_i is not in K^p, we have p divides a_i, implying $c_1, \ldots, c_m$ are p-independent in K. Then by Lemma 4.3.5, $b_1, \ldots, b_m$ are p-independent in K. But then we are done by Theorem 4.2.13. □

4.4. THE GALOIS GROUP A WREATH PRODUCT

In this section we restrict our arguments to the situation where $R = \mathbb{Z}$ and thus $K = \mathbb{Q}$. Recall $f_1(x) = x^n - b \in \mathbb{Z}[x]$ with $n = p^t$ for p an odd prime. We use the results from the previous sections to show $G_m \cong [C_{p^t}]^m$ except for at most finitely many $b \in \mathbb{Z}$.

We first introduce the following notation. Let T be algebraically independent over $\mathbb{Q}$ and let $F_1(x,T) = x^n - T$, $F_{m+1}(x,T) = F_1(F_m(x,T))$.

We will use the following result from [14].

Lemma 4.4.1

(a) For $m \geq 1$, let $H_m(T) = F_m(0,T)$. Then $H_m(T)$ is monic of degree n^m in $\mathbb{Z}[T]$.

(b) For every $m \geq 1$, $H_m(T)$ is squarefree in $\mathbb{C}[T]$.

Our work requires a special case of a result of LeVeque-Siegel [9].

Theorem 4.4.2 *Let $g(x) \in \mathbb{Z}[x]$ having at least three distinct zeros in $\mathbb{C}$. Let $r \geq 2$. Then*

$$y^r = g(x)$$

does not have an infinite set of solutions in $\mathbb{Z}$.

We now prove the main result of this section.

Theorem 4.4.3 *Let $f(x) = x^n - b \in \mathbb{Z}[x]$ with $n = p^t$, p an odd prime. Given $m \geq 1$, $G_m \cong [C_n]^m$ except for possibly finitely many $b \in \mathbb{Z}$, where G_m is the Galois group of $f_m(x)$ over $\mathbb{Q}(\epsilon_n)$ for ϵ_n a primitive n^{th} root of unity.*

Proof: By Theorem 4.3.6, if none of $c_1, \ldots, c_m$ is in $\mathbb{Q}^p$, then $G_m \cong [C_n]^m$. We show that given an $m \geq 1$, except for possibly finitely many $b \in \mathbb{Z}$, none of $c_1, \ldots, c_m$ is in $\mathbb{Q}^p$. Let k be such that $1 \leq k \leq m$. Using the notation given above, let $H_k(T) = F_k(0, T)$. Now, by definition (see Lemma 4.3.3) we have

$$\begin{aligned} c_k = \prod_{d|k} b_d^{\mu(k/d)} &= \prod_{d|k} f_d(0)^{\mu(k/d)} \\ &= \prod_{d|k} F_d(0, b)^{\mu(k/d)} \\ &= \prod_{d|k} H_d(b)^{\mu(k/d)} \\ &= h_k(b) \end{aligned}$$

where $h_k(T) = \prod_{d|k} H_d(T)^{\mu(k/d)} \in \mathbb{Z}[T]$ by Lemma 4.3.3 (with $R = \mathbb{Z}[T]$). But $h_k(T) = \prod_{d|k} H_d(T)^{\mu(k/d)} = \prod_{d|k} F_d(0, T)^{\mu(k/d)}$, with $F_d(0, T) = H_d(T)$ squarefree by Lemma 4.4.1.

Now by Theorem 4.4.2, if $h_k(T)$ has at least three distinct zeros in $\mathbb{C}$, then the equation

$$y^p = h_k(T), \tag{4.5}$$

has only finitely many solutions with $y, T \in \mathbb{Z}$.

Set $TD_i(T) = H_i(T)$ for $1 \leq i \leq k$. Then $D_i(T) \in \mathbb{Z}[T]$ is squarefree, and $\deg D_i(T) = n^i - 1$. Now we have

$$\begin{aligned} h_k(T) &= \prod_{d|k} F_d(0,b)^{\mu(k/d)} \\ &= \prod_{d|k} H_d(T)^{\mu(k/d)} \\ &= \prod_{d|k} T^{\mu(k/d)} D_d(T)^{\mu(k/d)} \\ &= T^{\tau(k)} \prod_{d|k} D_d(T)^{\mu(k/d)} \in \mathbb{Z}[T], \end{aligned}$$

for some integer $\tau(k)$.

We now claim $r = \deg D_k(T) - \deg\{lcm\{D_d(T) \mid d|k,\ d < k\}\} \geq 3$. If so, then we will have at least three distinct roots of $D_k(T)$ remaining in the product $\prod_{d|k} D_d(T)^{\mu(k/d)}$ (coming from the prime factors dividing $D_k(T)$ not dividing $D_d(T)$ for $d < k$). Now the maximum of

$$\begin{aligned} \deg\{lcm\{D_d(T) \mid d|k,\ d < k\}\} &= \sum_{d|k,\ d \neq k} \deg D_d(T) \\ &= \sum_{d|k,\ d \neq k} (n^d - 1). \end{aligned}$$

So we need to show $r = n^k - 1 - (n^1 - 1 + n^{d_1} - 1 + \cdots + n^{d_s} - 1) \geq 3$, for d_i the divisors of k. We note that

$$(n - 1 + n^2 - 1 + \cdots + n^{[\frac{k}{2}]} - 1) \geq (n^1 - 1 + n^{d_1} - 1 + \cdots + n^{d_s} - 1)$$

since $d|k$, $d \neq k$ implies $d \leq [\frac{k}{2}]$, where $[\frac{k}{2}]$ is the greatest integer less than or equal to $\frac{k}{2}$. Thus we have

$$\begin{aligned} r &\geq n^k - (1 + n + n^2 + \cdots + n^{[\frac{k}{2}]}) + [\frac{k}{2}] \\ &= n^k - \frac{n^{[\frac{k}{2}]+1} - 1}{n - 1} + [\frac{k}{2}] = s. \end{aligned}$$

We note $s \geq 3$ if $k \geq 4$. We have

$$\begin{aligned} s &\geq n^4 - \frac{n^3 - 1}{n - 1} + 2 \\ &= n^4 - (n^2 + n + 1) + 2 \\ &\geq 3^4 - (3^2 + 3 + 1) + 2 > 3, \end{aligned}$$

since $n = p^t \geq 3$. Next, if $k = 3$, we have $r = n^3 - 1 - (n-1) = n^3 - n \geq 3^3 - 3 > 3$, and if $k = 2$, we have $r = n^2 - 1 - (n-1) = n^2 - n \geq 3^2 - 3 > 3$. So for $k > 1$, we get $r \geq 3$. Therefore, $h_k(T)$ has at least three distinct zeros in $\mathbb{C}$ which implies there exist at most finitely many $b \in \mathbb{Z}$ with

$$y^p = h_k(b) = c_k. \tag{4.6}$$

Thus, for each k such that $1 \leq k \leq m$, there exist at most finitely many b with $c_k \in \mathbb{Z}^p$. Therefore, there exist infinitely many $b \in \mathbb{Z}$ with b not a solution to equation (4.6) for all $k \leq m$. Then for such b, $c_1, \ldots, c_m \notin \mathbb{Z}^p$ and by Theorem 4.3.6, $G_m \cong [C_n]^m$. □

We note the following result.

Corollary 4.4.4 *Let p be an odd prime and $f_1(x) = x^p - b$ irreducible in $\mathbb{Z}[x]$. Then $G_2 \cong [C_p]^2$.*

Proof: We show that $c_1, c_2 \notin \mathbb{Z}^p$. By definition, we have

$$\begin{aligned} b_1 &= f_1(0) = -b, \\ b_2 &= f_2(0) = f_1(-b) = (-b)^p - b = -b(b^{p-1} + 1) \end{aligned}$$

which gives

$$\begin{aligned} c_1 &= b_1 = -b \\ c_2 &= \frac{b_2}{b_1} = b^{p-1} + 1. \end{aligned}$$

By Theorem 4.3.6, $G_2 \cong [C_p]^2$ if $c_i \notin \mathbb{Z}^p$ $(i = 1, 2)$, that is, if $c_1 \notin \mathbb{Z}^p$ and if there are no solutions to the diophantine equation

$$y^p = b^{p-1} + 1. \tag{4.7}$$

By assumption, $f_1(x)$ is irreducible, so $c_1 = -b \notin \mathbb{Z}^p$. Since p is odd, $p-1$ is even, so $b^{(p-1)/2} = b_0 \in \mathbb{Z}$. Thus equation 4.7 becomes

$$y^p = (b^{(p-1)/2})^2 + 1 = b_0^2 + 1. \tag{4.8}$$

Solutions to 4.8 were proved impossible for $y > 1$ and p an odd prime in 1850 by Lebesgue [11]. Therefore, $c_2 \notin \mathbb{Z}^p$.

So for $f_1(x) = x^p - b$ irreducible in $\mathbb{Z}[x]$, $f_2(x)$ is always irreducible, and $G_2 \cong [C_p]^2$. □

We have one final remark concerning the Galois group of the iterates in the special case of $f(x) = x^p - b \in \mathbb{Z}[x]$, for p an odd prime. This will follow from the Schur–Zassenhaus Theorem from group theory [2]:

Theorem 4.4.5 (Schur–Zassenhaus) *Suppose E is a finite group with A normal in E, and $(|\, A \,|, |\, E/A \,|) = 1$. Then there exists a subgroup S of E with $A \cap S = \{1\}$ and $E = AS$. Moreover, if T is another such subgroup, then there exists an $e \in E$ with $T = eSe^{-1}$.*

Corollary 4.4.6 *Let p be an odd prime and $f_1(x) = x^p - b$ irreducible in $\mathbb{Z}[x]$. Let E_m be the splitting field of f_m, and let $G_m = Gal(E_m/\mathbb{Q}(\epsilon_p))$. Assume that $G_m \cong [C_p]^m$. Then for Ω_m, the Galois group of f_m over $\mathbb{Q}$, we have $\Omega_m = G_m S$, for some subgroup S of Ω_m with $G_m \cap S = \{1\}$.*

Proof: First, $\mathbb{Q}(\epsilon_p)/\mathbb{Q}$ is Galois (see [20]), so by Theorem 2.1.5 G_m is normal in Ω. Also, since p is prime, $[\mathbb{Q}(\epsilon_p) : \mathbb{Q}] = p - 1$. Also, by Lemma 4.1.2, we have

$|G_m| = p^{p^{m-1}+p^{m-2}+\cdots+p+1}$. Therefore $(|\ G_m\ |, |\ \Omega/G_m\ |) = (p^{p^{m-1}+p^{m-2}+\cdots+p+1}, p - 1) = 1$. Thus we are done by Theorem 4.4.5. □

Finally, we conclude by mentioning some of the unanswered questions which have arisen from this study. The general problem of determining whether or not all iterates of an irreducible binomial, $x^n - b \in \mathbb{Q}[x]$, are irreducible is still open. In the special case where p is an odd prime, and $x^p - b \in \mathbb{Z}[x]$ is irreducible, we have not determined G_m, the Galois group of E_m over $\mathbb{Q}(\epsilon_p)$, for $m > 2$ (recall E_m is the splitting field of $f_m(x)$). The more general problems of determining G_m for $x^n - b$ irreducible with $b \in \mathbb{Z}$ or $b \in \mathbb{Q}$ remain open. And thus, Ω_m, the Galois group of E_m over $\mathbb{Q}$, remains undetermined.

BIBLIOGRAPHY

[1] T.M. Apostol, *Introduction to Analytic Number Theory*, (Springer-Verlag New York Inc., 1976), pp. 24-51.

[2] K.S. Brown, *Cohomology of Groups*, (Springer–Verlag New York Inc., 1982), pp. 91-94.

[3] J.E. Cremona, *On the Galios groups of the iterates of* x^2+1, Mathematika **36**, 259 - 261 (1989).

[4] H. Darmon, A. Granville, *On the equations* $z^m = F(x,y)$ *and* $Ax^p + By^q = Cz^r$, University of Georgia Mathematics Preprint Series, Preprint No. 2, Volume 2 (1994).

[5] B. Fein, M. Schacher, *Properties of Iterates and Composites of Polynomials*, pre-print.

[6] T.W. Hungerford, *Algebra*, (Springer–Verlag New York Inc., 1974)

[7] K. Kubota, *Pythagorean Triples in Unique Factorization Domains*, Amer. Math. Monthly **79**, 503 - 505 (1972).

[8] S. Lang, *Algebra*, (Addison-Wesley Publishing Company, Inc., 1965), pp. 221-223.

[9] W.J. LeVeque, *On the equation* $y^m = f(x)$, Acta Arith. **9**, 209 - 219, (1964).

[10] P.J. McCarthy, *Algebraic Extensions of Fields,* (Blaisdell Publishing Company, 1966)

[11] L.J. Mordell, *Diophantine Equations,* (Academic Press Inc., 1969), p. 301.

[12] R.W.K. Odoni, *On the Prime Divisors of the Sequence* $w_{n+1} = 1 + w_1 \cdots w_n$, J. London Math. Soc. **32**, 1 - 11 (1985a).

[13] R.W.K. Odoni, *The galois theory of iterates and composites of polynomials*, Proc. London math. Soc. **51**, 385 - 414 (1985b).

[14] R.W.K. Odoni, *Realising wreath products of cyclic groups as Galois groups*, Mathematika **35**, 101 - 113 (1988).

[15] D.S. Passman, *Permutation Groups*, Chapter 1 (Benjamin, New York 1968).

[16] W.R. Scott, *Group Theory*, Chapter 6 (Prentice-Hall, Inc., 1964).

[17] H.N. Shapiro, *Introduction to the Theory of Numbers*, (John Wiley & Sons, Inc. 1983).

[18] M. Stoll, *Galois groups over $\mathbb{Q}$ of some iterated polynomials*, Arch. Math. **59**, 239 - 244 (1992).

[19] N.G. Tschebotarev, *Grundzüge der Galois' schen Theorie* (translated from Russian by H. Schwerdtfeger, P. Noordhof NV, Groningen, 1950).

[20] E. Weiss, *Algebraic Number Theory*, (McGraw-Hill, 1963).

[21] O. Zariski and P. Samuel, *Commutative Algebra*, (D. Van Nostrand Company, Inc., 1958).