POLYNOMIALS INTEGER-VALUED ON MAXIMAL ORDERS IN DIVISION ALGEBRAS

by

Asmita Chawla Sodhi

Submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy

at

Dalhousie University
Halifax, Nova Scotia
March 2020

In memory of Dr. Amarjit Singh Sodhi
November 26, 1957 – April 15, 2018

To Dad:

After your surgery, you told me "it sounds like you won't have a dad for much longer", and my first thought was "please just live long enough to see me get my PhD". You didn't, so this is for you. I hope you won't hold it against me that it took an extra semester to finish. I needed some time.

I'm glad you knew where I was going, even if you won't get to know where I'll end up. Thank you for everything. I miss you.

Table of Contents

List of Tables

List of Figures

Abstract

A polynomial $f(x) \in \mathbb{Q}[x]$ is called *integer-valued* if $f(n) \in \mathbb{Z}$ for all $n \in \mathbb{Z}$. Bhargava's p-orderings and p-sequences have been helpful tools in the study of integer-valued polynomials over subsets of $\mathbb{Z}$ and arbitrary Dedekind domains, and similar useful definitions exist of ν-orderings and ν-sequences in the case of certain noncommutative rings. In a 2015 paper by Evrard and Johnson, these ν-sequences are used to construct a regular p-local basis for the rational integer-valued polynomials over the ring of 2×2 integer matrices $M_2(\mathbb{Z})$ by way of moving the problem to maximal orders within an index 2 division algebra over $\mathbb{Q}_p$. In this work, we will demonstrate how the construction used there extends nicely to maximal orders in index p division algebras over $\mathbb{Q}_2$, where p is an odd prime, thereby giving the construction for a regular basis for polynomials that are integer-valued over this maximal order.

List of Abbreviations and Symbols Used

$\mathrm{Int}(Z)$ ..... the ring of integer-valued polynomials over $\mathbb{Z}$ (subring of $\mathbb{Q}[x]$)

$\binom{x}{k}$ ..... binomial polynomial defined as $\frac{x(x-1)\cdots(x-(k-1))}{k!}$

$\mathrm{Int}(S, Z)$ ..... the ring of integer-valued polynomials over a subset $S \subseteq \mathbb{Z}$

$\alpha_{S,p}$ ..... the associated p-sequence of a set $S \subseteq \mathbb{Z}$

ν_p ..... the p-adic valuation (as in $\mathbb{Q}_p$)

$x^{(n)_{S,p}}$ ..... the falling factorial of length n coming from a p-ordering of S

$k!_S$ ..... generalized factorial function of S

$B_{k,S}(x)$ ..... global falling factorial

$\mathrm{Int}(D)$ ... the ring of integer-valued polynomials over a commutative integral domain (subring of $K[x]$ where K is the quotient field of D)

$\mathrm{Int}(E, D)$ ..... the ring of integer-valued polynomials over a subset $E \subseteq D$

$\mathfrak{I}_n(E, D)$ ..... characteristic ideal of $\mathrm{Int}(E, D)$

$\mathfrak{I}_n(D)$ ..... characteristic ideal of $\mathrm{Int}(D)$

ν_P ..... the P-adic valuation (in a Dedekind domain)

$\alpha_{E,P}$ ..... the associated P-sequence of a subset $E \subseteq D$

char. pol.$_K\alpha$ ..... characteristic polynomial for α over K

$T_{A/K}$ ..... trace (computed using a K-basis for A)

$N_{A/K}$ ..... norm (computed using a K-basis for A)

min. pol.$_K\alpha$ ..... minimal polynomial for α over K

$M_n(R)$ ..... the set of $n \times n$ matrices with entries in R

I_n ..... the $n \times n$ identity matrix

$\mathbb{F}_{p^n}$ ..... the finite field containing p^n elements

$\mathbb{Q}_p$ ..... the p-adic numbers

$\mathbb{Z}_p$ ..... the p-adic integers

$\mathrm{Int}_{\mathbb{Q}}(M_n(\mathbb{Z}))$ ... the rational polynomials mapping integer matrices to integer matrices

$\mathcal{O}_\theta$ ..... the ring of algebraic integers in $\mathbb{Q}(\theta)$

$\mathrm{Int}_{\mathbb{Q}}(\mathcal{O}_\theta)$ ..... the algebra of rational polynomials preserving $\mathcal{O}_\theta$

$\mathrm{Int}_{\mathbb{Q}}(M_n(\mathbb{Z})_{(p)})$ ..... the localization of $\mathrm{Int}_{\mathbb{Q}}(M_n(\mathbb{Z}))$ at a rational prime p

$f_k(a_0, \ldots, a_{k-1})(x)$ ..... the minimal polynomial of the set $\{a_0, a_1, \ldots, a_{k-1}\}$

α_S ..... the ν-sequence of a subset S of a maximal order

$\alpha \wedge \beta$ ..... the shuffle of two nondecreasing sequences α and β

(kn) ..... the linear sequence whose n^{th} term is kn

$ch_z(x)$ ..... the characteristic polynomial of z

$\alpha^{\wedge n}$ ..... the sequence α shuffled with itself n times

$\lfloor x \rfloor$ ..... floor function; the greatest integer less than or equal to x

$\lim_{n\to\infty} \frac{\alpha(n)}{n}$ ..... the valuative capacity of a nondecreasing sequence α

$\nu_2(\phi_j)$ ..... shorthand for $\nu_2(\phi_j(m) - \phi_j(k))$

Δ_p ..... the maximal order of index p in $\mathbb{Q}_2$

$I_q(n)$ ..... the number of monic irreducible polynomials of degree n modulo q

μ ..... the Möbius function

$\lceil x \rceil$ . . . . . ceiling function; the smallest integer greater than or equal to x

$\langle a_0; a_1, a_2, \ldots, a_n \rangle$ . . . . . the continued fraction with $a_0, \ldots, a_n$ as coefficients

Acknowledgements

Bear with me – I have a lot of people to thank.

First of all, thank you to my supervisor, Dr. Keith Johnson, for your guidance, patience, and for introducing me to a nice little mathematical problem to work on. Thanks also for knowing when I needed a little nudge (or larger push) to get cracking – I am very appreciative for all your support and encouragement.

Thank you also to my readers, Dr. Karl Dilcher and Dr. Rob Noble, and my external examiner, Dr. Alan Loper, for taking the time to read my thesis and for all your suggestions and interesting questions about my work. An extra thanks as well to everyone involved in my defense for adapting to the unusual circumstances that led to me being the first student in the department to defend entirely remotely!

Many thanks to the many people who have made the Chase Building home these last few years. An extra special thank you to Dorette, for supporting my teaching and outreach interests and introducing me to the kids that make Monday nights the best part of my week.

Thank you to NSERC and the NS Graduate Scholarship for financial support throughout this degree, and to everyone involved in letting me take a break from my studies and scholarships to run away and do a work term for four months. The experience was incredibly valuable to me, and I'm grateful to my team for helping me regain confidence in my mathematical and research abilities.

An uncountable number of thank yous to Angelina for being the most encouraging friend on the planet and making sure I took the occasional work break, and to Nick for being my cheerleader through three degrees and for regular reminders not to take life too seriously. Thanks to Tine and Martin for academic commiseration chats from afar – we'll all be done soon! Thanks also to Alex, Vicki, Danielle, Rochelle, Elizabeth, and my many support group pals for cheering me on. I'm also very grateful to my friends at the Canadian Museum of Immigration at Pier 21 and the Discovery Centre for welcoming me into your communities and making my life outside of academia more fun!

Thank you, Jessica, for giving me an opportunity to discover just how much I love working with and supporting students, and for your encouragement through my own degree. I'm also grateful to Jordan, Jenny, Heather, Stillman, and Marriam for their open ears through these last few years.

Rasul, thank you for your phone calls and emails and for making sure I don't lose sight of one of my most important responsibilities in life: being your big sister.

Mum, thank you for your support through the rocky road of grad school, that was made even rockier by everything that happened in our family since I started this degree. Thank you for making an effort to understand my research experience, even though it looked so much different to yours. Thirty years later and now it's my turn for a PhD!

Finally, thank you, Dad, for so many things – but most of all for being my first and favourite math teacher. I wish you could be here to see me finish my PhD, get my first job, and tell Mum that those math sticker books you bought when I was four weren't a waste of money after all. I couldn't have asked for a better dad.

Chapter 1

Introduction

The goal of this research is to study the ring of integer-valued polynomials on $p \times p$ matrices for p a prime, and its integral closure, extending results for 2×2 matrices given in [11] and [6]. This introductory chapter seeks to introduce the reader to integer-valued polynomials over $\mathbb{Z}$, before discussing computational tools in $\mathrm{Int}(\mathbb{Z})$ and extending the results to integer-valued polynomials over a domain D.

Definition of ring of integer-valued polynomials

The *ring of integer-valued polynomials* $\mathrm{Int}(\mathbb{Z})$ is defined as the set of rational polynomials taking integer values over the integers:

$$\mathrm{Int}(\mathbb{Z}) = \{f \in \mathbb{Q}[x] : f(\mathbb{Z}) \subseteq \mathbb{Z}\} \ ,$$

which carries the structure of a subring of $\mathbb{Q}[x]$. The ring $\mathrm{Int}(\mathbb{Z})$ has a number of interesting properties, such as the fact that it is a polynomial ring with *regular basis* as a $\mathbb{Z}$-module comprised of the binomial polynomials

$$\left\{ \binom{x}{k} = \frac{x(x-1)\cdots(x-(k-1))}{k!} : k \in \mathbb{Z}_{>0} \right\} \ ,$$

with convention that $\binom{x}{0} = 1$ and $\binom{x}{1} = x$. This means that every $f \in \mathrm{Int}(\mathbb{Z})$ can be expressed uniquely as a $\mathbb{Z}$-linear combination of the $\binom{x}{k}$, the set of which contains exactly one polynomial of degree k for $k \geq 1$. [4]

We can also consider integer-valued polynomials on a subset $S \subseteq \mathbb{Z}$, which is defined by

$$\mathrm{Int}(S, \mathbb{Z}) = \{f \in \mathbb{Q}[x] : f(S) \subseteq \mathbb{Z}\} \ .$$

Note that $\mathrm{Int}(S, \mathbb{Z})$ is also a ring contained in $\mathbb{Q}[x]$.

The binomial polynomials $\binom{x}{n}$ have been long used in interpolation problems, but it was not until 1919 that separate papers by Pólya and Ostrowski studied integer-valued polynomials as a topic of their own. These polynomials are the subject of a monograph from 1997 by Cahen and Chabert [3], but the nature of the study of integer-valued polynomials changed in 2000 with the introduction of p-orderings and p-sequences by Bhargava [2].

Chapter 2

Summary of Known Results

2.1 Results over $\mathbb{Z}$

2.1.1 p-orderings and p-sequences

The notion of a p-ordering of a subset of $\mathbb{Z}$ and its application to the study of integer-valued polynomials was first introduced by Bhargava in [2].

Let S be any subset of $\mathbb{Z}$, and let p be a fixed prime. A *p-ordering* of S is a sequence $\{a_i\}_{i=0}^{\infty}$ of elements in S defined as follows: choose an element $a_0 \in S$ arbitrarily. Further elements are defined inductively where, given $a_0, a_1, \ldots, a_{k-1}$, the element $a_k \in S$ is chosen so as to minimize the highest power of p dividing

$$\prod_{i=0}^{k-1}(a_k - a_i) \ .$$

The choice of p-ordering of $S \subseteq \mathbb{Z}$ gives an associated integer sequence, the *associated p-sequence* of S, denoted $\{\alpha_{S,p}(k)\}_{k=0}^{\infty}$. The k^{th} element $\alpha_{S,p}(k)$ of this monotone increasing sequence is the power of p minimized at the k^{th} step of the process of defining a p-ordering.

If we let ν_p denote the p-adic valuation on $\mathbb{Z}$, where $\nu_p(x) = \max\{t \in \mathbb{N} : p^t | x\}$ if $x \neq 0$ and $\nu_p(0) = \infty$, then

$$\alpha_{S,p}(k) = \nu_p\left(\prod_{i=0}^{k-1}(a_k - a_i)\right) = \sum_{i=0}^{k-1}\nu_p(a_k - a_i) \ .$$

Though the choice of a p-ordering of S is not unique, we do get the following nice result:

Theorem 2.1.1 ([2], Thm 5)**.** The associated p-sequence of a subset $S \subseteq \mathbb{Z}$ is independent of the choice of p-ordering.

In order to give a proof of Theorem 2.1.1, we need a bit more machinery. Let $\{a_i\}$ be a fixed p-ordering of a set $S \subseteq \mathbb{Z}$. We can define the *falling factorials* $x^{(n)_{S,p}}$ by

$$x^{(n)_{S,p}} = (x - a_0)(x - a_1) \cdots (x - a_{n-1}) \ .$$

Lemma 2.1.2 ([2], Lemma 12)**.** A polynomial f over the integers, written in the form

$$f(x) = \sum_{i=0}^{k} c_i x^{(i)_{S,p}} = \sum_{i=0}^{k} c_i (x - a_0)(x - a_1) \cdots (x - a_{i-1}) \ , \tag{2.1}$$

vanishes on S modulo p^e if and only if $c_i x^{(i)_{S,p}}$ does for each $0 \leq i \leq k$.

Proof. Suppose f vanishes on $S \pmod{p^e}$, but that some term on the right side of Equation (2.1) does not. Let j be the smallest index for which $c_j x^{(j)_{S,p}}$ does not vanish on $S \pmod{p^e}$. By setting $x = a_j$, all terms on the right side with $i > j$ vanish identically, while the minimality of j tells us that all terms with $i < j$ vanish modulo p^e. Therefore $c_j a_j^{(j)_{S,p}}$ must also vanish modulo p^e, from which we see that $c_j x^{(j)_{S,p}}$ vanishes on all of $S \pmod{p^e}$, since $\{a_i\}$ is a p-ordering. This contradiction gives the desired result. □

Proof of Theorem 2.1.1, [2]. Given a set $S \subseteq \mathbb{Z}$, let d be a positive integer, choose a large positive integer e such that $e > \alpha_{S,p}(d)$. Consider the set G_d of all polynomials in $(\mathbb{Z}/p^e\mathbb{Z})[x]$ that vanish on S modulo p and have degree at most d – this set forms an additive group. By Lemma 2.1.2, the polynomials $x^{(i)_{S,p}}$ form a basis for the polynomials f which vanish on S modulo p^e. Since the $\{a_i\}$ are a p-ordering for S, we know these elements are chosen in such a way that minimizes $\alpha_{S,p}(k)$, and hence every falling factorial $x^{(i)_{S,p}}$ is divisible by $p^{\alpha_{S,p}(i)}$. This shows that as an abelian group, G_d is isomorphic to

$$\bigoplus_{k=0}^{d} \mathbb{Z}/p^{\alpha_{S,p}(k)}\mathbb{Z} \ .$$

Therefore the numbers $p^{\alpha_{S,p}(k)}$, for $0 \leq k \leq d$, form the structure coefficients for the abelian group G_d. By the structure theorem for finitely generated abelian groups, these constants depend only on G_d itself, which gives the result of Theorem 2.1.1. □

2.1.2 Generalized factorial

Bhargava's motivating question in [2] is not explicitly on the topic of integer-valued polynomials, but instead on extending the idea of the factorial (which relies on the fact that we are working over all of $\mathbb{Z}$) to subsets of the integers. Given the fact that the natural ordering of nonnegative integers $0, 1, 2, 3, \ldots$ gives a p-ordering of $\mathbb{Z}$ for all primes p simultaneously (see [2], Prop 6), Bhargava notes that using the definitions made in Section 2.1.1, we can define the usual factorial function over the integers just in terms of the invariants $\alpha_{\mathbb{Z},p}(k)$ as

$$k! = \prod_p p^{\alpha_{\mathbb{Z},p}(k)}$$

and the use of these invariants allows for the following definition.

Definition 2.1.3. Let S be a subset of $\mathbb{Z}$. Then the *factorial function* of S, denoted $k!_S$, is defined as

$$k!_S = \prod_p p^{\alpha_{S,p}(k)} \ .$$

Note that though the product is over the infinite set of all primes in $\mathbb{Z}$, for a fixed k only finitely many of the $\alpha_{S,p}(k)$ are not equal to 0. Thus this definition makes sense for all choices of S and k.

As referred to in the Introduction, we have the following result.

Theorem 2.1.4 (Pólya)**.** A polynomial is integer-valued on $\mathbb{Z}$ if and only if it can be written as a $\mathbb{Z}$-linear combination of the polynomials

$$\binom{x}{k} = \frac{x(x-1)\cdots(x-k+1)}{k!}$$

with $k = 0, 1, 2, \ldots$

As this conveniently characterizes all elements of $\mathrm{Int}(\mathbb{Z})$, we would like to be able to do the same for $\mathrm{Int}(S, \mathbb{Z})$. To do so, we first need the notion of the "global falling factorial" described in [2].

Definition 2.1.5. The *global falling factorial* polynomials $B_{k,S}$ are defined by

$$B_{k,S}(x) = (x - a_{0,k})(x - a_{1,k}) \cdots (x - a_{k-1,k}) \ , \tag{2.2}$$

where $\{a_{i,k}\}_{i=0}^{\infty}$ is a sequence in $\mathbb{Z}$ that, for some prime p dividing $k!_S$, is termwise congruent modulo $p^{\alpha_{S,p}(k)}$ to some p-ordering of S.

Note. Such a sequence $\{a_{i,k}\}_{i=0}^{\infty}$ as in Definition 2.1.5 exists by the Chinese Remainder Theorem.

This definition allows for the analogous result to Theorem 2.1.4 for subsets of the integers.

Theorem 2.1.6 ([2], Thm 23)**.** A polynomial is integer-valued on a subset $S \subseteq \mathbb{Z}$ if and only if it can be written as a $\mathbb{Z}$-linear combination of the polynomials

$$\frac{B_{k,S}}{k!_S} = \frac{(x - a_{0,k})(x - a_{1,k}) \cdots (x - a_{k-1,k})}{k!_S}$$

with $k = 0, 1, 2, \ldots$ and with $B_{k,S}$ defined as in Equation (2.2).

The study of integer-valued polynomials of subsets has long since extended to that of other commutative domains, which we discuss in Section 2.2.

2.2 Extensions of Results over $\mathbb{Z}$

The notion of rings of integer-valued polynomials can be generalized from $\mathbb{Z}$ to the following. Let D be a commutative integral domain with quotient field K. Then the integer-valued polynomials on D form a ring

$$\mathrm{Int}(D) = \{f \in K[x] : f(D) \subseteq D\} \ .$$

If E is a subset of D, we can also consider the integer-valued polynomials of E, defined as

$$\mathrm{Int}(E, D) = \{f \in K[x] : f(E) \subseteq D\} \ ,$$

and we note that $\mathrm{Int}(E, D)$ is also a ring contained in $K[x]$.

For a subset E of a domain D having quotient field K, we have the following chain of inclusions of rings:

$$D[x] \subseteq \mathrm{Int}(D) \subseteq \mathrm{Int}(E, D) \subseteq K[x] \ . \tag{2.3}$$

A common question in this area of study is under which conditions we have equality within this chain.

When considering integer-valued polynomials of a subset, it is possible that for two different subsets E and F of K, we have $\mathrm{Int}(E, D) = \mathrm{Int}(F, D)$.

Lemma 2.2.1 ([3], IV.1.1)**.** For each subset E of K, the subset

$$F = \{x \in K : f(x) \in D \text{ for all } f \in \mathrm{Int}(E, D)\}$$

is the largest subset of K such that $\mathrm{Int}(E, D) = \mathrm{Int}(F, D)$.

Definition 2.2.2 ([3], IV.1.2)**.**

i) Two subsets E and F of K are called *polynomially equivalent* if $\mathrm{Int}(E, D) = \mathrm{Int}(F, D)$.

ii) The largest subset of K that is D-equivalent to E is the *polynomial closure* of E.

iii) If E is equal to its polynomial closure, then E is *polynomially closed*.

iv) If E is a subset of the domain D which is polynomially equivalent to D, then E is a *polynomially dense subset* of D.

By this definition, the subset F of K in Lemma 2.2.1 is the polynomial closure of E. We also see that $\mathrm{Int}(D) = \mathrm{Int}(E, D)$ in the chain of rings in Equation (2.3) if E is a polynomially dense subset of D. [3]

2.2.1 Regular bases of $\mathbf{Int}(E, D)$

Definition 2.2.3. Let D be a domain and E a subset of D. Let $\mathfrak{I}_n(E, D)$ denote the set formed by the leading coefficients of all degree n polynomials in $\mathrm{Int}(E, D)$, with 0 also adjoined. Then each $\mathfrak{I}_n(E, D)$ is a fractional ideal of D, and we call them the *characteristic ideals* of $\mathrm{Int}(E, D)$. By $\mathfrak{I}_n(D)$, we denote the characteristic ideals of $\mathrm{Int}(D)$.

Proposition 2.2.4 ([3], II.1.4)**.** Let E be an infinite subset of the domain D. Then the D-module $\mathrm{Int}(E, D)$ admits a regular basis if and only if all the fractional ideals $\mathfrak{I}_n(E, D)$ are principal. In this case, a sequence $\{f_n\}_{n\geq 0}$ of polynomials in $\mathrm{Int}(E, D)$ where $\deg(f_n) = n$ forms a regular basis if and only if, for each n, the leading coefficient of f_n generates $\mathfrak{I}_n(E, D)$.

In the case where D is a discrete valuation domain with uniformizing parameter t, then all fractional ideals of D are of the form $t^k D$ for some $k \in \mathbb{Z}_{>0}$. Since D is principal, every subring B of $\mathrm{Int}(D)$ admits a regular basis ([3], II.1.6), and to determine this basis we consider the characteristic ideals $\mathfrak{I}_n(B)$, which are of the

form $\mathfrak{I}_n(B) = t^{-\alpha_B(n)}D$. We call the sequence $\{\alpha_B(n)\}$ the *characteristic sequence* of the ring B. By Proposition 2.2.4, a sequence $\{f_n\}$ of polynomials is a regular basis for B if and only if for each n, $\deg(f_n) = n$ and the leading coefficient of f_n has valuation $-\alpha_B(n)$ ([3], IX.3 pg. 241).

Definition 2.2.5. Let $\{a_n\}_{n\geq 0}$ be a sequence of distinct elements of a subset E of a domain D. We define the *generalized binomials* $\binom{x}{a_n}$ by

$$\binom{x}{a_0} = 1 \qquad\qquad \binom{x}{a_n} = \prod_{k=0}^{n-1} \frac{x - a_k}{a_n - a_k} \text{ , for } n \geq 1 \text{ .}$$

Proposition 2.2.6 ([4], 20)**.** Let E be an infinite subset of a domain D and $\{a_n\}_{n\geq 0}$ be a sequence of distinct elements of E. Then the following are equivalent:

i) The generalized binomials $\binom{x}{a_n}$ are integer-valued on E.

ii) The generalized binomials $\binom{x}{a_n}$ form a basis of the D-module $\mathrm{Int}(E, D)$.

iii) A polynomial $f \in K[x]$ of degree at most n is integer-valued on E if and only if it is integer-valued on the first $n + 1$ terms of the sequence $\{a_n\}_{n\geq 0}$.

It may be the case that there exists no such sequence as in Proposition 2.2.6, but for subsets of $\mathbb{Z}$ one can obtain such a sequence locally, namely by constructing a p-ordering (see Section 2.1.1).

2.2.2 Regular bases of subsets of Dedekind domains

In the case where D is a Dedekind domain with quotient field K, and E is any subset of D, it is possible to give an explicit description of $\mathrm{Int}(E, D)$. Due to Bhargava [1], there also exist necessary and sufficient conditions for the existence of a regular basis for $\mathrm{Int}(E, D)$, as well as a construction for the case where a regular basis exists. We discuss these results below.

First we will define what is meant by a P-ordering of a subset of a Dedekind domain in a fashion analogous to that in Section 2.1.1.

Definition 2.2.7. Let D be a Dedekind domain, E any nonempty subset of D, and P be a fixed nonzero prime ideal of D. We define a *P-ordering of E* as follows: let

$a_0 \in E$ be any element, and for $k = 1, 2, \ldots$ choose $a_k \in E$ to be an element which minimizes the exponent of the highest power of P containing

$$\prod_{i=0}^{k-1}(a_k - a_i) \ .$$

We denote by $\nu_P(a)$ the exponent of the highest power of P containing $a \in D$, called the *P-adic valuation of a*. Then given such a P-ordering $\{a_i\}_{i=0}^{\infty}$, we can define the *associated P-sequence of E* corresponding to the P-ordering $\{a_i\}$ as $\{\alpha_{E,P}(k)\}_{k=0}^{\infty}$, with each term of the sequence being defined by

$$\alpha_{E,P}(k) = \nu_P\left(\prod_{i=0}^{k-1}(a_k - a_i)\right) = \sum_{i=0}^{k-1}\nu_P(a_k - a_i) \ .$$

Also analogous to our discussion for subsets of the integers, we can define a factorial function.

Definition 2.2.8. For D a Dedekind domain and E an arbitrary subset, we define

$$\nu_E(k) = \prod_{P \text{ prime}} P^{\alpha_{E,P}(k)}$$

where the product above is taken over all proper prime ideals P of D for which $P^{\alpha_{E,P}(k)} \neq D$.

With these definitions, we may now relay some useful results.

Theorem 2.2.9 ([1], Theorem 11)**.** Let E be a subset of a Dedekind domain D, and let $f(x) \in D[x]$ be such that $\deg(f) = k$ and the coefficients of f generate D. If $I \subseteq D$ is the smallest ideal such that f maps E into I, then

$$\nu_E(k) \subseteq I \ .$$

Moreover, for any $k \in \mathbb{Z}_{>0}$, the case where $\nu_E(k) = I$ is achieved by the polynomial

$$S_k = (x - a_{0,k})(x - a_{1,k}) \cdots (x - a_{k-1,k})$$

where $\{a_{i,k}\}_{i=0}^{\infty}$ is a sequence in D which, for each prime ideal $P \supseteq \nu_E(k)$, is termwise congruent modulo $P^{\alpha_{E,P}(k)}$ to some P-ordering of E.

Theorem 2.2.10 ([1], Theorem 12)**.** The set of all leading coefficients of polynomials

of degree k in $\mathrm{Int}(E, D)$ is the fractional ideal given by $\nu_E(k)^{-1}$, with the convention that the inverse of the zero ideal is the quotient field K.

The following theorem shows that elements of $\mathrm{Int}(E, D)$ can be written in terms of the sequences $\{a_{i,k}\}_{i=0}^{\infty}$ and the polynomials S_k described in Theorem 2.2.9. It also describes the structure of $\mathrm{Int}(E, D)$ as a D-module.

Theorem 2.2.11 ([1], Theorem 13)**.** Let $f(x) \in \mathrm{Int}(E, D)$. Then f can be represented in the form

$$\sum_{k=0}^{n} b_k(x - a_{0,k})(x - a_{1,k}) \cdots (x - a_{k-1,k}) \ ,$$

where $n \in \mathbb{Z}$ and the $b_k \in \nu_E(k)^{-1}$ are uniquely determined by f. Conversely, any polynomial of the form above is an element of $\mathrm{Int}(E, D)$.

It follows that, as a D-module, $\mathrm{Int}(E, D)$ is isomorphic to the direct sum

$$\bigoplus_{k=0}^{\infty} \nu_E(k)^{-1} \ .$$

Now that the description of the D-module structure of $\mathrm{Int}(E, D)$ has been established, we can provide a criterion for the existence of a regular basis, as well as a construction for this regular basis when it exists.

Theorem 2.2.12 ([1], Theorem 14)**.** The ring $\mathrm{Int}(E, D)$ has a regular basis if and only if $\nu_E(k)$ is a nonzero principal ideal for all $k \geq 0$. In this case, a regular basis of $\mathrm{Int}(E, D)$ is given by the polynomials

$$\frac{(x - a_{0,k})(x - a_{1,k}) \cdots (x - a_{k-1,k})}{\beta_k}$$

for $k = 0, 1, 2, \ldots$, where β_k is a generator of the ideal $\nu_E(k)$.

Corollary 2.2.13 ([1], Corollary 3)**.** If D is a principal ideal domain, then for any infinite subset $E \subseteq D$ the ring $\mathrm{Int}(E, D)$ has a regular basis.

In particular, this means that for every infinite subset E of a discrete valuation ring D, the ring $\mathrm{Int}(E, D)$ has a regular basis. If we let ν denote the valuation in D and P the uniformizing parameter, then a P-ordering of E is a sequence $\{a_i\}_{i=0}^{\infty}$ of elements in S such that for each $k > 0$, the element a_k minimizes $\nu(\prod_{i=0}^{k-1}(a - a_i))$

over $a \in E$. In particular, the set of polynomials

$$\left\{ \prod_{i=0}^{k-1} \frac{x - a_i}{a_k - a_i} : k = 0, 1, 2, \dots \right\}$$

provides a regular basis for $\mathrm{Int}(E, D)$.

We now have a number of results regarding rings of polynomials of subsets over commutative domains. We would like to extend these results to noncommutative rings, which leads us to the description of the differences between polynomials in commutative and noncommutative rings.

2.3 Polynomials over Noncommutative Rings

As the goal of this research is to better understand the integer-valued polynomials over matrix rings $M_n(\mathbb{Z})$, it is important to comprehend the differences between polynomials over commutative rings and their noncommutative counterparts.

Let R be any ring, and let $R[x]$ be the polynomial ring in a single variable x over R, where x commutes elementwise with all of R. Given a polynomial

$$f(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$$

and some element $r \in R$, we define the *evaluation of f at r* by $f(r) = \sum_{i=0}^{n} a_i r^i \in R$. It is important to note that while

$$\sum_{i=0}^{n} a_i x^i = \sum_{i=0}^{n} x^i a_i$$

in the ring $R[x]$, the two elements $\sum_{i=0}^{n} a_i r^i$ and $\sum_{i=0}^{n} r^i a_i$ in R may be different if r does not commute with with all the coefficients a_i. Thus the standard definition of evaluation of f at r requires $f(x)$ to be expressed in the form $\sum_{i=0}^{n} a_i x^i$, and then substituting r for x. Another important difference between polynomials in general rings and in the commutative case is that evaluation at r is not generally a ring homomorphism from $R[x]$ to R, meaning that if $f(x) = g(x)h(x) \in R[x]$ it does not follow that $f(r) = g(r)h(r)$ for $r \in R$.

An element $r \in R$ is a *right root* of a polynomial $f(x) \in F[x]$ if $f(r) = 0$, but since we will only consider right roots, we will drop this defining adjective from what follows.

Proposition 2.3.1 ([12], 16.2)**.** An element $r \in R$ is a root of a nonzero polynomial $f(x) \in R[x]$ if and only if the linear factor $x - r$ is a right divisor of $f(x)$ in $R[x]$. The set of polynomials in $R[x]$ which have r as a root is the left ideal $R[x] \cdot (x - r)$.

2.3.1 Polynomials over division rings

Rather than considering general rings R, we now focus particularly on division rings, which will be the type of ring of interest for much of this thesis.

Proposition 2.3.2 ([12], 16.3)**.** Let D be a division ring, and let $f(x) = g(x)h(x) \in D[x]$. Let $d \in D$ be such that $a := h(d) \neq 0$. Then

$$f(d) = g(ada^{-1})h(d) \ .$$

In particular, if d is a root of f but not h, then ada^{-1} is a root of g.

Proof. Let $g(x) = \sum b_i x^i$, then $f(x) = \sum b_i h(x) x^i$. Evaluating at $d \in D$,

$$\begin{aligned} f(d) &= \sum b_i h(d) d^i \\ &= \sum b_i a d^i = \sum b_i a d^i a^{-1} a \\ &= \sum b_i (ada^{-1})^i a \\ &= g(ada^{-1})h(d) \ . \end{aligned}$$

The last statement follows because D has no zero-divisors. □

Over a field, polynomials of degree n have at most n distinct roots, but this is not the case over division rings. However, there is an analogue to this fact:

Theorem 2.3.3 (Gordon-Motzkin, [12] 16.4)**.** Let D be a division ring, and let f be a polynomial of degree n in $D[x]$. Then the roots of f lie in at most n conjugacy classes of D. This means that if $f(x) = (x - a_1) \cdots (x - a_n)$ with $a_1, \ldots, a_n \in D$, then any root of f is conjugate to some a_i.

Let F be the centre of a division ring D. Suppose that $a \in D$ is a root of the polynomial $f(x) \in F[x]$, then every conjugate of a is also a root of $f(x)$, which we can see by conjugating the equation $f(a) = 0$ by all nonzero elements of D.

Definition 2.3.4. Let D be a division ring, F its centre, and A a conjugacy class of D. We call the conjugacy class A *algebraic over* F if one (and therefore all) of its elements are algebraic over F.

In the case that the conjugacy class A is algebraic, then the elements of S have the same minimal polynomial over F, which we call the minimal polynomial of A.

Lemma 2.3.5 ([12], 16.5)**.** Let D be a division ring with centre F, and let A be a conjugacy class of D which is algebraic over F with minimal polynomial $f(x) \in F[x]$. If a nonzero polynomial $h(t) \in D[t]$ vanishes identically on A, then $\deg h \geq \deg f$.

A classical result about polynomials over division rings is given by Dickson, to which we will make future reference.

Theorem 2.3.6 (Dickson's Theorem, [12] 16.8)**.** Let D be a division ring and F its centre. Let $a, b \in D$ be two elements that are algebraic over F. Then a and b are conjugate in D if and only if they have the same minimal polynomial over F.

Proof. Suppose a and b are conjugate in D, and let f_a and f_b denote their minimal polynomials, respectively. Since a is a root of f_a, so too are all its conjugates, so $f_a(b) = 0$ from which we obtain $\deg(f_a) \geq \deg(f_b)$. Switching a and b gives $\deg(f_a) = \deg(f_b)$, and since both are monic the uniqueness of minimal polynomials shows that $f_a = f_b$.

Conversely, let A be the conjugacy class determined by a, and assume that a, b have the same minimal polynomial $f(x) \in F[x]$. Since $f(b) = 0$, we know $x - b$ is a factor of $f(x)$ in the polynomial over the field $F(b)$. Then there exists $h(x) \in F(b)[x]$ for which

$$f(x) = h(x)(x - b) = (x - b)h(x) \ .$$

By Lemma 2.3.5, $h(x)$ is not identically zero on A and thus there exists $a' \in A$ for which $h(a') \neq 0$. Since $f(a') = 0$, this implies that a conjugate of a' is a root of $t - b$, so that b is a conjugate of a'. Hence $b \in A$, and b is a conjugate of a. □

So far we have some results for the minimal polynomial of a single element, but would like to define the minimal polynomial of a finite list of elements (see Definition 2.5.7). The following theorem offers justification that such a polynomial should exist.

Theorem 2.3.7 (Bray-Whaples, [12] 16.13)**.** Let D be a division ring and $c_1, \ldots, c_n$ be n pairwise nonconjugate elements of D. Then there exists a unique polynomial $g(x) \in D[x]$ with $\deg(g) = n$ that is monic and such that $g(c_1) = \cdots = g(c_n) = 0$. Moreover, $g(x)$ has the following properties:

i) $c_1, \ldots, c_n$ are all the roots of $g \in D$.

ii) If $h(x) \in D[x]$ vanishes on all c_i with $1 \leq i \leq n$, then $h(x) \in D[x] \cdot g(x)$.

We can explicitly describe this minimal polynomial of a set, as given below.

Proposition 2.3.8 ([11], 2.4)**.** Let D be a subring of a division algebra, and $c_1, \ldots, c_n$ be n pairwise nonconjugate elements of D. Then the minimal polynomial of $\{c_1, \ldots, c_n\}$ is given inductively by

$$\begin{aligned}
f(c_1)(x) &= (x - c_1) \\
f(c_1, c_2)(x) &= (x - [f(c_1)(c_2)]c_2[f(c_1)(c_2)]^{-1})(x - c_1) \\
&\vdots \\
f(c_1, \ldots, c_n)(x) &= (x - [f(c_1, \ldots, c_{n-1})(c_n)]c_n[f(c_1, \ldots, c_{n-1})(c_n)]^{-1}) \cdot f(c_1, \ldots, c_{n-1})(x) \\
&= (x - [f(c_1, \ldots, c_{n-1})(c_n)]c_n[f(c_1, \ldots, c_{n-1})(c_n)]^{-1}) \\
&\qquad (x - [f(c_1, \ldots, c_{n-2})(c_{n-1})]c_{n-1}[f(c_1, \ldots, c_{n-2})(c_{n-1})]^{-1}) \cdots (x - c_1) \ .
\end{aligned}$$

We would ultimately like to describe rings of integer-valued polynomials on $n \times n$ matrices. To do this, we will look at integer-valued polynomials over the maximal order of a division ring.

2.4 Maximal Orders

As there is a strong link between the sets of integer-valued polynomials of algebraic integers and that of maximal orders (described in more detail in Section 2.5.1), we first introduce some theory behind maximal orders before discussing integer-valued polynomials of matrices.

Definition 2.4.1 ([14], Section 8)**.** Let R be a Noetherian integral domain with quotient field K, and A a finite-dimensional K-algebra.

i) Let V be a finite-dimensional K-space. A *full R-lattice* in V is a finitely-generated R-submodule M in V such that $K \cdot M = V$, where we define

$$K \cdot M = \left\{ \sum \alpha_i m_i : \alpha_i \in K, m_i \in M, \text{ sum is finite} \right\} \ .$$

ii) An *R-order* in A is a subring Λ of A which has the same unit element as A, and is such that Λ is a full R-lattice in A.

Note that every finite-dimensional K-algebra A contains R-orders, since there exist $y_1, y_2, \ldots, y_n \in A$ such that $A = \sum_{i=1}^{n} Ky_i$, and so $\Lambda = \sum_{i=1}^{n} Ry_i$ is a full R-lattice in A, and hence an R-order.

Given that $A = \sum_{i=1}^{n} Ky_i$, for $\alpha \in A$ we may write

$$\alpha \cdot y_j = \sum_{i=1}^{m} a_{ij} y_j$$

with $a_{ij} \in K$ and $1 \leq j \leq m$. Then we can define the *characteristic polynomial* for α over K by

$$\begin{aligned} \text{char. pol.}_K \alpha &= \det(\delta_{ij} x - a_{ij}) \\ &= x^m - (T_{A/K}\alpha)x^{m-1} + \cdots + (-1)^m N_{A/K}\alpha \end{aligned}$$

where we call $T_{A/K}$ the *trace* and $N_{A/K}$ the *norm* of α. The subscript A/K here (and in Theorem 2.4.2 for the characteristic polynomial) simply denotes the fact that these expressions are computed using a K-basis for A. The monic polynomial of least degree for which $f(\alpha) = 0$ divides the characteristic polynomial, and is called the *minimal polynomial* of $\alpha \in A$, denoted min. pol.$_K \alpha$.

Theorem 2.4.2 ([14], 8.6)**.** Every element of an R-order Λ is integral over R. Moreover, if R is integrally closed, then for every $a \in \Lambda$ both the minimal polynomial and characteristic polynomial for a over K are in $R[x]$, i.e.

$$\text{min. pol.}_K a \in R[x] \qquad\qquad \text{char. pol.}_{A/K} a \in R[x] \ .$$

Definition 2.4.3. A *maximal R-order* in A is an R-order which is not properly contained in any other R-order in A.

We will see in Section 2.4.1 that there are some cases where there is a unique maximal R-order. Finally, as we are ultimately concerned about matrices, we note the following result.

Theorem 2.4.4 ([14], 8.7)**.** If Λ is a maximal R-order in A, then for each n, $M_n(\Lambda)$ is a maximal R-order in $M_n(A)$. If R is integrally closed, then $M_n(R)$ is a maximal R-order in $M_n(K)$.

2.4.1 Maximal orders of division rings, local case

When R is a complete discrete valuation ring (i.e. R is a principal ideal domain with unique maximal ideal $P = \pi R \neq 0$, and R is complete with respect to the P-adic valuation), K is the quotient field of R, and D is a division ring whose centre contains K and is such that $[D : K] = m$ is finite, then D contains a unique maximal R-order Δ. This fact is shown below.

Let ν denote the P-adic valuation defined on K and let $N_{D/K}$ be the norm map, defined by

$$\text{char. pol.}_{D/K} a = x^m - (T_{D/K} a)x^{m-1} + \cdots + (-1)^m N_{D/K} a$$

for $a \in A$. We define a new function

$$w(a) = m^{-1} \cdot \nu(N_{D/K} a)$$

for $a \in D$. This new map w is a discrete valuation on D extending ν, meaning that $w(\alpha) = \nu(\alpha)$ for $\alpha \in K$ ([14] Theorem 8.7).

We also define

$$\begin{aligned} \Delta &= \{a \in D : w(a) \geq 0\} \\ &= \{a \in D : N_{D/K} a \in R\} \ . \end{aligned}$$

Then Δ is a ring containing R, and is finitely generated as an R-module. We call Δ the *valuation ring* of w, and

Theorem 2.4.5 ([14], 12.8)**.** Δ is the unique maximal R-order in D, and is the integral closure of R in D.

Theorem 2.4.6 ([14], 12.10)**.** The valuation w is the unique extension of ν to D that maintains the properties of a valuation, and has infinite cyclic value group (i.e. $\{w(a) : a \in D, a \neq 0\}$ is infinite cyclic).

2.4.2 Maximal orders of division rings, local case with finite residue class field

Now that it has been established that a division ring D contains a unique maximal R-order Δ when R is a complete discrete valuation ring with unique maximal ideal

P, K is the quotient field of R, and D has centre containing K such that $[D : K]$ is finite, we can look specifically at the case where the residue class field $\overline{R} = R/P$ is finite.

Assume the above with $\overline{R}$ a finite field containing q elements. Assume also that $[D : K] = n^2$; we call n the *index* of D. Let Δ be the unique maximal R-order in D. Then the structures of the division ring D and maximal order Δ can be described explicitly, and can be chosen to depend only on the index n.

The proof of Theorem 14.6 in [14] gives a construction[1] for D. Suppose, as we have been doing, that K is a complete field. Let the *inertia field* be $W = K(\omega)$, where ω is a primitive $(q^n - 1)^{\text{th}}$ root of unity. If a division ring D exists with centre K and index n, then W is a maximal subfield of D and hence splits D, so that $W \otimes_K D \cong M_n(W)$. Thus every element $d \in D$ is representable by a matrix $d^* \in M_n(W)$. We can therefore represent D by a set of matrices in $M_n(W)$ which constitute a division ring with the desired properties.

Let θ be the automorphism of W for which $\theta(\omega) = \omega^q$, and let $\pi \in R$ be a prime element. For $\alpha \in W$, define

$$\alpha^* = \begin{pmatrix} \alpha & 0 & 0 & \cdots & 0 \\ 0 & \theta(\alpha) & 0 & \cdots & 0 \\ 0 & 0 & \theta^2(\alpha) & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \theta^{n-1}(\alpha) \end{pmatrix}, \qquad \pi_D^* = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ \pi & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

For each $\alpha \in W$, the map $\alpha \to \alpha^*$ gives a K-isomorphism of W onto the field $W^* = K(\omega^*) \subseteq M_n(W)$, where each $\lambda \in K$ is identified with the diagonal matrix $\lambda I_n \in M_n(W)$. This identification gives us the properties

$$(\pi_D^*)^n = \pi I_n \qquad\qquad \pi_D^* \cdot \omega^* \cdot (\pi_D^*)^{-1} = (\omega^*)^q \ .$$

Setting

$$D = K[\omega^*, \pi_D^*]$$

gives a K-subalgebra of $M_n(W)$ which is the desired division ring (this is justified in

[1]The proof shows that there exists a division ring D with any Hasse invariant r/n for any choice of $r \in \mathbb{Z}$ such that $1 \leq r \leq n$ and $\gcd(r, n) = 1$. Since we only care about the existence of a division ring of index n and not a specific one, the description of the construction has been simplified slightly to the case where $r = 1$.

Section 14 of [14] but will not be done here). The unique maximal R-order of D is

$$\Delta = R[\omega^*, \pi_D^*] \ .$$

Since $\mathbb{F}_{p^n}$ is a splitting field for the polynomial $x^{p^n} - x$ over $\mathbb{F}_p$ with p prime and $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$, it follows that as ω is a $(q^n - 1)^{\text{th}}$ root of unity and hence a root of $x^{q^n} - x$, that $[W : K] = [K(\omega) : K] = n$. As π_D^* satisfies the polynomial $x^n - \pi$, the extension $[D : W] \leq n$ and hence $[D : K] \leq n^2$, and so any element $a \in D$ is expressible as a K-linear combination of the n^2 elements $\{(\omega^i)^* \cdot (\pi_D^*)^j\}$. Because $(\omega^*)^i = (\omega^i)^*$, we can also express a in the form

$$a = \sum_{j=0}^{n-1} \alpha_j^* (\pi_D^*)^j$$

with $a_j \in W$ and $(\pi_D^*)^j = \begin{pmatrix} 0 & I_{n-j} \\ \pi I_j & 0 \end{pmatrix}$.

In doing so, we can write an element a as

$$a = \begin{pmatrix} \alpha_0 & \alpha_1 & \alpha_2 & \cdots & \alpha_{n-1} \\ \pi\theta(\alpha_{n-1}) & \theta(\alpha_0) & \theta(\alpha_1) & \cdots & \theta(\alpha_{n-2}) \\ \pi\theta^2(\alpha_{n-2}) & \pi\theta^2(\alpha_{n-1}) & \theta^2(\alpha_0) & \cdots & \theta^2(\alpha_{n-3}) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \pi\theta^{n-2}(\alpha_2) & \pi\theta^{n-2}(\alpha_3) & \pi\theta^{n-2}(\alpha_4) & \cdots & \theta^{n-2}(\alpha_1) \\ \pi\theta^{n-1}(\alpha_1) & \pi\theta^{n-1}(\alpha_2) & \pi\theta^{n-1}(\alpha_3) & \cdots & \theta^{n-1}(\alpha_0) \end{pmatrix}$$

and hence if $a = 0$, we must have all $\alpha_i = 0$ as well. This shows that D is a vector space over W with basis $\{(\pi_D^*)^j : 0 \leq j \leq n-1\}$, and hence $[D : W] = n$ and therefore $[D : K] = n^2$.

2.4.3 Constructing a division ring of index 3 with $p = 2$

Let our complete field K be $\mathbb{Q}_2$, the complete field of 2-adic numbers, and let $\omega = \zeta_7$ be a primitive $(2^3 - 1)^{\text{th}}$ root of unity. Then we can let $W = \mathbb{Q}_2(\omega)$, and if there exists a division ring D with centre $\mathbb{Q}_2$ and index 3, then W must be a maximal subfield of D, and so $W \otimes_{\mathbb{Q}_2} D \cong M_3(W)$.

Let $\theta \in \text{Aut}(W)$ be the automorphism for which $\theta(\omega) = \omega^2$. We need to pick a prime element in $\mathbb{Z}_2$, the 2-adic integers, and we can choose $\pi = 2$. For an element

$\alpha \in W$, we can define

$$\alpha^* = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \theta(\alpha) & 0 \\ 0 & 0 & \theta^2(\alpha) \end{pmatrix} \qquad \pi_D^* = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 2 & 0 & 0 \end{pmatrix}$$

so that

$$\omega^* = \begin{pmatrix} \omega & 0 & 0 \\ 0 & \theta(\omega) & 0 \\ 0 & 0 & \theta^2(\omega) \end{pmatrix} = \begin{pmatrix} \omega & 0 & 0 \\ 0 & \omega^2 & 0 \\ 0 & 0 & \omega^4 \end{pmatrix}$$

The map $\alpha \mapsto \alpha^*$ gives a $\mathbb{Q}_2$-isomorphism $W \to W^* = \mathbb{Q}_2(\omega^*) \subseteq M_3(\mathbb{Q}_2)$ under which we identify scalars $\lambda \in \mathbb{Q}_2$ with the scalar matrix $\lambda I_3 \in M_3(\mathbb{Q}_2)$. We observe the following relations involving ω^* and π_D^*:

$$(\pi_D^*)^3 = 2I_3 \qquad \pi_D^* \cdot \omega^* = (\omega^*)^2 \cdot \pi_D^* \ .$$

Given this, we define

$$D = \mathbb{Q}_2[\omega^*, \pi_D^*] = \mathbb{Q}_2 \left[\begin{pmatrix} \omega & 0 & 0 \\ 0 & \omega^2 & 0 \\ 0 & 0 & \omega^4 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 2 & 0 & 0 \end{pmatrix} \right]$$

and the maximal order is similarly defined by $\Delta = \mathbb{Z}_2[\omega^*, \pi_D^*]$.

Each element $a \in D$ may be expressed as a $\mathbb{Q}_2$-linear combination of the elements $\{(\omega^*)^i \cdot (\pi_D^*)^j : 0 \leq i, j \leq 2\}$. Explicitly, these basis elements are

$$I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad \pi_D^* = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 2 & 0 & 0 \end{pmatrix} \qquad (\pi_D^*)^2 = \begin{pmatrix} 0 & 0 & 1 \\ 2 & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix}$$

$$\omega^* = \begin{pmatrix} \omega & 0 & 0 \\ 0 & \omega^2 & 0 \\ 0 & 0 & \omega^4 \end{pmatrix} \qquad \omega^*\pi_D^* = \begin{pmatrix} 0 & \omega & 0 \\ 0 & 0 & \omega^2 \\ 2\omega^4 & 0 & 0 \end{pmatrix} \qquad \omega^*(\pi_D^*)^2 = \begin{pmatrix} 0 & 0 & \omega \\ 2\omega^2 & 0 & 0 \\ 0 & 2\omega^4 & 0 \end{pmatrix}$$

$$(\omega^*)^2 = \begin{pmatrix} \omega^2 & 0 & 0 \\ 0 & \omega^4 & 0 \\ 0 & 0 & \omega \end{pmatrix} \quad (\omega^*)^2\pi_D^* = \begin{pmatrix} 0 & \omega^2 & 0 \\ 0 & 0 & \omega^4 \\ 2\omega & 0 & 0 \end{pmatrix} \quad (\omega^*)^2(\pi_D^*)^2 = \begin{pmatrix} 0 & 0 & \omega^2 \\ 2\omega^4 & 0 & 0 \\ 0 & 2\omega & 0 \end{pmatrix}$$

We will make use of this construction in Chapter 3. In future, for ease of notation, we will identify ω and ω^*, and π and π^*.

2.5 Integer-Valued Polynomials over Matrix Rings

As in our prior discussion, if we denote by $M_n(\mathbb{Z})$ the ring of $n \times n$ matrices with integer entries, then we can denote by

$$\mathrm{Int}_{\mathbb{Q}}(M_n(\mathbb{Z})) = \{f \in \mathbb{Q}[x] : f(M) \in M_n(\mathbb{Z}) \text{ for all } M \in M_n(\mathbb{Z})\}$$

the set of rational polynomials mapping integer matrices to integer matrices. This is a $\mathbb{Z}$-module for which we have the inclusion

$$\mathbb{Z}[x] \subseteq \mathrm{Int}_{\mathbb{Q}}(M_n(\mathbb{Z})) \subseteq \mathrm{Int}(\mathbb{Z}) \ . \tag{2.4}$$

To justify the existence of a regular basis for $\mathrm{Int}_{\mathbb{Q}}(M_n(\mathbb{Z}))$, we require the following result:

Corollary 2.5.1 (II.1.6, [3])**.** Let B be a domain such that $D[x] \subseteq B \subseteq \mathrm{Int}(E, D)$ for some infinite fractional subset E of D. If D is a principal ideal domain, then B has a regular basis.

Since $\mathbb{Z}$ is a principal ideal domain, and is an infinite fractional subset of itself, we may conclude from this corollary and Equation 2.4 that $\mathrm{Int}_{\mathbb{Q}}(M_n(\mathbb{Z}))$ has a regular basis. Unlike for $\mathrm{Int}(\mathbb{Z})$, however, it turns out that this regular basis is not easy to describe using a formula in closed form. [6]

2.5.1 The integral closure of $\mathbf{Int}_{\mathbb{Q}}(M_n(\mathbb{Z}))$

Recall the following standard definition from abstract algebra:

Definition 2.5.2. Let A and B be commutative unital rings, and let A be a subring of B. The set of elements of B that are integral over A is called the *integral closure* of A in B.

In particular we will see that for our interests, the integral closure of $\mathrm{Int}_{\mathbb{Q}}(M_n(\mathbb{Z}))$, the set of all polynomials $f(x) \in \mathbb{Q}[x]$ which are integral over $\mathrm{Int}_{\mathbb{Q}}(M_n(\mathbb{Z}))$, is a very useful object. We can learn information about computing regular bases for both of these rings by making use of the following two results of Frisch, and Loper and Werner, respectively.

Theorem 2.5.3 ([7], Lemma 3.4)**.** Let $f(x) = \frac{g(x)}{c}$ with $g(x) \in \mathbb{Z}[x]$ and $c \in \mathbb{Z} \setminus \{0\}$. Then $f(x)$ maps $M_n(\mathbb{Z})$ to itself if and only if $g(x)$ is divisible modulo $c\mathbb{Z}[x]$ by all monic polynomials in $\mathbb{Z}[x]$ of degree n.

Theorem 2.5.4 ([13], 3.8 and 4.6)**.** Let $\mathfrak{O}_n$ denote the set of all algebraic integers in number fields $\mathbb{Q}(\theta)$ with $[\mathbb{Q}(\theta) : \mathbb{Q}] = n$. Then the integral closure of $\mathrm{Int}_{\mathbb{Q}}(M_n(\mathbb{Z}))$ is equal to

$$\bigcap_{\theta \in \mathfrak{O}_n} \mathrm{Int}_{\mathbb{Q}}(\mathcal{O}_\theta) \ ,$$

where $\mathcal{O}_\theta$ denotes the ring of algebraic integers in $\mathbb{Q}(\theta)$, and $\mathrm{Int}_{\mathbb{Q}}(\mathcal{O}_\theta)$ denotes the algebra of rational polynomials preserving $\mathcal{O}_\theta$.

To study the integral closure of $\mathrm{Int}_{\mathbb{Q}}(M_n(\mathbb{Z}))$ we would like to describe its localizations at rational primes, which can be done using the localizations of the algebras $\mathrm{Int}_{\mathbb{Q}}(\mathcal{O}_\theta)$ from Theorem 2.5.4. Loper and Werner [13] suggest that a basis for the integral closure of $\mathrm{Int}(M_n(\mathbb{Z}))$ can be found by computing $\mathrm{Int}_{\mathbb{Q}}(\mathcal{O}_\theta)_{(p)}$ for all possible $\mathcal{O}_\theta$ and a given rational prime p, and then intersect, but computing the intersection becomes complicated.

Another way by which we can study the integral closure of $\mathrm{Int}_{\mathbb{Q}}(M_n(\mathbb{Z}))$ is by using results about division algebras over local fields.

Theorem 2.5.5 (Embedding Theorem, in appendix of [16])**.** If D is a division algebra of degree n^2 over a local field K and F is a field extension of degree n of K, then F can be embedded as a maximal commutative subfield of D.

From this theorem, it follows that if R_n is the maximal order of D, then by inclusion $\mathrm{Int}_{\mathbb{Q}}(R_n)$ lies in the intersection of all the rings $\mathrm{Int}_{\mathbb{Q}}(\mathcal{O}_\theta)$ (since each $\mathbb{Q}(\theta)$ can be embedded as a maximal commutative subfield of D). The rings $\mathrm{Int}_{\mathbb{Q}}(R_n)$ and $\bigcap_{\theta \in \mathfrak{O}_n} \mathrm{Int}_{\mathbb{Q}}(\mathcal{O}_\theta)$ are, in fact, equal, and so constructing an R_n basis for $\mathrm{Int}_{\mathbb{Q}}(R_n)$ via p-orderings (see Section 2.5.2) will give the means to describe the integral closure of $\mathrm{Int}_{\mathbb{Q}}(M_n(\mathbb{Z}))$.

Let p be a fixed prime, let D be a division algebra of degree n^2 over K a local field, and let R_n denote the maximal order in D (see Section 2.4). In all applications, we will take $K = \mathbb{Q}_p$ the p-adic numbers, equipped with the usual p-adic valuation.

Proposition 2.5.6 ([13] 4.6, [6], 2.1)**.** The integral closure of $\mathrm{Int}_{\mathbb{Q}}(M_n(\mathbb{Z})_{(p)})$ is $\mathrm{Int}_{\mathbb{Q}}(R_n)$

Proof. Suppose $f \in \mathrm{Int}_{\mathbb{Q}}(R_n)$. Let F be a degree n extension of $\mathbb{Q}_p$, then by Theorem 2.5.5 F is a maximal commutative subfield of D, hence its ring $\mathcal{O}_F$ of algebraic

integers is a subring of the maximal order R_n. By restriction, $f \in \mathrm{Int}_{\mathbb{Q}}(\mathcal{O}_F)$ so by Theorem 2.5.4, f is in the integral closure of $\mathrm{Int}_{\mathbb{Q}}(M_n(\mathbb{Z}))$ and hence f is in the integral closure of $\mathrm{Int}_{\mathbb{Q}}(M_n(\mathbb{Z})_{(p)})$.

Conversely, suppose that $f \in \mathbb{Q}[x]$ and that $f \in \mathrm{Int}(\mathcal{O}_\theta)$ for all $\theta \in \mathfrak{O}_n$. Let $z \in R_n$. Then z is an integral element of $\mathbb{Q}_p(z)$ (by Theorem 2.4.2), a commutative subfield of D (by Theorem 2.5.5). Therefore $f(z) \in \mathcal{O}_z$ and so $f \in R_n$. □

Proposition 2.5.6 demonstrates that the problem of describing the integral closure of $\mathrm{Int}_{\mathbb{Q}}(M_n(\mathbb{Z})_{(p)})$ is exactly that of describing $\mathrm{Int}_{\mathbb{Q}}(R_n)$, so we move our attention towards studying integer-valued polynomials over maximal orders.

2.5.2 ν-orderings of subsets of maximal orders in division algebras

To describe $\mathrm{Int}_{\mathbb{Q}}(R_n)$, we establish results analogous to the p-orders of Section 2.1.1, extending to maximal orders of division algebras over a local field. While in the previous case we referred to p-orderings, since the p-adic valuation is a natural valuation defined over $\mathbb{Z}$, in a general local field we will consider an associated valuation ν, and hence may establish the definition of a ν-ordering.

Definition 2.5.7. ([11], 1.1) Let K be a local field with valuation ν, D be a division algebra over K to which ν extends, R the maximal order in D, and S a subset of R. Then a *ν-ordering* of S is a sequence $\{a_i : i = 0, 1, 2, \dots\} \subseteq S$ such that for each $k > 0$, the element a_k minimizes the quantity $\nu(f_k(a_0, \dots, a_{k-1})(a))$ over $a \in S$, where $f_k(a_0, \dots, a_{k-1})(x)$ is the minimal polynomial of the set $\{a_0, a_1, \dots, a_{k-1}\}$, with the convention that $f_0 = 1$. We call the sequence of valuations $\{\nu(f_k(a_0, \dots, a_{k-1})(a_k)) : k = 0, 1, \dots\}$ the *ν-sequence* of S.

Proposition 2.5.8 ([11], 1.2)**.** As in Definition 2.5.7, let K be a local field with valuation ν, D be a division algebra over K to which ν extends, R the maximal order in D, and S a subset of R. Additionally, let $\pi \in R$ be a uniformizing element, meaning an element for which $(\pi^n) = (p)$, let $\{a_i : i = 0, 1, 2, \dots\} \subseteq S$ be a ν-ordering, and let $f_k(a_0, \dots, a_{k-1})$ be the minimal polynomial of $\{a_0, a_1, \dots, a_{k-1}\}$. Then the sequence $\{\alpha_S(k) = \nu(f_k(a_0, \dots, a_{k-1})(a_k)) : k = 0, 1, 2, \dots\}$ depends only on the set S, and not on the choice of ν-ordering. The sequence of polynomials

$$\{\pi^{-\alpha_S(k)} f_k(a_0, \dots, a_{k-1})(x) : k = 0, 1, 2, \dots\}$$

forms a regular R-basis for the R-algebra of polynomials which are integer-valued on S.

To utilize Proposition 2.5.8, we first need to be able to construct a ν-ordering of our maximal order R_n. A recursive method for constructing ν-orderings for elements of a maximal order is based on two lemmas.

Lemma 2.5.9 (see [11], 6.2)**.** Let $\{a_i : i = 0, 1, 2, \dots\}$ be a ν-ordering of a subset S of R with associated ν-sequence $\{\alpha_S(i) : i = 0, 1, 2, \dots\}$ and let b be an element in the centre of R. Then:

i) $\{a_i + b : i = 0, 1, 2, \dots\}$ is a ν-ordering of $S + b$, and the ν-sequence of $S + b$ is the same as that of S

ii) If p is the characteristic of the residue field of K (so that $(p) = (\pi)^n$ in R), then $\{pa_i : i = 0, 1, 2, \dots\}$ is a ν-ordering for pS and the ν-sequence of pS is $\{\alpha_S(i) + in : i = 0, 1, 2, \dots\}$

Definition 2.5.10. The *shuffle* of two nondecreasing sequences of integers is their disjoint union sorted into nondecreasing order. If the sequences are $\{b_i\}$ and $\{c_i\}$, their shuffle is denoted $\{b_i\} \wedge \{c_i\}$.

Lemma 2.5.11 ([11], 5.2)**.** Let S_1 and S_2 be disjoint subsets of S with the property that there is a non-negative integer k such that $\nu(s_1 - s_2) = k$ for any $s_1 \in S_1$ and $s_2 \in S_2$, and that S_1 and S_2 are each closed with respect to conjugation by elements of R, by which we mean $rsr^{-1} \in S_1$ for all $r \in R$ and $s \in S_1$, and respectively for S_2. If $\{a_i\}$ is a ν-ordering of $S_1 \cup S_2$ then the subsequence of this ordering consisting of those elements in S_1 is a ν-ordering of S_1 and similarly for S_2.

Conversely, if $\{b_i\}$ and $\{c_i\}$ are ν-orderings of S_1 and S_2 respectively with associated ν-sequence $\{\alpha_{S_1}(i)\}$ and $\{\alpha_{S_2}(i)\}$, then the ν-sequence of $S_1 \cup S_2$ is the sum of the linear sequence $\{ki : i = 0, 1, 2, \dots\}$ with the shuffle $\{\alpha_{S_1}(i) - ki\} \wedge \{\alpha_{S_2}(i) - ki\}$, and this shuffle applied to $\{b_i\}$ and $\{c_i\}$ gives a ν-ordering of $S_1 \cup S_2$.

As the linear sequence mentioned in the above Lemma will come up many times in this document, we formalize its notation here:

Definition 2.5.12. The sequence (kn) denotes the linear sequence $\{kn : n = 0, 1, 2, \dots\}$, whose n^{th} term is kn.

The case where $n = 2$, in which D is a division algebra of degree 4, has been described for the case where $p = 2$ in [11] and extended to the case where p is an odd prime in [6]. As all results extend to the latter case, we will describe the results as given in [6].

2.5.3 Constructing a ν-order for R_2

Using the construction described in Section 2.4.2, we can build the division algebra D_2 and hence the maximal order R_2, and decompose R_2 into a disjoint union of subsets to which Lemma 2.5.11 applies.

Let $K = \mathbb{Q}_p$ the p-adic numbers, let ω be a primitive $(p^2-1)^{\text{th}}$ root of unity, and let $W = \mathbb{Q}_p(\omega)$, an unramified extension of $\mathbb{Q}_p$ of degree 2. Let θ be the automorphism of W for which $\theta(\omega) = \omega^p$, and let π be a uniformizing element of R_2, so that $(\pi^2) = (p)$. Commutativity relations within D_2 are determined by $\pi\omega\pi^{-1} = \omega^p$ (or $\pi\omega = \omega^p\pi$), and an element $z \in D_2$ can be expressed uniquely in the form $z = \alpha_0 + \alpha_1\pi$ with $\alpha_0, \alpha_1 \in W$. R_2 consists of those elements z for which α_0, α_1 are integers in W, so that $\nu(\alpha_0), \nu(\alpha_1) \geq 0$.

With this presentation, the trace and norm of an element $z \in D_2$ are given by

$$Tr(z) = \alpha_0 + \theta(\alpha_0) \qquad\qquad N(z) = \alpha_0\theta(\alpha_0) - \alpha_1\theta(\alpha_1)p \ .$$

The characteristic polynomial for z is given by $ch_z(x) = x^2 - T(z)x + N(z)$.

The ideal (π) in R_2 is a two-sided prime ideal, and $z \in R_2$ is in (π) if and only if $N(z) \equiv 0 \pmod{p}$. We have $R_2/(\pi) \cong \mathbb{F}_{p^2}$, and the powers of ω provide a set of representatives for the nonzero residue classes mod π. In particular powers of ω^{p+1} gives representatives of the residue classes of the subfield $\mathbb{F}_p$.

We can decompose R_2 into the following sets:

Definition 2.5.13 ([6], 2.6)**.**

i) Let $S_0 = \{z \in R_2 : z \equiv 0 \pmod{\pi}\}$.

ii) For $i = 1, 2, \ldots, p-1$, let $S_i = S_0 + i$. Note that each $1 \leq i \leq p-1$ is an element of the centre of R_2 and so this addition makes sense.

iii) For $a, b \in \mathbb{F}_p$ such that $x^2 - ax + b$ is irreducible in $\mathbb{F}_p[x]$, let $S_{a,b} = \{z \in R_2 : Tr(z) \equiv a \pmod{p}, N(z) \equiv b \pmod{p}\}$.

With these sets S_i and $S_{a,b}$ defined, we have the following result.

Lemma 2.5.14 ([6], 2.7)**.**

i) If $z \in S_i$, then $ch_z(x) \equiv (x-i)^2 \pmod{p}$.

ii) If $z \in S_{a,b}$, then $ch_z(x) \equiv x^2 - ax + b \pmod{p}$.

iii) There are $(p^2-p)/2$ distinct sets $S_{a,b}$.

iv) Each of the sets S_i, $S_{a,b}$ is closed with respect to conjugation by elements of R_2.

v) The disjoint union of all S_i and $S_{a,b}$ is equal to R_2.

Proof.

i) If $z \in S_0$, then $z^2 \equiv 0 \pmod{\pi^2}$, so z is a root of the polynomial x^2 modulo $\pi^2 = p$. The same argument applied to $z - i$ demonstrates that if $z \in S_i$, then z is a root of $(x-i)^2$ modulo $\pi^2 = p$.

ii) Follows from the definition of a characteristic polynomial.

iii) Follows from a well-known formula for the number of irreducible quadratics modulo p.

iv) Follows from Dickson's Theorem (Theorem 2.3.6), which states that conjugate elements share a characteristic polynomial.

v) Is implied by the uniqueness of the characteristic polynomial.

□

By the results of Lemma 2.5.14, the sets S_i, $S_{a,b}$ satisfy the hypotheses of Lemma 2.5.11, and therefore it suffices to find the ν-orderings for each separately. We do this for each set $S_{a,b}$ in Proposition 2.5.20. Each of the sets S_i for $i = 1, 2, \ldots, p-1$ is a translate of S_0 by elements in the centre of R_2, so by Lemma 2.5.9 it suffices to just order S_0. We further decompose the set S_0 to aid in finding the ν-ordering.

Definition 2.5.15 ([6], 2.8)**.** For $i = 0, \ldots, p-1$, let $T_i = \{z \in R_2 : N(z) \equiv ip \pmod{p^2}\}$.

Lemma 2.5.16 ([6], 2.9)**.**

i) Each element of S_0 is in exactly one of the sets T_i.

ii) Each set T_i is closed with respect to conjugation by elements of R_2.

iii) If $z \in T_i$, $w \in T_j$ with $i \neq j$, then $\nu(z - w) = 1$.

iv) For each $z \in T_i$ with $i \neq 0$, the characteristic polynomial $C_z(x) \equiv x^2 - jpx + ip \pmod{p^2}$ for some j.

v) $T_0 = pR$.

Proof.

i) Follows from the definition of the sets T_i.

ii) Follows from the multiplicativity of the norm.

iii) Since $z, w \in S_0$ we know that $\nu(z-w) \geq 1$. If we had $\nu(z-w) > 1$, then z and w would be in the same residue class modulo π^2, in which case their norms would be congruent modulo p^2. Therefore we must have $\nu(z-w) = 1$.

iv) Follows from the definition of T_i along with the fact that $Tr(z) \equiv 0 \pmod{p}$ for $z \in S_0$.

v) We have $T_0 = \{z \in R_2 : N(z) \equiv 0 \pmod{p^2}\}$, so $z \in T_0$ if and only if z is divisible by $\pi^2 = p$ in R_2, and since p is in the centre of R_2, the result follows.

□

Between Lemmas 2.5.16 and 2.5.11, we know that we can express a ν-ordering for S_0 as a shuffle of those for the sets T_i with $i > 0$ and the set T_0. Note that by Lemmas 2.5.9 and 2.5.16 v), we can express the ν-ordering of T_0 in terms of that of R_2.

The decomposition of R_2 into a disjoint union of sets $S_{a,b}$ and T_i, $i > 0$, combined with the results of Lemmas 2.5.9 and 2.5.11, yield a recursive formula for a ν-ordering of R_2.

It is shown in Proposition 2.5.20 that all the ν-sequences for the sets $S_{a,b}$ are the same, and likewise for the T_is with $i > 0$. We denote these ν-sequences by α_S and α_T, respectively, and recall the notation for a linear sequence given in Definition 2.5.12. This gives us the following result.

Proposition 2.5.17 ([6] 2.10)**.** The ν-sequence of R_2, denoted α_R, satisfies and is determined by the formula

$$\alpha_R = [[(\alpha_R + (n)) \wedge (\alpha_T - (n))^{\wedge p-1}] + (n)]^{\wedge p} \wedge (\alpha_S^{\wedge (p^2-p)/2}) \tag{2.5}$$

Given the ν-sequences α_S and α_T, Equation (2.5) uniquely determines $\alpha_R(n)$ for all n. It now remains to compute the ν-sequences and ν-orderings for the sets $S_{a,b}$ and T_i. The method from [6] given below for p a prime in general is an extension of the $p = 2$ case given in [11].

Definition 2.5.18 ([6], 2.11)**.**

i) Let $a, b \in \mathbb{F}_p$ be given and let $n = \sum_{i\geq 0} n_i p^i$ be the expansion of n in base p. Define the map

$$\phi = (\phi_1, \phi_2) : \mathbb{Z}^{\geq 0} \to (a + p\mathbb{Z}^{\geq 0}) \times (b + p\mathbb{Z}^{\geq 0})$$
$$\phi(n) = \left(a + p\sum_{i\geq 0} n_{2i} p^i,\ b + p\sum_{i\geq 0} n_{2i+1} p^i \right)$$

Additionally, let the polynomial $f_n(x)$ be defined by

$$f_n(x) = \prod_{i=0}^{n-1} (x^2 - \phi_1(i)x + \phi_2(i)) \ .$$

ii) Let $0 < j < p$ be given and let $n = \sum_{i\geq 0} n_i p^i$ be the expansion of n in base p. Define the map

$$\psi = (\psi_1, \psi_2) : \mathbb{Z}^{\geq 0} \to (p\mathbb{Z}^{\geq 0}) \times (jp + p^2\mathbb{Z}^{\geq 0})$$
$$\psi(n) = \left(p\sum_{i\geq 0} n_{2i} p^i,\ jp + p^2\sum_{i\geq 0} n_{2i+1} p^i \right)$$

Additionally, let the polynomial $g_n(x)$ be defined by

$$g_n(x) = \prod_{i=0}^{n-1} (x^2 - \psi_1(i)x + \psi_2(i)) \ .$$

Note. To remain consistent with [6], here we have ordered our component polynomials ϕ and ψ so that ϕ_2, ψ_2 correspond to the constant terms of quadratic polynomials in f_n and g_n. For ease of notation in future chapters, we will let the polynomial component ϕ_i denote the coefficient of x^i.

Lemma 2.5.19 ([6], 2.12)**.**

i) If $z \in S_{a,b}$ then $\nu(f_n(z)) \geq 2n + 2\sum_{k>0} \left\lfloor \frac{n}{p^{2k}} \right\rfloor$ with equality if $Tr(z) = \phi_1(n)$ and $N(z) = \phi_2(n)$.

ii) If $z \in T_j$ for $j > 0$ then $\nu(g_n(z)) \geq 3n + \sum_{k>0} \left\lfloor \frac{n}{p^k} \right\rfloor$ with equality if $Tr(z) = \psi_1(n)$ and $N(z) = \psi_2(n)$.

The proof of Lemma 2.5.19 is omitted from this section as a similar computation is presented in Section 3.3 for the case of 3×3 matrices.

From the embedding theorem (Theorem 2.5.5), for any choice of n there are elements $a_n, b_n \in R_2$ that are roots of the polynomials $x^2 - \phi_1(n)x + \phi_2(n)$ and $x^2 - \psi_1(n)x + \psi_2(n)$, respectively. The definition of f_n and g_n given in Definition 2.5.18 imply that $f_{2n}(x)$ is the minimal polynomial of the set

$$\{a_0, \theta(a_0), a_1, \theta(a_1), \ldots, a_n, \theta(a_n)\}$$

while $g_n(x)$ is the minimal polynomial of

$$\{b_0, \theta(b_0), b_1, \theta(b_1), \ldots, b_n, \theta(b_n)\} \ .$$

This result suggests that

Proposition 2.5.20 ([6], 2.13)**.**

i) The sequence $\{a_0, \theta(a_0), a_1, \theta(a_1), \ldots\}$ is a ν-ordering of $S_{a,b}$ and the associated ν-sequence is

$$\alpha_S(2n) = \alpha_S(2n+1) = 2n + 2\sum_{k>0} \left\lfloor \frac{n}{p^{2k}} \right\rfloor \ .$$

ii) The sequence $\{b_0, \theta(b_0), b_1, \theta(b_1), \ldots\}$ is a ν-ordering of T_j and the associated ν-sequence is

$$\alpha_T(2n) = \alpha_T(2n+1) - 1 = 3n + \sum_{k>0} \left\lfloor \frac{n}{p^k} \right\rfloor \ .$$

Corollary 2.5.21 (to Prop 2.5.20, see [6], 2.14)**.**

i) The sequence of polynomials

$$\{\pi^{-\alpha_S(2n)} f_n(x),\ \pi^{-\alpha_S(2n+1)} x f_n(x) : n = 0, 1, 2, \ldots\}$$

forms a regular R_2-basis for $\mathrm{Int}(S_{a,b})$.

ii) The sequence of polynomials

$$\{\pi^{-\alpha_T(2n)} g_n(x),\ \pi^{-\alpha_T(2n+1)} x g_n(x) : n = 0, 1, 2, \ldots\}$$

forms a regular R_2-basis for $\mathrm{Int}(T_j)$.

We have now established that the ring of integer-valued polynomials of each component in our disjoint union characterizing R_2 has a regular basis, and we would like to put these together to obtain a regular R_2-basis for $\mathrm{Int}_{\mathbb{Q}}(R_2)$ itself. The following lemma provides the means of doing so with basis elements of a convenient form.

Lemma 2.5.22 ([6], 2.15)**.** If two subsets of R_2 satisfying the hypotheses of Lemma 2.5.11 each has a regular basis whose elements are each quotients of polynomials in $\mathbb{Z}[x]$ by powers of π, then their union also has a regular basis of this form.

Proof. Let $\{\pi^{-\alpha_1(n)}h_n(x) : n = 0, 1, 2 \dots\}$ and $\{\pi^{-\alpha_2(n)}k_n(x) : n = 0, 1, 2 \dots\}$ be the two bases in question, with $h_n(x), k_n(x) \in \mathbb{Z}[x]$. Since by assumption the sets satisfy the hypotheses of Lemma 2.5.11, we already know that the ν-sequence α of their union is the shuffle of the sequences α_1 and α_2.

For each n, there is a pair of integers ℓ and m such that $\ell + m = n$, and either

$$\alpha(n) = \alpha_1(\ell) \text{ and } \alpha(n) \geq \alpha_2(m) \qquad \text{or} \qquad \alpha(n) = \alpha_1(m) \text{ and } \alpha(n) \geq \alpha_2(\ell)$$

or both. This implies that $\pi^{-\alpha(n)}h_\ell(x)k_m(x)$ is a polynomial of degree n which is R_2-valued on the union of the two sets, and has the same denominator as the polynomial of degree n in a regular basis for the ring of polynomials that are R_2-valued on the union. By choosing one of these polynomials for each degree n, we obtain a regular basis of the desired form. □

Since each of the polynomials $f_n(x), g_n(x)$ have integer coefficients, we can apply Lemma 2.5.22 to our maximal order to obtain:

Corollary 2.5.23 ([6], 2.16)**.** $\mathrm{Int}(R_2)$ has a regular basis whose elements are each a quotient of a polynomial in $\mathbb{Z}[x]$ by a power of π.

Corollary 2.5.24 ([6], 2.17)**.** The p-sequence of $\mathrm{Int}_{\mathbb{Q}}(R_2)$ is $\{\lfloor \alpha_{R_2}(n)/2 \rfloor : n = 0, 1, 2, \dots\}$.

2.5.4 Valuative capacity

One thing that is of interest to describe is the asymptotic behaviour of a ν-sequence $\alpha(n)$.

Definition 2.5.25 ([5], §4)**.** The *valuative capacity* of a set S is described by

$$\lim_{n\to\infty} \frac{\alpha_S(n)}{n}$$

if this limit exists, where $\alpha_S(n)$ is the characteristic sequence of S.

Proposition 2.5.26 ([10], Prop 7)**.** If α, β are nondecreasing unbounded sequences with

$$\lim_{n\to\infty} \frac{\alpha(n)}{n} = a > 0 \qquad \text{and} \qquad \lim_{n\to\infty} \frac{\beta(n)}{n} = b > 0$$

then

$$\lim_{n\to\infty} \frac{(\alpha \wedge \beta)(n)}{n} = \left(a^{-1} + b^{-1}\right)^{-1} .$$

Continuing the example given for R_2 over $\mathbb{Q}_p$ from earlier in this section, we obtain the following result for the valuative capacity of R_2.

Proposition 2.5.27. The valuative capacity of R_2 over $\mathbb{Q}_p$ is given by

$$\lim_{n\to\infty} \frac{\alpha_{R_2}(n)}{n} = \frac{2}{p^2 + p - 2} .$$

Proof. Since we have

$$\alpha_{R_2} = [[(\alpha_{R_2} + (n)) \wedge (\alpha_T - (n))^{\wedge p-1}] + (n)]^{\wedge p} \wedge \left(\alpha_S^{\wedge (p^2-p)/2}\right) ,$$

we see from Proposition 2.5.26 that

$$\lim_{n\to\infty} \frac{\alpha_{R_2}(n)}{n} = \cfrac{1}{\cfrac{(p^2-p)/2}{\lim_{n\to\infty} \frac{\alpha_S(n)}{n}} + \cfrac{p}{1 + \cfrac{1}{\cfrac{p-1}{\lim_{n\to\infty} \frac{\alpha_T(n)}{(n)} - 1} + \cfrac{1}{\lim_{n\to\infty} \frac{\alpha_{R_2}(n)}{n} + 1}}}} .$$

Since

$$\alpha_S(2n) = \alpha_S(2n+1) = 2n + 2\sum_{k>0} \left\lfloor \frac{n}{p^{2k}} \right\rfloor$$
$$\alpha_T(2n) = \alpha_T(2n+1) - 1 = 3n + \sum_{k>0} \left\lfloor \frac{n}{p^k} \right\rfloor$$

it can be directly computed that

$$\lim_{n\to\infty} \frac{\alpha_S(n)}{n} = \frac{p^2}{p^2-1} \qquad \text{and} \qquad \lim_{n\to\infty} \frac{\alpha_T(n)}{n} = \frac{3}{2} + \frac{1}{2(p-1)} ,$$

from which it becomes clear that the valuative capacity of R_2 is the positive solution to the quadratic equation

$$x = \cfrac{1}{\cfrac{(p^2-p)/2}{p^2/(p^2-1)} + \cfrac{p}{1 + \cfrac{1}{\cfrac{p-1}{1/2+1/2(p-1)} + \cfrac{1}{x+1}}}}$$

$$= \cfrac{1}{\cfrac{(p+1)(p-1)^2}{2p} + \cfrac{p}{1 + \cfrac{1}{\cfrac{2(p-1)^2}{p} + \cfrac{1}{x+1}}}}$$

from which we obtain

$$\lim_{n\to\infty} \frac{\alpha_{R_2}(n)}{n} = \frac{2}{p^2+p-2} \ .$$

□

Chapter 3

The Index 3, 2-local Case

3.1 Notation

We are working within the division algebra D_3 and its maximal order Δ_3, represented as subsets of the 3×3 matrices as described in Section 2.4.3:

$$D_3 = \mathbb{Q}_2[\omega, \pi] \qquad \Delta_3 = \mathbb{Z}_2[\omega, \pi]$$

where $\mathbb{Q}_2, \mathbb{Z}_2$ denote the 2-adic numbers and integers, respectively, and

$$\omega = \begin{pmatrix} \zeta_7 & 0 & 0 \\ 0 & \zeta_7^2 & 0 \\ 0 & 0 & \zeta_7^4 \end{pmatrix} \qquad \pi = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 2 & 0 & 0 \end{pmatrix}$$

with ζ_7 a primitive 7^{th} root of unity. Note that we have the relations $\pi^3 = 2I_3$ and $\pi \cdot \omega \cdot \pi^{-1} = \omega^2$, and also a valuation ν in Δ_3 described by $\nu(z) = \nu_2(\det(z))$ for $z \in \Delta_3$ realized as a matrix, where ν_2 denotes the 2-adic valuation.

3.2 Subsets Closed Under Conjugation in Δ_3

3.2.1 Conjugacy classes of Δ_3 modulo π

Each element in Δ_3 is expressible as a $\mathbb{Z}_2$-linear combination of the nine elements $\{\omega^i \cdot \pi^j : 0 \leq i, j \leq 2\}$. The quotient $\Delta_3/(\pi)$ is isomorphic to the finite field $\mathbb{F}_{2^3} = \mathbb{F}_8$ with nonzero residue classes modulo π represented by powers of ω. We would like to decompose Δ_3 using the conjugacy classes of Δ_3 modulo π, and denote these classes as follows:

Definition 3.2.1. Define the sets

$$\begin{aligned} T &= \{z \in \Delta_3 : z \equiv 0 \pmod{\pi}\} = \pi\Delta \\ T+1 &= \{z \in \Delta_3 : z \equiv I_3 \pmod{\pi}\} \\ S &= \{z \in \Delta_3 : z \equiv \omega \text{ or } \omega^2 \text{ or } \omega^4 \pmod{\pi}\} \\ S+1 &= \{z \in \Delta_3 : z \equiv \omega^3 \text{ or } \omega^6 \text{ or } \omega^5 \pmod{\pi}\} \\ &= \{z \in \Delta_3 : z \equiv \omega + I_3 \text{ or } \omega^2 + I_3 \text{ or } \omega^4 + I_3 \pmod{\pi}\} . \end{aligned}$$

Lemma 3.2.2.

i) If $z \in T$, then the characteristic polynomial of z is congruent to $x^3 \pmod 2$.

ii) If $z \in T+1$, then the characteristic polynomial of z is congruent to $(x-1)^3 \pmod 2$.

iii) if $z \in S$, then the characteristic polynomial of z is congruent to $x^3 + x + 1 \pmod 2$.

iv) if $z \in S+1$, then the characteristic polynomial of z is congruent to $x^3 + x^2 + 1 \pmod 2$.

v) Each of the sets $T, T+1, S, S+1$ is closed with respect to conjugation by elements of Δ_3, where "a conjugated by b" is the element bab^{-1}.

vi) Each element of Δ_3 lies in exactly one of the sets $T, T+1, S, S+1$, so that their disjoint union is all of Δ_3.

vii) If $z, w \in \Delta_3$ are not both simultaneously in one of T, $T+1$, S, or $S+1$, then $\nu(z-w) = 0$.

Proof.

i) If $z \in T$, then $z^3 \equiv 0 \pmod{\pi^3}$ so $z^3 \equiv 0 \pmod 2$, and hence z is a root of $x^3 \pmod 2$.

ii) If $z \in T+1$, then $(z - I_3)^3 \equiv 0 \pmod{\pi^3}$ so $(z-I_3)^3 \equiv 0 \pmod 2$, and hence z is a root of $(x-1)^3 \pmod 2$.

iii) When viewed as a matrix, ω has characteristic polynomial $x^3 + x + 1 \pmod 2$. As it is a diagonal matrix, it is easily seen that ω has the same eigenvalues as ω^2 and ω^4, so all three elements of Δ_3 have the same characteristic polynomial.

If instead $z \equiv \omega, \omega^2$, or $\omega^4 \pmod{\pi}$ then z is still a root of the polynomial $x^3 + x + 1 \pmod 2$. Since this is an irreducible cubic polynomial, we can be certain that this is actually the characteristic polynomial of z.

iv) When viewed as a matrix, $\omega + I_3$ has characteristic polynomial $x^3 + x^2 + 1 \pmod 2$. This matrix is diagonal and it is easily seen that $\omega^2 + I_3$ and $\omega^4 + I_3$ have the same entries as $\omega + I_3$, only permuted, and hence all three elements of Δ_3 have the same characteristic polynomial. If instead $z \equiv \omega + I_3, \omega^2 + I_3$, or $\omega^4 + I_3 \pmod{\pi}$ then z is still a root of the polynomial $x^3 + x^2 + 1 \pmod 2$. Since this is an irreducible cubic polynomial, we can be certain that this is actually the characteristic polynomial of z.

v) This follows from Dickson's Theorem (Theorem 2.3.6).

vi) It is easy to see, since all nonzero residue classes of $\Delta_3 \pmod{\pi}$ are represented by powers of ω, that $T \cup (T+1) \cup S \cup (S+1) = \Delta_3$. The fact that each element of Δ_3 lies in exactly one of these four sets follows by the uniqueness of the characteristic polynomial.

vii) If z, w are in different sets $T, T+1, S, S+1$, then z and w are by definition in different residue classes modulo π. Therefore $z - w \not\equiv 0 \pmod{\pi}$ and hence $\nu(z - w) = 0$ for all choices of $z, w \in \Delta_3$ such that z and w are not in the same subset of Δ_3 given in Definition 3.2.1.

□

Knowing this decomposition of Δ_3 into the union of disjoint sets, we can apply Lemma 2.5.11 to determine a recursive definition for the ν-ordering of Δ_3. Also by Lemma 2.5.9, we need only concern ourselves with the ν-sequences of the sets T and S, as $T+1$ and $S+1$ are simply translates, under which ν-sequences are invariant. However, we can further decompose Δ_3 by examining the subsets closed under conjugation modulo higher powers of π within the set T.

3.2.2 Decomposition of T

Definition 3.2.3. Let

$$T_1 = \{z \in \Delta_3 : z \equiv 0 \pmod{\pi^2}\} = \pi^2 \Delta$$
$$T_2 = \{z \in \Delta_3 : z \equiv \omega^i \pi \pmod{\pi^2} \text{ for some } 0 \leq i \leq 6\}$$

Lemma 3.2.4.

i) Every element in T is in exactly one of T_1 and T_2.

ii) Each of T_1 and T_2 is closed with respect to conjugation by elements of Δ_3.

iii) If $z \in T_1$ and $w \in T_2$, then $\nu(z - w) = 1$.

Proof.

i) As all $z \in T$ are such that $z \equiv 0 \pmod{\pi}$, the fact that either $z \in T_1$ or $z \in T_2$ follows from the definition of these sets.

ii) The fact that T_1 is closed under conjugation is clear from its definition. In the case of T_2, we can write any element of Δ as a linear combination of the elements $\omega^k \pi^\ell$ with $0 \leq k \leq 6$, $0 \leq \pi \leq 2$. Using the known relations between ω and π, it follows that conjugating $\pi \in \Delta_3$ by an arbitrary element $\omega^k \pi^\ell$ of Δ_3 gives $\omega^k \pi^\ell \cdot \pi \cdot \pi^{-\ell} \omega^{-k} = \omega^{7-k} \pi$. Thus every element $\omega^i \pi$ is in the same orbit as π under the action of conjugation, hence T_2 is closed under conjugation by elements of Δ_3.

iii) If $z \in T_1$ and $w \in T_2$ then $z - w \equiv \omega^i \pi \pmod{\pi^2}$ for some $0 \leq i \leq 6$. Therefore $\nu(z - w) = \nu(\omega^i \pi) = 1$ for any choice of $z \in T_1$ and $w \in T_2$.

□

We can, in fact, break the set T_1 into components even further.

Definition 3.2.5. Let

$$T_3 = \{z \in \Delta_3 : z \equiv 0 \pmod{\pi^3}\} = 2\Delta_3$$
$$T_4 = \{z \in \Delta_3 : z \equiv \omega^i \pi^2 \pmod{\pi^3} \text{ for some } 0 \leq i \leq 6\}$$

Lemma 3.2.6.

i) Every element of T_1 is in exactly one of T_3 and T_4.

ii) Each of T_3 and T_4 is closed with respect to conjugation by elements of Δ_3.

iii) If $z \in T_3$ and $w \in T_4$, then $\nu(z - w) = 2$.

Proof.

i) As all $z \in T_1$ are such that $z \equiv 0 \pmod{\pi^2}$, the fact that either $z \in T_3$ or $z \in T_4$ follows from the definition of these sets.

ii) The fact that T_3 is closed under conjugation is clear from its definition. In the case of T_4, we can write any element of Δ_3 as a linear combination of the elements $\omega^k\pi^\ell$ with $0 \leq k \leq 6$, $0 \leq \pi \leq 2$. Using the known relations between ω and π, it follows that conjugating $\pi^2 \in \Delta_3$ by an arbitrary element $\omega^k\pi^\ell$ of Δ_3 gives $\omega^k\pi^\ell \cdot \pi^2 \cdot \pi^{-\ell}\omega^{-k} = \omega^{4k}\pi^2$. Since the equation $4k \equiv n \pmod{7}$ has a solution for every $n \in \mathbb{Z}/(7)$, it follows that every element $\omega^i\pi^2$ is in the same orbit as π^2 under the action of conjugation, hence T_4 is closed under conjugation by elements of Δ_3.

iii) If $z \in T_3$ and $w \in T_4$, then $z - w \equiv \omega^i\pi^2 \pmod{\pi^3}$ for some $0 \leq i \leq 6$. Therefore $\nu(z - w) = \nu(\omega^i\pi^2) = 2$ for any choice of $z \in T_3$ and $w \in T_4$.

□

From this analysis, it follows that

$$\begin{aligned} T &= T_1 \cup T_2 \\ &= (T_3 \cup T_4) \cup T_2 \\ &= 2\Delta_3 \cup T_4 \cup T_2 \end{aligned}$$

with all unions disjoint, and with all sets fulfilling the conditions of Lemma 2.5.11. The decomposition of Δ_3 into sets is demonstrated graphically in Figure 3.1. By Lemma 2.5.9, the ν-sequence of $T_3 = 2\Delta_3$ can be written in terms of the ν-sequence for Δ_3, which provides the eventual recursive definition of α_{Δ_3} we seek, given in Proposition 3.2.7. Thus, to define the ν-sequence of T, it is sufficient to determine the ν-sequences of T_2 and T_4.

3.2.3 The ν-sequence of Δ_3

From the description of the decomposition of Δ_3 into appropriate disjoint sets as in Section 3.2.2, coupled with the results of Lemmas 2.5.9 and 2.5.11, we obtain the following result.

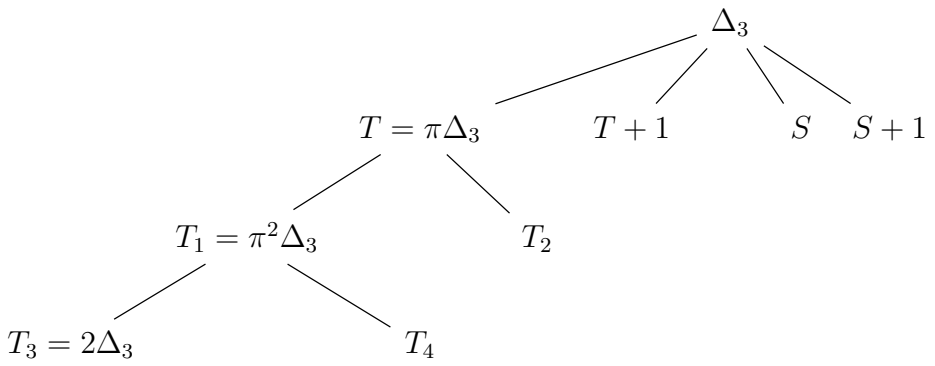

Figure 3.1: Tree summarizing decomposition of Δ_3.

Proposition 3.2.7. The ν-sequence of Δ_3, denoted α_{Δ_3}, satisfies and is determined by the formula

$$\alpha_{\Delta_3} = \Big(\big[([(\alpha_{\Delta_3} + (n)) \wedge (\alpha_{T_4} - (2n))] + (n)) \wedge (\alpha_{T_2} - (n))\big] + (n)\Big)^{\wedge 2} \wedge (\alpha_S)^{\wedge 2} \ ,$$

where (kn) denotes the linear sequence whose n^{th} term is kn.

Proof. This formula follows from Lemmas 2.5.9, 2.5.11, 3.2.2, 3.2.4, and 3.2.6.

Since $T_3 = 2\Delta_3$, we have $\alpha_{T_3} = \alpha_{\Delta_3} + (3n)$. We then know that

$$\begin{aligned} \alpha_{T_1} &= [(\alpha_{\Delta_3} + (3n) - (2n)) \wedge (\alpha_{T_4} - (2n))] + (2n) \\ &= [(\alpha_{\Delta_3} + (n)) \wedge (\alpha_{T_4} - (2n))] + (2n) \end{aligned}$$

and therefore

$$\begin{aligned} \alpha_T &= [(\alpha_{T_1} - (n)) \wedge (\alpha_{T_2} - (n))] + (n) \\ &= [([(\alpha_{\Delta_3} + (n)) \wedge (\alpha_{T_4} - (2n))] + (2n) - (n)) \wedge (\alpha_{T_2} - (n))] + (n) \\ &= [([(\alpha_{\Delta_3} + (n)) \wedge (\alpha_{T_4} - (2n))] + (n)) \wedge (\alpha_{T_2} - (n))] + (n) \ . \end{aligned}$$

We know that $T + 1$ is a translate of T and $S + 1$ of S, so that $\alpha_T = \alpha_{T+1}$ and $\alpha_S = \alpha_{S+1}$. Therefore

$$\begin{aligned} \alpha_{\Delta_3} &= \alpha_T \wedge \alpha_{T+1} \wedge \alpha_S \wedge \alpha_{S+1} \\ &= (\alpha_T^{\wedge 2}) \wedge (\alpha_S^{\wedge 2}) \\ &= ([([(\alpha_{\Delta_3} + (n)) \wedge (\alpha_{T_4} - (2n))] + (n)) \wedge (\alpha_{T_2} - (n))] + (n))^{\wedge 2} \wedge (\alpha_S)^{\wedge 2} \end{aligned}$$

as claimed. □

Once we have determined the ν-sequences for S, T_2, and T_4, this formula will uniquely determine $\alpha_{\Delta_3}(i)$ for all i. For every $i > 0$, the i^{th} term on the right-hand side consists of terms from α_S, α_{T_2}, and α_{T_4}, and also terms $\alpha_{\Delta_3}(j)$ for some $j < i$. As the first term of any ν-sequence is always 0, this formula gives an expression of α_{Δ_3} for all i.

3.2.4 Characteristic polynomials of subsets of Δ_3

We would like to be able to completely describe the subsets of Δ_3 in terms of the 2-adic valuation of coefficients in their characteristic polynomials. First, we show that these polynomials are irreducible.

Lemma 3.2.8. Let $z \in \Delta_3$ be a non-constant element. The characteristic polynomial of z is irreducible over $\mathbb{Q}_2$.

Proof. Since $z \in \Delta_3 \subseteq \mathbb{Q}_2[\omega, \pi]$ then $\mathbb{Q}_2 \leq \mathbb{Q}_2[z] \leq \mathbb{Q}_2[\omega, \pi]$ as field extensions. The characteristic polynomial of $z \in \Delta_3$ over $\mathbb{Q}_2$ has degree 3, so $[\mathbb{Q}_2[z] : \mathbb{Q}_2] \leq 3$. Since $[\mathbb{Q}_2[z] : \mathbb{Q}_2]$ divides $[\mathbb{Q}_2[\omega, \pi] : \mathbb{Q}_2] = 9$ we therefore have $[\mathbb{Q}_2[z] : \mathbb{Q}_2] = 3$ or $[\mathbb{Q}_2[z] : \mathbb{Q}_2] = 1$. Since z is non-constant, $z \notin \mathbb{Q}_2$ and thus $[\mathbb{Q}_2[z] : \mathbb{Q}_2] = 3$. Since this is equal to the degree of the characteristic polynomial of z, it is therefore the minimal polynomial of z over $\mathbb{Q}_2$ and hence is irreducible. □

The fact that characteristic polynomials of non-constant elements of Δ_3 are irreducible allows us to make use of the following result, which has been restated for the degree 3 case with the convention of writing general polynomials as $f(x) = \sum_{i=0}^{n} a_i x^i$.

Lemma 3.2.9 ([14], 12.9 restated)**.** Let $f(x) = a_0 + a_1 x + a_2 x^2 + x^3 \in K[x]$ be irreducible. Then

$$\nu(a_j) \geq \frac{3-j}{3}\nu(a_0) \ , \qquad 0 \leq j \leq 2 \ .$$

This lemma does not give us much information when it comes to the set S, as here $\nu(a_0) = 0$. In the case of this set, we do know definitively that the characteristic polynomial of $z \in S$ is equivalent to $x^3 + x + 1 \pmod 2$. This gives the result that if $f(x) = a_0 + a_1 x + a_2 x^2 + x^3$ the minimal polynomial of $z \in S$, then

$$\nu_2(a_0) = 0 \qquad \nu_2(a_1) = 0 \qquad \nu_2(a_2) \geq 1 \ . \tag{3.1}$$

However, the aforementioned lemma does give us useful information for determining coefficients of the characteristic polynomial for elements in T_2 and T_4.

Proposition 3.2.10.

i) Let $z \in T_2$, with $f(x) = a_0 + a_1x + a_2x^2 + x^3$ the minimal polynomial of $z \in \mathbb{Q}_2[x]$. Then

$$\nu_2(a_0) = 1 \qquad \nu_2(a_1) \geq 1 \qquad \nu_2(a_2) \geq 1$$

ii) Let $z \in T_4$, with $f(x) = a_0 + a_1x + a_2x^2 + x^3$ the minimal polynomial of $z \in \mathbb{Q}_2[x]$. Then

$$\nu_2(a_0) = 2 \qquad \nu_2(a_1) \geq 2 \qquad \nu_2(a_2) \geq 1$$

Proof.

i) We can write $T_2 = \pi\Delta_3 \setminus \pi^2\Delta_3$, so that every element $z \in T_2$ has $\nu(z) = 1$. Therefore $\nu(a_0) = \nu_2(\det(z)) = \nu(z) = 1$. Since $a_0 \equiv 0 \pmod 2$ but $a_0 \not\equiv 0 \pmod 4$, it must be the case that $a_0 \equiv 2 \pmod 4$. Lemma 3.2.9 gives the result.

ii) We can write $T_4 = \pi^2\Delta_3 \setminus 2\Delta_3$, so that every element $z \in T_4$ has $\nu(z) = 2$. Therefore $\nu(a_0) = \nu_2(\det(z)) = \nu(z) = 2$. Since $a_0 \equiv 0 \pmod 4$ but $a_0 \not\equiv 0 \pmod 8$, it must be the case that $a_0 \equiv 4 \pmod 8$. Lemma 3.2.9 gives the result.

□

With this knowledge of the 2-adic valuations of coefficients of the characteristic polynomials, we can begin to construct elements that will feature in the integer-valued polynomials for these sets.

3.3 Towards Computing ν-sequences

Given the expression of our sets in terms of characteristic polynomials given in Equation (3.1) and Lemma 3.2.10, we can compute the ν-orderings and ν-sequences for S, T_2, and T_4. In this section, we establish some facts about the valuation of certain polynomials, with the goal of establishing these as the minimal polynomials of elements within their respective sets.

3.3.1 Characteristic polynomials for elements in S

For elements $z \in S$, we have

$$Tr(z) \equiv 0 \pmod 2 \qquad \beta(z) \equiv 1 \pmod 2 \qquad \det(z) \equiv 1 \pmod 2$$

Let us define the function

$$\phi = (\phi_2, \phi_1, \phi_0) : \mathbb{Z}_{\geq 0} \to 2\mathbb{Z}_{\geq 0} \times (1 + 2\mathbb{Z}_{\geq 0}) \times (1 + 2\mathbb{Z}_{\geq 0})$$
$$\phi(n) = \left(2\sum_{i\geq 0} n_{3i} 2^i, 1 + 2\sum_{i\geq 0} n_{3i+1} 2^i, 1 + 2\sum_{i\geq 0} n_{3i+2} 2^i \right)$$

where $n = \sum_{i\geq 0} n_i 2^i$ is the expansion of n in base 2. Let

$$f_n(x) = \prod_{k=0}^{n-1} \left(x^3 - \phi_2(k)x^2 + \phi_1(k)x - \phi_0(k) \right) \ .$$

Lemma 3.3.1. If $z \in S$ then

$$\nu(f_n(z)) \geq 3n + 3\sum_{k>0} \left\lfloor \frac{n}{8^k} \right\rfloor$$

with equality if $Tr(z) = \phi_2(n)$, $\beta(z) = \phi_1(n)$, and $\det(z) = \phi_0(n)$.

Proof. Let $z \in S$, and let $Tr(z) = 2\sum_{k\geq 0} a_k 2^k$ be the expansion of $Tr(z)$ in base 2. Similarly, let $\beta(z) = 1 + 2\sum_{k\geq 0} b_k 2^k$ and $\det(z) = 1 + 2\sum_{k\geq 0} c_k 2^k$ be the base 2 expansions of $\beta(z), \det(z)$. Define $m := \sum_{k\geq 0} a_k 2^{3k} + b_k 2^{3k+1} + c_k 2^{3k+2}$, so that $\phi(m) = (Tr(z), \beta(z), \det(z))$.

For any $0 \leq k \leq n$,

$$\begin{aligned} z^3 - \phi_2(k)z^2 + \phi_1(k)z - \phi_0(k) & \\ &= z^3 - \phi_2(k)z^2 + \phi_1(k)z - \phi_0(k) - (z^3 - Tr(z)z^2 + \beta(z)z - \det(z)) \\ &= (Tr(z) - \phi_2(k))z^2 + (\phi_1(k) - \beta(z))z + (\det(z) - \phi_0(k)) \\ &= (\phi_2(m) - \phi_2(k))z^2 + (\phi_1(k) - \phi_1(m))z + (\phi_0(m) - \phi_0(k)) \ . \end{aligned}$$

Since the characteristic polynomial for $z \in S$ is $x^3 + x + 1 \pmod 2$ and is irreducible over $\mathbb{F}_2$, it follows by Hensel's lemma that if $az^2 + bz + c \equiv 0 \pmod \pi$ in Δ_3 then $a \equiv b \equiv c \equiv 0 \pmod 2$. Because $z \in S$ we have $\nu(z) = 0$, and so we obtain that $\nu(az^2 + bz + c) = 3\min(\nu_2(a), \nu_2(b), \nu_2(c))$. We abuse notation and let $\nu_2(\phi_j) =$

$\nu_2(\phi_j(m) - \phi_j(k))$ for $j = 0, 1, 2$ and so that

$$\nu(z^3 - \phi_2(k)z^2 + \phi_1(k)z - \phi_0(k)) = 3\min(\nu_2(\phi_2), \nu_2(\phi_1), \nu_2(\phi_0))$$

which gives

$$\nu(f_n(z)) = 3\sum_{k=0}^{n-1} \min(\nu_2(\phi_2), \nu_2(\phi_1), \nu_2(\phi_0)) \ .$$

If $k = \sum k_i 2^i$, $m = \sum m_i 2^i$ denote the expansions of k and m in base 2, then

$$\begin{aligned}
\nu_2(m-k) &= \min(i : k_i \neq m_i) \\
\nu_2(\phi_2) &= \min(i : k_{3i} \neq m_{3i}) + 1 \\
\nu_2(\phi_1) &= \min(i : k_{3i+1} \neq m_{3i+1}) + 1 \\
\nu_2(\phi_0) &= \min(i : k_{3i+2} \neq m_{3i+2}) + 1
\end{aligned}$$

Thus, we have

$$\min(\nu_2(\phi_2), \nu_2(\phi_1), \nu_2(\phi_0)) = \left\lfloor \frac{\nu_2(m-k)}{3} \right\rfloor + 1 \ .$$

Since $\left\lfloor \frac{\nu_2(m-k)}{3} \right\rfloor$ is the highest power of 8 dividing $m - k$, for simplicity let us denote $\nu_8(m-k) := \left\lfloor \frac{\nu_2(m-k)}{3} \right\rfloor$.

Using the fact that $\nu_p(n!) = \sum_{i=1}^{n} \nu_p(i) = \sum_{i>0} \left\lfloor \frac{n}{p^i} \right\rfloor = \frac{n - \sum n_i}{p-1}$ with $n = \sum n_i p^i$ for any prime p extends also to powers of primes, we obtain the result

$$\sum_{i=1}^{n} \nu_8(i) = \sum_{i>0} \left\lfloor \frac{n}{8^i} \right\rfloor = \frac{n - \sum n_i}{7}$$

where $n = \sum n_i 8^i$ is the expansion of n in base 8. Thus, we have

$$\begin{aligned}
\nu(f_n(z)) &= 3\sum_{k=0}^{n-1} \left(\left\lfloor \frac{\nu_2(m-k)}{3} \right\rfloor + 1 \right) \\
&= 3n + 3\left(\sum_{k=1}^{m} \left\lfloor \frac{\nu_2(k)}{3} \right\rfloor - \sum_{k=1}^{m-n} \left\lfloor \frac{\nu_2(k)}{3} \right\rfloor \right) \\
&= 3n + 3\left(\sum_{i>0} \left\lfloor \frac{m}{8^i} \right\rfloor - \sum_{i>0} \left\lfloor \frac{m-n}{8^i} \right\rfloor \right)
\end{aligned}$$

$$= 3n + 3\left(\frac{m - \sum m_i}{7} - \frac{(m-n) - \sum (m-n)_i}{7}\right)$$

with $m = \sum m_i 8^i$, $m - n = \sum (m-n)_i 8^i$ as expansions base 8.

Noting that

$$\frac{m - \sum m_i}{7} - \frac{(m-n) - \sum (m-n)_i}{7} - \frac{n - \sum n_i}{7} = \frac{\sum (m-n)_i + \sum n_i - \sum m_i}{7} \geq 0$$

since this is the number of carries in adding n and $m - n$ in base 8, and so is always non-negative and equals zero only if $n = m$, we see that

$$\nu(f_n(z)) \geq 3n + 3\sum_{k>0} \left\lfloor \frac{n}{8^k} \right\rfloor$$

for $z \in S$, with equality if $\phi(n) = (Tr(z), \beta(z), \det(z))$. □

Lemma 3.3.2. Let a be a root of the polynomial $f(x) = x^3 - \phi_2(n)x^2 + \phi_1(n)x - \phi_0(n)$ in S, with θ the automorphism in Δ_3 given by $\theta(t) = \pi t \pi^{-1}$. The set of roots $a, \theta(a), \theta^2(a)$ are distinct modulo π, so that $\nu(\theta^i(a) - \theta^j(a)) = 0$ for $i \neq j$.

Proof. By Theorem 2.3.6, if a is a root of $f(x)$ then so too are $\theta(a)$ and $\theta^2(a)$. The element $a \equiv \omega^j \pmod{\pi}$ for some choice of $1 \leq j \leq 7$, and since $\theta(\omega^j) = \omega^{2j}$, it follows that the set of roots $\{a, \theta(a), \theta^2(a)\} \equiv \{\omega^j, \omega^{2j}, \omega^{4j}\} \pmod{\pi}$ and that these roots are distinct modulo π, as $\gcd(j, 7) = \gcd(2j, 7) = \gcd(4j, 7) = 1$. The result $\nu(\theta^i(a) - \theta^j(a)) = 0$ for $i \neq j$ follows. □

Lemma 3.3.3. The ν-sequence of α_S of $S \subseteq \Delta_3$ is given by

$$\alpha_S(3n) = \alpha_S(3n+1) = \alpha_S(3n+2) = 3n + 3\sum_{i>0} \left\lfloor \frac{n}{8^i} \right\rfloor$$

Proof. Via Theorem 2.5.5, for any $n \in \mathbb{Z}_{\geq 0}$ there exists an element $a_n \in \Delta_3$ which is a root of the polynomial $x^3 - \phi_2(n)x^2 + \phi_1(n)x - \phi_0(n)$. Recalling that

$$f_n(x) = \prod_{k=0}^{n-1} \left(x^3 - \phi_2(k)x^2 + \phi_1(k)x - \phi_0(k)\right)$$

we can see that $f_n(x)$ is the minimal polynomial of the set

$$\{a_0, \theta(a_0), \theta^2(a_0), a_1, \theta(a_1), \theta^2(a_1), \ldots, a_{n-1}, \theta(a_{n-1}), \theta^2(a_{n-1})\}$$

where θ is a non-trivial automorphism in Δ_3. This shows that

$\{a_0, \theta(a_0), \theta^2(a_0), a_1, \theta(a_1), \theta^2(a_1), \dots\}$ forms a ν-ordering for S, and since the minimal polynomials of $\{a_0, \dots, \theta^2(a_{n-1}), a_n\}$ and $\{a_0, \dots, \theta^2(a_{n-1}), a_n, \theta(a_n)\}$ are $f_n(x)(x - a_n)$ and $f_n(x)(x-a_n)(x-\theta(a_n))$ respectively, and $\nu(a_n - \theta(a_n)) = 0$ by Lemma 3.3.2, by Lemma 3.3.1 we have

$$\alpha_S(3n) = \alpha_S(3n+1) = \alpha_S(3n+2) = 3n + 3\sum_{i>0} \left\lfloor \frac{n}{8^i} \right\rfloor \ .$$

□

3.3.2 Characteristic polynomials for elements in T_2

For elements $z \in T_2$, we have

$$Tr(z) \equiv 0 \pmod 2 \qquad \beta(z) \equiv 0 \pmod 2 \qquad \det(z) \equiv 2 \pmod 4$$

Let us define the function

$$\psi = (\psi_2, \psi_1, \psi_0) : \mathbb{Z}_{\geq 0} \to 2\mathbb{Z}_{\geq 0} \times 2\mathbb{Z}_{\geq 0} \times (2 + 4\mathbb{Z}_{\geq 0})$$
$$\psi(n) = \left(2\sum_{i\geq 0} n_{3i+1}2^i, 2\sum_{i\geq 0} n_{3i}2^i, 2 + 4\sum_{i\geq 0} n_{3i+2}2^i \right)$$

where $n = \sum_{i\geq 0} n_i 2^i$ is the expansion of n in base 2. Let

$$g_n(x) = \prod_{k=0}^{n-1} \left(x^3 - \psi_2(k)x^2 + \psi_1(k)x - \psi_0(k) \right) \ .$$

Lemma 3.3.4. If $z \in T_2$ then

$$\nu(g_n(z)) \geq 4n + \sum_{i>0} \left\lfloor \frac{n}{2^i} \right\rfloor \ .$$

Proof. Let $z \in T_2$, and let $Tr(z) = 2\sum_{k\geq 0} a_k 2^k$ be the expansion of $Tr(z)$ in base 2. Similarly, let $\beta(z) = 2\sum_{k\geq 0} b_k 2^k$ and $\det(z) = 2 + 4\sum_{k\geq 0} c_k 2^k$ be the base 2 expansions of $\beta(z), \det(z)$. Define $m := \sum_{k\geq 0} a_k 2^{3k+1} + b_k 2^{3k} + c_k 2^{3k+2}$, so that $\psi(m) = (Tr(z), \beta(z), \det(z))$.

For any $0 \leq k \leq n$,

$$\begin{aligned} z^3 - \psi_2(k)z^2 + \psi_1(k)z - \psi_0(k) & \\ &= z^3 - \psi_2(k)z^2 + \psi_1(k)z - \psi_0(k) - (z^3 - Tr(z)z^2 + \beta(z)z - \det(z)) \\ &= (\psi_2(m) - \psi_2(k))z^2 + (\psi_1(k) - \psi_1(m))z + (\psi_0(m) - \psi_0(k)) \end{aligned}$$

Since $z \in T_2$ we have $\nu(z) = 1$, and therefore $\nu(az^2) = 2 + 3\nu_2(a)$, $\nu(bz) = 1 + 3\nu_2(b)$, and $\nu(c) = 3\nu_2(c)$. Because these have different residues modulo 3, we have

$$\nu(az^2 + bz + c) = \min(2 + 3\nu_2(a), 1 + 3\nu_2(b), 3\nu_2(c)) \ .$$

For the sake of simplicity, we abuse notation and let $\nu_2(\psi_j) = \nu_2(\psi_j(m) - \psi_j(k))$ for $j = 0, 1, 2$ and so

$$\nu(z^3 - \psi_2(k)z^2 + \psi_1(k)z - \psi_0(k)) = \min(2 + 3\nu_2(\psi_2), 1 + 3\nu_2(\psi_1), 3\nu_2(\psi_0)) \ ,$$

giving

$$\nu(g_n(z)) = \sum_{k=0}^{n-1} \min(2 + 3\nu_2(\psi_2), 1 + 3\nu_2(\psi_1), 3\nu_2(\psi_0)) \ .$$

If $k = \sum k_i 2^i$, $m = \sum m_i 2^i$ denote the expansions of k and m in base 2, then

$$\begin{aligned} \nu_2(m - k) &= \min(i : k_i \neq m_i) \\ \nu_2(\psi_2) &= \min(i : k_{3i+1} \neq m_{3i+1}) + 1 \\ \nu_2(\psi_1) &= \min(i : k_{3i} \neq m_{3i}) + 1 \\ \nu_2(\psi_0) &= \min(i : k_{3i+2} \neq m_{3i+2}) + 2 \end{aligned}$$

In this case, we find that the lower bounds on the $\nu(\psi_j)$ change depending on the residue of $\nu_2(m - k)$ (mod 3). We summarize the results in Table 3.1.

$\nu_2(m-k) \pmod 3$:	0	1	2
$2 + 3\nu_2(\psi_2)$	$\geq 5 + \nu_2(m-k)$	$= 4 + \nu_2(m-k)$	$\geq 6 + \nu_2(m-k)$
$1 + 3\nu_2(\psi_1)$	$= 4 + \nu_2(m-k)$	$\geq 6 + \nu_2(m-k)$	$\geq 5 + \nu_2(m-k)$
$3\nu_2(\psi_0)$	$\geq 6 + \nu_2(m-k)$	$\geq 5 + \nu_2(m-k)$	$= 4 + \nu_2(m-k)$

Table 3.1: Summary of lower bounds in T_2

From the table, we see that

$$\min(2+3\nu_2(\psi_2), 1+3\nu_2(\psi_1), 3\nu_2(\psi_0)) = 4+\nu_2(m-k)\ ,$$

giving

$$\begin{aligned}
\nu(g_n(z)) &= \sum_{k=0}^{n-1}(4+\nu_2(m-k)) \\
&= 4n + \sum_{k=0}^{n-1}\nu_2(m-k) \\
&= 4n + \sum_{k=1}^{m}\nu_2(k) - \sum_{k=1}^{m-n}\nu_2(k) \\
&= 4n + \sum_{i>0}\left\lfloor\frac{m}{2^i}\right\rfloor - \left\lfloor\frac{m-n}{2^i}\right\rfloor \\
&\geq 4n + \sum_{i>0}\left\lfloor\frac{n}{2^i}\right\rfloor
\end{aligned}$$

for $z \in T_2$, with equality if $\psi(n) = (Tr(z), \beta(z), \det(z))$. □

Lemma 3.3.5. Let b be a root of the polynomial $g(x) = x^3 - \psi_2(n)x^2 + \psi_1(n)x - \psi_0(n)$ in T_2, with θ the automorphism in Δ_3 given by $\theta(t) = \pi t \pi^{-1}$. The set of roots $b, \theta(b), \theta^2(b)$ are distinct modulo π^2, so that $\nu(\theta^i(b) - \theta^j(b)) = 1$ for $i \neq j$.

Proof. If $b \equiv \pi \pmod{\pi^2}$, take instead $b \equiv \omega\pi \pmod{\pi^2}$ – this choice can be made since π and $\omega\pi$ are conjugates: $\omega^{-1}\pi\omega = \omega\pi$. By Theorem 2.3.6, if b is a root of $g(x)$ then so too are $\theta(b)$ and $\theta^2(b)$. The element $b \equiv \overline{b}\pi \pmod{\pi^2}$ for some choice of $\overline{b} \not\equiv 0 \pmod{\pi}$. Applying our automorphism, we obtain modulo π^2

$$\theta(b) = \theta(\overline{b}\pi) = \theta(\overline{b})\theta(\pi) = \theta(\overline{b})\pi\ .$$

As in the proof of Lemma 3.3.2, the collection of elements $\{\overline{b}, \theta(\overline{b}), \theta^2(\overline{b})\}$ are distinct modulo π, and hence $\{b, \theta(b), \theta^2(b)\}$ are distinct modulo π^2. The result $\nu(\theta^i(b) - \theta^j(b)) = 1$ for $i \neq j$ follows. □

Lemma 3.3.6. The ν-sequence α_{T_2} of $T_2 \subseteq \Delta_3$ is given by

$$\alpha_{T_2}(3n) = \alpha_{T_2}(3n+1) - 1 = \alpha_{T_2}(3n+2) - 2 = 4n + \sum_{i>0}\left\lfloor\frac{n}{2^i}\right\rfloor$$

Proof. Via Theorem 2.5.5, for any $n \in \mathbb{Z}_{\geq 0}$ there exists an element $b_n \in \Delta_3$ which is

a root of the polynomial $x^3 - \psi_2(n)x^2 + \psi_1(n)x - \psi_0(n)$. Recalling that

$$g_n(x) = \prod_{k=0}^{n-1} \left(x^3 - \psi_2(k)x^2 + \psi_1(k)x - \psi_0(k)\right)$$

we can see that $g_n(x)$ is the minimal polynomial of the set

$$\{b_0, \theta(b_0), \theta^2(b_0), a_1, \theta(b_1), \theta^2(b_1), \ldots, b_{n-1}, \theta(b_{n-1}), \theta^2(b_{n-1})\}$$

where θ is a non-trivial automorphism in Δ_3. This shows that $\{b_0, \theta(b_0), \theta^2(b_0), b_1, \theta(b_1), \theta^2(b_1), \ldots\}$ forms a ν-ordering for T_2, and since $\nu(b_n - \theta(b_n)) = 1$ by Lemma 3.3.5, by Lemma 3.3.4 we have

$$\alpha_{T_2}(3n) = \alpha_{T_2}(3n+1) - 1 = \alpha_{T_2}(3n+2) - 2 = 4n + \sum_{i>0} \left\lfloor \frac{n}{2^i} \right\rfloor \ .$$

□

3.3.3 Characteristic polynomials for elements in T_4

For elements $z \in T_4$, we have

$$Tr(z) \equiv 0 \pmod 2 \qquad \beta(z) \equiv 0 \pmod 4 \qquad \det(z) \equiv 4 \pmod 8$$

Let us define the function

$$\sigma = (\sigma_2, \sigma_1, \sigma_0) : \mathbb{Z}_{\geq 0} \to 2\mathbb{Z}_{\geq 0} \times 4\mathbb{Z}_{\geq 0} \times (4 + 8\mathbb{Z}_{\geq 0})$$
$$\sigma(n) = \left(2\sum_{i\geq 0} n_{3i}2^i, 4\sum_{i\geq 0} n_{3i+1}2^i, 4 + 8\sum_{i\geq 0} n_{3i+2}2^i\right)$$

where $n = \sum_{i\geq 0} n_i 2^i$ is the expansion of n in base 2. Let

$$h_n(x) = \prod_{k=0}^{n-1} \left(x^3 - \sigma_2(k)x^2 + \sigma_1(k)x - \sigma_0(k)\right) \ .$$

Lemma 3.3.7. If $z \in T_4$ then

$$\nu(h_n(z)) \geq 7n + \sum_{i>0} \left\lfloor \frac{n}{2^i} \right\rfloor$$

with equality if $Tr(z) = \sigma_2(n)$, $\beta(z) = \sigma_1(n)$, and $\det(z) = \sigma_0(n)$.

Proof. Let $z \in T_4$, and let $Tr(z) = 2\sum_{k\geq 0} a_k 2^k$ be the expansion of $Tr(z)$ in base 2. Similarly, let $\beta(z) = 4\sum_{k\geq 0} b_k 2^k$ and $\det(z) = 4 + 8\sum_{k\geq 0} c_k 2^k$ be the base 2 expansions of $\beta(z), \det(z)$. Define $m := \sum_{k\geq 0} a_k 2^{3k} + b_k 2^{3k+1} + c_k 2^{3k+2}$, so that $\sigma(m) = (Tr(z), \beta(z), \det(z))$.

For any $0 \leq k \leq n$,

$$\begin{aligned} z^3 - \sigma_2(k)z^2 + \sigma_1(k)z - \sigma_0(k) \\ &= z^3 - \sigma_2(k)z^2 + \sigma_1(k)z - \sigma_0(k) - (z^3 - Tr(z)z^2 + \beta(z)z - \det(z)) \\ &= (\sigma_2(m) - \sigma_2(k))z^2 + (\sigma_1(k) - \sigma_1(m))z + (\sigma_0(m) - \sigma_0(k)) \end{aligned}$$

Since $z \in T_4$ we have $\nu(z) = 2$, and therefore $\nu(az^2) = 4 + 3\nu_2(a)$, $\nu(bz) = 2 + 3\nu_2(b)$, and $\nu(c) = 3\nu_2(c)$. Because these have different residues modulo 3, we have

$$\nu(az^2 + bz + c) = \min(4 + 3\nu_2(a), 2 + 3\nu_2(b), 3\nu_2(c)) \ .$$

For the sake of simplicity, we abuse notation and let $\nu_2(\sigma_j) = \nu_2(\sigma_j(m) - \sigma_j(k))$ for $j = 0, 1, 2$ and so

$$\nu(z^3 - \sigma_2(k)z^2 + \sigma_1(k)z - \sigma_0(k)) = \min(4 + 3\nu_2(\sigma_2), 2 + 3\nu_2(\sigma_1), 3\nu_2(\sigma_0)) \ ,$$

giving

$$\nu(h_n(z)) = \sum_{k=0}^{n-1} \min(4 + 3\nu_2(\sigma_2), 2 + 3\nu_2(\sigma_1), 3\nu_2(\sigma_0)) \ .$$

If $k = \sum k_i 2^i$, $m = \sum m_i 2^i$ denote the expansions of k and m in base 2, then

$$\begin{aligned} \nu_2(m - k) &= \min(i : k_i \neq m_i) \\ \nu_2(\sigma_2) &= \min(i : k_{3i} \neq m_{3i}) + 1 \\ \nu_2(\sigma_1) &= \min(i : k_{3i+1} \neq m_{3i+1}) + 2 \\ \nu_2(\sigma_0) &= \min(i : k_{3i+2} \neq m_{3i+2}) + 3 \end{aligned}$$

In this case, we find that the lower bounds on the $\nu(\sigma_j)$ change depending on the residue of $\nu_2(m - k) \pmod 3$. We summarize the results in Table 3.2.

From the table, we see that

$$\min(4 + 3\nu_2(\sigma_2), 2 + 3\nu_2(\sigma_1), 3\nu_2(\sigma_0)) = 7 + \nu_2(m - k) \ ,$$

$\nu_2(m-k) \pmod 3$:	0	1	2
$4+3\nu_2(\sigma_2)$	$= 7+\nu_2(m-k)$	$\geq 9+\nu_2(m-k)$	$\geq 8+\nu_2(m-k)$
$2+3\nu_2(\sigma_1)$	$\geq 8+\nu_2(m-k)$	$= 7+\nu_2(m-k)$	$\geq 9+\nu_2(m-k)$
$3\nu_2(\sigma_0)$	$\geq 8+\nu_2(m-k)$	$\geq 9+\nu_2(m-k)$	$= 7+\nu_2(m-k)$

Table 3.2: Summary of lower bounds in T_4

giving

$$\begin{aligned}
\nu(h_n(z)) &= \sum_{k=0}^{n-1}(7+\nu_2(m-k)) \\
&= 7n + \sum_{k=0}^{n-1}\nu_2(m-k) \\
&= 7n + \sum_{k=1}^{m}\nu_2(k) - \sum_{k=1}^{m-n}\nu_2(k) \\
&= 7n + \sum_{i>0}\left\lfloor\frac{m}{2^i}\right\rfloor - \left\lfloor\frac{m-n}{2^i}\right\rfloor \\
&\geq 7n + \sum_{i>0}\left\lfloor\frac{n}{2^i}\right\rfloor
\end{aligned}$$

for $z \in T_4$, with equality if $\sigma(n) = (Tr(z), \beta(z), \det(z))$. □

Lemma 3.3.8. Let c be a root of the polynomial $h(x) = x^3 - \sigma_2(n)x^2 + \sigma_1(n)x - \sigma_0(n)$ in T_4, with θ the automorphism in Δ_3 given by $\theta(t) = \pi t \pi^{-1}$. The set of roots $c, \theta(c), \theta^2(c)$ are distinct modulo π^3, so that $\nu(\theta^i(c) - \theta^j(c)) = 2$ for $i \neq j$.

Proof. If $c \equiv \pi^2 \pmod{\pi^3}$, take instead $c \equiv \omega\pi^2 \pmod{\pi^3}$ – this choice can be made since π^2 and $\omega\pi^2$ are conjugates: $\omega^{-1}\pi^2\omega = \omega\pi$. By Theorem 2.3.6, if c is a root of $h(x)$ then so too are $\theta(c)$ and $\theta^2(c)$. The element $c \equiv \overline{c}\pi^2 \pmod{\pi^3}$ for some choice of $\overline{c} \not\equiv 0 \pmod{\pi}$. Applying our automorphism, we obtain modulo π^3

$$\theta(c) = \theta(\overline{c}\pi) = \theta(\overline{c})\theta(\pi) = \theta(\overline{c})\pi \ .$$

As in the proof of Lemma 3.3.2, the collection of elements $\{\overline{c}, \theta(\overline{c}), \theta^2(\overline{c})\}$ are distinct modulo π, and hence $\{c, \theta(c), \theta^2(c)\}$ are distinct modulo π^3. The result $\nu(\theta^i(c) - \theta^j(c)) = 2$ for $i \neq j$ follows. □

Lemma 3.3.9. The ν-sequence α_{T_4} of $T_4 \subseteq \Delta_3$ is given by

$$\alpha_{T_4}(3n) = \alpha_{T_4}(3n+1) - 2 = \alpha_{T_4}(3n+2) - 4 = 7n + \sum_{i>0} \left\lfloor \frac{n}{2^i} \right\rfloor$$

Proof. Via Theorem 2.5.5, for any $n \in \mathbb{Z}_{\geq 0}$ there exists an element $c_n \in \Delta_3$ which is a root of the polynomial $x^3 - \sigma_2(n)x^2 + \sigma_1(n)x - \sigma_0(n)$. Recalling that

$$h_n(x) = \prod_{k=0}^{n-1} \left(x^3 - \sigma_1(k)x^2 + \sigma_2(k)x - \sigma_3(k)\right)$$

we can see that $h_n(x)$ is the minimal polynomial of the set

$$\{c_0, \theta(c_0), \theta^2(c_0), c_1, \theta(c_1), \theta^2(c_1), \ldots, c_{n-1}, \theta(c_{n-1}), \theta^2(c_{n-1})\}$$

where θ is a non-trivial automorphism in Δ_3. This shows that $\{c_0, \theta(c_0), \theta^2(c_0), c_1, \theta(c_1), \theta^2(c_1), \ldots\}$ forms a ν-ordering for T_4, and since $\nu(c_n - \theta(c_n)) = 2$ by Lemma 3.3.5, by Lemma 3.3.7 we have

$$\alpha_{T_4}(3n) = \alpha_{T_4}(3n+1) - 2 = \alpha_{T_4}(3n+2) - 4 = 7n + \sum_{i>0} \left\lfloor \frac{n}{2^i} \right\rfloor \ .$$

□

3.4 Valuative Capacity of Δ_3

As introduced in Section 2.5.4, we are interested in the valuative capacity of Δ_3, given by $\lim_{n\to\infty} \frac{\alpha_{\Delta_3}(n)}{n}$. To describe this value, we must first determine the valuative capacities of the subsets S, T_2, and T_4 of Δ_3.

Lemma 3.4.1. For the set $S \subseteq \Delta_p$,

$$\lim_{n\to\infty} \frac{\alpha_S(n)}{n} = \frac{8}{7} \ .$$

Proof. By Lemma 3.3.3, we have $\alpha_S(3n) = 3n + 3\sum_{i>0} \left\lfloor \frac{n}{8^i} \right\rfloor$. Therefore

$$\lim_{n\to\infty} \frac{\alpha_S(n)}{n} = \lim_{3n\to\infty} \frac{\alpha_S(3n)}{3n} = 1 + \lim_{3n\to\infty} \frac{1}{n} \sum_{i>0} \left\lfloor \frac{n}{8^i} \right\rfloor \ .$$

Since $\sum_{i>0} \frac{1}{8^i} = \frac{1}{7}$,

$$\begin{aligned}
\sum_{i>0} \frac{n-1}{8^i} \leq &\sum_{i>0} \left\lfloor \frac{n}{8^i} \right\rfloor \leq \sum_{i>0} \frac{n}{8^i} \\
\frac{n-1}{7} \leq &\sum_{i>0} \left\lfloor \frac{n}{8^i} \right\rfloor \leq \frac{n}{7} \\
\lim_{3n\to\infty} \frac{n-1}{7n} \leq &\lim_{3n\to\infty} \frac{1}{n} \sum_{i>0} \left\lfloor \frac{n}{8^i} \right\rfloor \leq \lim_{3n\to\infty} \frac{1}{7} \\
\frac{1}{7} \leq &\lim_{3n\to\infty} \frac{1}{n} \sum_{i>0} \left\lfloor \frac{n}{8^i} \right\rfloor \leq \frac{1}{7}
\end{aligned}$$

so that

$$\lim_{n\to\infty} \frac{\alpha_S(n)}{n} = 1 + \lim_{3n\to\infty} \frac{1}{n} \sum_{i>0} \left\lfloor \frac{n}{8^i} \right\rfloor = 1 + \frac{1}{7} = \frac{8}{7} \ .$$

□

Lemma 3.4.2. For $T_2 \subseteq \Delta_3$,

$$\lim_{n\to\infty} \frac{\alpha_{T_2}(n)}{n} = \frac{5}{3} \ .$$

Proof. By Lemma 3.3.6, we have $\alpha_{T_2}(3n) = 4n + \sum_{i>0} \left\lfloor \frac{n}{2^i} \right\rfloor$. Therefore

$$\lim_{n\to\infty} \frac{\alpha_{T_2}(n)}{n} = \lim_{3n\to\infty} \frac{\alpha_{T_2}(3n)}{3n} = \frac{4}{3} + \lim_{3n\to\infty} \frac{1}{3n} \sum_{i>0} \left\lfloor \frac{n}{2^i} \right\rfloor \ .$$

Since $\sum_{i>0} \frac{1}{2^i} = 1$,

$$\begin{aligned}
\sum_{i>0} \frac{n-1}{2^i} \leq &\sum_{i>0} \left\lfloor \frac{n}{2^i} \right\rfloor \leq \sum_{i>0} \frac{n}{2^i} \\
n-1 \leq &\sum_{i>0} \left\lfloor \frac{n}{2^i} \right\rfloor \leq n \\
\lim_{3n\to\infty} \frac{n-1}{3n} \leq &\lim_{3n\to\infty} \frac{1}{3n} \sum_{i>0} \left\lfloor \frac{n}{2^i} \right\rfloor \leq \lim_{3n\to\infty} \frac{1}{3} \\
\frac{1}{3} \leq &\lim_{3n\to\infty} \frac{1}{3n} \sum_{i>0} \left\lfloor \frac{n}{2^i} \right\rfloor \leq \frac{1}{3}
\end{aligned}$$

so that

$$\lim_{n\to\infty} \frac{\alpha_{T_2}(n)}{n} = \frac{4}{3} + \lim_{3n\to\infty} \frac{1}{3n} \sum_{i>0} \left\lfloor \frac{n}{2^i} \right\rfloor = \frac{4}{3} + \frac{1}{3} = \frac{5}{3} \ .$$

□

Lemma 3.4.3. For $T_4 \subseteq \Delta_3$,

$$\lim_{n\to\infty} \frac{\alpha_{T_4}(n)}{n} = \frac{8}{3} \ .$$

Proof. By Lemma 3.3.9, we have $\alpha_{T_4}(3n) = 7n + \sum_{i>0} \left\lfloor \frac{n}{2^i} \right\rfloor$. Therefore

$$\lim_{n\to\infty} \frac{\alpha_{T_4}(n)}{n} = \lim_{3n\to\infty} \frac{\alpha_{T_4}(3n)}{3n} = \frac{7}{3} + \lim_{3n\to\infty} \frac{1}{3n} \sum_{i>0} \left\lfloor \frac{n}{2^i} \right\rfloor \ .$$

By the result for the valuative capacity of T_2, $\lim_{3n\to\infty} \frac{1}{3n} \sum_{i>0} \left\lfloor \frac{n}{2^i} \right\rfloor = \frac{1}{3}$ so that

$$\lim_{n\to\infty} \frac{\alpha_{T_4}(n)}{n} = \frac{7}{3} + \lim_{3n\to\infty} \frac{1}{3n} \sum_{i>0} \left\lfloor \frac{n}{2^i} \right\rfloor = \frac{7}{3} + \frac{1}{3} = \frac{8}{3} \ .$$

□

Proposition 3.4.4. The valuative capacity of Δ_3 is given by

$$\lim_{n\to\infty} \frac{\alpha_{\Delta_3}(n)}{n} = \frac{-439 + \sqrt{469\ 921}}{770} \approx 0.32014 \ .$$

Proof. Recall by Proposition 3.2.7 that the ν-sequence of Δ_3 is given by the expression

$$\alpha_{\Delta_3} = \Big(\big[([(\alpha_{\Delta_3} + (n)) \wedge (\alpha_{T_4} - (2n))] + (n)) \wedge (\alpha_{T_2} - (n)) \big] + (n) \Big)^{\wedge 2} \wedge (\alpha_S)^{\wedge 2} \ .$$

Using Proposition 2.5.26, we obtain

$$\lim_{n\to\infty} \frac{\alpha_{\Delta_3}(n)}{n} = \cfrac{1}{\cfrac{2}{\lim_{n\to\infty} \frac{\alpha_S(n)}{n}} + \cfrac{2}{1 + \cfrac{1}{\cfrac{1}{\lim_{n\to\infty} \frac{\alpha_{T_2}(n)}{n} - 1} + \cfrac{1}{1 + \cfrac{1}{\cfrac{1}{\lim_{n\to\infty} \frac{\alpha_{T_4}(n)}{n} - 2} + \cfrac{1}{\lim_{n\to\infty} \frac{\alpha_{\Delta_3}(n)}{n} + 1}}}}}}$$

so that the valuative capacity of Δ_3 is the positive solution to the expression

$$
\begin{aligned}
x &= \cfrac{1}{\cfrac{2}{8/7}+\cfrac{2}{1+\cfrac{1}{\cfrac{1}{5/3-1}+\cfrac{1}{1+\cfrac{1}{\cfrac{1}{8/3-2}+\cfrac{1}{x+1}}}}}} \\
&= \cfrac{1}{\cfrac{7}{4}+\cfrac{2}{1+\cfrac{1}{\cfrac{3}{2}+\cfrac{1}{1+\cfrac{1}{\cfrac{3}{2}+\cfrac{1}{x+1}}}}}} \\
&= \frac{4(45+31x)}{563+385x} \\
&\Rightarrow 385x^2+439x-180=0
\end{aligned}
$$

and so

$$\lim_{n\to\infty}\frac{\alpha_{\Delta_3}(n)}{n}=\frac{-439+\sqrt{469\ 921}}{770}\ .$$

□

Chapter 4

The Prime Index, 2-local Case

4.1 Sets Closed Under Conjugation in Δ_p

We observed that in the index 3 case, the elements of Δ_3 can be divided into the sets T, $T+1$, S, and $S+1$, where T consists of all elements $z \in \Delta_3$ with $z \equiv 0 \pmod{\pi}$, $T+1$ consists of all $z \in \Delta_3$ with $z \equiv 1 \pmod{\pi}$, and S and $S+1$ are conjugacy classes represented by irreducible polynomials of degree 3 modulo 2. Each of these polynomials has three distinct roots of the form ω^i with $1 \leq i \leq 6$, and together these four sets T, $T+1$, S, and $S+1$ account for all elements of Δ_3 modulo π.

We now extend this reasoning to the index p case, with p an odd prime. The maximal order Δ_p will be the extension of $\mathbb{Z}_2$ generated by the $p \times p$ matrices

$$\omega = \begin{pmatrix} \zeta & 0 & 0 & \cdots & 0 \\ 0 & \zeta^2 & 0 & \cdots & 0 \\ 0 & 0 & \zeta^4 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \cdots \\ 0 & 0 & 0 & \cdots & \zeta^{2^{p-1}} \end{pmatrix} \qquad \pi = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 2 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

where ζ is a primitive $(2^p-1)^{\text{th}}$ root of unity. The following relations hold for ω and π:

$$\pi^p = 2I_p \qquad \pi\omega\pi^{-1} = \omega^2 \qquad \omega^{2^p-1} = I_p \ .$$

The conjugacy class containing ω^i in Δ_p consists of the p elements

$$\omega^i, \omega^{2i}, \omega^{2^2 i}, \ldots, \omega^{2^{p-1} i}$$

since $\pi\omega^i\pi^{-1} = \omega^{2i}$ and $\omega^{2^p} = \omega \cdot \omega^{2^p-1} = \omega \cdot I_p = \omega$, hence $\omega^{2^p i} = \omega^i$. We will show that each conjugacy class of elements $\omega^i \pmod{\pi}$ corresponds to an irreducible polynomial of degree p modulo 2.

How many such polynomials are there? In general, the number of monic irreducible polynomials of degree n over a finite field of size q is expressed by the following formula, given as a corollary in §7.2 of [9],

$$I_q(n) = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d} \ ,$$

where μ is the Möbius function. In our case, $n = p$ a prime, and $q = 2$, so that

$$\begin{aligned} I_2(p) &= \frac{1}{p} \sum_{d|p} \mu(d) 2^{p/d} \\ &= \frac{1}{p} \left(\mu(1) 2^p + 2\mu(p) \right) \\ &= \frac{1}{p} (2^p - 2) \end{aligned}$$

This agrees with the earlier observation that the $2^p - 2$ elements $\omega, \omega^2, \omega^3, \ldots, \omega^{2^p-2}$ modulo π will be divided into conjugacy classes each of size p.

Therefore, the maximal order Δ_p is divided into conjugacy classes T, $T+1$, and a collection of $\frac{1}{p}(2^p - 2)$ sets $\{S_i\}$, where $T = \{z \in \Delta_p : z \equiv 0 \pmod{\pi}\}$, $T + 1 = \{z \in \Delta_p : z \equiv I_p \pmod{\pi}\}$, and the sets $\{S_i\}$ are each determined by a monic irreducible polynomial $f(x)$ of degree p.

As in the 3×3 case, we would now like to verify that our tree of sets closed under conjugation below T is binary, namely that our sets are of the form $\pi^j \Delta_p$ and $\pi^{j-1}\Delta_p \setminus \pi^j \Delta_p$.

Lemma 4.1.1. The set $\pi^j \Delta_p = \{z \in \Delta_p : z \equiv 0 \pmod{\pi^j}\}$ splits, modulo π^{j+1}, into the sets $\pi^{j+1}\Delta_p = \{z \in \Delta_p : z \equiv 0 \pmod{\pi^{j+1}}\}$ and $\pi^j \Delta_p \setminus \pi^{j+1}\Delta_p = \{z \in \Delta_p : z \equiv \omega^i \pi^j \pmod{\pi^{j+1}}, 1 \leq i \leq 2^p - 1\}$, both of which are closed under conjugation by elements of Δ_p.

Proof. It is clear that $\{z \in \Delta_p : z \equiv 0 \pmod{\pi^{j+1}}\}$ is closed under conjugation. Let $z = \pi^j \pmod{\pi^{j+1}} \in \Delta_p$. Then, conjugating z by an element of the form $\omega^k \pi^\ell$, we obtain

$$\begin{aligned}\omega^k\pi^\ell \cdot \pi^j \cdot \pi^{-\ell}\omega^{-k} &= \omega^k\pi^j\omega^{-k} \\ &= \omega^k\omega^{2^j(-k)}\pi^j \\ &= \omega^{k(1-2^j)}\pi^j\end{aligned}$$

with j fixed such that $1 \leq j \leq p-1$, and $1 \leq \ell \leq p-1$, $1 \leq k \leq 2^p - 1$. This set of elements will be all of $\pi^j\Delta_p \smallsetminus \pi^{j+1}\Delta_p$ if and only if $k(1-2^j)$ forms a complete set of residues modulo $2^p - 1$, with j fixed and k variable.

We note the following result about Mersenne numbers, listed as Fact 13 in Section 4.2 of [15]:

$$\text{If } a, b \in \mathbb{Z}_{>0} \text{ then } \gcd(2^a - 1, 2^b - 1) = 2^{\gcd(a,b)} - 1.$$

Since $1 \leq j \leq p-1$ is fixed, we must have $\gcd(j, p) = 1$ and therefore $\gcd(2^j - 1, 2^p - 1) = \gcd(1 - 2^j, 2^p - 1) = 1$. Since $1 - 2^j$ and $2^p - 1$ are relatively prime, and k is an integer in the range $[1, 2^p - 1]$, it follows that $k(1 - 2^j)$ forms a complete set of residues modulo $2^p - 1$.

Therefore the set $\{\omega^{k(1-2^j)}\pi^j \pmod{\pi^{j+1}} : 1 \leq k \leq 2^p - 1\}$ is equivalent to the set $\{\omega^i\pi^j \pmod{\pi^{j+1}} : 1 \leq i \leq 2^p - 1\}$. □

4.2 Characteristic Polynomials of the Subsets of Δ_p

As done in Chapter 3, we would like to be able to completely describe the subsets of Δ_p in terms of the 2-adic valuation of coefficients in their characteristic polynomials. To do this, we would like to use a result from [14], but first need to know that such characteristic polynomials are irreducible.

Lemma 4.2.1. Let $z \in \Delta_p$ be a non-constant element. The characteristic polynomial of z is irreducible over $\mathbb{Q}_2$.

Proof. Since $z \in \Delta_p \subseteq \mathbb{Q}_2[\omega_p, \pi_p]$ then $\mathbb{Q}_2 \leq \mathbb{Q}_2[z] \leq \mathbb{Q}_2[\omega_p, \pi_p]$ as field extensions. The characteristic polynomial of $z \in \Delta_p$ over $\mathbb{Q}_2$ has degree p, so $[\mathbb{Q}_2[z] : \mathbb{Q}_2] \leq p$. Since $[\mathbb{Q}_2[z] : \mathbb{Q}_2]$ divides $[\mathbb{Q}_2[\omega_p, \pi_p] : \mathbb{Q}_2] = p^2$ we therefore have $[\mathbb{Q}_2[z] : \mathbb{Q}_2] = p$ or $[\mathbb{Q}_2[z] : \mathbb{Q}_2] = 1$. Since z is non-constant, $z \notin \mathbb{Q}_2$ and thus $[\mathbb{Q}_2[z] : \mathbb{Q}_2] = p$. Since this is equal to the degree of the characteristic polynomial of z, it is therefore the minimal polynomial of z over $\mathbb{Q}_2$ and hence is irreducible. □

Knowing that the characteristic polynomials of all non-constant elements in Δ_p are irreducible allows us to make use of the following result (which has been restated to adhere to the usual convention of writing general polynomials as $f(x) = \sum_{i=0}^{n} a_i x^i$).

Lemma 4.2.2 ([14], 12.9 restated)**.** Let $f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n \in K[x]$ be irreducible. Then

$$\nu(a_j) \geq \frac{n-j}{n}\nu(a_0) \ , \qquad 0 \leq j \leq n-1 \ .$$

In order to say more about the 2-adic valuation of the coefficients of the characteristic polynomial of non-constant elements in Δ_p, we need to know more information about $\nu_2(a_0)$.

Lemma 4.2.3. Let Δ_p denote the maximal order of dimension p^2 over $\mathbb{Q}_2$, and let $z \in \pi^k\Delta_p$, with $f(x) = a_0 + a_1 x + \cdots + a_{p-1}x^{p-1} + x^p$ the minimal polynomial of $z \in \mathbb{Q}_2[x]$. Then $\nu_2(a_0) \geq k$.

Proof. We have $a_0 = \det(z)$, so that $\nu_2(a_0) = \nu_2(\det(z)) = \nu(z)$ by definition of the valuation in Δ_p. Since $\nu(z)$ simply counts the lowest power of π found in the expression for z, and $z \in \pi^k\Delta_p$, we have $\nu_2(a_0) = \nu(z) \geq k$. □

Lemma 4.2.4. Let Δ_p denote the maximal order of dimension p^2 over $\mathbb{Q}_2$, and let $z \in \pi^k\Delta_p \smallsetminus \pi^{k+1}\Delta_p$, with $f(x) = a_0 + a_1 x + \cdots + a_{p-1}x^{p-1} + x^p$ the minimal polynomial of $z \in \mathbb{Q}_2[x]$. Then $\nu_2(a_0) = k$ and $a_0 \equiv 2^k \pmod{2^{k+1}}$.

Proof. As before, $\nu_2(a_0) = \nu_2(\det(z)) = \nu(z)$ and since $z \in \pi^k\Delta_p \smallsetminus \pi^{k+1}\Delta_p$, the lowest power of π appearing in the expression for z must be π^k and hence $\nu_2(a_0) = \nu(z) = k$. Since $a_0 \equiv 0 \pmod{2^k}$ but $a_0 \not\equiv 0 \pmod{2^{k+1}}$, it must be the case that $a_0 \equiv 2^k \pmod{2^{k+1}}$. □

These lemmas lead to the following result.

Proposition 4.2.5.

i) Let $T_{2k-3} = \pi^k\Delta_p = \{z \in \Delta_p : z \equiv 0 \pmod{\pi^k}\}$ for $k \geq 2$. Then for $z \in T_{2k-3}$, the coefficients of the characteristic polynomial $f_z(x) = a_0 + a_1 x + \cdots + a_{p-1}x^{p-1} + x^p$ satisfy
$$\nu_2(a_j) \geq k\left(\frac{p-j}{p}\right) = k\left(1 - \frac{j}{p}\right) \ .$$

ii) Let $T_{2k} = \pi^k\Delta_p \smallsetminus \pi^{k+1}\Delta_p = \{z \in \Delta_p : z \equiv \omega^i\pi^k \pmod{\pi^{k+1}}, 1 \leq i \leq 2^p - 1\}$ for $k \geq 1$. Then for $z \in T_{2k}$, the coefficients of the characteristic polynomial $f_z(x) = a_0 + a_1 x + \cdots + a_{p-1}x^{p-1} + x^p$ satisfy

$$\begin{aligned}\nu_2(a_0) &= k \\ a_0 &\equiv 2^k \pmod{2^{k+1}} \\ \nu_2(a_j) &\geq k\left(\frac{p-j}{p}\right) = k\left(1-\frac{j}{p}\right)\end{aligned}$$

and, conversely, any element $z \in \Delta_p$ with characteristic polynomial satisfying the above conditions is an element of T_{2k}.

Proof.

i) This result follows from the definition of T_{2k-3} along with Lemmas 4.2.2, 4.2.3, and 4.2.4.

ii) The first part of the proof follows from the definition of T_{2k} along with Lemmas 4.2.2, 4.2.3, and 4.2.4.

For the converse, we note that $T_{2k} = \pi^k\Delta_p \smallsetminus \pi^{k+1}\Delta_p$ can be described precisely as $T_{2k} = \{z \in \Delta_p : \nu(z) = k\}$. We claim that

$$\begin{aligned}T_{2k} = \{z \in \Delta_p : \mathrm{ch}_z(x) = x^p + a_{p-1}x^{p-1} + \cdots + a_1x + a_0 \\ \text{with } a_0 \equiv 2^k \pmod{2^{k+1}}, a_j \equiv 0 \pmod{2^{\left\lceil \frac{p-j}{p}k\right\rceil}})\} \ .\end{aligned}$$

By the above remark, we have already demonstrated the containment

$$\begin{aligned}\{z \in \Delta_p : \nu(z) = k\} \supseteq \{z \in \Delta_p : \mathrm{ch}_z(x) = x^p + \sum_{i=0}^{p-1} a_ix^i \\ \text{with } a_0 \equiv 2^k \pmod{2^{k+1}}, a_j \equiv 0 \pmod{2^{\left\lceil \frac{p-j}{p}k\right\rceil}})\}\end{aligned}$$

For the opposite conclusion, suppose an element $z \in \Delta_p$ has characteristic polynomial with the properties above, namely $a_0 \equiv 2^k \pmod{2^{k+1}}$. Since $a_0 = \det(z)$ and by definition, $\nu(z) = \nu_2(\det(z))$, we will have $\nu(z) = \nu_2(a_0) = k$. This completes the proof.

□

With this knowledge of the 2-adic valuations of coefficients of the characteristic polynomials, we can begin to construct elements that will feature in the integer-valued polynomials for these sets.

4.3 Towards Constructing Integer-Valued Polynomials

4.3.1 The Sets S_i

As discussed in Section 4.1, among the conjugacy classes of Δ_p are a collection of sets $\{S_i\}$ which are defined by monic irreducible polynomials $f(x)$ of degree p, and there are $\frac{1}{p}(2^p - 2)$ such sets.

Let S be one of the sets in the collection $\{S_i\}$. Such a set S has an associated monic irreducible polynomial $f(x) = a_0 + a_1 x + \cdots + a_{p-1}x^{p-1} + x^p$. Define a binary sequence $\{\delta_j\}_{j=0}^{p-1}$ by

$$a_0 \equiv 1 \pmod 2 \qquad\qquad a_j \equiv \delta_j \pmod 2$$

where either $\delta_j \equiv 0$ or $\delta_j \equiv 1$, depending on the value of j (and at least one $\delta_j \equiv 0 \pmod 2$), and define a function $\phi = (\phi_0, \phi_1, \ldots, \phi_{p-1})$ by

$$\begin{aligned} \phi &: \mathbb{Z} \to \prod_{i=0}^{p-1} (\delta_j + 2\mathbb{Z}) \\ \phi_j(b) &= \delta_j + 2\sum_{i\geq 0} b_{pi+(p-j)} 2^i \ , \end{aligned}$$

where $\delta_0 = 1$, and $b = \sum_{i\geq 0} b_i 2^i$ is the expansion of b in base 2. Let

$$f_n(x) = \prod_{b=0}^{n-1} (x^p - \phi_{p-1}(b)x^{p-1} + \phi_{p-2}(b)x^{p-2} - \cdots + (-1)^p \phi_0(b)) \ .$$

We will determine a lower bound on $\nu(f_n(z))$ for $z \in S$. In order to do this, it is helpful to note the following results regarding valuations of polynomials of degree at most $p-1$.

Lemma 4.3.1. If $z \in S$ and $c_i \in \mathbb{Z}_2$ are such that

$$c_{p-1}z^{p-1} + c_{p-2}z^{p-2} + \cdots + c_0 \equiv 0 \pmod \pi$$

in Δ_p, then we have $c_i \equiv 0 \pmod 2$ for all $0 \leq i \leq p-1$.

Proof. The polynomial $\sum_{i=0}^{p-1} c_i x^i$ has z as a root modulo π, and since z is a root of $f(x)$ modulo 2, it so too must be a root of $f(x)$ modulo π. Since z is a root of both

polynomials, it must be the case that $\sum_{i=0}^{p-1} c_i x^i$ divides $f(x)$. But $f(x)$ is irreducible, and therefore $\sum_{i=0}^{p-1} c_i x^i$ must be identically zero modulo 2. □

Lemma 4.3.2. If $z \in S$ and $c_i \in \mathbb{Z}_2$ for $0 \leq i \leq p-1$, then

$$\nu\left(\sum_{i\geq 0}^{p-1} c_i z^i\right) = \min_{0\leq i\leq p-1} \nu(c_i z^i) = p \min_{0\leq i\leq p-1} \nu_2(c_i) \ .$$

Proof. Since each $c_i \equiv 0 \pmod 2$, write $c_i = 2^{\gamma_i}\hat{c}_i$ with $\hat{c}_i$ odd, $\gamma_i \geq 0$. Then

$$\sum_{i\geq 0}^{p-1} c_i z^i = \sum_{i\geq 0}^{p-1} 2^{\gamma_i}\hat{c}_i z^i = 2^{\min_j \gamma_j} \sum_{i\geq 0}^{p-1} 2^{\gamma_i - \min_j \gamma_j}\hat{c}_i z^i$$

with at least one of the $\gamma_i - \min_j \gamma_j = 0$. Therefore the expression

$$\sum_{i\geq 0}^{p-1} 2^{\gamma_i - \min_j \gamma_j}\hat{c}_i z^i$$

has at least one odd coefficient, and by Lemma 4.3.1 it follows that

$$\nu\left(\sum_{i\geq 0}^{p-1} 2^{\gamma_i - \min_j \gamma_j}\hat{c}_i z^i\right) = 0 \ .$$

From this, we see that

$$\begin{aligned}
\nu\left(\sum_{i\geq 0}^{p-1} c_i z^i\right) &= \nu\left(2^{\min_j \gamma_j} \sum_{i\geq 0}^{p-1} 2^{\gamma_i - \min_j \gamma_j}\hat{c}_i z^i\right) \\
&= p\nu_2(2^{\min_j \gamma_j}) + \nu\left(\sum_{i\geq 0}^{p-1} 2^{\gamma_i - \min_j \gamma_j}\hat{c}_i z^i\right) \\
&= p\nu_2(2^{\min_j \gamma_j}) \\
&= p \min_j \gamma_j \\
&= p \min_j \nu_2(c_j)
\end{aligned}$$

which gives the result. □

With these lemmas in hand, we can now establish the following result for $\nu(f_n(z))$.

Lemma 4.3.3. If $z \in S$ then

$$\nu(f_n(z)) \geq pn + p\sum_{i>0} \left\lfloor \frac{n}{2^{pi}} \right\rfloor$$

with equality if $\phi(n) = (\phi_0(n), \ldots, \phi_{p-1}(n))$ gives the tuple of coefficients $a_0, \ldots, a_{p-1}$ of the characteristic polynomial for $z \in S$.

Proof. Let $z \in S$, and let $m \in \mathbb{Z}$ be such that $\phi(m)$ gives a tuple consisting of the coefficients of the characteristic polynomial of z, with $\phi_j(m)$ being the coefficient of x^j. Then for any $0 \leq b \leq n$,

$$\begin{aligned} z^p - \phi_{p-1}(b)z^{p-1} + \phi_{p-2}(b)z^{p-2} - \cdots + (-1)^p\phi_0(b) & \\ = z^p - \phi_{p-1}(b)z^{p-1} + \phi_{p-2}(b)z^{p-2} - \cdots + (-1)^p\phi_0(b) - (\mathrm{ch}_z(z)) & \\ = (\phi_{p-1}(m) - \phi_{p-1}(b))z^{p-1} + (\phi_{p-2}(b) - \phi_{p-2}(m))z^{p-2} & \\ + \cdots + (-1)^p(\phi_0(b) - \phi_0(m)) & \end{aligned}$$

Since for any $z \in S$ we have $\nu(z) = 0$, the results of Lemmas 4.3.1 and 4.3.2 give that

$$\begin{aligned} \nu(z^p - \phi_{p-1}(b)z^{p-1} + \phi_{p-2}(b)z^{p-2} - \cdots + (-1)^p\phi_0(b)) &= \min_{0\leq j\leq p-1} \nu(\phi_j z^j) \\ &= \min_{0\leq j\leq p-1} [p\nu_2(\phi_j) + j\nu(z)] \\ &= p \min_{0\leq j\leq p-1} \nu_2(\phi_j) \end{aligned}$$

where $\nu_2(\phi_j) := \nu_2(\phi_j(m) - \phi_j(b))$ for $0 \leq j \leq p-1$.

Let $b = \sum b_i 2^i$, $m = \sum m_i 2^i$ denote the expansions of b and m in base 2. Then

$$\begin{aligned} \nu_2(m-b) &= \min(i : b_i \neq m_i) \\ \nu_2(\phi_j) &= \min(i : b_{pi+(p-j)} \neq m_{pi+(p-j)}) + 1 \end{aligned}$$

for each $0 \leq j \leq p-1$. Thus, we have

$$\min_{0\leq j\leq p-1} \nu_2(\phi_j) = \left\lfloor \frac{\nu_2(m-b)}{p} \right\rfloor + 1 \ .$$

Since $\left\lfloor \frac{\nu_2(m-b)}{p} \right\rfloor$ is the highest power of 2^p dividing $m - b$, for simplicity let us

denote $\nu_{2^p}(m-b) = \left\lfloor \frac{\nu_2(m-b)}{p} \right\rfloor$. The fact that

$$\nu_p(n!) = \sum_{i=1}^{n} \nu_p(i) = \sum_{i>0} \left\lfloor \frac{n}{p^i} \right\rfloor = \frac{n - \sum n_i}{p-1}$$

extends to powers of primes as well, so that

$$\sum_{i=1}^{n} \nu_{2^p}(i) = \sum_{i>0} \left\lfloor \frac{n}{2^{pi}} \right\rfloor = \frac{n - \sum n_i}{2^p - 1}$$

where $n = \sum n_i 2^{pi}$ is the expansion of n in base 2^p. Thus, we have

$$\begin{aligned}
\nu_2(f_n(z)) &= p \sum_{b=0}^{n-1} \left(\left\lfloor \frac{\nu_2(m-k)}{p} \right\rfloor + 1 \right) \\
&= pn + p \left(\sum_{b=1}^{m} \left\lfloor \frac{\nu_2(b)}{p} \right\rfloor - \sum_{b=1}^{m-n} \left\lfloor \frac{\nu_2(b)}{p} \right\rfloor \right) \\
&= pn + p \left(\sum_{b=1}^{m} \nu_{2^p}(b) - \sum_{b=1}^{m-n} \nu_{2^p}(b) \right) \\
&= pn + p \left(\sum_{i>0} \left\lfloor \frac{m}{2^{pi}} \right\rfloor - \sum_{i>0} \left\lfloor \frac{m-n}{2^{pi}} \right\rfloor \right) \\
&= pn + p \left(\frac{m - \sum m_i}{2^p - 1} - \frac{(m-n) - \sum (m-n)_i}{2^p - 1} \right)
\end{aligned}$$

with $m = \sum m_i 2^{pi}$, $m - n = \sum (m-n)_i 2^{pi}$ as expansions base 2^p.

Noting that

$$\frac{m - \sum m_i}{2^p - 1} - \frac{(m-n) - \sum (m-n)_i}{2^p - 1} - \frac{n - \sum n_i}{2^p - 1} = \frac{\sum (m-n)_i + \sum n_i - \sum m_i}{2^p - 1} \geq 0$$

since this is the number of carries in adding n and $m-n$ in base 2^p, and so is always non-negative and equals zero only if $n = m$, we see that

$$\nu(f_n(z)) \geq pn + p \sum_{i>0} \left\lfloor \frac{n}{2^{pi}} \right\rfloor$$

for $z \in S$, with equality if $\phi(n) = (\phi_0(n), \ldots, \phi_{p-1}(n))$ gives the tuple containing coefficients $a_0, \ldots, a_{p-1}$ of the characteristic polynomial for $z \in S$. □

Corollary 4.3.4. All conjugacy classes $S \subseteq \Delta_p$ determined by a monic irreducible polynomial of degree p have the same ν-sequence.

Proof. Nowhere in the proof of Lemma 4.3.3 did we rely on the irreducible polynomial defining S in question (namely, the choices of δ_j). Therefore we obtain the same result for all such conjugacy classes S in Δ_p, which gives the same ν-sequence for all $\frac{1}{p}(2^p-2)$ such sets. □

4.3.2 The Sets T_{2k}

Recall from Proposition 4.2.5 ii) that we have the following characterization for the sets T_{2k}, for which we require a description of the ν-sequence in order to determine the ν-sequence of Δ_p itself:

$$T_{2k} = \Big\{ z \in \Delta_p : \mathrm{ch}_z(x) = x^p + a_{p-1}x^{p-1} + \cdots + a_1 x + a_0 \\ \text{with } a_0 \equiv 2^k \pmod{2^{k+1}}, a_j \equiv 0 \pmod{2^{\lceil \frac{p-j}{p} k \rceil}} \Big\} \ .$$

Let

$$\psi : \mathbb{Z} \to (2^k + 2^{k+1}\mathbb{Z}) \times \prod_{j=1}^{p-1} 2^{\lceil \frac{(p-j)k}{p} \rceil}\mathbb{Z}$$
$$\psi = (\psi_0, \psi_1, \ldots, \psi_{p-1})$$

be defined on $\mathbb{Z}$ so that

$$\psi_0(b) = 2^k + 2^{k+1} \sum_{i \geq 0} b_{pi+p-1} 2^i \tag{4.1}$$

$$\psi_j(b) = 2^{\lceil \frac{(p-j)k}{p} \rceil} \sum_{i \geq 0} b_{pi+((jk-1) \pmod p)} 2^i \tag{4.2}$$

where $1 \leq j \leq p-1$ and $b = \sum_{i \geq 0} b_i 2^i$ is the expansion of $b \in \mathbb{Z}$ in base 2. For $n \geq 0$, define polynomials

$$g_n^{(k)}(x) = \prod_{b=0}^{n-1} (x^p - \psi_{p-1}(b)x^{p-1} + \psi_{p-2}(b)x^{p-2} - \cdots + (-1)^p \psi_0(b)) \ .$$

Let $z \in T_{2k}$, and let $m \in \mathbb{Z}$ be such that $\psi(m)$ gives a tuple consisting of the coefficients of the characteristic polynomial of z, with $\psi_j(m)$ being the coefficient of x^j. Then for any $0 \leq b \leq n$,

$$\begin{aligned} z^p - \psi_{p-1}(b)z^{p-1} + \psi_{p-2}(b)z^{p-2} - \cdots + (-1)^p\psi_0(b) & \\ &= z^p - \psi_{p-1}(b)z^{p-1} + \psi_{p-2}(b)z^{p-2} - \cdots + (-1)^p\psi_0(b) - (\mathrm{ch}_z(z)) \\ &= (\psi_{p-1}(m) - \psi_{p-1}(b))z^{p-1} + (\psi_{p-2}(b) - \psi_{p-2}(m))z^{p-2} + \cdots \\ &\qquad + (-1)^p(\psi_0(b) - \psi_0(m)) \end{aligned}$$

We would like to take the valuation of this expression. Recall that for any valuation ν defined on a field K with $a, b \in K$, that $\nu(a+b) \geq \min(\nu(a), \nu(b))$ with equality if $\nu(a) \neq \nu(b)$. In particular, if in a sum of n components each has a unique residue modulo p, then the valuation of the sum is the minimum of the valuations of the components.

Notice that for any $0 \leq j \leq p-1$,

$$\begin{aligned} \nu((\psi_j(m) - \psi_j(k))z^j) &= p\nu_2(\psi_j(m) - \psi_j(k)) + \nu(z^j) \\ &= p\nu_2(\psi_j(m) - \psi_j(k)) + j\nu(z) \\ &\equiv j\nu(z) \pmod{p} \end{aligned} \tag{4.3}$$

so as j varies we will have a complete set of residues modulo p, and hence

$$\begin{aligned} \nu(z^p - \psi_{p-1}(b)z^{p-1} + \psi_{p-2}(b)z^{p-2} - \cdots + (-1)^p\psi_0(b)) & \\ = \min((p-1)\nu(z) + p\nu_2(\psi_{p-1}), (p-2)\nu(z) + p\nu_2(\psi_{p-2}), \ldots, & \\ \nu(z) + p\nu_2(\psi_1), p\nu(\psi_0)) & \\ = \min((p-1)k + p\nu_2(\psi_{p-1}), (p-2)k + p\nu_2(\psi_{p-2}), \ldots, & \\ k + p\nu_2(\psi_1), p\nu(\psi_0)) & \end{aligned}$$

here, as before, we write $\nu_2(\psi_j) = \nu_2(\psi_j(m) - \psi_j(b))$ for $0 \leq j \leq n-1$.

The ψ_i are ordered in such a way that

$$\begin{aligned} \nu_2(m-b) &= \min(i : b_i \neq m_i) \\ \nu_2(\psi_{p-1}) &= \min(i : b_{pi+(((p-1)k-1) \pmod p)} \neq m_{pi+(((p-1)k-1) \pmod p)}) + \left\lceil \frac{p-(p-1)}{p} k \right\rceil \\ \nu_2(\psi_{p-2}) &= \min(i : b_{pi+(((p-2)k-1) \pmod p)} \neq m_{pi+(((p-2)k-1) \pmod p)}) + \left\lceil \frac{p-(p-2)}{p} k \right\rceil \\ &\vdots \end{aligned}$$

$$\nu_2(\psi_1) = \min(i : b_{pi+((k-1) \pmod p)} \neq m_{pi+((k-1) \pmod p)}) + \left\lceil \frac{p-1}{p} k \right\rceil$$

$$\nu_2(\psi_0) = \min(i : b_{pi+(p-1)} \neq m_{pi+(p-1)}) + (k+1)$$

where $b = \sum_{i \geq 0} b_i 2^i$ and $m = \sum_{i \geq 0} m_i 2^i$ are the expansions of b and m in base 2.

Proposition 4.3.5. With the above notation for the set $T_{2k} \subseteq \Delta_p$, we have

$$\nu(z^p - \psi_{p-1}(b) z^{p-1} + \psi_{p-2}(b) z^{p-2} - \cdots + (-1)^p \psi_0(b)) = pk + 1 + \nu_2(m-b) \ .$$

Proof. The value of $jk + p\nu_2(\psi_j)$ will depend on the residue of $\nu_2(m-b)$ modulo p.

Considering all residues of $\nu_2(m-b) \pmod p$, we will have:

$$p\nu_2(\psi_0) \begin{cases} \geq p\left(\frac{\nu_2(m-b)-i}{p} + (k+1)\right) & \text{for } \nu_2(m-b) \equiv i \pmod p, 0 \leq i \leq p-2 \\ = p\left(\frac{\nu_2(m-b)-(p-1)}{p} + (k+1)\right) & \text{for } \nu_2(m-b) \equiv p-1 \pmod p \end{cases}$$

$$jk + p\nu_2(\psi_j) \begin{cases} \geq jk + p\left(\frac{\nu_2(m-b)-i}{p} + \left\lceil \frac{p-j}{p} k \right\rceil\right) & \text{for } \nu_2(m-b) \equiv i \pmod p, \\ & \quad 0 \leq i \leq (jk-2 \pmod p) \\ = jk + p\left(\frac{\nu_2(m-b)-(jk-1 \pmod p)}{p} + \left\lceil \frac{p-j}{p} k \right\rceil\right) & \text{for } \nu_2(m-b) \equiv jk-1 \pmod p \\ \geq jk + p\left(\frac{\nu_2(m-b)-i}{p} + \left\lceil \frac{p-j}{p} k \right\rceil + 1\right) & \text{for } \nu_2(m-b) \equiv i, \\ & \quad (jk \pmod p) \leq i \leq p-1 \end{cases}$$

Simplified, these expressions become:

$$p\nu_2(\psi_0) \begin{cases} \geq p(k+1) - i + \nu_2(m-b) & \text{for } \nu_2(m-b) \equiv i \pmod p, 0 \leq i \leq p-2 \\ = pk + 1 + \nu_2(m-b) & \text{for } \nu_2(m-b) \equiv p-1 \pmod p \end{cases}$$

$$jk + p\nu_2(\psi_j) \begin{cases} \geq jk + p\left\lceil \frac{p-j}{p} k \right\rceil - i + \nu_2(m-b) & \text{for } \nu_2(m-b) \equiv i \pmod p, \\ & \quad 0 \leq i \leq (jk-2 \pmod p) \\ = jk + p\left\lceil \frac{p-j}{p} k \right\rceil - (jk-1 \pmod p) + \nu_2(m-b) & \text{for } \nu_2(m-b) \equiv jk-1 \pmod p \\ \geq jk + p\left\lceil \frac{p-j}{p} k \right\rceil + p - i + \nu_2(m-b) & \text{for } \nu_2(m-b) \equiv i, \\ & \quad (jk \pmod p) \leq i \leq p-1 \end{cases}$$

It is straightforward to observe that, across all residues of $\nu_2(m-b) \pmod p$,

$$\min(jk + p\nu_2(\psi_j)) = \begin{cases} pk + 1 + \nu_2(m-b) & \text{if } j = 0 \\ jk + p\left\lceil \frac{p-j}{p} k \right\rceil - (jk-1 \pmod p) + \nu_2(m-b) & \text{if } 1 \leq j \leq p-1 \end{cases}$$

with this minimum occurring precisely when $\nu_2(m-b) \equiv jk-1 \pmod p$.

Note that for $1 \leq j \leq p-1$, since $1 \leq k \leq p-1$, we know that $jk \not\equiv 0 \pmod{p}$ so that

$$(jk-1) \pmod{p} = (jk \pmod{p}) - 1 \ ,$$

and note also that

$$jk - (jk \pmod{p}) = p \left\lfloor \frac{jk}{p} \right\rfloor \ .$$

Therefore

$$\begin{aligned} jk + p\left\lceil \frac{p-j}{p} k \right\rceil - (jk - 1 \pmod{p}) + \nu_2(m-b) & \\ &= jk - (jk \pmod{p}) + p\left\lceil \frac{p-j}{p} k \right\rceil + 1 + \nu_2(m-b) \\ &= p\left\lfloor \frac{jk}{p} \right\rfloor + p\left\lceil k - \frac{jk}{p} \right\rceil + 1 + \nu_2(m-b) \\ &= p\left\lfloor \frac{jk}{p} \right\rfloor + p\left(k - \left\lfloor \frac{jk}{p} \right\rfloor\right) + 1 + \nu_2(m-b) \\ &= pk + 1 + \nu_2(m-b) \end{aligned}$$

Hence

$$\min_{0 \leq j \leq p-1} (jk + p\nu_2(\psi_j)) = pk + 1 + \nu_2(m-b) \ ,$$

and we obtain the result

$$\begin{aligned} \nu(z^p - \psi_{p-1}(b)z^{p-1} + \psi_{p-2}(b)z^{p-2} - \cdots + (-1)^p\psi_0(b)) & \\ &= \min((p-1)k + p\nu_2(\psi_{p-1}), (p-2)k + p\nu_2(\psi_{p-2}), \ldots, \\ &\qquad\qquad k + p\nu_2(\psi_1), p\nu(\psi_0)) \\ &= pk + 1 + \nu_2(m-b) \end{aligned}$$

□

Lemma 4.3.6. If $z \in T_{2k}$ then

$$\nu(g_n^{(k)}(z)) \geq (pk+1)n + \sum_{i>0} \left\lfloor \frac{n}{2^i} \right\rfloor$$

with equality if $\psi(n) = (\psi_0(n), \ldots, \psi_{p-1}(n))$ gives the tuple of coefficients $a_0, \ldots, a_{p-1}$ of the characteristic polynomial for $z \in T_{2k}$.

Proof. As $g_n^{(k)}(z)$ is defined by

$$g_n^{(k)}(x) = \prod_{b=0}^{n-1}(x^p - \psi_{p-1}(b)x^{p-1} + \psi_{p-2}(b)x^{p-2} - \cdots + (-1)^p\psi_0(b))$$

and

$$\nu(z^p - \psi_{p-1}(b)z^{p-1} + \psi_{p-2}(b)z^{p-2} - \cdots + (-1)^p\psi_0(b)) = pk + 1 + \nu_2(m-b)$$

by Proposition 4.3.5, it follows that

$$\begin{aligned}
\nu(g_n^{(k)}(z)) &= \sum_{b=0}^{n-1}(pk + 1 + \nu_2(m-b)) \\
&= (pk+1)n + \sum_{b=0}^{n-1}\nu_2(m-b) \\
&= (pk+1)n + \sum_{b=1}^{n}\nu_2(b) - \sum_{b=1}^{m-n}\nu_2(b) \\
&= (pk+1)n + \sum_{i>0}\left(\left\lfloor\frac{m}{2^i}\right\rfloor - \left\lfloor\frac{m-n}{2^i}\right\rfloor\right) \\
&\geq (pk+1)n + \sum_{i>0}\left\lfloor\frac{n}{2^i}\right\rfloor
\end{aligned}$$

with equality if $\psi(n) = (\psi_0(n), \ldots, \psi_{p-1}(n))$ gives the tuple of coefficients $a_0, \ldots, a_{p-1}$ of the characteristic polynomial for $z \in T_{2k}$. □

4.3.3 ν-sequences of S and T_{2k}

Given the inequalities for $\nu(f_n(z))$ and $\nu(g_n^{(k)}(z))$ that we have determined, we now wish to establish a formula for the ν-sequences α_S and $\alpha_{T_{2k}}$. By the embedding theorem (Theorem 2.5.5), for any n there exist elements $a_n, b_n \in \Delta_p$ which are roots of the polynomials

$$\begin{aligned}
&x^p - \phi_{p-1}(n)x^{p-1} + \phi_{p-2}(n)x^{p-2} - \cdots + (-1)^p\phi_0(n) \\
&x^p - \psi_{p-1}(n)x^{p-1} + \psi_{p-2}(n)x^{p-2} - \cdots + (-1)^p\psi_0(n)
\end{aligned}$$

respectively. This observation leads to the following results.

Lemma 4.3.7. Let a be a root of the polynomial $f(x) = x^p - \phi_{p-1}(n)x^{p-1} + \phi_{p-2}(n)x^{p-2} - \cdots + (-1)^p\phi_0(n)$ in S_i as given in Section 4.3.1, with θ the automorphism in Δ_p given by $\theta(t) = \pi t \pi^{-1}$. The set of roots $a, \theta(a), \ldots, \theta^{p-1}(a)$ are distinct modulo π, so that $\nu(\theta^i(a) - \theta^j(a)) = 0$ for $i \neq j$.

Proof. By Theorem 2.3.6, if a is a root of $f(x)$ then so too are all $\theta^i(a)$. The element $a \equiv \omega^j \pmod{\pi}$ for some choice of $1 \leq j \leq 2^p - 1$, and since $\theta(\omega^j) = \omega^{2j}$, it follows that the set of roots $\{\theta^i(a)\}_{i=0}^{p-1} \equiv \{\omega^{2^i j}\}_{i=0}^{p-1} \pmod{\pi}$, and that these roots are distinct modulo π. Since conjugate elements $\theta^i(a)$ and $\theta^j(a)$ will lie in different cosets modulo π, the result $\nu(\theta^i(a) - \theta^j(a)) = 0$ for $i \neq j$ follows. □

Lemma 4.3.8. The ν-sequence α_S of $S \subseteq \Delta_p$ is given by

$$\alpha_S(pn) = \alpha_S(pn+1) = \cdots = \alpha_S(pn+(p-1)) = pn + p\sum_{i>0} \left\lfloor \frac{n}{2^{pi}} \right\rfloor \ .$$

Proof. Recalling that

$$f_n(x) = \prod_{b=0}^{n-1} (x^p - \phi_{p-1}(b)x^{p-1} + \phi_{p-2}(b)x^{p-2} - \cdots + (-1)^p\phi_0(b)) \ ,$$

we can see that $f_n(x)$ is the minimal polynomial of the set

$$\{a_0, \theta(a_0), \theta^2(a_0), \ldots, \theta^{p-1}(a_0), a_1, \theta(a_1), \ldots, \theta^{p-1}(a_1), \ldots, a_{n-1}, \theta(a_{n-1}), \ldots, \theta^{p-1}(a_{n-1})\}$$

where θ is the automorphism $\theta(t) = \pi t \pi^{-1}$ in Δ_p. By Definition 2.5.7, this shows that

$$\{a_0, \theta(a_0), \theta^2(a_0), \ldots, \theta^{p-1}(a_0), a_1, \theta(a_1), \ldots, \theta^{p-1}(a_1), \ldots\}$$

forms a ν-ordering for S. By Lemma 4.3.7, each set of p elements $a_i, \theta(a_i), \ldots, \theta^{p-1}(a_i)$ will give rise to the same value in the ν-sequence for S, and so by the inequality given in Lemma 4.3.3,

$$\alpha_S(pn) = \alpha_S(pn+1) = \cdots = \alpha_S(pn+(p-1)) = pn + p\sum_{i>0} \left\lfloor \frac{n}{2^{pi}} \right\rfloor \ .$$

□

Lemma 4.3.9. Let b be a root of the polynomial $g(x) = x^p - \psi_{p-1}(n)x^{p-1} + \psi_{p-2}(n)x^{p-2} - \cdots + (-1)^p\psi_0(n)$ in T_{2k} as given in Section 4.3.2, with θ the automorphism in Δ_p given by $\theta(t) = \pi t \pi^{-1}$. The set of roots $b, \theta(b), \ldots \theta^{p-1}(b)$ are distinct modulo π^{k+1}, so that $\nu(\theta^i(b) - \theta^j(b)) = k$ for $i \neq j$.

Proof. If $b \equiv \pi^k \pmod{\pi^{k+1}}$, take instead $b \equiv \omega\pi^k \pmod{\pi^{k+1}}$ – this choice can be made since π^k and $\omega\pi^k$ are conjugates: $\omega^{-1}\pi^k\omega = \omega\pi^k$. By Theorem 2.3.6, if b is a root of $g(x)$ then so too are all $\theta^i(b)$. The element $b \equiv \bar{b}\pi^k \pmod{\pi^{k+1}}$ for some choice of $\bar{b} \not\equiv 0 \pmod{\pi}$. Applying our automorphism, we obtain modulo π^{k+1}

$$\theta(b) = \theta(\bar{b}\pi^k) = \theta(\bar{b})\theta(\pi^k) = \theta(\bar{b})\pi^k \ .$$

As in the proof of Lemma 4.3.7, the collection of elements $\{\theta^i(\bar{b})\}_{i=0}^{p-1}$ are distinct modulo π, and hence $\{\theta^i(b)\}_{i=0}^{p-1}$ are distinct modulo π^{k+1}. Since conjugate elements $\theta^i(b)$ and $\theta^j(b)$ will lie in different cosets modulo π^{k+1}, the result $\nu(\theta^i(b) - \theta^j(b)) = k$ for $i \neq j$ follows. □

Lemma 4.3.10. The ν-sequence $\alpha_{T_{2k}}$ of $T_{2k} \subseteq \Delta_p$ is given by

$$\begin{aligned}\alpha_{T_{2k}}(pn) = \alpha_{T_{2k}}(pn+1) - k = \alpha_{T_{2k}}(pn+2) - 2k = \cdots \\ = \alpha_{T_{2k}}(pn+(p-1)) - (p-1)k = (pk+1)n + \sum_{i>0}\left\lfloor \frac{n}{2^i} \right\rfloor \ .\end{aligned}$$

Proof. Similar to the previous proof,

$$g_n^{(k)}(x) = \prod_{b=0}^{n-1}(x^p - \psi_{p-1}(b)x^{p-1} + \psi_{p-2}(b)x^{p-2} - \cdots + (-1)^p\psi_0(b))$$

is the minimal polynomial of the set

$$\{b_0, \theta(b_0), \theta^2(b_0), \ldots, \theta^{p-1}(b_0), b_1, \theta(b_1), \ldots, \theta^{p-1}(b_1), \ldots, b_{n-1}, \theta(b_{n-1}), \ldots, \theta^{p-1}(b_{n-1})\}$$

where θ is the automorphism $\theta(t) = \pi t \pi^{-1}$ in Δ_p.Therefore

$$\{b_0, \theta(b_0), \theta^2(b_0), \ldots, \theta^{p-1}(b_0), b_1, \theta(b_1), \ldots, \theta^{p-1}(b_1), \ldots\}$$

forms a ν-ordering for T_{2k}. By Lemma 4.3.9, the difference in valuation associated with elements $a_i, \theta(a_i), \ldots, \theta^{p-1}(a_i)$ will be an increase of k each time. By the inequality given in Lemma 4.3.10,

$$\begin{aligned}\alpha_{T_{2k}}(pn) = \alpha_{T_{2k}}(pn+1) - k = \alpha_{T_{2k}}(pn+2) - 2k = \cdots \\ = \alpha_{T_{2k}}(pn+(p-1)) - (p-1)k = (pk+1)n + \sum_{i>0}\left\lfloor \frac{n}{2^i} \right\rfloor \ .\end{aligned}$$

□

4.4 The ν-sequence of Δ_p

In Section 4.1, we described the various conjugacy classes in Δ_p. This information is summarized in the form of the tree shown in Figure 4.1, together with the binary tree in Figure 4.2.

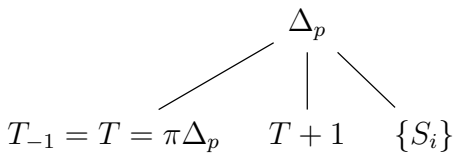

Figure 4.1: Tree summarizing the first level of decomposition of Δ_p into conjugacy classes.

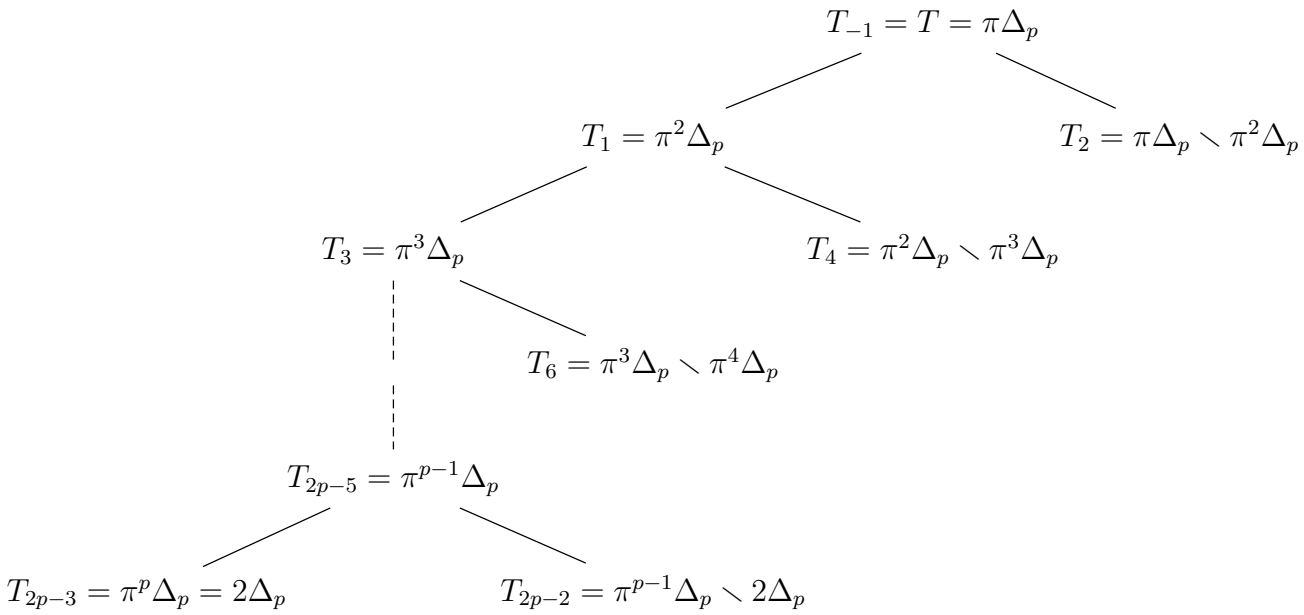

Figure 4.2: Tree summarizing decomposition of $T \subseteq \Delta_p$.

Given this information, it is apparent that the ν-sequence of Δ_p will be recursively defined, and will furthermore depend on the ν-sequences of T and the collection $\{S_i\}$. The ν-sequence for T will itself be dependent on that of Δ_p and all of the sets T_{2k} with $1 \leq k \leq p-1$.

To determine the ν-sequence of the set T, we will use downward induction to determine the ν-sequence of T_{2k-3}, with T corresponding to the case that $k = 1$.

Proposition 4.4.1. Let $1 \leq k \leq p-1$. Then the ν-sequence of T_{2k-3}, denoted $\alpha_{T_{2k-3}}$ is given by the expression

$$\begin{aligned}\alpha_{T_{2k-3}} = \Big[\cdots \Big[\Big[(\alpha_{\Delta_p} + (n)) \wedge \Big(\alpha_{T_{2(p-1)}} - ((p-1)n)\Big) + (n)\Big] \\ \wedge \Big(\alpha_{T_{2(p-2)}} - ((p-2)n)\Big) + (n)\Big] \wedge \cdots\Big] \wedge (\alpha_{T_{2k}} - (kn)) + (kn)\end{aligned}$$

where $T_{-1} = T = \pi\Delta_p$.

Proof. By Lemmas 2.5.9 and 2.5.11 and the tree diagram for the decomposition of Δ_p given in Figure 4.1, we see that

$$\begin{aligned}\alpha_{T_{2k-3}} &= \alpha_{T_{2k-1} \cup T_{2k}} \\ &= (\alpha_{T_{2k-1}} - (kn)) \wedge (\alpha_{T_{2k}} - (kn)) + (kn) \\ \alpha_{T_{2p-3}} &= \alpha_{\Delta_p} + (pn)\end{aligned}$$

We proceed with the proof using downward induction, starting with the base case where $k = p - 1$. In this case, we are computing the ν-sequence for T_{2p-5}.

$$\begin{aligned}\alpha_{T_{2p-5}} &= (\alpha_{T_{2p-3}} - ((p-1)n)) \wedge (\alpha_{T_{2p-2}} - ((p-1)n)) + ((p-1)n) \\ &= (\alpha_{\Delta_p} + (pn) - ((p-1)n)) \wedge (\alpha_{T_{2p-2}} - ((p-1)n)) + ((p-1)n) \\ &= (\alpha_{\Delta_p} + (n)) \wedge (\alpha_{T_{2p-2}} - ((p-1)n)) + ((p-1)n) \\ &= (\alpha_{\Delta_p} + (n)) \wedge (\alpha_{T_{2(p-1)}} - ((p-1)n)) + ((p-1)n)\end{aligned}$$

which is what we expect from the Proposition statement.

Suppose the statement is true for some $1 < k \leq p - 1$, we want to show that it is also true for $k - 1$, namely for the set T_{2k-5}. For ease of notation, let us denote $\boldsymbol{\alpha} = \alpha_{T_{2k-3}} - (kn)$.

$$\begin{aligned}\alpha_{T_{2k-5}} &= (\alpha_{T_{2k-3}} - ((k-1)n)) \wedge (\alpha_{T_{2k-2}} - ((k-1)n)) + ((k-1)n) \\ &= (\boldsymbol{\alpha} + (kn) - ((k-1)n)) \wedge (\alpha_{T_{2(k-1)}} - ((k-1)n)) + ((k-1)n) \\ &= (\boldsymbol{\alpha} + (n)) \wedge (\alpha_{T_{2(k-1)}} - ((k-1)n)) + ((k-1)n)\end{aligned}$$

so that

$$\begin{aligned}\alpha_{T_{2k-5}} = \Big[\Big[\cdots\Big[\Big[(\alpha_{\Delta_p}+(n))\wedge\Big(\alpha_{T_{2(p-1)}}-((p-1)n)\Big)+(n)\Big] \\ \wedge\ \Big(\alpha_{T_{2(p-2)}}-((p-2)n)\Big)+(n)\Big]\wedge\cdots\Big]\wedge(\alpha_{T_{2k}}-(kn))+(n)\Big] \\ \wedge\Big(\alpha_{T_{2(k-1)}}-((k-1)n)\Big)+((k-1)n)\end{aligned}$$

proving the Proposition. □

From this, we easily obtain the following corollary.

Corollary 4.4.2. The ν-sequence α_T of the set $T=\pi\Delta_p$ is given by

$$\begin{aligned}\alpha_T = \Big[\cdots\Big[\Big[(\alpha_{\Delta_p}+(n))\wedge\Big(\alpha_{T_{2(p-1)}}-((p-1)n)\Big)+(n)\Big] \\ \wedge\ \Big(\alpha_{T_{2(p-2)}}-((p-2)n)\Big)+(n)\Big]\wedge\cdots\Big]\wedge(\alpha_{T_2}-(n))+(n)\end{aligned}$$

Proof. The result immediately follows from Proposition 4.4.1 with $k=1$ and the understanding that $T_{-1}=T=\pi\Delta_p$. □

Having determined a formula for α_T, we can now give an expression for the ν-sequence of Δ_p that depends only on itself, the ν-sequence of S, and that of each set $T_{2k}, 1\le k\le p-1$.

Proposition 4.4.3. The ν-sequence α_{Δ_p} of the maximal order Δ_p is determined by the recursive formula

$$\begin{aligned}\alpha_{\Delta_p} = \Big[\Big[\cdots\Big[\Big[(\alpha_{\Delta_p}+(n))\wedge\Big(\alpha_{T_{2(p-1)}}-((p-1)n)\Big)+(n)\Big] \\ \wedge\ \Big(\alpha_{T_{2(p-2)}}-((p-2)n)\Big)+(n)\Big]\wedge\cdots\Big]\wedge(\alpha_{T_2}-(n))+(n)\Big]^{\wedge 2}\wedge\alpha_S^{\wedge\frac{1}{p}(2^p-2)}\end{aligned}$$

Proof. By the observation in Corollary 4.3.4 all conjugacy classes in Δ_p that are defined by a monic irreducible polynomial of degree p have the same ν-sequence, of which there are $\frac{1}{p}(2^p-2)$ such sets. We also note that by Lemma 2.5.9 the ν-sequences of T and $T+1$ are equal. This gives

$$\alpha_{\Delta_p}=\alpha_T^{\wedge 2}\wedge\alpha_S^{\wedge\frac{1}{p}(2^p-2)},$$

which, given the result for α_T in Corollary 4.4.2, provides the result. □

Corollary 4.4.4.

The first 200 terms of α_{Δ_3} are

$$0,0,0,0,0,0,0,0,1,1,2,2,3,3,3,3,3,3,3,3,5,5,6,$$
$$6,6,6,6,6,6,6,7,7,8,8,9,9,9,9,9,9,10,10,12,12,$$
$$12,12,12,12,12,12,13,13,14,14,15,15,15,15,15,15,15,$$
$$15,17,17,18,18,18,18,18,18,18,18,19,19,21,21,21,21,$$
$$21,21,21,21,23,23,25,25,26,26,27,27,27,27,27,27,27,$$
$$27,28,28,30,30,30,30,30,30,30,30,31,31,32,32,33,33,$$
$$33,33,33,33,33,33,36,36,36,36,36,36,36,36,37,37,38,$$
$$38,39,39,39,39,39,39,39,39,41,41,42,42,42,42,42,42,$$
$$42,42,43,43,45,45,45,45,45,45,45,45,47,47,48,48,48,$$
$$48,48,48,49,49,51,51,52,52,53,53,54,54,54,54,54,54,$$
$$54,54,56,56,57,57,57,57,57,57,57,57,58,58,60,60,60,$$
$$60,60,60$$

The first 200 terms of α_{Δ_5} are

$$0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,$$
$$0,0,0,0,0,0,0,0,0,0,0,0,2,2,3,3,4,4,5,5,5,5,5,5,$$
$$5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,$$
$$5,5,5,6,6,8,8,9,9,10,10,10,10,10,10,10,10,10,10,$$
$$10,10,10,10,10,10,10,10,10,10,10,10,10,10,10,10,10,$$
$$10,10,10,10,10,11,11,12,12,13,13,15,15,15,15,15,15,$$
$$15,15,15,15,15,15,15,15,15,15,15,15,15,15,15,15,15,$$
$$15,15,15,15,15,15,15,15,15,17,17,18,18,19,19,20,20,$$
$$20,20,20,20,20,20,20,20,20,20,20,20,20,20,20,20,20,$$
$$20,20,20,20,20,20,20,20,20,20,20,20,20,21,21,22,22,$$
$$24,24,25,25,25,25,25,25,25,25$$

Note. The above results were generated using Mathematica. The code for the algorithms used to compute α_{Δ_3} and α_{Δ_5} can be found in Appendices A.1 and A.2, respectively.

4.5 A Regular Basis for Δ_p

Following the results of Lemmas 4.3.8 and 4.3.10, we obtain the following result as a corollary of Proposition 2.5.8.

Corollary 4.5.1.

i) The sequence of polynomials

$$\left\{\pi^{-\alpha_S(pn)} f_n(x), \pi^{-\alpha_S(pn+1)} x f_n(x), \ldots, \pi^{-\alpha_S(pn+(p-1))} x^{p-1} f_n(x) : n = 0, 1, 2 \ldots\right\}$$

forms a regular Δ_p-basis for $\mathrm{Int}(S_i, \Delta_p)$.

ii) The sequence of polynomials

$$\left\{\pi^{-\alpha_{T_{2k}}(pn)} g_n^{(k)}(x), \pi^{-\alpha_{T_{2k}}(pn+1)} x g_n^{(k)}(x), \ldots, \pi^{-\alpha_{T_{2k}}(pn+(p-1))} x^{p-1} g_n^{(k)}(x) : n = 0, 1, 2 \ldots\right\}$$

forms a regular Δ_p-basis for $\mathrm{Int}(T_{2k}, \Delta_p)$.

The result of Lemma 2.5.22 ([6], 2.15) regarding regular bases for subsets of Δ_2 in no way relies on the fact that our maximal order is of index 2, and can be extended without any trouble to Δ_p.

Lemma 4.5.2 (c.f. [6], 2.15)**.** If two subsets of Δ_p satisfying the hypotheses of Lemma 2.5.11 each have a regular basis whose elements are each quotients of polynomials in $\mathbb{Z}[x]$ by powers of π then their union has a basis of this form also.

Corollary 4.5.3 (c.f. [6], 2.16)**.** $\mathrm{Int}(\Delta_p)$ has a regular basis whose elements are each a quotient of a polynomial in $\mathbb{Z}[x]$ by a power of π.

4.6 Valuative Capacity

As introduced in Section 2.5.4, of some interest is the valuative capacity of the set Δ_p. This section seeks to establish an explicit formula for the valuative capacity $\lim_{n\to\infty} \frac{\alpha_{\Delta_p}(n)}{n}$. To understand this quantity, we must first describe the valuative capacities of subsets S and T_{2k} of Δ_p.

Lemma 4.6.1. For $S \subseteq \Delta_p$ characterized by an irreducible monic polynomial,

$$\lim_{n\to\infty} \frac{\alpha_S(n)}{n} = \frac{2^p}{2^p - 1} \ .$$

Proof. By Lemma 4.3.8, we have $\alpha_S(pn) = pn + p\sum_{i>0}\left\lfloor \frac{n}{2^{pi}} \right\rfloor$. Therefore

$$\lim_{n\to\infty} \frac{\alpha_S(n)}{n} = \lim_{pn\to\infty} \frac{\alpha_S(pn)}{pn} = 1 + \lim_{pn\to\infty} \frac{1}{n} \sum_{i>0} \left\lfloor \frac{n}{2^{pi}} \right\rfloor \ .$$

Since $\sum_{i>0} \frac{1}{2^{pi}} = \frac{1}{2^p-1}$,

$$\begin{aligned}
\sum_{i>0} \frac{n-1}{2^{pi}} \leq &\sum_{i>0} \left\lfloor \frac{n}{2^{pi}} \right\rfloor \leq \sum_{i>0} \frac{n}{2^{pi}} \\
\frac{n-1}{2^p-1} \leq &\sum_{i>0} \left\lfloor \frac{n}{2^{pi}} \right\rfloor \leq \frac{n}{2^p-1} \\
\lim_{pn\to\infty} \frac{n-1}{n(2^p-1)} \leq &\lim_{pn\to\infty} \frac{1}{n} \sum_{i>0} \left\lfloor \frac{n}{2^{pi}} \right\rfloor \leq \lim_{pn\to\infty} \frac{1}{2^p-1} \\
\frac{1}{2^p-1} \leq &\lim_{pn\to\infty} \frac{1}{n} \sum_{i>0} \left\lfloor \frac{n}{2^{pi}} \right\rfloor \leq \frac{1}{2^p-1}
\end{aligned}$$

so that

$$\lim_{n\to\infty} \frac{\alpha_S(n)}{n} = 1 + \lim_{pn\to\infty} \frac{1}{n} \sum_{i>0} \left\lfloor \frac{n}{2^{pi}} \right\rfloor = 1 + \frac{1}{2^p-1} = \frac{2^p}{2^p-1} \ .$$

□

Lemma 4.6.2. For $T_{2k} \subseteq \Delta_p$,

$$\lim_{n\to\infty} \frac{\alpha_{T_{2k}}(n)}{n} = \frac{pk+2}{p} \ .$$

Proof. By Lemma 4.3.10, we have $\alpha_{T_{2k}}(pn) = (pk+1)n + \sum_{i>0} \left\lfloor \frac{n}{2^i} \right\rfloor$. Therefore

$$\lim_{n\to\infty} \frac{\alpha_{T_{2k}}(n)}{n} = \lim_{pn\to\infty} \frac{\alpha_{T_{2k}}(pn)}{pn} = \frac{pk+1}{p} + \lim_{pn\to\infty} \frac{1}{pn} \sum_{i>0} \left\lfloor \frac{n}{2^i} \right\rfloor \ .$$

Since $\sum_{i>0} \frac{1}{2^i} = 1$,

$$\begin{aligned}
\sum_{i>0} \frac{n-1}{2^i} \leq &\sum_{i>0} \left\lfloor \frac{n}{2^i} \right\rfloor \leq \sum_{i>0} \frac{n}{2^i} \\
n-1 \leq &\sum_{i>0} \left\lfloor \frac{n}{2^i} \right\rfloor \leq n \\
\lim_{pn\to\infty} \frac{n-1}{pn} \leq &\lim_{pn\to\infty} \frac{1}{pn} \sum_{i>0} \left\lfloor \frac{n}{2^i} \right\rfloor \leq \lim_{pn\to\infty} \frac{1}{p} \\
\frac{1}{p} \leq &\lim_{pn\to\infty} \frac{1}{pn} \sum_{i>0} \left\lfloor \frac{n}{2^i} \right\rfloor \leq \frac{1}{p}
\end{aligned}$$

so that

$$\lim_{n\to\infty}\frac{\alpha_{T_{2k}}(n)}{n}=\frac{pk+1}{p}+\lim_{pn\to\infty}\frac{1}{pn}\sum_{i>0}\left\lfloor\frac{n}{2^i}\right\rfloor=\frac{pk+1}{p}+\frac{1}{p}=\frac{pk+2}{p}\ .$$

□

Corollary 4.6.3. For $T_{2k}\subseteq\Delta_p$,

$$\lim_{n\to\infty}\frac{\alpha_{T_{2k}}(n)}{n}-k=\frac{2}{p}\ .$$

Proposition 4.6.4. The valuative capacity of the set $T=\pi\Delta_p$ is given by the finite continued fraction

$$\lim_{n\to\infty}\frac{\alpha_T(n)}{n}=\left\langle\underbrace{1;\frac{p}{2},1,\frac{p}{2},\ldots,1,\frac{p}{2}}_{p-1\text{ times}},1+\lim_{n\to\infty}\frac{\alpha_{\Delta_p}(n)}{n}\right\rangle\ .$$

Proof. By Corollary 4.4.2,

$$\begin{aligned}\alpha_T=\Big[\cdots\Big[\Big[(\alpha_{\Delta_p}+(n))\wedge\Big(\alpha_{T_{2(p-1)}}-((p-1)n)\Big)+(n)\Big]\\ \wedge\ \Big(\alpha_{T_{2(p-2)}}-((p-2)n)\Big)+(n)\Big]\wedge\cdots\Big]\wedge(\alpha_{T_2}-(n))+(n)\end{aligned}$$

Using Proposition 2.5.26, we have

$$\begin{aligned}\lim_{n\to\infty}\frac{\alpha_T(n)}{n}&=1+\cfrac{1}{\cfrac{1}{\lim_{n\to\infty}\frac{\alpha_{T_2}(n)}{n}-1}+\cfrac{1}{\lim_{n\to\infty}\frac{\alpha_{T_1}(n)}{n}-1}}\\&=1+\cfrac{1}{\cfrac{1}{\lim_{n\to\infty}\frac{\alpha_{T_2}(n)}{n}-1}+\cfrac{1}{1+\cfrac{1}{\cfrac{1}{\lim_{n\to\infty}\frac{\alpha_{T_4}(n)}{n}-2}+\cfrac{1}{\lim_{n\to\infty}\frac{\alpha_{T_3}(n)}{n}-2}}}}\\&\ \ \vdots\end{aligned}$$

$$= \left\langle 1; \frac{1}{\lim_{n\to\infty} \frac{\alpha_{T_2}(n)}{n} - 1}, 1, \frac{1}{\lim_{n\to\infty} \frac{\alpha_{T_4}(n)}{n} - 2}, 1, \ldots, \right.$$
$$\left. 1, \frac{1}{\lim_{n\to\infty} \frac{\alpha_{T_{2(p-1)}}(n)}{n} - (p-1)}, \frac{1}{1 + \lim_{n\to\infty} \frac{\alpha_{\Delta_p}(n)}{n}} \right\rangle$$

By Corollary 4.6.3, we can simplify this expression to

$$\lim_{n\to\infty} \frac{\alpha_T(n)}{n} = \left\langle 1; \frac{1}{\lim_{n\to\infty} \frac{\alpha_{T_2}(n)}{n} - 1}, 1, \frac{1}{\lim_{n\to\infty} \frac{\alpha_{T_4}(n)}{n} - 2}, 1, \ldots, \right.$$
$$\left. 1, \frac{1}{\lim_{n\to\infty} \frac{\alpha_{T_{2(p-1)}}(n)}{n} - (p-1)}, \frac{1}{1 + \lim_{n\to\infty} \frac{\alpha_{\Delta_p}(n)}{n}} \right\rangle$$
$$= \left\langle \underbrace{1; \frac{1}{2/p}, 1, \frac{1}{2/p}, \ldots, 1, \frac{1}{2/p}}_{p-1 \text{ times}}, 1 + \lim_{n\to\infty} \frac{\alpha_{\Delta_p}(n)}{n} \right\rangle$$
$$= \left\langle \underbrace{1; \frac{p}{2}, 1, \frac{p}{2}, \ldots, 1, \frac{p}{2}}_{p-1 \text{ times}}, 1 + \lim_{n\to\infty} \frac{\alpha_{\Delta_p}(n)}{n} \right\rangle .$$

□

Given a closed-form expression for the valuative capacity of T, we can now determine a formula for the valuative capacity of Δ_p.

Theorem 4.6.5. The valuative capacity of Δ_p, denoted by $\lim_{n\to\infty} \frac{\alpha_{\Delta_p}(n)}{n}$, is the positive solution to the quadratic equation

$$\frac{1}{x} = \frac{(2^{p-1}-1)(2^p-1)}{p2^{p-1}} + \frac{2}{\left\langle \underbrace{1; \frac{p}{2}, 1, \frac{p}{2}, \ldots, 1, \frac{p}{2}}_{p-1 \text{ times}}, 1 + x \right\rangle} .$$

Proof. By Proposition 2.5.26 and the fact that $\alpha_{\Delta_p} = \alpha_T^{\wedge 2} \wedge \alpha_S^{\wedge \frac{1}{p}(2^p-2)}$, we have

$$\lim_{n\to\infty} \frac{\alpha_{\Delta_p}(n)}{n} = \frac{1}{\frac{(2^p-1)/p}{\lim_{n\to\infty} \frac{\alpha_S(n)}{n}} + \frac{2}{\lim_{n\to\infty} \frac{\alpha_T(n)}{n}}} .$$

By Lemma 4.6.1 and Proposition 4.6.4, this can be written as

$$\lim_{n\to\infty}\frac{\alpha_{\Delta_p}(n)}{n} = \frac{1}{\frac{(2^p-1)/p}{2^p/2^p-1}+\frac{2}{\left\langle \underbrace{1;\frac{p}{2},1,\frac{p}{2},\ldots,1,\frac{p}{2}}_{p-1\text{ times}},1+\lim_{n\to\infty}\frac{\alpha_{\Delta_p}(n)}{n}\right\rangle}}$$

$$= \frac{1}{\frac{(2^{p-1}-1)(2^p-1)}{p2^{p-1}}+\frac{2}{\left\langle \underbrace{1;\frac{p}{2},1,\frac{p}{2},\ldots,1,\frac{p}{2}}_{p-1\text{ times}},1+\lim_{n\to\infty}\frac{\alpha_{\Delta_p}(n)}{n}\right\rangle}}$$

so that

$$\frac{1}{\lim_{n\to\infty}\frac{\alpha_{\Delta_p}(n)}{n}} = \frac{(2^{p-1}-1)(2^p-1)}{p2^{p-1}}+\frac{2}{\left\langle \underbrace{1;\frac{p}{2},1,\frac{p}{2},\ldots,1,\frac{p}{2}}_{p-1\text{ times}},1+\lim_{n\to\infty}\frac{\alpha_{\Delta_p}(n)}{n}\right\rangle}.$$

Letting $x = \lim_{n\to\infty}\frac{\alpha_{\Delta_p}(n)}{n}$, we see that this value is equivalent to the positive root of the quadratic

$$\frac{1}{x} = \frac{(2^{p-1}-1)(2^p-1)}{p2^{p-1}}+\frac{2}{\left\langle \underbrace{1;\frac{p}{2},1,\frac{p}{2},\ldots,1,\frac{p}{2}}_{p-1\text{ times}},1+x\right\rangle},$$

proving the theorem. □

Example 1. When $p = 2$, the valuative capacity $\lim_{n\to\infty}\frac{\alpha_{\Delta_2}(n)}{n}$ of Δ_2 is the positive solution to the expression

$$\frac{1}{x} = \frac{(2^{2-1}-1)(2^2-1)}{2\cdot 2^{2-1}}+\frac{2}{\left\langle 1;\frac{2}{2},1+x\right\rangle}$$

$$= \frac{3}{4}+\frac{2}{\langle 1;1,1+x\rangle}$$

which has positive solution $x = \frac{1}{2}$. This agrees with the result in [11] presented in

Section 2.5.4.

Example 2. When $p = 3$, the valuative capacity $\lim_{n\to\infty} \frac{\alpha_{\Delta_2}(n)}{n}$ of Δ_3 is the positive solution to the expression

$$\begin{aligned}\frac{1}{x} &= \frac{(2^{3-1}-1)(2^3-1)}{3\cdot 2^{3-1}} + \frac{2}{\left\langle 1; \frac{3}{2}, 1, \frac{3}{2}, 1+x \right\rangle} \\ &= \frac{7}{4} + \frac{2}{\left\langle 1; \frac{3}{2}, 1, \frac{3}{2}, 1+x \right\rangle}\end{aligned}$$

which has positive solution

$$x = \frac{-439 + \sqrt{469\ 921}}{770} \approx 0.32014\ .$$

Chapter 5

Conclusion

5.1 Summary

In this text, we examined explicitly a construction to describe the integer-valued polynomials on the maximal order in a division algebra of index 3 over $\mathbb{Q}_2$. We then successfully extended this to the index p case, when p is an odd prime. This was done using a method analogous to that used by Evrard and Johnson in [6] and [11] in the index 2 case, by way of representing the maximal order Δ_p as an extension of $\mathbb{Z}_2$ by $p \times p$ matrices, splitting Δ_p into sets closed under conjugation modulo powers of π, determining characteristic polynomials which describe these sets, and using ν-orderings and ν-sequences to establish a regular basis for integer-valued polynomials over these sets.

5.2 Future Work

We have learned much about describing the integer-valued polynomials of maximal orders over division algebras of prime index over $\mathbb{Q}_2$, but there remain some natural questions.

5.2.1 The index n, 2-local case

> *What happens if we drop the restriction that the index of the division algebra is prime?*

In the case that $n > 1$ is composite, there are two places where we will see problems arising in the decomposition of Δ_n into sets that are closed under conjugation. The first is in the fact that there will be some ω^i for $1 \leq i \leq 2^n - 2$, with ω a $(2^n - 1)^{\text{th}}$ root

of unity, that do not lie in a set determined by an irreducible polynomial modulo 2. Recall from Section 4.1 that the number of monic irreducible polynomials of degree n over $\mathbb{F}_2$ is given by

$$I_2(n) = \frac{1}{n}\sum_{d|n} \mu(d) 2^{n/d} \ ,$$

where μ is the Möbius function. The sequence $I_2(n)$ is A001037 in the OEIS [8]. Note that under the conjugation $\pi\omega^i\pi^{-1} = \omega^{2i}$ and because $\omega^{2^n} = \omega \cdot \omega^{2^p-1} = \omega$, the collection $\{\omega^{2^k i}\}_{i=0}^{n-1}$ of at most n elements will constitute a conjugacy class modulo π, though these elements may not be distinct.

If $n = p$ a is prime, then $I_2(p) = \frac{1}{p}(2^p - 2)$ polynomials with p corresponding roots each means that all $2^p - 2$ elements $\omega, \omega^2, \ldots, \omega^{2^p-2}$ are accounted for. However, it appears that if $n \in \mathbb{Z}_{>1}$ is composite, then

$$nI_2(n) < 2^n - 2 \ .$$

This holds up to $n = 100,000$, as shown by the Mathematica code in Appendix A.3, and we conjecture that it holds true in general. If this statement is true, then consequently there exists some element ω^i which is not the root of an irreducible polynomial of degree n – and of course, because n is composite, this ω^i can (and will) instead be the root of an irreducible polynomial of degree dividing n. As a result, we will need to devise a way of determining the ν-sequence for a set S for which all $z \in S$ satisfy $\nu(z) = 0$, but S is determined by a polynomial which is reducible modulo 2.

Another problem will arise when splitting the set $\pi^d\Delta_n$ into sets closed under conjugation modulo π^{d+1} for $1 \leq d < n$ such that $\gcd(d, n) > 1$. Consider an element $\omega^k\pi^d \in \pi^d\Delta_n \setminus \pi^{d+1}\Delta_n$, conjugated by an arbitrary element $\omega^i\pi^j$:

$$\begin{aligned}
(\omega^i\pi^j)\omega^k\pi^d(\pi^{-j}\omega^{-i}) &= \omega^i\pi^j\omega^k\pi^{d-j}\omega^{-i} \\
&= \omega^i\pi^j\omega^k\omega^{-2^{d-j}i}\pi^{d-j} \\
&= \omega^i\pi^j\omega^{k-2^{d-j}i}\pi^{d-j} \\
&= \omega^i\omega^{2^j(k-2^{d-j}i)}\pi^d \\
&= \omega^{2^j(k-2^{d-j}i)+i}\pi^d \\
&= \omega^{2^jk-(2^d-1)i}\pi^d
\end{aligned}$$

Note that the elements $\omega^k\pi^d$ with $k \equiv 0 \pmod{2^d - 1}$ will form their own set that is closed under conjugation, so that $\pi^d\Delta_n$ will split into at least three subsets closed under conjugation: $\pi^{d+1}\Delta_n$, $\{z \equiv \omega^{(2^d-1)\ell}\pi^d \pmod{\pi^{d+1}}\}$, and a collection of sets

(possibly only one) whose union is $\{z \equiv \omega^k \pi^d \pmod{\pi^{d+1}}, k \not\equiv 0 \pmod{2^d - 1}\}$. It may prove difficult to describe these sets in terms of the residues of coefficients of their characteristic polynomials, posing yet another challenge in our goal of finding an analogous construction to that in the index p case.

Even if we are able to describe these sets in terms of characteristic polynomials, in a similar vein to Equation 4.3 in Section 4.3.2, we will see that if we try to apply our previous construction to obtain the valuation of such a polynomial, we will obtain

$$\begin{aligned}\nu((\psi_j(m) - \psi_j(k))z^j) &= n\nu_2(\psi_j(m) - \psi_j(k)) + \nu(z^j) \\ &= n\nu_2(\psi_j(m) - \psi_j(k)) + j\nu(z) \\ &\equiv j\nu(z) \pmod{n}\end{aligned}$$

which will *not* result in a complete set of residues modulo n as j varies in the case that $\gcd(\nu(z), n) > 1$. Computational results in index 4 show that the original construction will result in the minimum valuation of a polynomial with coefficients satisfying the same congruences as the characteristic polynomial having two possible values, depending on a valuation that involves an arbitrary quantity. It seems that an alternate approach may be necessary to come up with an analogous construction for sets when $\gcd(\nu(z), n) > 1$.

5.2.2 The prime index case, localized at an odd prime q

What happens if our division algebra is over $\mathbb{Q}_q$, with q an odd prime?

In [11], Johnson established a description for the integer-valued polynomials in the 2-local case for index 2, and these results were later generalized by Evrard and Johnson in [6] for the p-local case for index 2 – one may be interested in such an extension in the index p case, q-locally (with q an odd prime).

The construction of minimal polynomials as discussed in Section 4.3.2 can be extended to the q-local case, as shown in Appendix B. This result does not assume any knowledge of the structure of Δ_p over $\mathbb{Q}_q$ such as the structure of its subsets that are closed under conjugation or the corresponding characteristic polynomial, but instead works very generally and may be specified upon further study of the decomposition of the maximal order in the q-local case.

Bibliography

[1] M. Bhargava. p-orderings and polynomial functions on arbitrary subsets of Dedekind rings. *Journal fur die reine und angewandte Mathematik*, 490:101–127, 1997.

[2] M. Bhargava. The factorial function and generalizations. *The American Mathematical Monthly*, 107(9):783–799, 2000.

[3] P.-J. Cahen and J.-L. Chabert. *Integer-Valued Polynomials*, volume 48 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, USA, 1997.

[4] P.-J. Cahen and J.-L. Chabert. What you should know about integer-valued polynomials. *The American Mathematical Monthly*, 123(4):311–337, 2016.

[5] J.-L. Chabert. Generalized factorial ideals. *The Arabian Journal for Science and Engineering*, 26:51–68, 2001.

[6] S. Evrard and K. Johnson. The ring of integer valued polynomials on 2×2 matrices and its integral closure. *Journal of Algebra*, 441:660–677, 2015.

[7] S. Frisch. Polynomial separation of points in algebras. *Arithmetical Properties of Commutative Rings and Monoids (Chapel Hill Conf. 2003), Lect. Notes in Pure and Appl. Math*, 241:253–259, 2005.

[8] The OEIS Foundation Inc. A001037: Number of degree-n irreducible polynomials over GF(2), February 2020.

[9] K. Ireland and M. Rosen. *A Classical Introduction to Modern Number Theory*. Springer-Verlag, New York, 1982.

[10] K. Johnson. Limits of characteristic sequences of integer-valued polynomials on homogeneous sets. *Journal of Number Theory*, 129:2933–2942, 2009.

[11] K. Johnson. p-orderings of noncommutative rings. *Proceedings of the American Mathematical Society*, 143(8):3265–3279, 2015.

[12] T.Y. Lam. *A First Course in Noncommutative Rings*. Number 131 in Graduate Texts in Mathematics. Springer-Verlag, New York, 2nd edition, 2001.

[13] K.A. Loper and N.J. Werner. Generalized rings of integer-valued polynomials. *Journal of Number Theory*, 132:2481–2490, 2012.

[14] I. Reiner. *Maximal Orders*. London Mathematical Society. Academic Press, London, 1975.

[15] K.H. Rosen. *Handbook of Discrete and Combinatorial Mathematics*. CRC Press, Boca Raton, 2nd edition, 2017.

[16] J-P. Serre. Local class field theory. In J.W.S. Cassels and A. Frohlich, editors, *Algebraic Number Theory*, chapter VI, pages 128–161. Thompson Book Company Inc., Washington, D.C., 1967.

Appendix A

Mathematica Code

A.1 Generating α_{Δ_3}

The following code generates the *v*-sequence α for $\Delta 3$.

Generate elements of αS, wedge with self to obtain αS2

In[194]:=
```
αS = {}; For[n = 0, n < 20, n++,
 For[j = 0, j < 3, j++,
  AppendTo[αS,
   3 * n + 3 * Sum[Floor[n / 8^i], {i, 1, 3}]]]];
αS2 = Sort[Join[αS, αS]];
```

Generate elements of αT2

In[195]:=
```
αT2 = {}; For[n = 0, n < 30, n++,
 For[j = 0, j < 3, j++,
  AppendTo[αT2,
   j + 4 * n + Sum[Floor[n / 2^i], {i, 1, 5}]]]]
```

Generate elements of αT4

In[196]:=
```
αT4 = {}; For[n = 0, n < 30, n++,
 For[j = 0, j < 3, j++,
  AppendTo[αT4,
   2 * j + 7 * n + Sum[Floor[n / 2^i], {i, 1, 5}]]]]
```

Compute αT2 - (n) and αT4 - (2n)

In[197]:=
```
nn = {}; For[n = 0, n < 100, n++, AppendTo[nn, n]];
αT2n = αT2 - Take[nn, Length[αT2]];
αT4n = αT4 - 2 * Take[nn, Length[αT4]];
```

Initialize α and α + (n) by taking first element of αS2

In[198]:=
```
α = {};
αn = {};
a = TakeDrop[αS2, 1];
α = Join[α, a[[1]]];
αn = Join[αn, a[[1]]];
αS2 = a[[2]];
```

Initialize (α + (n)) ∧ (αT4 - (2n)) and [(α + (n)) ∧ (αT4 - (2n))] + (n) by taking first element of αT4 - (2n)

In[199]:=
```
αnT4 = {};
αnT4n = {};
b = TakeDrop[αT4n, 1];
αnT4 = Join[αnT4, b[[1]]];
αnT4n = Join[αnT4n, b[[1]]];
αT4n = b[[2]];
```

Initialize [[[(α + (n)) ∧ (αT4 - (2n))] + (n)] ∧ (αT2 - (n))] + (n) by taking first element of αT2 - (n); initialize the wedge of this sequence with itself

In[200]:=
```
αnT4T2n = {};
b = TakeDrop[αT2n, 1];
αnT4T2n = Join[αnT4T2n, b[[1]] + Length[αnT4T2n]];
αT2n = b[[2]];
αnT4T2n2 = Sort[Join[αnT4T2n, αnT4T2n]];
```

Loop through elements of sequences to generate α

In[201]:=
```
While[αS2 ≠ {} && αT2n ≠ {} && αT4n ≠ {},
 (* append an element to α *)
 If[First[αS2] ≤ First[αnT4T2n2],
  (* if first element of αS2 is smaller, pick that one *)
  a = TakeDrop[αS2, 1];
  α = Join[α, a[[1]]];
  αS2 = a[[2]];
  AppendTo[αn, Last[α] + Length[α] - 1],
  (**)
  (* otherwise take first element of αnT4T2n2 *)
  a = TakeDrop[αnT4T2n2, 1];
  α = Join[α, a[[1]]];
  αnT4T2n2 = a[[2]];
  AppendTo[αn, Last[α] + Length[α] - 1]];
 (* update αnT4T2n based on new α value *)
 (* first update αnT4n by appending
  appending the smallest element of αT4n or αn *)
 If[First[αT4n] ≤ First[αn],
  (* if first element of αT4n is smaller, pick that one *)
  b = TakeDrop[αT4n, 1];
  αnT4 = Join[αnT4, b[[1]]];
  αT4n = b[[2]];
  AppendTo[αnT4n, Last[αnT4] + Length[αnT4] - 1],
  (**)
  (* otherwise take first element of αn *)
  b = TakeDrop[αn, 1];
  αnT4 = Join[αnT4, b[[1]]];
  αn = b[[2]];
  AppendTo[αnT4n, Last[αnT4] + Length[αnT4] - 1]];
 (* update αnT4T2n by appending
  appending the smallest element of αT2n or αnT4n *)
 If[First[αT2n] ≤ First[αnT4n],
  (* if first element of αT2n is smaller, pick that one *)
  c = TakeDrop[αT2n, 1];
  αnT4T2n = Join[αnT4T2n, c[[1]] + Length[αnT4T2n]];
  αT2n = c[[2]],
  (**)
  (* otherwise take first element of αnT4n *)
  c = TakeDrop[αnT4n, 1];
  αnT4T2n = Join[αnT4T2n, c[[1]] + Length[αnT4T2n]];
  αnT4n = c[[2]]];
 (* append last element of αnT4T2n
  to αnT4T2n2 twice to get wedge with self *)
 AppendTo[αnT4T2n2, Last[αnT4T2n]];
 AppendTo[αnT4T2n2, Last[αnT4T2n]]]
```

In[202]:= α

Out[202]= {0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 2, 2, 3, 3, 3, 3, 3, 3, 3, 5, 5, 6, 6, 6, 6, 6, 6, 6,
6, 7, 7, 8, 8, 9, 9, 9, 9, 9, 9, 10, 10, 12, 12, 12, 12, 12, 12, 12, 12, 13, 13,
14, 14, 15, 15, 15, 15, 15, 15, 15, 15, 17, 17, 18, 18, 18, 18, 18, 18, 18, 18,
19, 19, 21, 21, 21, 21, 21, 21, 21, 21, 23, 23, 25, 25, 26, 26, 27, 27, 27,
27, 27, 27, 27, 27, 28, 28, 30, 30, 30, 30, 30, 30, 30, 30, 31, 31, 32, 32,
33, 33, 33, 33, 33, 33, 33, 33, 36, 36, 36, 36, 36, 36, 36, 36, 37, 37, 38}

A.2 Generating α_{Δ_5}

The following code generates the *v*-sequence α for Δ5.

Generate elements of αS, wedge with self six times to obtain αS6

In[365]:=
```
αS = {}; For[n = 0, n < 10, n++,
 For[j = 0, j < 5, j++,
  AppendTo[αS,
   5 * n + 5 * Sum[Floor[n / 32^i], {i, 1, 3}]]]];
αS6 = Sort[Join[αS, αS, αS, αS, αS, αS]];
```

Generate elements of αT2

In[366]:=
```
αT2 = {}; For[n = 0, n < 40, n++,
 For[j = 0, j < 5, j++,
  AppendTo[αT2,
   1 * j + (5 * 1 + 1) * n + Sum[Floor[n / 2^i], {i, 1, 5}]]]]
```

Generate elements of αT4

In[367]:=
```
αT4 = {}; For[n = 0, n < 40, n++,
 For[j = 0, j < 5, j++,
  AppendTo[αT4,
   2 * j + (5 * 2 + 1) * n + Sum[Floor[n / 2^i], {i, 1, 5}]]]]
```

Generate elements of αT6

In[368]:=
```
αT6 = {}; For[n = 0, n < 40, n++,
 For[j = 0, j < 5, j++,
  AppendTo[αT6,
   3 * j + (5 * 3 + 1) * n + Sum[Floor[n / 2^i], {i, 1, 5}]]]]
```

Generate elements of αT8

In[369]:=
```
αT8 = {}; For[n = 0, n < 40, n++,
 For[j = 0, j < 5, j++,
  AppendTo[αT8,
   4 * j + (5 * 4 + 1) * n + Sum[Floor[n / 2^i], {i, 1, 5}]]]]
```

Compute αT2 - (n) , αT4 - (2n) , αT6 - (3n) , αT8 - (4n)

In[370]:=
```
nn = {}; For[n = 0, n < 250, n++, AppendTo[nn, n]];
αT2n = αT2 - Take[nn, Length[αT2]];
αT4n = αT4 - 2 * Take[nn, Length[αT4]];
αT6n = αT6 - 3 * Take[nn, Length[αT6]];
αT8n = αT8 - 4 * Take[nn, Length[αT8]];
```

Initialize α and α + (n) by taking first element of αS6

In[372]:=
```
α = {};
αn = {};
a = TakeDrop[αS6, 1];
α = Join[α, a[[1]]];
αn = Join[αn, a[[1]]];
αS6 = a[[2]];
```

Initialize $(\alpha + (n)) \wedge (\alpha T8 - (4n))$ and $[(\alpha + (n)) \wedge (\alpha T8 - (4n))] + (n)$ by taking first element of $\alpha T8 - (4n)$

In[373]:=
```
αnT8 = {};
αnT8n = {};
b = TakeDrop[αT8n, 1];
αnT8 = Join[αnT8, b[[1]]];
αnT8n = Join[αnT8n, b[[1]]];
αT8n = b[[2]];
```

Initialize $[(\alpha + (n)) \wedge (\alpha T8 - (4n))] + (n)] \wedge (\alpha T6 - (3n))$ and $[[[(\alpha + (n)) \wedge (\alpha T8 - (4n))] + (n)] \wedge (\alpha T6 - (3n))] + (n)$ by taking first element of $\alpha T6 - (3n)$

In[374]:=
```
αnT8T6 = {};
αnT8T6n = {};
b = TakeDrop[αT6n, 1];
αnT8T6 = Join[αnT8T6, b[[1]]];
αnT8T6n = Join[αnT8T6n, b[[1]]];
αT6n = b[[2]];
```

Initialize $[[[[(\alpha + (n)) \wedge (\alpha T8 - (4n))] + (n)] \wedge (\alpha T6 - (3n))] + (n)] \wedge (\alpha T4 - (2n))$ and $[[[[[(\alpha + (n)) \wedge (\alpha T8 - (4n))] + (n)] \wedge (\alpha T6 - (3n))] + (n)] \wedge (\alpha T4 - (2n))] + (n)$ by taking first element of $\alpha T4 - (2n)$

In[375]:=
```
αnT8T6T4 = {};
αnT8T6T4n = {};
b = TakeDrop[αT4n, 1];
αnT8T6T4 = Join[αnT8T6T4, b[[1]]];
αnT8T6T4n = Join[αnT8T6T4n, b[[1]]];
αT4n = b[[2]];
```

Initialize $[[[[[[[(\alpha + (n)) \wedge (\alpha T8 - (4\ n))] + (n)] \wedge (\alpha T6 - (3\ n))] + (n)] \wedge (\alpha T4 - (2\ n))] + (n)] \wedge (\alpha T2 - (n))] + (n)$ by taking first element of $\alpha T2 - (n)$; initialize the wedge of this sequence with itself

In[376]:=
```
αnT8T6T4T2n = {};
b = TakeDrop[αT2n, 1];
αnT8T6T4T2n = Join[αnT8T6T4, b[[1]] + Length[αnT8T6T4T2n]];
αT2n = b[[2]];
αnT8T6T4T2n2 = Sort[Join[αnT8T6T4T2n, αnT8T6T4T2n]];
```

Loop through elements of sequences to generate α

In[377]:=
```
While[αS6 ≠ {} && αT2n ≠ {} && αT4n ≠ {} && αT6n ≠ {} && αT8n ≠ {},
 (* append an element to α *)
```

```
If[First[αS6] ≤ First[αnT8T6T4T2n2],
 (* if first element of αS6 is smaller, pick that one *)
 a = TakeDrop[αS6, 1];
 α = Join[α, a[[1]]];
 αS6 = a[[2]];
 AppendTo[αn, Last[α] + Length[α] - 1],
 (**)
 (* otherwise take first element of αnT8T6T4T2n2 *)
 a = TakeDrop[αnT8T6T4T2n2, 1];
 α = Join[α, a[[1]]];
 αnT8T6T4T2n2 = a[[2]];
 AppendTo[αn, Last[α] + Length[α] - 1]];
(* update αnT8T6T4T2n based on new α value *)
(* first update αnT8n by appending
 appending the smallest element of αT8n or αn *)
If[First[αT8n] ≤ First[αn],
 (* if first element of αT8n is smaller, pick that one *)
 b = TakeDrop[αT8n, 1];
 αnT8 = Join[αnT8, b[[1]]];
 αT8n = b[[2]];
 AppendTo[αnT8n, Last[αnT8] + Length[αnT8] - 1],
 (**)
 (* otherwise take first element of αn *)
 b = TakeDrop[αn, 1];
 αnT8 = Join[αnT8, b[[1]]];
 αn = b[[2]];
 AppendTo[αnT8n, Last[αnT8] + Length[αnT8] - 1]];
(* update αnT8T6n by appending
 appending the smallest element of αT6n or αnT8n *)
If[First[αT6n] ≤ First[αnT8n],
 (* if first element of αT6n is smaller, pick that one *)
 c = TakeDrop[αT6n, 1];
 αnT8T6 = Join[αnT8T6, c[[1]]];
 αT6n = c[[2]];
 AppendTo[αnT8T6n, Last[αnT8T6] + Length[αnT8T6] - 1],
 (**)
 (* otherwise take first element of αnT8n *)
 c = TakeDrop[αnT8n, 1];
 αnT8T6 = Join[αnT8T6, c[[1]]];
 αnT8n = c[[2]];
 AppendTo[αnT8T6n, Last[αnT8T6] + Length[αnT8T6] - 1]];
(* update αnT8T6T4n by appending
 appending the smallest element of αT4n or αnT8T6n *)
If[First[αT4n] ≤ First[αnT8T6n],
 (* if first element of αT4n is smaller, pick that one *)
 d = TakeDrop[αT4n, 1];
```

```
 αnT8T6T4 = Join[αnT8T6T4, d[[1]]];
 αT4n = d[[2]];
 AppendTo[αnT8T6T4n, Last[αnT8T6T4] + Length[αnT8T6T4] - 1],
 (**)
 (* otherwise take first element of αnT8T6n *)
 d = TakeDrop[αnT8T6n, 1];
 αnT8T6T4 = Join[αnT8T6T4, d[[1]]];
 αnT8T6n = d[[2]];
 AppendTo[αnT8T6T4n, Last[αnT8T6T4] + Length[αnT8T6T4] - 1]];
(* update αnT8T6T4T2n by appending
 appending the smallest element of αT2n or αnT8T6T4n *)
If[First[αT2n] ≤ First[αnT8T6T4n],
 (* if first element of αT2n is smaller, pick that one *)
 e = TakeDrop[αT2n, 1];
 αnT8T6T4T2n = Join[αnT8T6T4, e[[1]] + Length[αnT8T6T4T2n]];
 αT2n = e[[2]],
 (**)
 (* otherwise take first element of αnT8T6T4n *)
 e = TakeDrop[αnT8T6T4n, 1];
 αnT8T6T4T2n = Join[αnT8T6T4, e[[1]] + Length[αnT8T6T4T2n]];
 αnT8T6T4n = e[[2]]];
(* append last element of αnT4T2n
 to αnT4T2n2 twice to get wedge with self *)
AppendTo[αnT8T6T4T2n2, Last[αnT8T6T4T2n]];
AppendTo[αnT8T6T4T2n2, Last[αnT8T6T4T2n]]]
```

In[378]:=
```
α
```

Out[378]=
```
{0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
 0, 0, 0, 0, 0, 0, 0, 0, 2, 2, 3, 3, 4, 4, 5, 5, 5, 5, 5, 5, 5, 5, 5, 5, 5, 5,
 5, 5, 5, 5, 5, 5, 5, 5, 5, 5, 5, 5, 5, 5, 5, 5, 5, 5, 5, 5, 5, 6, 6, 8, 8, 9,
 9, 10, 10, 10, 10, 10, 10, 10, 10, 10, 10, 10, 10, 10, 10, 10, 10, 10, 10, 10,
 10, 10, 10, 10, 10, 10, 10, 10, 10, 10, 10, 10, 10, 10, 10, 11, 11, 12, 12,
 13, 13, 15, 15, 15, 15, 15, 15, 15, 15, 15, 15, 15, 15, 15, 15, 15, 15, 15,
 15, 15, 15, 15, 15, 15, 15, 15, 15, 15, 15, 15, 15, 15, 15, 15, 17, 17,
 18, 18, 19, 19, 20, 20, 20, 20, 20, 20, 20, 20, 20, 20, 20, 20, 20, 20, 20,
 20, 20, 20, 20, 20, 20, 20, 20, 20, 20, 20, 20, 20, 20, 20, 20, 20, 20, 20,
 21, 21, 22, 22, 24, 24, 25, 25, 25, 25, 25, 25, 25, 25, 25, 25, 25, 25, 25,
 25, 25, 25, 25, 25, 25, 25, 25, 25, 25, 25, 25, 25, 25, 25, 25, 25, 25, 25,
 25, 25, 26, 26, 27, 27, 28, 28, 29, 29, 30, 30, 30, 30, 30, 30, 30, 30,
 30, 30, 30, 30, 30, 30, 30, 30, 30, 30, 30, 30, 30, 30, 30, 30, 30, 30, 30}
```

A.3 The Number of Monic Irreducible Polynomials of Degree n

The following code supports the assertion that nI_2(n) < 2^n - 2 up to n=100,000.

Generate the first 10 elements in the sequence I_2(n), starting at n=1.

```
In[1]:= f[n_] := Block[{d = Divisors@n}, Plus @@ (MoebiusMu[n / d] * 2^d / n)];
        l = Array[f, 10]
Out[1]= {2, 1, 2, 3, 6, 9, 18, 30, 56, 99}
```

Populate the list m with the values n*I_2(n) - 2^n + 2 for n not prime, which we conjecture to be strictly less that 0 when n is composite. Note that the first element of the list, corresponding to n=1, remains positive.

```
In[2]:= m = {};
        For[i = 1, i ≤ Length[l], i++,
         If[PrimeQ[i] == False, AppendTo[m, i * l[[i]] - 2^i + 2], 0]];
        m
Out[2]= {2, -2, -8, -14, -6, -32}
```

Generate the first 100,000 elements in the sequence I_2(n), starting at n=1.

```
In[3]:= f[n_] := Block[{d = Divisors@n}, Plus @@ (MoebiusMu[n / d] * 2^d / n)];
        l = Array[f, 100000];
```

Populate the list m with the values n*I_2(n) - 2^n + 2 for n not prime. Sort this list in increasing order, and print the last five elements in this sorted list.

```
In[4]:= m = {};
        For[i = 1, i ≤ Length[l], i++,
         If[PrimeQ[i] == False, AppendTo[m, i * l[[i]] - 2^i + 2], 0]];;
        Take[Sort[m], -5]
Out[4]= {-14, -8, -6, -2, 2}
```

Since the only non-prime positive integer which results in a positive entry in m is n=1, we can conclude that our conjecture holds for all composite n up to 100,000.

Appendix B

Results on the prime index, q-local case

Let q be an odd prime, and $M_p(\mathbb{Q}_q)$ be the ring of $p \times p$ matrices over the q-adic numbers. Additionally, let S be a subset of a maximal order Δ_p that is closed under conjugation by elements of Δ_p. Let $z \in S$ have characteristic polynomial

$$ch_z(x) = x^p + a_{p-1}x^{p-1} + \cdots + a_1 x + a_0 \ .$$

For $0 \leq j \leq p-1$, let $c_j, r_j \in \mathbb{Z}$ with $r_j \geq 1$ and $0 \leq c_j \leq q^{r_j} - 1$ be defined so that

$$a_j \equiv c_j \pmod{q^{r_j}}$$

where r_j is the largest power of q for which we can ensure that the coefficient of x^j in the characteristic polynomial for any $z \in S$ is the same modulo q^{r_j}.

Let $\phi = (\phi_0, \phi_1, \ldots, \phi_{p-1})$ be defined on $\mathbb{Z}$ so that

$$\phi_j(k) = c_j + q^{r_j} \sum_{i \geq 0} k_{pi+(p-1)-j} q^i \tag{B.1}$$

where $k = \sum_{i \geq 0} k_i q^i$ is the expansion of k in base q. Define a function

$$f_n(x) = \prod_{k=0}^{p-1} (x^p - \phi_{p-1}(k)x^{p-1} + \phi_{p-2}(k)x^{p-2} + \cdots + (-1)^p \phi_0(k)) \ .$$

Let $z \in S$, and let $m \in \mathbb{Z}$ be such that $\phi(m)$ gives a tuple consisting of the coefficients of the characteristic polynomial of z, with $\phi_j(m)$ being the coefficient of x^j. Then for

any $0 \leq k \leq p$,

$$\begin{aligned} z^p - \phi_{p-1}(k)z^{p-1} + \phi_{p-2}(k)z^{p-2} + \cdots + (-1)^p\phi_0(k) & \\ = z^p - \phi_{p-1}(k)z^{p-1} + \phi_{p-2}(k)z^{p-2} + \cdots + (-1)^p\phi_0(k) - (ch_z(z)) & \\ = (\phi_{p-1}(m) - (\phi_{p-1}(k))z^{p-1} + (\phi_{p-2}(k) - \phi_{p-2}(m))z^{p-2} + \cdots & \\ + (-1)^p(\phi_0(k) - \phi_0(m)) & \end{aligned}$$

We would like to take the valuation of this expression. Recall that for any valuation ν defined on a field K with $a, b \in K$, that $\nu(a+b) \geq \min(\nu(a), \nu(b))$ with equality if $\nu(a) \neq \nu(b)$. In particular, if in a sum of p components each has a unique residue modulo p, then the valuation of the sum is the minimum of the valuations of the components.

Notice that for any $1 \leq j \leq p$,

$$\begin{aligned} \nu((\phi_j(m) - \phi_j(k))z^j) &= p\nu_q(\phi_j(m) - \phi_j(k)) + \nu(z^j) \\ &= p\nu_q(\phi_j(m) - \phi_j(k)) + j\nu(z) \\ &\equiv j\nu(z) \pmod{p} \end{aligned}$$

Since p is prime, as j varies this expression will give a complete set of residues modulo p. We then have

$$\begin{aligned} \nu(z^p - \phi_{p-1}(k)z^{p-1} + \phi_{p-2}(k)z^{p-2} + \cdots + (-1)^p\phi_0(k)) & \\ = \min((p-1)\nu(z) + p\nu_q(\phi_{p-1}), (p-2)\nu(z) + p\nu_q(\phi_{p-2}), \ldots, & \\ \nu(z) + p\nu_q(\phi_1), p\nu(\phi_0)) & \end{aligned}$$

where $\nu_q(\phi_j) := \nu_q(\phi_j(m) - \phi_j(k))$ for $0 \leq j \leq p-1$.

Let the ϕ_i be ordered in such a way that

$$\begin{aligned} \nu_q(m-k) &= \min(i : k_i \neq m_i) \\ \nu_q(\phi_{p-1}) &= \min(i : k_{pi} \neq m_{pi}) + r_{p-1} \\ \nu_q(\phi_{p-2}) &= \min(i : k_{pi+1} \neq m_{pi+1}) + r_{p-2} \\ &\vdots \\ \nu_q(\phi_0) &= \min(i : k_{pi+(p-1)} \neq m_{pi+(p-1)}) + r_0 \end{aligned}$$

where $k = \sum_{i \geq 0} k_i q^i$ and $m = \sum_{i \geq 0} m_i q^i$ are the expansions of k and m in base q, and the r_j are defined as in Equation (B.1).

Lemma B.0.1. With the above notation, if the components $\phi_0, \phi_1, \ldots, \phi_{p-1}$ are ordered in such a way that

$$(p-1)\nu(z) + pr_{p-1} \leq (p-2)\nu(z) + pr_{p-2} \leq \cdots \leq \nu(z) + pr_1 \leq pr_0$$

with

$$(p-1)\nu(z) + pr_{p-1} = j\nu(z) + pr_j - p + (j+1)$$

for each $0 \leq j \leq p-2$, then

$$\nu(z^p - \phi_1(k)z^{p-1} + \phi_2(k)z^{p-2} + \cdots + (-1)^p\phi_p(k)) = (p-1)\nu(z) + pr_{p-1} + \nu_q(m-k)\ .$$

Proof. The value of $j\nu(z) + p\nu_q(\phi_j)$ will depend on the residue of $\nu_q(m-k)$ modulo p.

If $\nu_q(m-k) \equiv 0 \pmod{p}$, then

$$\begin{aligned}
(p-1)\nu(z) + p\nu_q(\phi_{p-1}) &= (p-1)\nu(z) + p\left(\frac{\nu_q(m-k)}{p} + r_{p-1}\right) \\
&= (p-1)\nu(z) + pr_{p-1} + \nu_q(m-k) \\
(p-2)\nu(z) + p\nu_q(\phi_{p-2}) &\geq (p-2)\nu(z) + p\left(\frac{\nu_q(m-k)}{p} + r_{p-2}\right) \\
&= (p-2)\nu(z) + pr_{p-2} + \nu_q(m-k) \\
&\vdots \\
p\nu_q(\phi_0) &\geq p\left(\frac{\nu_q(m-k)}{p} + r_0\right) \\
&= pr_0 + \nu_q(m-k)
\end{aligned}$$

In general, if $\nu_q(m-k) \equiv j \pmod{p}$, then

$$\begin{aligned}
(p-1)\nu(z) + p\nu_q(\phi_{p-1}) &\geq (p-1)\nu(z) + p\left(\frac{\nu_q(m-k)-j}{p} + r_{p-1} + 1\right) \\
&= (p-1)\nu(z) + pr_{p-1} + p - j + \nu_q(m-k) \\
&\vdots \\
(p-j)\nu(z) + p\nu_q(\phi_{p-j}) &\geq (p-j)\nu(z) + p\left(\frac{\nu_q(m-k)-j}{p} + r_{p-j} + 1\right) \\
&= (p-j)\nu(z) + pr_{p-j} + p - j + \nu_q(m-k) \\
(p-(j+1))\nu(z) + p\nu_q(\phi_{p-(j+1)}) &= (p-(j+1))\nu(z) + p\left(\frac{\nu_q(m-k)-j}{p} + r_{p-(j+1)}\right)
\end{aligned}$$

$$
\begin{aligned}
&= (p-(j+1))\nu(z) + pr_{p-(j+1)} - j + \nu_q(m-k) \\
(p-(j+2))\nu(z) + p\nu_q(\phi_{p-(j+2)}) &\geq (p-(j+2))\nu(z) + p\left(\frac{\nu_q(m-k)-j}{p} + r_{p-(j+2)}\right) \\
&= (p-(j+2))\nu(z) + pr_{p-(j+2)} - j + \nu_q(m-k) \\
&\vdots \\
p\nu_q(\phi_0) &\geq p\left(\frac{\nu_q(m-k)-j}{p} + r_0\right) \\
&= pr_0 - j + \nu_q(m-k)
\end{aligned}
$$

Continuing in this way, the minimum value for the expression $j\nu(z)+p\nu_q(\phi_j)$ over all residues of $\nu_q(m-k) \pmod p$ is equal to

$$j\nu(z) + pr_j - p + (j+1) + \nu_q(m-k) \ ,$$

and this minimum occurs precisely when $\nu_q(m-k) \equiv -(j+1) \pmod p$. Therefore, if we would like to attain a strict minimum for $\nu(z^p - \phi_{p-1}(k)z^{p-1} + \phi_{p-2}(k)z^{p-2} + \cdots + (-1)^p\phi_0(k))$ for a general k without having an inequality, we would like to attain this minimum for each residue.

If indeed it is the case that

$$
\begin{aligned}
&\min((p-1)\nu(z) + p\nu_q(\phi_{p-1}), (p-2)\nu(z) + p\nu_q(\phi_{p-2}), \ldots, p\nu_q(\phi_0)) \\
&\qquad = (p-j)\nu(z) + pr_j - p + (j+1) + \nu_q(m-k)
\end{aligned}
$$

when $\nu_q(m-k) \equiv -(j+1)$, then comparing each minimum expression to all inequalities in the expressions for $(p-\ell)\nu(z)+p\nu_q(\phi_\ell)$ where $\ell \neq j$ and considering the result for all j together, we easily obtain the chain of inequalities

$$(p-1)\nu(z) + pr_{p-1} \leq (p-2)\nu(z) + pr_{p-2} \leq \cdots \leq \nu(z) + pr_1 \leq pr_0 \ .$$

Additionally, to have a minimum that is consistent and holds for all choices of k, we must also require that all the minimums are equal, meaning that

$$j\nu(z) + pr_j - p + (j+1) + \nu_q(m-k) = \ell\nu(z) + pr_\ell - p + (\ell+1) + \nu_q(m-k)$$

for $j \neq \ell$, or, equivalently,

$$(p-1)\nu(z) + pr_{p-1} = j\nu(z) + pr_j - p + (j+1)$$

for all $0 \leq j \leq p-2$. With this condition, we see that

$$\begin{aligned}
&\nu(z^p - \phi_1(k)z^{p-1} + \phi_2(k)z^{p-2} + \cdots + (-1)^p\phi_p(k)) \\
&\qquad = \min_{1\leq j\leq p}(j\nu(z) + p\nu_q(\phi_j)) \\
&\qquad = \min_{1\leq j\leq p}(j\nu(z) + pr_j - p + (j+1) + \nu_q(m-k)) \\
&\qquad = (p-1)\nu(z) + pr_{p-1} + \nu_q(m-k)\ ,
\end{aligned}$$

giving the desired result. □