Polynomials that are Integer Valued on the Image of an Integer-Valued Polynomial

by

Mario V. Marshall

A Dissertation Submitted to the Faculty of

The Charles E. Schmidt College of Science

in Partial Fulfillment of the Requirements for the Degree of

Doctor of Philosophy

Florida Atlantic University

Boca Raton, Florida

August 2009

Polynomials that are Integer Valued on the Image of an Integer-Valued Polynomial

by

Mario V. Marshall

This dissertation was prepared under the direction of the candidate's dissertation advisor, Dr. Lee Klingler, Department of Mathematical Sciences, and it has been approved by the members of his supervisory committee. It was submitted to the faculty of the Charles E. Schmidt College of Science and was accepted in partial fulfillment of the requirements for the degree of Doctor of Philosophy.

SUPERVISORY COMMITTEE:

Lee Klingler

Lee Klingler, Ph.D.
Dissertation Advisor

Frederick Hoffman

Frederick Hoffman, Ph.D.

Spyros Magliveras, Ph.D.

Fred Richman

Fred Richman, Ph.D.

Lee Klingler

Lee Klingler, Ph.D.
Chair, Department of Mathematical Sciences

G W Perry

Gary W. Perry, Ph.D.
Dean, The Charles E. Schmidt College of Science

Barry T. Rosson

Barry T. Rosson, Ph.D.
Dean, Graduate College

July 7, 2009

Date

Acknowledgements

I would like to thank Professor Klingler, my advisor, for introducing me to integer-valued polynomials, and for the time spent with me on this project. Professor Brewer, for introducing me to algebra. Professor Richman, for making some valuable comments on the thesis. Thanks also for attending many of the courses I sat in throughout my years at FAU especially for the commutative algebra seminars with Professor Brewer. Professor Hoffman, for taking the time to read my thesis, his suggestions. Also thanks for designing a fair work schedule in the summer of 2008, that was a crucial time when the ground work of the thesis was being laid. Professor Magliveras, who was also the head of department throughout my years here at FAU, for his fairness in all matters I encountered and for taking the time to read my thesis.

Dr Solan, lecturer at University of the West Indies in Jamaica, for informing me of the opportunities to further my studies in the United States. Dr Buckley, for being an inspiration during both my graduate and undergraduate years.

Thanks also to my friends and family, for without their moral support this would not have been possible. Thanks especially to the "Marshalls": My grandmother "Miss Leetie", cousin Jody , "Uncle Cham", Aldin, Mitzy ("Auntie Tricky"), Mollene ("Auntie Viv"), my brothers Michael, Matthew and Merrick, my step mother Valerie, and most of all, I thank my dad Norman.

Abstract

Author:	Mario V. Marshall
Title:	Polynomials that are Integer-Valued on the Image of an Integer-Valued Polynomial
Institution:	Florida Atlantic University
Thesis Advisor:	Prof. Lee Klingler
Degree:	Doctor of Philosophy
Year:	2009

Let D be an integral domain and f a polynomial that is integer-valued on D. We prove that $\text{Int}(f(D), D)$ has the Skolem Property and give a description of its spectrum. For certain discrete valuation domains we give a basis for the ring of integer-valued even polynomials. For these discrete valuation domains, we also give a series expansion of continuous integer-valued functions.

Dedication

This research is dedicated my first teacher, Prudence Wellington, thanks mom for laying the foundation.

"Courage is knowing what not to fear!" – Plato

Contents

Chapter 1

Introduction

Let D be an integral domain with quotient field K and E a nonempty subset of D. The ring of polynomials integer-valued on E, $\text{Int}(E, D) = \{f \in K[x] | f(E) \subset D\}$ is well studied, especially for the case where $D = \mathbb{Z}$. (In the case where $E = D$, one usually writes $\text{Int}(D)$ instead of $\text{Int}(D, D)$.) Here we will be studying the case for which $E = f(D)$, where $f \in \text{Int}(D)$. The motivation comes from a question in the problem book by Pólya and Szegö, see [25]. In the section on integer-valued polynomials in [25], one question gives a $\mathbb{Z}$-basis for the subring of $\text{Int}(\mathbb{Z})$ consisting of integer-valued even polynomials. This ring is isomorphic to $\text{Int}(E, \mathbb{Z})$ where $E = \{n^2 | n \in \mathbb{Z}\}$. Since most of the properties are dependent on E being the image of an integer-valued polynomial we present many of our results for the more general ring $\text{Int}(f(D), D)$, where D is usually assumed to be a Dedekind domain with finite residue fields, and f an arbitrary (nonconstant) integer-valued polynomial on D. In the following sections we present a brief account of theory related to the results proven in the later chapters.

1.1 Basis elements

As early as the seventeenth century, see the historical introduction in [5],it was known that the functions $\binom{x}{n} = \frac{x(x-1)\cdots(x-n+1)}{n!}$ form a $\mathbb{Z}$-basis for $\mathrm{Int}(\mathbb{Z})$. An analogue was given for discrete valuation domains in [5, Theorem II.2.7]. Pólya and Szegö gave a similar result for the even and odd integer-valued polynomials in $\mathrm{Int}(\mathbb{Z})$. We will give an analogue for these odd and integer-valued even polynomials for certain discrete valuation domains.

1.2 The Spectrum

The spectrum of an integral domain is the set of prime ideals of that domain. For the ring $\mathrm{Int}(\mathbb{Z})$, it turns out that the prime ideals above $p\mathbb{Z}$ for prime $p \in \mathbb{Z}$, are in one-to-one correspondence with the p-adic integers.

The prime ideals above (0) are in one-to-one correspondence with the monic irreducible polynomials in $\mathbb{Q}[x]$. For certain integral domains similar results hold for $\mathrm{Int}(E, D)$. (For example $\hat{D}$, the completion of D in the M-adic topology, must be an integral domain.) Among other things, our result will show that the prime ideals in the ring of integer-valued even polynomials above $p\mathbb{Z}$ are in one-to-one correspondence with the set of p-adic integers that are perfect squares.

1.3 Skolem Property

One major result in $\mathrm{Int}(\mathbb{Z})$ is that it has the Skolem property: If $g_1, \ldots, g_k$ are integer-valued polynomials such that $g_1(n), \ldots, g_k(n)$ are relatively prime for each integer n, then there exist integer-valued polynomials $u_1, \ldots, u_k$ such that $u_1 g_1 + \cdots + u_k g_k = 1$. Like almost all results pertaining to $\mathrm{Int}(\mathbb{Z})$, this has been generalized. A stronger form of the Skolem property is that the property holds for arbitrary ideals generated by $g_1(n), \ldots, g_k(n)$. $\text{Int}(E, D)$ has the strong Skolem property if, given two finitely generated ideals I and J of $\text{Int}(E, D)$, if for all $a \in E$ it is the case that $I(a) = J(a)$ then $I = J$. From [9], certain conditions on E and D ensure that $\text{Int}(E, D)$ has the strong Skolem property. We give conditions on the integral domain D that ensure that $\text{Int}(f(D), D)$ has the strong Skolem property for every nonconstant integer-valued polynomial f.

1.4 Factorization Properties

In section VI.3 of [5], it was shown that the basis elements for $\text{Int}(\mathbb{Z})$ are irreducible in $\text{Int}(\mathbb{Z})$. We will show that the $\mathbb{Z}$-basis elements for the ring of integer-valued even polynomials noted by Pólya and Szegö are irreducible in the ring of integer-valued even polynomials.

1.5 Stone-Weierstrass Theorem

The Stone-Weierstrass theorem for discrete valuation domains tells us that continuous integer-valued *functions* can be approximated by integer-valued *polynomials*. We show that for certain discrete valuation domains, even (respectively odd) continuous integer-valued functions may be approximated by even (respectively odd) integer-valued polynomials. One consequence of this fact is that we will get an alternative to the Mahler expansion. A p-adic continuous function can be expressed in the form $\sum_{i=0}^{\infty} \alpha_n \binom{x}{i}$ where $\{\alpha_n\}$ is a null sequence. This expansion known as the Mahler expansion and it was generalized in [5, section III.3] to discrete valuation domains. We give a similar expansion for both even and odd continuous functions.

Chapter 2

Integer-valued Polynomials

Let D be an infinite integral domain with field of fractions K and f a nonconstant element of $\mathrm{Int}(D)$. A subset E of K is called a *fractional subset* if there exists nonzero $d \in D$ such that $dE \subset D$. In this section we give results for $\mathrm{Int}(f(D), D)$. For general fractional subsets $E \subset K$, the ring $\mathrm{Int}(E, D)$ has been studied thoroughly, including the case where E is an infinite subset of D. We get stronger results for $\mathrm{Int}(f(D), D)$, because $f(D)$ has some special properties.

We shall begin by showing that $\mathrm{Int}(f(D), D) \cong D_f$, where $D_f = \mathrm{Int}(D) \bigcap K[f(x)]$. Note that if the characteristic of D is not 2, then D_{x^2} is the ring of integer-valued even polynomials.

If D is a Noetherian domain, then f is continuous in the I-adic topology for any ideal I of D. From this we can describe the topological closure of $f(D)$ in $\hat{D}_M$, the M-adic completion of D in K where M is a maximal ideal of D. This will be used to give a description the spectrum of $\mathrm{Int}(f(D), D)$.

Suppose that for all $g, h \in K[x]$ such that $g(a)|h(a)$ for all $a \in E \subset K$ we have $g(x)|h(x)$ in $K[x]$. Then E is called a d-set. We shall show that, under certain mild condtions which we shall present later, $f(D)$ is a d-set.

If $a \in E$, we call a an isolated point of E if $\mathrm{Int}(E, D) \subsetneq \mathrm{Int}(E - \{a\}, D)$. Note that, if f is integer-valued on E, then certainly it is integer-valued on any subset of E; hence $\mathrm{Int}(E, D) \subset \mathrm{Int}(F, D)$ for any $F \subset E$. We will show that $f(D)$ has no isolated points. This property, along with being a d-set, is used to show that under certain conditions on D, $\mathrm{Int}(f(D), D)$ has the strong Skolem property.

$\mathrm{Int}(f(D), D)$ has been previously studied. For example, [15] gave conditions on a subset $E \subset \mathbb{Z}$ that it be polynomially equivalent to $f(E)$, where two sets E and F are polynomially equivalent with respect to the domain D if $\mathrm{Int}(E, D) = \mathrm{Int}(F, D)$. Nothing has been done on the algebraic properties of $\mathrm{Int}(f(D), D)$; however, algebraic properties of $\mathrm{Int}(E, D)$ for certain special subsets E and domains D have been studied. Some algebraic properties of $\mathrm{Int}(\mathbb{P}, \mathbb{Z})$, for example, where $\mathbb{P}$ is the set of rational prime numbers, were investigated in [7], such as whether it satisfies the strong Skolem property (it does not), as well as a description of the spectrum.

We now give the isomorphism between $\mathrm{Int}(f(D), D)$ and D_f.

Proposition 2.1. *Let D be an integral domain with quotient field K, $f \in \mathrm{Int}(D)$ a nonconstant integer-valued polynomial $D_f = \mathrm{Int}(D) \bigcap K[f(x)]$, then $\mathrm{Int}(f(D), D) \cong D_f$.*

Proof. Let $h(x) \in \mathrm{Int}(f(D), D)$ map to $h(f(x))$. This is the natural isomorphism from $K[x]$ to $K[f(x)]$ restricted to $\mathrm{Int}(f(D), D)$. It is clear that the image of this restriction is D_f. □

Note that D_f is closed under composition, while $\mathrm{Int}(f(D), D)$ is not, despite both rings being isomorphic subrings of $K[x]$. For example consider, $D = \mathbb{Z}$ and $f(x) = x^2$, then $h(x) = x + 2 \in \mathrm{Int}(f(\mathbb{Z}, \mathbb{Z})$ as is $g(x) = \frac{x(x-1)}{4}$, but $g(h(1)) = \frac{3}{2} \notin \mathbb{Z}$.

2.1 A description of the spectrum of $\mathrm{Int}(f(D), D)$

Our task in this subsection is to give a description of the spectrum of $\mathrm{Int}(f(D), D)$. The spectrum for $\mathrm{Int}(E, D)$ for a Noetherian local one-dimensional domain D, with finite residue field, where E is a fractional subset of D, is given in (Theorem V.2.10, [5]).

Let I be an ideal of D, the I-adic topology is the topology on D obtained by using $\mathcal{F} = \{x + I^n\}_{n=1}^{\infty}$ as a system of neighborhoods of $x \in D$, which makes D a topological ring. For information on the I-adic topology we refer the reader to [20, Section 8].

Lemma 2.1. *For any domain D with ideal I and polynomial $f \in D[x]$ with coefficients in D, then f is continuous in the I-adic topology, (see Lemma III.2.3,[5]).*

Proof. This follows immediately from the fact that addition and multiplication are continuous. □

Now we want to show that $f \in \mathrm{Int}(D)$ is a continuous function. In the next lemma we show that, for a Noetherian domain D with ideal I, if we divide a continuous function by a nonzero constant and the result is still a function on D, then it is continuous. Since this is the situation for integer-valued polynomials, its continuity will follow immediately. This is [5, Lemma III.2.3], but the result stated there is for integer-valued polynomials, and we generalize this to continuous functions. The proof of the next theorem will make use of the Artin-Rees Lemma which states that, for a Noetherian domain D with ideals I and J, there exists a positive integer k such that, for all positive integers n, $I^{n+k} \cap J = I^n(I^k \cap J)$.

Proposition 2.2. *Let I be an ideal of a Noetherian domain D and $\phi : D \to D$ a function on D. If there exists a nonzero constant $d \in D$ such that $d\phi$ is continuous in the I-adic topology, then ϕ is continuous in the I-adic topology.*

Proof. It is sufficient to show that, given an element $y \in D$ and positive integer n, there exists a positive integer m such that $\phi(y + I^m) \subset \phi(y) + I^n$.

By the Artin-Rees Lemma, there exists an integer k such that $I^{n+k} \bigcap (d) = I^n(I^k \bigcap (d)) \subseteq dI^n$. Because $d\phi$ is continuous, there exists a positive integer m such that $(d\phi)(y + I^m) \subseteq (d\phi)(y) + I^{n+k}$. Clearly $(d\phi)(y + I^m) \subset (d)$, hence $d\phi(y+I^m) \subseteq (d\phi)(y)+[I^{n+k} \bigcap (d)]$. Now $I^{n+k} \bigcap (d) \subseteq dI^n$, by the Artin Rees Lemma, implies $(d\phi)(y + I^m) \subseteq (d\phi)(y) + dI^n$. Dividing by d gives $\phi(y + I^m) \subseteq \phi(y) + I^n$ as desired. $\square$

It follows from the previous two results that the integer-valued polynomials are continuous on a Noetherian domain D.

Corollary 2.1. *Let I be an ideal of the Noetherian domain D. Then each integer-valued polynomial $f \in \mathrm{Int}(D)$ is continuous on D in the I-adic topology.*

If D is a Noetherian domain then for any ideal I, we will show that $f \in \mathrm{Int}(D)$ is continuous in the I-adic topology. This was also shown in [5, Lemma III.2.3]. Now for $i < j$ we can form the natural map $\phi_{ij} : D/I^j \to D/I^i$ hence forming the inverse system of rings, $D/I \leftarrow D/I^2 \leftarrow D/I^3 \leftarrow \cdots$. The limit of this inverse system is the I-adic completion of D, which we denote by $\hat{D}$. Note that the I-adic completion of D is the set of all sequences $(a_1, a_2, \ldots)$, with $a_n \in D/I^n$ and $a_n - a_{n-1} \in I^{n-1}$. We call a domain D analytically irreducible, if its completion $\hat{D}$ in the M-adic topology is a domain for all maximal ideals M of D. Note also that for, $D = \mathbb{Z}$ and $I = (p)$ a prime ideal of $\mathbb{Z}$, we get the p-adic integers.

Lemma V.1.3 of [5] tells us the following. Let $\mathfrak{p}$ be a prime ideal of D and a be an element of E. Then

$$\mathfrak{P}_{\mathfrak{p},a} = \{f \in \mathrm{Int}(E, D) | f(a) \in \mathfrak{p}\}$$

is a prime ideal of $\mathrm{Int}(E, D)$ above $\mathfrak{p}$, and $\mathrm{Int}(E, D)/\mathfrak{P}_{\mathfrak{p},a} \equiv D/\mathfrak{p}$.

The proof of the lemma is clear since $\mathfrak{P}_{\mathfrak{p},a}$ is the kernel of the ring homomorphism obtained by composing the evaluation map at a, followed by reduction modulo $\mathfrak{p}$, and clearly the image of this map is $D/\mathfrak{p}$. Thus, if $\mathfrak{p}$ is maximal, then so is $\mathfrak{P}_{\mathfrak{p},a}$.

Let D be a Noetherian local one dimensional analytically irreducible domain with finite residue field and E a fractional subset of D. Then the prime ideals of $\mathrm{Int}(E, D)$ above the maximal ideal $\mathfrak{m}$ of D are in one-to-one correspondence with the elements of $\hat{E}$, the $\mathfrak{m}$-adic completion of E: to each element α in $\hat{E}$ corresponds the prime

$$\mathfrak{M}_{\mathfrak{m},\alpha} = \{f \in \mathrm{Int}(E, D) | f(\alpha) \in \hat{\mathfrak{m}}\}.$$

Because D is one-dimensional, these ideals $\mathfrak{M}_{\mathfrak{m},\alpha}$ account for all of the prime ideals of $\mathrm{Int}(E, D)$ that do not contract to (0) in D.

To find the closure of $f(D)$ we first show that, for Noetherian domains D, the completion $\hat{D}$ is compact in the M-adic topology. In [5, Proposition III.1.2] it is shown that, if R is a Noetherian ring with an ideal I such that $\bigcap_{k=0}^{\infty} I^n = 0$, then R/I is finite if and only if the completion $\hat{R}$ of R in the I-adic topology is compact. For this thesis, we restrict ourselves to domains. For Noetherian domains, for any proper ideal I it is always the case that $\bigcap_{k=0}^{\infty} I^k = (0)$. (This is Krull's intersection theorem; see [20, Theorem 8.10.ii].) Thus, the following lemma follows.

Lemma 2.2. *Let D be a Noetherian domain, I a proper ideal of D such that D/I is* *finite. The completion $\hat{D}$ of D in the I-adic topology is compact.*

Recall that, $d(x, y) = 2^{-k}$, where $k = \sup\{k | x - y \in I^k\}$, results in a metric induced by the I-adic topology. We refer the reader to [5, Section III.1] for more information.

Now we are ready to describe the closure of $f(D)$ in the M-adic topology in the case where D is a Noetherian domain with D/M finite.

Lemma 2.3. *Let D be a Noetherian domain that is not a field, and M an ideal such that D/M is finite. Then every infinite sequence of elements in the completion $\hat{D}$ of D, has a convergent subsequence in the M-adic topology.*

Proof. From Krull's intersection theorem, $\bigcap_{k=0}^{\infty} M^k = (0)$. Hence the Lemma follows from Proposition III.1.2 of [5], which tells us that $\hat{D}$ is compact, together with a standard topological argument; for example, see the proof of [23, Theorem 28.2]. □

Proposition 2.3. *Let D be a Noetherian domain with quotient field K, M an ideal of D such that D/M is finite, and $f \in \mathrm{Int}(D)$. Then the topological closure of $f(D)$ in the M-adic completion of K is $f(\hat{D})$, where $\hat{D}$ is the M-adic completion of D.*

Proof. Let α be an element of the topological closure of $f(D)$, so α is the limit of some sequence of elements of $f(D)$, say $\{f(\alpha_i)\}$, where for each i, $a_i \in D$. By Lemma 2.3, the sequence $\{a_i\}$ has a convergent subsequence with limit a. From the continuity of f , Corollary 2.1, it follows that $\alpha = f(a)$, so that the topological closure of $f(D)$ is contained in $f(\hat{D})$. The other containment is clear. □

We can now describe the spectrum for $\mathrm{Int}(f(D), D)$, in the case where D is a Noetherian local one-dimensional domain with finite residue field.

Theorem 2.1. *Let D be a one-dimensional local Noetherian domain with finite residue field and maximal ideal M and quotient field K and $f \in \mathrm{Int}(D)$. The prime ideals of $\mathrm{Int}(f(D), D)$ above M are in one-to-one correspondence with the elements of $f(\hat{D})$: to each element α in $f(\hat{D})$ corresponds the prime ideal $\mathfrak{M}_\alpha = \{g \in \mathrm{Int}(f(D), D) | g(\alpha) \in \hat{M}\}$, and $\mathrm{Int}(f(D), D)/\mathfrak{M}_\alpha \cong D/M$.*

The nonzero prime ideals above (0) are in one-to-one correspondence with the monic polynomials irreducible in $K[x]$: to the irreducible polynomial q corresponds the prime $\mathfrak{P}_q = qK[x] \cap \mathrm{Int}(D)$. If $q(\alpha) = 0$ then $\mathfrak{P}_q$ is contained in $\mathfrak{M}_\alpha$. If D is a discrete valuation domain, then $\mathfrak{P}_q$ is contained in $\mathfrak{M}_\alpha$ if and only if $q(\alpha) = 0$.

Proof. By Proposition 2.2, the closure of $f(D)$ is $f(\hat{D})$, hence the results stated about $\mathfrak{M}_\alpha$ follow immediately from [5, Proposition V.2.1]. □

We globalize [5, Lemma V.2.1] to get the following lemma from which we will get a global version of the previous theorem.

Proposition 2.4. *Let D be a one dimensional Noetherian domain with finite residue field at each maximal ideal. Each maximal ideal of $\mathrm{Int}(E, D)$ above a maximal ideal M of D is of the form*

$$\mathcal{M}_{\alpha,M} = \{f \in \mathrm{Int}(E, D) | f(\alpha) \in \hat{M}\}$$

where α is in the closure of E in the M-adic completion of D_M.

Proof. Since D is Noetherian, from [5, Proposition I.2.7 (i)], for any multiplicative subset $S \subset D$, $S^{-1}\operatorname{Int}(E,D) = \operatorname{Int}(E,S^{-1}D)$. Now let $\mathfrak{M}$ be a prime ideal in $\operatorname{Int}(E,D)$ above maximal ideal M of D. Let $S_M = D - M$ and note that this is a multiplicative subset of $\operatorname{Int}(E,D)$. It follows that $S^{-1}\operatorname{Int}(E,D) = \operatorname{Int}(E,D_M)$. Now from standard results on localization (see [18, chapter II]), we know the prime ideals above M in $\operatorname{Int}(E,D)$ correspond naturally to the prime ideals above M in $\operatorname{Int}(E,D_M)$. Hence by the previous theorem gives a one-to-one correspondence between the primes above M in $\operatorname{Int}(E,D)$ and the elements in $\hat{E}$, the completion in $\hat{K}$. □

Thus, the following corollary follows.

Corollary 2.2. *Let D be a one dimensional Noetherian domain with finite residue field at each maximal ideal and $f \in \operatorname{Int}(D)$. Then the maximal ideals of $\operatorname{Int}(f(D),D)$ are in one-to-one correspondence with the elements of $f(\hat{D})$, that is, to each $\alpha \in f(\hat{D})$ corresponds the maximal ideal $\mathcal{M}_{\alpha,M} = \{h \in \operatorname{Int}(f(D),D) | h(\alpha) \in \hat{M}\}$.*

As an example of the utility of the main result, we obtain the spectrum of $\mathbb{Z}_{x^2}$, the ring of integer-valued even polynomials on $\mathbb{Z}$.

Corollary 2.3. *Let p be a prime of $\mathbb{Z}$. Then the prime ideals of $\mathbb{Z}_{x^2}$ over a prime ideal $p\mathbb{Z}$ of $\mathbb{Z}$ are in one-to-one correspondence with the perfect squares of the p-adic integers: to each perfect square α^2 in $\hat{\mathbb{Z}}_{(p)}$ corresponds the prime ideal $\mathfrak{M}^*_{p,\alpha^2} = \{g(x^2) \in \mathbb{Z}_{x^2} | g(\alpha) \in (\hat{p})\}$. The nonzero primes over (0) are in one-to-one correspondence with the monic irreducible polynomials in $\mathbb{Q}[x^2]$: to each irreducible polynomial q corresponds the prime $\mathfrak{P}^*_q = \mathbb{Q}[x^2] \cap \mathbb{Z}_{x^2}$.*

Proof. From Proposition 2.1 $\mathbb{Z}_{x^2}$ is isomorphic to $\operatorname{Int}(E,\mathbb{Z})$ where $E = \{n^2 | n \in \mathbb{Z}\}$. Now let $\mathfrak{P}$ be a prime ideal of $\operatorname{Int}(E,\mathbb{Z})$ and $\mathfrak{P}^*$ be the image of $\mathfrak{P}$ under the isomorphism obtained by mapping $g(x)$ to $g(x^2)$. Therefore, the prime $\mathfrak{M}_{p,\alpha} = \{g(x) \in \operatorname{Int}(E,\mathbb{Z}) | g(\alpha^2) \in (p)\}$ of $\operatorname{Int}(E,\mathbb{Z})$ corresponds to $\mathfrak{M}^*_{p,\alpha} = \{g(x^2) \in \mathbb{Z}_{x^2} | g(\alpha) \in (p)\}$. Similarly, the prime ideal $\mathfrak{P}_q = q\mathbb{Q}[x] \cap \operatorname{Int}(f(\mathbb{Z}),\mathbb{Z})$ corresponds to $\mathfrak{P}^*_q = q(x^2)\mathbb{Q}[x^2] \cap \mathbb{Z}_{x^2}$. □

Note that, for an odd prime p, an element $b \in \hat{\mathbb{Z}}_{(p)}$ is a perfect square if the image of b in $\mathbb{Z}_p$ under the natural homomorphism is a perfect square. For $p = 2$, b is a perfect square if $b \equiv 1 \mod 8$. These results can be shown using Hensel's lemma. (For a proof we refer the reader to [12, Section 7.2].)

2.2 The Strong Skolem Property

We now turn our attention to another algebraic property of $\operatorname{Int}(f(D),D)$ for an integral domain D: that it have the strong Skolem property. The notion of a d-ring was introduced by Gunji and McQuillan in [16]. A ring D is a d-ring if, whenever f and g are polynomials in $D[x]$ with the property that $f(a)$ divides $g(a)$ in D for almost all elements a in D, then f divides g in $K[x]$. Gunji and McQuillan showed that the ring of algebraic integers in an algebraic number field is a d-ring. Now Chabert, Chapman, and Smith in [9] generalized the notion of a d-ring to that of a d-subset. E is a *divisor subset of* D (or a d-subset) if, for all polynomials $f, g \in K[x]$ such that $f(a)$ divides $g(a)$ in D for almost all elements a in E, then $f | g$ in $K[x]$. An element $a \in E$ is an *isolated* point of E if $\operatorname{Int}(E,D)$ is properly contained in $\operatorname{Int}(E - \{a\}, D)$. In Theorem 4.6 of [9] it was shown that if $\operatorname{Int}(E,D)$ is a Prüfer domain, and E a d-subset of D that has no isolated points, then $\operatorname{Int}(E,D)$ has the strong Skolem property. We first show that $f(D)$ is a d-subset if D is a d-ring.

Theorem 2.2. *Let D be an integral domain, and f an integer-valued polyonomial on D. Then $f(D)$ is a d-subset of D if and only if D is a d-ring.*

Proof. Suppose first that D is a d-ring, and g and h are elements of $\mathrm{Int}(f(D), D)$, such that $g(a)|h(a)$ for almost all $a \in f(D)$. This means that $g(f(a))|h(f(a))$ for almost all $a \in D$; since D is a d-subset this implies that $g(f(x))|h(f(x))$ in $K[x]$. So there exists a polynomial l in $K[x]$ such that $l(x) = h(f(x))/g(f(x))$. We now show that $l(x) = m(f(x))$ for some $m \in K[x]$. Write $\frac{h(x)}{g(x)} = m(x) + \frac{n(x)}{g(x)}$ for some $m, n \in K[x]$ with $\deg(n) < \deg(g)$. Then $l(x) = m(f(x)) + \frac{n(f(x))}{g(f(x))}$ with $\deg(n(f(x))) < \deg(g(f(x)))$. But $\frac{n(f(x))}{g(f(x))} = l(x) - m(f(x)) \in K[x]$, so it must be the case that $n = 0$, proving that $l(x) = m(f(x))$. Therefore $g|h$, making $f(D)$ a d-subset.

Conversely, if $f(D)$ is a d-subset, then since $f(D) \subset D$, it follows immediately that D is a d-ring. □

Next we show that, if D is an integral domain that is not a field, then $f(D)$ has no isolated points.

Theorem 2.3. *Let D be an integral domain that is not a field and f a nonconstant integer-valued polynomial on D. Then $f(D)$ has no isolated points.*

Proof. Let $E = f(D) - \{a\}$, and suppose that g is an element of $\mathrm{Int}(E, D)$ of degree n. Now $g(f(x))$ is integer-valued for all integers with the possible exception of those in $f^{-1}(a)$. Since $f^{-1}(a)$ is finite, the polynomial $g(f(x))$ is almost integer-valued, and since D is infinte by [5, Proposition I.1.5], the polynomial $g(f(x))$ is indeed integer-valued. Therefore $g(x)$ is an element of $\text{Int}(f(D), D)$, and hence $f(D)$ has no isolated points. $\square$

Lemma 2.4. *Let $E \subset F$ be infinite subsets of a domain D. If $a \in E$ is an isolated point of F, then a is an isolated point of E.*

Proof. Since a is an isolated point of F, there exists $h \in \text{Int}(F - \{a\}, D)$ such that $h(a) \notin D$. Since $\text{Int}(F - \{a\}, D) \subseteq \text{Int}(E - \{a\}, D)$, a is an isolated point of E. $\square$

Example 2.1. *We now give some examples of subsets in which every point is isolated.*

1. *The set of rational primes $\mathbb{P} \subset \mathbb{Z}$*
2. *The set $E = \{a_1, a_2, \ldots\}$ such that $(a_n) = (t)^n$ of an integral domain D with maximal prime ideal (t).*
3. *$E_a = \{a^n | n \subset \mathbb{N}\}$ for some $a \in \mathbb{N} - \{1\}$.*

Proof.

1. This was shown in [7], where they used the polynomial $\frac{(x-1)\cdots(x-p+1)}{p}$ to illustrate that the prime p is an isolated point.
2. For $a_n \in E$ we may use the polynomial $g(x) = \frac{x(x-a_1)\cdots(x-a_{n-1})}{t^k}$ where $k = \frac{n(n+1)}{2} + 1$. Let a be a nonzero element of D, define $v(a) = \min\{k | a \in (t)^k\}$. Now $v(g(a_n)) = -1$ hence $g(a_n) \notin D$. Let h be a positive integer, $v(g(a_{n+h})) = h - 1 \geq 0$ hence $g \in \text{Int}(E - \{a_n\}, D)$

3. This is a special case of 2.

□

We can use this example to make some interesting observation about $f(D)$ and in particular $f(\mathbb{Z})$.

Since if f is a nonzero integer-valued polynomial, $f(D)$ has no isolated points then the previous lemma yields the following proposition.

Proposition 2.5. *If E is a subset of a domain D with quotient field K, such that E contains an isolated point, then $f(D) \nsubseteq E$.*

We now give a corollary about the image $f(\mathbb{Z})$ where f is in $\text{Int}(\mathbb{Z})$.

Corollary 2.4. *If $f(x)$ is a polynomial in $\mathbb{Q}[x]$, then*

1. $f(\mathbb{Z}) \nsubseteq \mathbb{P}$

2. $f(\mathbb{Z}) \nsubseteq \{a^n | n \in \mathbb{N}\}$

.

Proof. These follow from the fact that $f(\mathbb{Z})$ has no isolated points, while for the other sets, all elements are isolated. □

Recall that a Prüfer domain is an integral domain D in which for every maximal ideal M of D, D_M is a valuation domain. In [3] it was established that $\text{Int}(\mathbb{Z})$ is a Prüfer domain. More generally, from [5, Theorem VI.1.8], if D is a Dedekind domain with finite residue fields, then $\mathrm{Int}(D)$ is a Prüfer domain. Moreover, if $\mathrm{Int}(D)$ is a Prüfer domain, then $\mathrm{Int}(f(D), D)$ is a Prüfer domain (because an overring of a Prüfer domain is a Prüfer domain, [13]). Conditions relating $\mathrm{Int}(D)$ to Prüfer domains have been studied intensively, and we refer the reader to [21],[5].

Theorem 2.4. *If D is a d-ring and f is an integer-valued polynomial on D such that $\mathrm{Int}(f(D), D)$ is a Prüfer domain, then $\mathrm{Int}(f(D), D)$ has the strong Skolem property.*

Proof. Since D is an integral domain, $f(D)$ has no isolated points by Theorem 2.4, and since D is a d-ring, $f(D)$ is a d-subset by Theorem 2.2, so the result follows immediately from [9, Theorem 4.6]. $\square$

The previous theorem tells us that if D is a d-ring and a Dedekind domain with finite residue fields, then $\mathrm{Int}(f(D), D)$ is strongly Skolem. We now give a consequence of this.

Corollary 2.5. *Let D be a d-ring, and a Dedekind domain with finite residue fields, c an element in D, and $f_1 \dots f_n$ elements of $\mathrm{Int}(D)$ such that for all $a \in D$, $(c) = \langle f_1(a), \dots, f_n(a) \rangle$. Then there exist an integer-valued polynomial $u_1, \dots, u_k$ such that $u_1 f_1 + \cdots + u_n f_n = c$. Furthermore, if for an integer-valued polynomial h, all $f_i \in D_h$, then we can take all $u_i \in D_h$.*

Proof. From the strong Skolem property, there exist integer-valued polynomials $u_1, \dots, u_n$ such that $u_1 f_1 + \cdots + u_n f_n = c$. Now if each f_i is in D_h, say $f_i(x) = m_i(h(x))$, then each m_i is in $\mathrm{Int}(h(D), D)$, so we can apply the strong Skolem property on $\mathrm{Int}(h(D), D)$ to conclude that $c = u'_1 m_1 + \cdots + u'_n m_n$. Substituting h for x in this equation gives the desired result. $\square$

Chapter 3

Even and Odd Integer-Valued Polynomials

Recall that a function $f(x)$ is called even if $f(x) = f(-x)$, and is called odd if $f(x) = f(-x)$. For an integral domain D with quotient field K, we let D_{x^2} be the ring of integer valued polynomials in $K[x^2]$, and D_o the D-module of odd integer-valued polynomials. Note that in analysis, because of the symmetric properties, breaking functions into even and odd parts is a typical technique. For instance, in [24], a paper on the digamma function, the authors found it sufficient to reduce their investigation to periodic even functions. Also, we note the paper by Whitney [28] on even differentiable functions in which it was shown that, if f is an even differentiable function, then f may be written as $f(x) = g(x^2)$, and which goes on further to give various conditions on f and how they affect g.

It was not until the seventies that the ring of integer-valued polynomials on $\mathbb{Z}$ was noticed as an interesting ring of study, see [22, Section C.11]. For example, in [3], it was shown that $\mathrm{Int}(\mathbb{Z})$ is a Prüfer domain.

In [25], Pólya and Szegö's famous analysis problem solving book, one question asks to show that the sequence of polynomials $E_n = \frac{x}{n}\binom{x+n}{2n+1}$ forms a $\mathbb{Z}$-basis for the ring of integer-valued even polynomials, and that the sequence of polynomials $O_n = \binom{x+k-1}{2k-1}$ forms a $\mathbb{Z}$-basis for the module of odd integer-valued polynomials $\mathbb{Z}_o$. The major goal of this chapter is to obtain analogues of these bases for some discrete valuation domains with finite residue field. Also, we will show some factorization properties of $\mathbb{Z}_{x^2}$. Using some of the tools developed for getting an analogue to Pólya and Szegö's basis elements, we will prove some factorization properties for V_{x^2} for certain discrete valuation rings.

Observe that, for any integral domain D, with $E = \{a^2 | a \in D\}$, $\mathrm{Int}(E, D) \cong D_{x^2}$, so some of the previous section hold for D_{x^2}.

Our first lemma gives a concrete description of the integer-valued even functions.

Lemma 3.1. *If D is an integral domain of characteristic not equal to 2, then the ring of integer-valued even polynomials on D is the intersection of the ring of integer-valued polynomials with $K[x^2]$, $D_{x^2} = \mathrm{Int}(D) \cap K[x^2]$.*

Proof. Write $f = \sum_{i=0}^{n} a_i x^i$, so that $f(x) = \sum_{i=0}^{n} a_i(-x)$. If f is even, then $f(x) = f(-x)$ forces $a_i = 0$ for odd i, hence the ring of integer-valued even polynomials is equal to the ring $\mathrm{Int}(D) \cap K[x^2]$. □

We show that $\mathrm{Int}(D)$ is integral over D_{x^2}, although it is not an overring, because they do not have the same field of fractions. We caution the reader that many results on integrality also depend on one ring being an overring of the other.

Theorem 3.1. *For any integral domain D, $\mathrm{Int}(D)$ is integral over D_{x^2}.*

Proof. Let $f \in \mathrm{Int}(D)$ be an integer-valued polynomial, $e_1 = f(x) + f(-x)$ and $e_2 = f(x)f(-x)$. The monic polynomial $G(X) = X^2 - e_1X + e_2$ is an element of $D_{x^2}[X]$. Since $G(f) = 0$, $\mathrm{Int}(D)$ is integral over D_{x^2}. □

3.1 Extendable Very Well Distributed and Well Ordered Sequences

In [5] analogues to the binomial polynomials $\binom{x}{n}$ are defined for discrete valuation domains, by utilizing a special sequence in a discrete valuation domain, which we now define.

Definition 3.1. *A sequence $\{u_n\}_{n\in\mathbb{N}}$ of elements of a discrete valuation ring V with valuation v and residue field of order q is said to be a* very well distributed and well ordered sequence *(in short a V.W.D.W.O. sequence) if, for all non-negative integers n and m, $v(u_n - u_m) = v_q(n - m)$, where $v_q(a)$ is the largest power of q that divides a.*

A V.W.D.W.O. sequence is a generalization of the sequence of natural numbers in the ring of p-adic integers. One fact about a V.W.D.W.O. sequence $\{u_i\}$ which we shall use later is that, for any polynomial $f \in K[x]$, where K is the quotient field of the discrete valuation domain V, if $\deg(f) = n$, then $f \in \mathrm{Int}(V)$ if and only if $f(u_i) \in V$ for all $i \leq n$. See [5, Proposition II.2.8].

We now describe a certain class of V.W.D.W.O. sequences which we will use to define analogues of the functions E_n and O_n for certain discrete valuation domains.

Definition 3.2. *Let V be a discrete valuation domain, and $\{u_n\}_{n\in\mathbb{N}}$ a V.W.D.W.O.*

sequence of elements of V. For any positive integer k, let

$$c_n^k = \begin{cases} -u_{k-n} & \text{if } n < k \\ u_{n-k} & \text{if } n \geq k \end{cases}$$

We call $\{u_n\}$ an extendable V.W.D.W.O. (E.V.W.D.W.O.) if $\{c_n^k\}$ is a V.W.D.W.O. for every positive integer k, in which case we call $\{c_n^k\}_{n\in\mathbb{N}}$ the k-extension of $\{u_n\}$.

We now show that a necessary condition for a V.W.D.W.O. $\{u_n\}$ to be an E.V.W.D.W.O. is that $u_0 = 0$.

Lemma 3.2. *Let V be a discrete valuation domain , if $\{u_n\}$ is an E.V.W.D.W.O. sequence of V, then $u_0 = 0$.*

Proof. Let h and i be nonnegative integers such that $0 \leq i < h$. Then

$$c_i^h + c_{2h-i}^h = -u_{h-i} + u_{h-i} = 0$$

Therefore for all positive integers k, $c_i^h \notin M^k$ (else both c_i^h and c_{2h-i}^h would be in M^k), so that $c_h^h = u_0 \in M^k$. Thus, $u_0 \in \cap_{k=0}^{\infty} M^k = 0$ (because V is a Noetherian domain). □

In [5] it was shown that every discrete valuation domain has a V.W.D.W.O. Not every discrete valuation domain has an E.V.W.D.W.O; next we determine which discrete valuation domains do have an E.V.W.D.W.O.

Theorem 3.2. *Let V be a discrete valuation domain with maximal ideal $M = (t)$ and $|V/M| = q$.*

1. *If q is odd then V has an E.W.V.D.W.O.*

2. *If q is even, then V has an E.W.V.D.W.O. if and only if $q = 2$ and $M = 2V$.*

Proof.

1. Let $q' = \frac{q-1}{2}$ and $\{u_0 = 0, \pm u_1, \ldots, \pm u_{q'}\}$ be a set of representatives of residue classes modulo M. Every positive integer m has a unique representation in the form
$$m = a_k q^k + \cdots + a_1 q + a_0,$$
in which $-q' \leq a_i \leq q'$ for each index i, and $a_k \neq 0$. If we let
$$u_m = u_{a_k} t^k + \cdots + u_{a_1} t + u_{a_0}$$
where $u_{-i} = -u_i$, we claim that $\{u_n\}_{n\geq 0}$ is an E.V.W.D.W.O. Consider $v(u_n - u_m)$, where
$$\begin{aligned} m &= a_k q^k + \cdots + a_1 q + a_0 \\ n &= b_{k'} q^{k'} + \cdots + b_1 q + b_0. \end{aligned}$$
Then $v(u_n - u_m)$ is the smallest i such that $a_i - b_i$ is nonzero, which is also equal to $v_q(n - m)$. This shows that for any integer k, $\{c_n^k\}_{n\in\mathbb{N}}$, the k-extension of $\{u_n\}$ is a V.W.D.W.O. hence $\{u_n\}$ is an E.V.W.D.W.O.

2. If $\{u_n\}$ is an E.V.W.D.W.O., then $-u_1, u_0, u_1, u_2, \ldots$ is a V.W.D.W.O. Note that $u_1 - (-u_1) = 2u_1 \in M$. Now if $q > 2$ then $-u_1, u_0, \ldots, u_{q-2}$ would form a

complete set of residues (modulo M) but $-u_1$ and u_1 are in the same congruence class, hence $q = 2$. Also, $-u_1, u_0, u_1$, and u_2 forms a complete set of residues modulo M^2, hence $-u_1$ and u_1 must be in different congruence classes modulo M^2, so $2u_1 = u_1 - (u_1) \notin M^2$ which implies $2 \notin M^2$, hence $M = 2V$.

Conversely, if $q = 2$ and $M = 2V$, then $\mathbb{N}$ is an E.V.W.D.W.O. for V. Note that since $M^k = 2^k V$, it is the case that $v(m-n) = v_2(m-n)$. (To see this, we examine the base 2 expansion as was done for the case where q is odd).

□

Note that if V has an E.V.W.D.W.O., then the characteristic of V is not 2, hence by Lemma 3.1, $V_{x^2} = V_e$.

3.2 A V-basis for V_{x^2} and V_o

For a discrete valuation domain V, with finite residue field and quotient field K, [5, Corollary II.2.8] tells us that any polynomial f in $K[x]$ of degree n is integer valued if it is integer valued on the first $n+1$ elements of a V.W.D.W.O. Observe that, if $\{u_i\}$ is an E.W.V.W.D.O., then for $f \in K_{x^2}$ of degree $2n$, if f is integer valued on the first $n+1$ elements of an E.W.V.D.W.O., then f is integer valued on the first $2n+1$ elements of the n-extension of the E.V.W.D.W.O., hence $f \in V_{x^2}$. We now present an analogue to Pólya and Szegö's basis for the ring of integer-valued even polynomials.

Theorem 3.3. *Let $\{u_n\}_{n\in\mathbb{N}}$ be a E.V.W.D.W.O. sequence of V, where V is a discrete valuation domain with finite residue field. The sequence of polynomials $\{E_n\}_{n\in\mathbb{N}}$, where $E_0 = 1$ and $E_n = \prod_{k=0}^{n-1}\left(\frac{x^2-u_k^2}{u_n^2-u_k^2}\right)$ for $n > 0$, is a V-basis of V_{x^2}.*

Proof. Let s be a fixed but arbitrary integer, and set

$$c_n^s = \begin{cases} -u_{s-n} & \text{if } n < s \\ u_{n-s} & \text{if } n \geq s \end{cases}$$

Since $\{u_n\}$ is a E.V.W.D.W.O., by definition $\{c_n^s\}$ is a V.W.D.W.O. Squaring c_n^s gives

$$(c_n^s)^2 = \begin{cases} (u_{s-n})^2 & \text{if } n < s \\ (u_{n-s})^2 & \text{if } n \geq s \end{cases}$$

Observe that

$$E_s(c_n^s) = \begin{cases} 0 & \text{if } n < 2s \\ 1 & \text{if } n = 2s \end{cases}$$

Hence $E_s(c_0^s), E_s(c_1^s), \ldots, E_s(c_{2s}^s) \in V$, and clearly E_s is a polynomial in $K[x]$ of degree $2s$, so by [5, Corollary II.2.8], $E_s \in \mathrm{Int}(V)$. Also note that E_s is in $K[x^2]$, and therefore $E_s \in V_{x^2}$.

For the rest of the proof, we imitate the proof of [5, Theorem II.2.7]. It is clear that the sequence of polynomials E_n form a K-basis for $K[x^2]$, since the degree of E_n is $2n$ for each n. So if $f \in V_{x^2} \subset K[x^2]$ is of degree $2n$, we can write

$$f = \lambda_0 E_0 + \cdots + \lambda_n E_n$$

for some $\lambda_0, \lambda_1, \ldots, \lambda_n$ in K. Note that $\lambda_0 = f(u_0) \in V$. Suppose, by induction on $k \leq n$, that $\lambda_i \in V$ for $i < k$. Then

$$\begin{aligned} g_k &= \lambda_k E_k + \cdots + \lambda_n E_n \\ &= f - (\lambda_0 E_0 + \ldots + \lambda_{k-1} E_{k-1}) \in V_{x^2} \end{aligned}$$

Since g_k is an integer-valued polynomial, $\lambda_k = g_k(u_k) \in V$. $\square$

Let V be a discrete valuation domain, v the valuation on the quotient field K of V, h be an integer, q be the cardinality of the residue field and f be a polynomial in $\mathrm{Int}(V)$ such that $\deg(f) < q^h$. From [5, Proposition III.3.1], if $f(0) = 0$, then $v(a) \geq r + h$ implies that $v(f(a)) \geq r + 1$. This was actually proved by considering $g(x) = f(x + b) - f(b)$ and establishing the result that $v(b - a) \geq r + h$ implies $v(g(a - b)) \geq r + 1$.

We now apply the basis elements of V_{x^2} to relate $v(a)$ to $v(f(a))$, for $a \in V$, but note that in V_{x^2} we do not have the luxury of strengthening results from $v(a)$ to $v(b - a)$ as was done for $\mathrm{Int}(V)$, since for $f \in V_{x^2}$, $g(x) = f(x + b) - f(b)$ is not necessarily in V_{x^2}.

Theorem 3.4. *Let V be a discrete valuation domain with finite residue field of cardinality q, h an integer, and f a polynomial in V_{x^2} such that $f(0) = 0$ and* $\deg(f) < 2q^h$. *Suppose that V_{x^2} has an E.V.W.D.W.O. sequence. If r is an integer such that $v(a) \geq r + h$ then $v(f(a)) \geq r + 1$.*

Proof. Let $\{u_i\}$ be a E.V.W.D.W.O. sequence. Recall that the sequence $E_n = \prod_{k=0}^{n-1} \left(\frac{x^2 - u_k^2}{u_n^2 - u_k^2} \right)$ form a V-basis for V_{x^2}. For $n \geq 1$ we have

$$E_n(x) = \frac{x^2}{u_n^2} \prod_{k=1}^{n-1} \frac{(x - u_k)(x + u_k)}{(u_n - u_k)(u_n + u_k)}$$

so that

$$E_n(a) = \frac{a^2}{u_n^2} \prod_{k=1}^{n-1} \frac{(a - u_k)(a + u_k)}{(u_n - u_k)(u_n + u_k)}$$

Note that $O_n(x) = \frac{x}{u_n}\prod_{k=1}^{n-1}\frac{(x-u_k)(x+u_k)}{(u_n-u_k)(u_n+u_k)}$ is integer-valued because it is a polynomial in $K[x]$ of degree $2n-1$ and integer valued on $\{-u_{n-1},\ldots,u_0,\ldots,u_{n-1},u_n\}$, which are $2n$ consecutive elements on a V.W.D.W.O. sequence. For $0 < n < q^h$, we have $v(u_n) = v_q(n) < h$; therefore

$$\begin{aligned} v(E_n(a)) &= v(a) + v(O_n(a)) - v(u_n) \\ &\geq v(a) - v(u_n) \\ &\geq r + h - h + 1 \\ &\geq r + 1 \end{aligned}$$

Since $\deg(f) < 2q^h$ and $f(0) = 0$, we can express f as a linear combination of the polynomials $E_1, \ldots, E_{q^h-1}$, so that $f(a) = \sum_{i=1}^{q^h-1} a_i E_i(a)$ for some $a_1, \ldots, a_{q^h-1} \in V$, and hence $v(f(a)) \geq r+1$ $\square$

Clearly, the natural numbers $\mathbb{N}$ form an E.V.W.D.W.O sequence locally at every prime of $\mathbb{Z}$. We now pause briefly to look at an example related to the previous theorem, which yields a sharper result than that given in [5, Proposition III.3.1].

Example 3.1. *If $n < \frac{q^h}{2}$ (hence $\deg(E_n) < q^h$), then from Proposition III.3.1 of [5] we know that $v(a) \geq r+h$ implies $v(E_n(a)) \geq r+1$. The previous theorem sharpens this result to $n < q^h$. For example, since $5 < \frac{3^3}{2}$, from [5], if $3^{r+3}|a$ then $3^{r+1}|E_5(a)$. On the other hand, from the previous theorem, since $5 < 3^2$, we are able to improve the result to $3^{r+2}|a$ implies $3^{r+1}|E_5(a)$.*

We now note an analogue for discrete valuation domains of Pólya and Szegö's basis elements for the $\mathbb{Z}$-module of odd integer-valued functions on $\mathbb{Z}$.

Theorem 3.5. *Let $\{u_n\}_{n\in\mathbb{N}}$ be a E.V.W.D.W.O. sequence of V, where V is a discrete valuation domain with finite residue field. The sequence of polynomials $\{O_n\}_{n\in\mathbb{N}}$, $O_n(x) = \frac{x}{u_n}\prod_{k=1}^{n-1}\frac{(x-u_k)(x+u_k)}{(u_n-u_k)(u_n+u_k)}$ for $n > 0$, is a V-basis of V_o, the V-module of odd integer-valued polynomials on V.*

Proof. The fact that O_n is an integer-valued polynomial is stated (with reason) in the proof of Theorem 3.4. Note that these polynomials have the property that $O_n(u_n) = 1$ and $O_n(u_k) = 0$ for $k < n$, hence the proof is similar to that for the case of the integer-valued even polynomials. □

3.3 The irreducibility of the basis elements of V_{x^2}

We now show that Pólya's basis elements E_k are irreducible in $\mathbb{Z}_{x^2}$, for all integers k.

Theorem 3.6. *Let $f = \sum_{k=0}^{n} a_k E_k \in \mathbb{Z}_{x^2}$ for some $a_0, \ldots, a_n \in \mathbb{Z}$. Suppose that $gcd\{a_0, \ldots, a_n\} = 1$ and a_n is not divisible by $\binom{2n}{2r}$ for all $r < n$. Then f is irreducible in $\mathbb{Z}_{x^2}$.*

Proof. If $f = ag$ for $a \in \mathbb{Z}$, then a divides $a_0, \ldots, a_n$ in $\mathbb{Z}$, hence $a = \pm 1$. Now suppose that $f = gh$ for nonconstant polynomials $g, h \in \mathbb{Z}_{x^2}$, and let n, r, s be the degrees of f, g and h respectively. Suppose $g = \sum_{i=0}^{r} b_i E_i$ and $h = \sum_{i=0}^{s} c_i E_i$; observe that $2n = 2r + 2s$. Then comparing the leading coefficients of f, g, and h yields

$$\frac{2a_n}{(2n)!} = \frac{2b_n}{(2r)!}\frac{2c_n}{(2s)!}$$

so that

$$\begin{aligned} a_n &= b_n c_n \frac{(2n)!}{(2r)!(2s)!} \\ &= b_n c_n \binom{2n}{2r} \end{aligned}$$

contradicting the assumption that $\binom{2n}{2r}$ does not divide a_n. $\square$

We immediately get the following consequence.

Corollary 3.1. *For each $n \geq 1$, the polynomial E_n is irreducible in $\mathbb{Z}_{x^2}$.*

The following definition is taken from [10], which describes a certain factorization property.

Definition 3.3. *Let R be an integral domain and n a positive integer. We define $\Phi(R, n)$ to be the supremum of the number of possible lengths of decompositions into products of irreducible elements which otherwise factor as a product of length n.*

We show that $\Phi(\mathbb{Z}_{x^2}, 2) = \infty$.

Corollary 3.2. $2k(2k-1)E_k(x) = E_{k-1}(x)(x^2 - (k-1)^2)$*, and hence* $\Phi(\mathbb{Z}_{x^2}, 2) = \infty$.

Proof.

$$\begin{aligned} E_k(x) &= \frac{x}{k}\binom{x+k-1}{2k-1} \\ &= \frac{x}{k}\frac{(x+k-1)(x+k-2)\cdots(x-k+1)}{(2k-1)!} \\ &= \frac{2\prod_{i=0}^{k-1}(x^2-i^2)}{(2k)!} \\ &= \frac{2\prod_{i=0}^{k-2}(x^2-i^2)}{(2(k-1))!}\frac{x^2-(k-1)^2}{(2k-1)2k} \\ &= \frac{E_{k-1}(x)(x^2-(k-1)^2)}{2k(2k-1)} \end{aligned}$$

Therefore,

$$2k(2k-1)E_k(x) = E_{k-1}(x)(x^2-(k-1)^2).$$

Note that $x^2-(k-1)^2$ is irreducible in $\mathbb{Z}_{x^2}$. □

For further results on factorization of integer-valued polynomials we refer the reader to [1].

Now we show that for a discrete valuation domain with finite residue field of odd order, the basis elements E_n are irreducible. We use an analogue of the factorial function.

Definition 3.4. *Given an E.V.W.D.W.O. $\{u_n\}$ for the discrete valuation domain V, let $u_n! = (u_n^2 - u_{n-1}^2)\cdots(u_n^2-u_1^2)(u_n^2)$ for $n \geq 1$, and $u_0! = 1$.*

The definition is an instance of the Bhargava factorial; see [2]. Note that, with this notation, the leading coefficient of E_k is $\frac{1}{u_k!}$.

Lemma 3.3. *Suppose that V is a discrete valuation ring with an E.W.V.D.W.O. sequence $\{u_i\}$. Let q be the cardinality of the residue field. Then for n any power of q, and all positive integers r, s, such that $n = r + s$, $\frac{u_n!}{u_r! u_s!}$ is a non-unit element of V.*

Proof. First assume q is odd. Let $\{c_k\}$ be the n-extension of $\{u_i\}$. We will make use of the fact that, since q is odd, for any integer a, $v_q(2a) = v_q(a)$. Also without loss of generality we may assume $2r < q$. Then

$$\begin{aligned}
v(u_n!) &= \sum_{i=0}^{n-1} v(u_n - u_i) + \sum_{i=0}^{n-1} v(u_n + u_i) \\
&= \sum_{i=0}^{n-1} v(c_{2n} - c_{n+i}) + \sum_{i=0}^{n-1} v(c_{2n} - c_{n-i}) \\
&= \sum_{i=0}^{n-1} v_q(n-i) + \sum_{i=0}^{n-1} v_q(n+i) \\
&= \sum_{i=1}^{n} v_q(i) + \sum_{i=n}^{2n-1} v_q(i) \\
&= \left(\sum_{i=1}^{2n-1} v_q(i) \right) + v_q(n) \\
&= \sum_{i=1}^{2n} v_q(i)
\end{aligned}$$

Hence

$$\begin{aligned}
v(\frac{u_n!}{u_r!u_s!}) &= v(u_n!) - v(u_r!) - v(u_s!) \\
&= \sum_{i=1}^{2n} v_q(i) - \sum_{i=1}^{2r} v_q(i) - \sum_{i=1}^{2s} v_q(i) \\
&= \sum_{i=1}^{2n} v_q(i) - \sum_{i=1}^{2r} v_q(2q^k - i) - \sum_{i=1}^{2s} v_q(i) \\
&= \sum_{i=1}^{2n} v_q(i) - \sum_{i=2s}^{q^k-1} v_q(i) - \sum_{i=1}^{2s} v_q(i) \\
&= v_q(q^k) - v_q(2s) > 0
\end{aligned}$$

Recall that if q is even, then $q = 2$ because V has an E.W.V.D.W.O. sequence. The result for $q = 2$ is proved in a similar way. We provide the details for the reader's convenience. Here we will use the fact that $v_2(2n) = v_2(n) + 1$

$$\begin{aligned}
v(u_n!) &= \sum_{i=0}^{n-1} v(u_n - u_i) + \sum_{i=0}^{n-1} v(u_n + u_i) \\
&= \sum_{i=0}^{n-1} v(c_{2n} - c_{n+i}) + \sum_{i=0}^{n-1} v(c_{2n} - c_{n-i}) \\
&= \sum_{i=0}^{n-1} v_2(n-i) + \sum_{i=0}^{n-1} v_2(n+i) \\
&= \sum_{i=1}^{n} v_2(i) + \sum_{i=n}^{2n-1} v_2(i) \\
&= \left(\sum_{i=1}^{2n-1} v_2(i)\right) + v_2(n) \\
&= \sum_{i=1}^{2n} v_2(i) - 1
\end{aligned}$$

Hence

$$
\begin{aligned}
v\left(\frac{u_n!}{u_r!u_s!}\right) &= v(u_n!) - v(u_r!) - v(u_s!) \\
&= \sum_{i=1}^{2n} v_2(i) - \sum_{i=1}^{2r} v_2(i) - \sum_{i=1}^{2s} v_2(i) + 1 \\
&= \sum_{i=1}^{2n} v_2(i) - \sum_{i=1}^{2r} v_2(2^{k+1} - i) - \sum_{i=1}^{2s} v_2(i) + 1 \\
&= \sum_{i=1}^{2n} v_2(i) - \sum_{i=2s}^{2^{k+1}-1} v_2(i) - \sum_{i=1}^{2s} v_2(i) + 1 \\
&= v_2(2^{k+1}) - v_2(2s) + 1 = k - v_2(s) + 1 > 0
\end{aligned}
$$

□

Theorem 3.7. *Let V be a discrete valaution domain with an E.W.V.D.W.O. sequence $\{u_i\}$ and $f = \sum_{k=0}^{n} a_k E_k$ in V_{x^2}, where E_k are the basis polynomials associated with the E.W.V.D.W.O. $\{u_i\}$, $|V/M| = q$. If $n = q^k$ for some positive integer k, if for all r, s such that $n = r + s$, it is the case that $a_n \notin (\frac{u_n!}{u_r!u_s!})$, and if there exists a_k, for which a_k is a unit, then f is irreducible.*

Proof. If we can factor $f = ag$ for some constant $a \in V$, then since a_k is a unit for some k, it follows that a also has to be a unit. Now suppose that we can factor $f = gh$ for some nonconstant polynomials, $g = \sum_{i=0}^{r} b_i E_i$ and $h = \sum_{i=0}^{s} c_i E_i$; hence $2n = 2r + 2s$. Comparing leading coefficients of f, g, and h yields

$$
\frac{a_n}{u_n!} = \frac{b_r}{u_r!}\frac{c_s}{u_s!}
$$

so that

$$a_n = b_r c_s \frac{u_n!}{u_r! u_s!}$$

contradicting the assumption that $a_n \notin (\frac{u_n!}{u_r! u_s!})$. $\square$

The case $a_n = 1$ yields the following consequence.

Corollary 3.3. *If V is a discrete valaution domain with an E.W.V.D.W.O. sequence $\{u_i\}$,q the cardinality of the residue field of V and k a postive integer then the basis element E_{q^k} associated with $\{u_i\}$ is irreducible in V_{x^2}.*

Chapter 4

Application: Stone-Weierstrass Theorem

Weierstrass in 1885 [27], showed that, for any finite interval $I = [a, b]$ in the real numbers, the set of all polynomials is dense in the ring of continuous functions on I. This result has spawned countless variations and generalizations (for example, the famous one by Stone, [26]), and it could be argued that this result is the start of approximation theory. One such variation is that every continuous periodic function can be approximated by a trigonometric polynomial, which is now used in many applications, such as time series and signal processing. One technique of finding the trigonometric series of a function entails splitting it as a sum of even and odd parts; then even functions are written as cosine series and odd functions are written as sine series. An analogue of the Stone-Weierstrass theorem for the p-adic integers was given by Dieudonné in [11], and this was generalized by Kaplansky in [17] to rank-one valuation rings. Mahler in [19] gave a more concrete variation of Dieudonné's result, showing that every p-adic continuous function can be expressed as a series of the the form $\sum_{i=0}^{\infty} a_i \binom{x}{i}$. This has been generalized to discrete valuation domains by using the fact that every DVR has a V.W.D.W.O. sequence (see [5]).

In this section we use the basis elements for the even and odd integer-valued polynomials from the last section to give analogues of the Stone Weierstrass theorem for odd and integer-valued even polynomials. This representation is similar to that of a continuous periodic function as the sum of sine and cosine series. The proofs are inspired by the case for the ring of integer-valued polynomials on a discrete valuation ring, which can be found in [5, Chapter III]. In [5] it was shown that, if the characteristic functions of cosets of ideals can be approximated, then all continuous functions can be approximated. Since the characteristic function is neither even nor odd, we use the odd and even parts of the characteristic function, coupled with the existence of an E.V.W.D.W.O. sequence and the basis elements of the previous chapter, to get our results. Note also that [5] has results for all discrete valuation domains, while we use discrete valuation domains with an E.V.W.D.W.O. sequence , in order to use the results of the previous chapter.

Using the V-basis for V_{x^2}, we now provide an analogue to the Stone-Weierstrass theorem for even continuous functions. That is, we show that every even continuous integer-valued function can be approximated by an integer-valued even polynomial. Note that, if ϕ is a continuous function on V, then we may extend ϕ to a continuous function $\hat{\phi} : \hat{V} \to \hat{V}$ by letting $\hat{\phi}(\hat{t}) = \hat{\phi}(\lim_{n\to\infty} t_n) = \lim_{n\to\infty} \phi(t_n)$, where $\{t_n\}$ is a sequence in V such that $\lim_{n\to\infty} t_n = t \in \hat{V}$. For completness, we first define "approximated".

Definition 4.1. *Let V be a discrete valuation ring with maximal ideal M and $\hat{V}$ its completion. Let ϕ be a continuous function on V. We say that a polynomial f approximates ϕ modulo M^n, if for all $a \in V$, we have $f(a) - \phi(a) \in M^n$*

We will also use the characteristic functions on cosets.

Definition 4.2. *Let M be the maximal ideal of a discrete valuation domain V. For any element $a \in V$ and any integer h, let*

$$\chi_{a+M^h}(t) = \begin{cases} 1 & \text{if } t - a \in M^h \\ 0 & \text{if } t - a \notin M^h \end{cases}$$

Definition 4.3. *Let M be the maximal ideal of a discrete valuation domain V. For any element $a \in V$ and any integer h, let*

$$\epsilon_a = \begin{cases} \chi_{a+M^h} & \text{if } a + M^h = -a + M^h \\ \chi_{a+M^h} + \chi_{-a+M^h} & \text{otherwise} \end{cases}$$

Definition 4.4. *Let M be the maximal ideal of a discrete valuation domain V. For any element $a \in V$ and any integer h, let*

$$\gamma_a = \chi_{a+M^h} - \chi_{-a+M^h}$$

4.1 Approximation theorem for even continuous integer-valued functions

We first show that, in order to be able to approximate all even continuous functions on the completion, it is suffices to be able to approximate the even part of the characteristic functions. We denote the ring of even functions continuous on the domain D by $\mathcal{C}^e(D, D)$.

Theorem 4.1. *Let V be a discrete valuation ring with maximal ideal M and $|V/M| = q < \infty$. For all positive integers n, the following assertions are equivalent.*

1. *Every even function continuous on $\hat{V}$ in the $\hat{M}$-adic toplogy can be approximated by an integer-valued even polynomial $f \in V_{x^2}$ modulo $\hat{M}^n$.*

2. *For all positive integers h and $a \in V$, the functions ϵ_a^h can be approximated, modulo M^n, by a polynomial $f \in V_{x^2}$.*

Proof. (1⇒2) For any h, the extension $\hat{\epsilon}_a^h$ of ϵ_a^h, is the sum of characteristic functions on $a + \hat{M}^h$ and $-a + \hat{M}^h$ in $\hat{V}$ and hence is an even continuous function. Let f be an integer-valued even polynomial on V; we show that f approximates $\hat{\epsilon}_a^h$ on $\hat{V}$ modulo $\hat{M}^n$ if and only if f approximates ϵ_a^h on V modulo M^n.

If f approximates $\hat{\epsilon}_a^h$ modulo $\hat{M}^n$ on $\hat{V}$, then in $\hat{V}$, $f(r) - \hat{\epsilon}_a^h(r) \in \hat{M}^n$ for all $r \in \hat{V}$ implies $f(r) - \epsilon_a^h(r) \in M^n$ for all $r \in V$. If f approximates ϵ modulo M^n on V, then $f(r) - \epsilon(r) \in M^n$ for all $r \in V$. Since $f - \epsilon_a^h$ is continuous and V is a compact metric space, $f - \epsilon_a^h$ is actually uniformly continuous and hence extends to the completion; that is, $(f - \epsilon_a^h)(x) \in \hat{M}^n$ for all $x \in \hat{V}$.

(1⇐2) Conversely, let ϕ be an even function continuous on $\hat{V}$. Again since $\hat{V}$ is compact, and ϕ is uniformly continuous, for all positive integers n there exists an integer h such that $a - b \in \hat{M}^h$ implies $\phi(a) - \phi(b) \in \hat{M}^n$. In other words, there exists an integer h such that ϕ is constant modulo $\hat{M}^n$ on $a + \hat{M}^h$, since $b \in a + \hat{M}^h$ if and only if $a - b \in \hat{M}^h$.

Note that since ϕ is even and constant on $a + \hat{M}^h \mod \hat{M}^h$. it follows that, $\phi(x) \equiv \sum \epsilon_a(x)\phi(a)(\mod \hat{M}^n)$, where a ranges over coset representatives for $\hat{M}^h$ such that if $a + \hat{M}^h \neq -a + \hat{M}^h$, then we include only one representative for both cosets. Now by hypothesis, for each a there exists a polynomial $f_a \in V_{x^2}$ such that

$f_a \equiv \epsilon_a^h \mod M^n$; hence, $\sum \phi(a) f_a(x) = \phi(x) \mod \hat{M}^n$. Since V is dense in $\hat{V}$, (2) implies (1). $\square$

We will now show that every even continuous function can be approximated modulo $\hat{M}^n$ by an integer-valued even polynomial $f \in V_{x^2}$. From the previous theorem it is sufficient to show that for each integer h, the characteristic function ϵ_a^h can be approximated modulo M^n.

Theorem 4.2. *Let V be a discrete valaution domain with an E.V.W.D.W.O. sequence, maximal ideal M and ϕ be an even continuous function on $\hat{V}$, the completion of V in the $\hat{M}$-adic topology. Then for all positive integers n, ϕ can be approximated modulo $\hat{M}^n$ by an integer-valued even polynomial $f \in V_{x^2}$; that is, for all $\phi \in \mathcal{C}^e(\hat{V}, \hat{V})$, and all positive integers n, there exists $f \in V_{x^2}$ such that $\phi(a) \equiv f(a) \mod \hat{M}^n$ for all $a \in \hat{V}$.*

Proof. We first show the approximation for continuous functions modulo $\hat{M}$. Let $|V/M| = q$. From [5], for each integer-valued even polynomial f such that $\deg(f) < q^h$, we have that $a \equiv b \mod M^h$ implies that $f(a) \equiv f(b) \mod M$; in other words, for any $a \in V$, if $\deg(f) < q^h$ then f is constant modulo M on $a + M^h$. Let $\{u_i\}$ be an E.W.V.D.W.O. and $\{E_n\}$ be the V-basis for V_{x^2} associated with this E.W.V.D.W.O. Then for $0 < n < \frac{q^h}{2}$, let $q' = \frac{q^h - 1}{2}$ if q is odd and $q' = \frac{q^h}{2}$ if $q = 2$. We have

$$E_n \equiv \sum_{i=-q'}^{q'} E_n(u_i) \chi_{u_i + M^h}$$

Since for $n > 1$, $E_n(u_0) = 0$

$$\begin{aligned}
&\equiv \sum_{i=1}^{q'} E_n(u_i)\chi_{u_i+M^h} + \sum_{i=-1}^{-q'} E_n(u_i)\chi_{u_i+M^h} \\
&\equiv \sum_{i=1}^{q'} E_n(u_i)\left(\chi_{u_i+M^h} + \chi_{-u_i+M^h}\right) \\
&\equiv \sum_{i=1}^{q'} E_n(u_i)\epsilon_{u_i}^h
\end{aligned}$$

For the case that $q = 2$ (which implies that $M = 2V$), $-a + M^h = a + M^h \Rightarrow 2a \in M^h = 2^h V \Rightarrow a \in 2^{h-1}V = M^{h-1}$, so there are only two such cosets $0 + M^h$ and $2^{h-1} + M^h$, which makes the sum range over $q' + 1$ coset representatives. Note also that this equation also holds for $n = 0$, and thus, for $n = 0, ..., q'$ we have $q' + 1$ relations $E_n = \sum_{i=1}^{q'} E_n(u_i)\epsilon_{u_i}^h + \delta_n$, where $\delta_n \in MV_{x^2}$. These relations may be represented in matrix form, $\mathbb{E} = \mathbb{M}\Upsilon + \Delta$, where $\mathbb{E}, \Upsilon$ and Δ are $(q' + 1) \times 1$ column matrices whose coefficients are, respectively, the functions E_n, ϵ_{u_i} and δ_n, and $\mathbb{M}$ is the $(q' + 1) \times (q' + 1)$ matrix (a_{ij}) such that $a_{ij} = E_i(u_j)$. Note that $\mathbb{M}$ is upper triangular with coefficients on the diagonal equal to 1; hence $\mathbb{M}$ is invertible over V. So $\Upsilon = \mathbb{M}^{-1}\mathbb{E} - \mathbb{M}^{-1}\Delta$. Therefore, the functions ϵ_i^h are approximated by integer-valued even polynomials modulo M. The result for $\hat{M}$ now follows from the previous theorem.

Now we consider the approximation for $\hat{M}^n$. Let $\phi \in \mathcal{C}^e(\hat{V}, \hat{V})$, the ring of even continuous integer-valued functions on $\hat{V}$. Then by the case already proven, $\phi = g_0 + \delta_0$, where $g_0 \in V_{x^2}$ and δ_0 takes its values in $\hat{M}$. Let t be a generator for the ideal M, hence, $\phi = g_0 + t\phi_1$ where $\phi_1 \in \mathcal{C}^e(\hat{V}, \hat{V})$. Applying the same result to $\phi_1, \phi = g_0 + tg_1 + t^2\phi_2$. By induction, it follows that $\phi = g_0 + tg_1 + \cdots + t^n g^n + t^{n+1}\phi_{n+1}$.

Therefore, ϕ is approximated modulo $\hat{M}^n$ by an even polynomial. $\square$

For a discrete valuation domain with an E.V.W.D.W.O., every even continuous function may be expressed as a series using the basis for integer-valued even polynomials.

Theorem 4.3. *Let V be a valuation domain with an E.V.W.D.W.O. sequence. Every continuous function $\phi \in \mathcal{C}^e(\hat{V}, \hat{V})$ can be expressed as a sum of series*

$$\phi = \sum_{i=0}^{\infty} a_i E_i, \text{ where } a_i \in \hat{V} \text{ and } v(a_i) \to +\infty.$$

Moreover, the coefficients a_i are uniquely determined by the recursive formula

$$\phi(u_i) = a_n + \sum_{i=0}^{n-1} a_i E_i(u_n),$$

where $\{u_n\}$ is the E.V.W.D.W.O. sequence corresponding to the basis $\{E_i\}$.

Proof. Let (t) be the maximal ideal of V. Now for each n, there exists an integer-valued even polynomial f'_n such that $f'_n(x) \equiv \phi(x)$ modulo M^n. We may write $\phi = \sum_{i=0}^{n} t^i f_i + t^{n+1}\phi_n$ for integer-valued even polynomials $f_0, \ldots, f_n$ and continuous function ϕ_n; hence, we have $\phi = \sum_{n=0}^{\infty} t^n f_n(x)$, where f_n are integer-valued even polynomials.

Now for each n, $f_n = \sum_{i=0}^{k_n} a_{i,n} E_i$ where $a_{i,n}$ in V. For $i > k_n$ set $a_{i,n} = 0$. Let $a_i = \sum_{l=0}^{\infty} a_{i,n}$, and $k^{(n)} = \sup\{k_0, \ldots, k_n\}$. If $i > k^{(r)}$ then $a_i = \sum_{n=r}^{\infty} a_{i,n}$ and hence $v(a_i) > r$ and so $v(a_i) \to +\infty$. Now $\sum_{i=0}^{\infty} a_i E_i$ is convergent since $a_i f_i \to 0$, so $\phi = \sum_{i=0}^{\infty} a_i E_i$ is convergent. Also $\sum_{n=0} t^n f_n - \sum_{i=0}^{k_r} a_i E_i$ is divisible by t^{k+1}, and so $\phi = \sum_{i=0}^{\infty} a_i E_i$. $\square$

4.2 Approximation theorem for odd continuous integer-valued functions

In this section we prove analogues of the results in the previous section for odd continuous functions. The purpose of this is to obtain an expansion for discrete valuation rings with odd residue field. We will show that every odd continuous function can be approximated by an odd integer-valued polynomial. We denote the set of odd continuous functions on D by $C^o(D, D)$. The next theorem tells us that if we can approximate the odd part of all characteristic functions by odd integer-valued polynomials, then we can approximate all odd continuous functions by odd integer-valued polynomials.

Theorem 4.4. *Let V be a discrete valuation domain and M the maximal ideal of $\hat{V}$. For each integer n, the following assertions are equivalent.*

1. *Each continuous function $\phi \in \mathcal{C}^o(\hat{V}, \hat{V})$ can be approximated by an odd integer-valued polynomial $f \in V_o$ modulo $\hat{M}^n$.*
2. *For each integer h, and each $a \in V$,the function $\gamma_a = \chi_{a+M^h} - \chi_{-a+M^h}$ in V can be approximated by an odd integer-valued polynomial $f \in V_o$ modulo M^n.*

Proof. (1⇒2) For any h, and $a \in V$, the extension $\hat{\gamma}_a^h$ of γ_a^h is $\hat{\chi}_{a+M^h} - \hat{\chi}_{-a+M^h}$ hence is an odd continuous function. Let f be an odd integer-valued polynomial, f approximates $\hat{\gamma}_a^h$ in $\hat{V}$ modulo $\hat{M}^n$ if and only if f approximates γ_a^h in V modulo M^n.

(1 ⇐ 2) Conversely, let $\phi \in \mathcal{C}^o(\hat{V}, \hat{V})$. Since $\hat{V}$ is compact, ϕ is uniformly continuous, so there exists an integer h such that $a - b \in \hat{M}$ implies that $\phi(a) - \phi(b) \in$

M^n. Now ϕ is odd and constant on each $a + \hat{M}^h$ modulo $\hat{M}^n$. Thus the result follows as in the proof of Theorem 4.1. □

Theorem 4.5. *Let V be a discrete valuation domain with an E.W.V.D.W.O. sequence For all integers n, each odd continuous function $\phi \in \mathcal{C}^o(\hat{V}, \hat{V})$ can be approximated modulo $\hat{M}^n$ by an odd integer-valued polynomial $f \in V_o$.*

Proof. Let h be an integer. From [5, Proposition III.3.1], if $2n - 1 < q^h$ (that is $n < \frac{q^h+1}{2}$) then $O_n(x) = \frac{x}{u_n} \prod_{k=1}^{n-1} \frac{(x-u_k)(x+u_k)}{(u_n-u_k)(u_n+u_k)}$ is constant on $u_i + M^h$, where $\{u_i\}$ the E.W.V.D.W.O. associated with O_n. Now

$$\begin{aligned}
O_n(x) &\equiv \sum_{i=-\frac{q^h-1}{2}}^{\frac{q^h-1}{2}} O_n(u_i)\chi_{u_i+M^h} \\
&\equiv \sum_{i=1}^{\frac{q^h-1}{2}} O_n(u_i)\chi_{u_i+M^h} + \sum_{i=-1}^{-\frac{q^h-1}{2}} O_n(u_i)\chi_{u_i+M^h} \\
&\equiv \sum_{i=1}^{\frac{q^h-1}{2}} O_n(u_i)\left(\chi_{u_i+M^h} - \chi_{-u_i+M^h}\right) \\
&\equiv \sum_{i=1}^{\frac{q^h-1}{2}} O_n(u_i)(\gamma_{u_i}^h)
\end{aligned}$$

So we have $\frac{q^h-1}{2}$ relations $O_n = \sum_{1 \le i < \frac{q^h-1}{2}} O_n(u_i)\gamma_(u_i) + \delta_n$ where $\delta_n \in MV_o$. These relations may be represented in matrix form, $O = \mathbb{M}\Gamma + \Delta$, where $\mathbb{O}, \Phi$ and Δ are column matrices whose coefficients are, respectively, the functions O_n, γ_{u_i} and δ_n, and $\mathbb{M}$ is the matrix (a_{ij}) such that $a_{ij} = O_i(u_j)$ note that $\mathbb{M}$ is upper triangular with coefficients on the diagonal equal to 1; hence, $\mathbb{M}$ is invertible. So $\Gamma = \mathbb{M}^{-1}\mathbb{O} - \mathbb{M}^{-1}\Delta$.

Hence the functions γ_i are approximated by odd integer-valued polynomials modulo $\hat{M}$. The result for $n = 1$ follows from the previous theorem. Now we consider the approximation for $\hat{M}^n$. If $\phi \in \mathcal{C}^o(\hat{V}, \hat{V})$, then by the previous theorem $\phi = g_0 + \delta_0$, where $g_0 \in V_o$ and δ_0 takes its values in $\hat{M}$. Hence $\phi = g_0 + t\phi_1$ where $\phi_1 \in \mathcal{C}^o(\hat{V}, \hat{V})$. Applying the same result to $\phi_1, \phi = g_0 + tg_1 + t^2\phi_2$. By induction it follows that $\phi = g_0 + tg_1 + \cdots + t^n g^n + t^{n+1}\phi_{n+1}$. Therefore ϕ is approximated modulo $\hat{M}^n$ by an odd integer-valued polynomial. □

Theorem 4.6. *Let V be a discrete valuation domain with an E.W.V.D.W.O. Every odd continuous function $\phi \in \mathcal{C}(\hat{V}, \hat{V})$ can be expressed as the sum of series*

$$\phi = \sum_{i=1}^{\infty} a_i O_i, \text{ where } a_i \in \hat{V} \text{ and } v(a_i) \to +\infty.$$

Proof. Same proof as that for the even continuous functions, using [5, Theorem III.3.7] □

We end with a corollary that gives an analogue of Fourier series expansion.

Corollary 4.1. *Let V be a discrete valuation domain with residue field of odd cardinality. Every continuous function $\phi \in \mathcal{C}(\hat{V}, \hat{V})$, can be expressed as the sum of series*

$$\phi = \sum_{i=0}^{\infty} a_i E_i + \sum_{i=1}^{\infty} b_i O_i, \text{ where } a_i, b_i \in \hat{V}, \text{ and } v(a_i), v(b_i) \to +\infty.$$

Proof. $2\phi(x) = \phi(x) + \phi(-x) + \phi(x) - \phi(-x)$ which is the sum of an even and odd continuous function each of which can be written as the relevant series. That is from Theorem 4.3 we have $\phi(x) + \phi(-x) = \sum_{i=0}^{\infty} a_i E_i$ and from Theorem 4.6 we have

$\phi(x) - \phi(-x) = \sum_{i=1}^{\infty} b_i O_i$ Since the characteristic of V/M is odd, 2 is a unit in V, hence dividing both sides by 2 yields the result. $\square$

Bibliography

[1] D. Anderson, P. Cahen, S. Chapman and W. Smith *Some factorization properties of the ring of integer-valued polynomials* Lecture notes in Pure and Applied Mathematics, Marcel Dekker **171** (1995) 125–142

[2] J. Brewer, S. Glaz, W. Heinzer and B. Olberding, *Multiplicative ideal theory in commutative algebra: A tribute to the work of Robert Gilmer*, Springer, (2006)

[3] D. Brizolis *A theorem on ideals in Prüfer rings of integral-valued polynomials* Commutative Algebra, **7** (1979), 1065–1077

[4] J.-L. Chabert *Integer-valued polynomials on prime numbers and logarithm power expansion* European Journal of Combinatorics, **28** (2007), 754–761

[5] P.-J. Cahen and J.-L. Chabert, *Integer-valued polynomials*, Mathematical Surveys and Monographs, American Mathematical Society, Providence, **48** (1997).

[6] P.-J. Cahen and J.-L. Chabert, *On the ultrametric Stone-Weierstrass theorem and Mahler's expansion*, Journal de Théorie des Nombres de Bordeaux, **14** (2002), 43–57.

[7] P.-J. Cahen, J.-L. Chabert and W. Smith *Algebraic properties of the ring of integer-valued Polynomials on Prime Numbers* Communications in Algebra, **25** (1997), 1945–1959.

[8] J.-L. Chabert, S. Chapman and W. Smith *A basis for the ring of polynomials integer-valued on prime numbers*, Lecture Notes in Pure and Applied Mathematics, **189** (1997), 271–284

[9] J.-L. Chabert, S. T. Chapman and W. Smith, *The Skolem property in rings of integer-valued polynomials*, Proc. of the American Mathematical Society, **11** (1998), 3151–3159.

[10] S. Chapman and W. Smith *Factorization in Dedekind domains with finite class group* Israel Journal of Mathematics, **71** (1990), 65–95

[11] J. Dieudonné *Sur les fonctions continues p-adiques* Bull. Sci. Math., 2éme série, **68** (1944), 79–95

[12] D. Eisenbud *Commutative algebra with a view towards algebraic geometry* Springer-Verlag, (2004)

[13] L. Fuchs and L. Salce, *Modules over non-Noetherian domains* Mathematical Surveys and Monographs, American Mathematical Society, Providence, **84** (2000).

[14] R. Gilmer and W. Smith *Finitely generated ideals of the ring of integer-valued polynomials*, J. Algebra, **81** (1983), 150–164.

[15] R. Gilmer and W. Smith *On the polynomial equivalence of subsets E and $f(E)$ of* $\mathbb{Z}$ Arch. Math., **73** (1999), 355–365

[16] H. Gunji and D. McQuillan, *On rings with a certain divisibilty property* Michigan Mathematics Journal, **22** (1975), 289–299.

[17] I. Kaplansky *The Weierstrass theorem in fields with valuations* Proceedings of the American Mathematical Society, **1** (1950), 356–357

[18] S. Lang *Algebra* Springer-Verlag, (2002)

[19] K. Mahler, *An interpolation series for continuous functions of a p-adic variable*, Journal für die reine und angewandte Mathematatik, **199** (1958).

[20] H. Matsumura *Commutative ring theory* Cambridge Studies in Advanced Mathematics, (1989)

[21] D. McQuillan, *On the ideals in Prüfer domains of polynomials* J. reine angew. Math,**45** (1985), 162–178

[22] A. V. Mikhalev and G. V. Plitz *The concise handbook of algebra* Springer, (2002)

[23] J. Munkres *Topology* second edition, Prentice hall

[24] M. Murty and N. Saradha, *Trancendental values of the digamma function* Journal of Number Theory,**125** (2007), 298-318

[25] G. Pólya and G. Szegö *Problems and theorems in analysis II*, Springer-Verlag, (1972)

[26] M. Stone *A generalized Weierstrass approximation theorem* Studies in Modern Analysis (M.A.A.), 1962

[27] K. Weierstrass *Über die analytische Darstellbarkeit sogenannter willkürlicher Functionen einer reellen Veränderlichen* Sitzungsberichte der Akademie zu Berlin 633–639 and 789–805, 1885

[28] H. Whitney, *Differentiable even functions* Duke Mathematical Journal, **10** (1943), 159–160.