8-2018

Factorization in integral domains.

Ryan H. Gipson
University of Louisville

FACTORIZATION IN INTEGRAL DOMAINS

By

Ryan H. Gipson
B.S., Murray State University, 2012
M.A., University of Louisville, 2015

A Dissertation
Submitted to the Faculty of the
College of Arts and Sciences of the University of Louisville
in Partial Fulfillment of the Requirements
for the Degree of

Doctor of Philosophy
in
Applied and Industrial Mathematics

Department of Mathematics
University of Louisville
Louisville, KY

August 2018

FACTORIZATION IN INTEGRAL DOMAINS

Submitted by

Ryan H. Gipson

A Dissertation Approved on

May 14, 2018

by the Following Dissertation Committee:

Dr. Hamid Kulosman, Dissertation Director

Dr. Aaron Hill

Dr. Jinjia Li

Dr. Steve Seif

Dr. David N. Brown

DEDICATION

Dedicated to my Past, my Present, and my Future.

To my parents for their unending encouragement and guidance.

To my wife who patiently endures my incessant mathematical ramblings.

To my daughter who will go further and achieve more than I could ever dream.

ACKNOWLEDGEMENTS

First, I would like to express both my sincere appreciation and admiration for my academic advisor and thesis director, Dr. Hamid Kulosman. I am indeed grateful, and indebted, for his tireless efforts and assistance in directing my research and mathematical interests. His contributions to my professional development cannot be overstated, and I feel to be truly blessed to have had the privilege of his mentorship.

Next, I would also thank the members of my Dissertation Committee, Dr. Steven Seif, Dr. Jinjia Li, Dr. Aaron Hill, and Dr. David Brown for all their time and suggestions in making this dissertation a reality. I would also extend my appreciation to the faculties of both the University of Louisville and Murray State University; in particular, I would like to extend a very special thanks to Dr. Timothy Schroeder who inspired my mathematical aspirationas as a freshman at Murray State University and to Dr. Thomas Riedel, Department Chair of the University of Louisville, for his continuing support and assistance beyond his prescribed duties; his genuine interest in students' success has neither gone unnoticed nor unappreciated.

Naturally, there are many scholars, professors, colleagues, friends, and family who have all played a unique, and invaluable, role in my achievement and are worthy of due honor. In particular, I would give special honor to my "Mama" who has believed in me before I was born, to my Dad who planted a seed of curiosity and wonder within me, and most especially to my beautiful wife Michele whose loving patience is a pillar of my life.

Finally, and above all else, I would like to acknowledge the grace and blessings of the Lord Jesus Christ by whose providences I have been blessed to know those mentioned herein, as well as, to have produced this dissertation to what I hope is His glory.

−*Soli Deo Gloria!*

ABSTRACT

FACTORIZATION IN INTEGRAL DOMAINS

Ryan H. Gipson

May 1, 2017

We investigate the atomicity and the AP property of the semigroup rings $F[X; M]$, where F is a field, X is a variable and M is a submonoid of the additive monoid of nonnegative rational numbers. In this endeavor, we introduce the following notions: essential generators of M and elements of height $(0, 0, 0, \dots)$ within a cancellative torsion-free monoid Γ. By considering the latter, we are able to determine the irreducibility of certain binomials of the form $X^{\pi} - 1$, where π is of height $(0, 0, 0, \dots)$, in the monoid domain. Finally, we will consider relations between the following notions: M has the gcd/lcm property, $F[X; M]$ is AP, and M has no elements of height $(0, 0, 0, \dots)$.

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1
INTRODUCTION

The purpose of this dissertation is to explore various factorization properties in integral domains. More specifically, we investigate the atomicity and AP properties in a special class of commutative rings called monoid domains. For the sake of comprehension, it is assumed that the reader has completed a minimum of a year's sequence in graduate level algebra, however, all relevant notions will be treated in-turn within this text. Specifically, we will devote the bulk of Chapter 2 to introduce necessary definitions and propositions to further acquaint the reader to integral domains, but first we will provide a brief glimpse into the mathematical development of the topic.

The study of factorization in integral domains concerns itself with the decomposition of nonunit nonzero elements into irreducibles. Historically, this study has focused on those domains in which every nonzero nonunit element permits such a factorization and said factorization is unique up to the order of the factors and associates [1]. Indeed, this case has been well-studied and there are exellent resources on the topic, however, in practice, most domains permit much more general factorizations. There are domains R, in which, there is an element, say x, that admits multiple factorizations unique only in the number of irreducible factors. In fact, there are domains in which an element may have infinitely many factorizations, only one of which is finite. Indeed, factorization (or the lack thereof) may be characterized in many forms, and in recent decades, great efforts have been made to explore its various characterizations.

In 1968, Paul Cohn in [7] presented a paper on Bézout rings where he introduced the notion of an *atom* as well as the class of integral domains known as *atomic domains.* Interestingly, in this paper, he mistakenly classified atomic domains as being equivalent to ACCP domains (these are integral domains in which the ascending chain condition is satisfied for all principal ideals). Indeed, in 1974, Anne Grams, in her paper titled *Atomic rings and the ascending chain condition for principal ideals*, [15], provides an example of an atomic domain that does not satisfy the ACCP condition.

Clearly, the mathematical community needed a more robust classification for domains with decidedly more general factorization properties. This dilemma was remedied greatly in 1990 when D. D. Anderson, D. F. Anderson, and M. Zafrullah, categorized all domains whose nonzero nonunit elements admitted at least one factorization into a finite number of atoms in their paper *Factorization in Integral Domains*, [1].

Gilmer's research of commutative semigroup rings $R[X;S]$ has provided a compelling course in this area of mathematical research. In [12] he proposed the generic question that he denotes as (Q_E). Here, E represents some particular ring-theoretic property, say unique factorization, and Q represents the question, "Under what conditions on S and R does the semigroup ring $R[X;S]$ satisfy the given property E?" For various concrete properties E Gilmer provided answers in [13], e.g., related to our work, he provides sufficient and necessary conditions for which a semigroup ring satisfies the unique factorization property.

In collaboration with Dr. Hamid Kulosman, I have extended the work of these mathematicians and have provided sufficient and necessary conditions for which semigroup rings exhibit ring-theoretic properities: atomicity and AP. To this end, we introduce new notions such as *essential generators* of a monoid M, elements of *height* $(0,0,0,\dots)$ in a torsion-free monoid M, Matsuda's monoids, and others.

In chapters 3,4, and 5 we will present the results of our investigation in order of inspiration/motivation. In Chapter 3, we submit a new characterization of principal ideal domains and in doing so we discover our impetus for researching monoid domains. In Chapter 4, we will investigate the atomicity and AP condition of the monoid domain $F[X;M]$ where M is a submonoid of $(\mathbb{Q}_+,+)$. Then, in Chapter 5, we will fully justify some assertions from Chapter 4 by providing a proof for the irreducibility of certain binomials $X^{\pi}-1$ in the monoid domains. Chapter 6 will be our last chapter of study and with it we will explore the existence of relations between the following properties: the monoid M has the gcd/lcm property, $F[X;M]$ has the AP-property, and there are no elements of height $(0,0,0,\dots)$ in M.

Finally, in chapter 7, we will discuss the many avenues of future research that our results have presented. More concretely, we will present several questions that are either further generalizations or natural extensions of our work.

CHAPTER 2
PRELIMINARIES

Throughout this text, we will be discussing various properties of commutative rings. For this purpose, we will list some basic definitions and well-known propositions beginning with a precise definition of a ring. All the notions that we use in this thesis, but do not define them, can be found in [10] and [19].

2.1 Rings

Definition 2.1. *A* ***ring*** *is a nonempty set R equipped with two binary operations $+ : R \times R \to R$ (addition) and $\cdot : R \times R \to R$ (multiplication), satisfying the following conditions:*

(M1) Under addition R is an abelian group;

(M2) Multiplication is associative;

(M3) There exists an element $1 \in R$ such that $1 \cdot x = x \cdot 1 = x$ for all $x \in R$. (We call this element the ***multiplicative identity****.)*

(M4) The left and right distributivity of multiplication with respect to addition hold.

A ring R is said to be a *commutative ring* when $x \cdot y = y \cdot x$ for all elements x, y in R. It should be noted that most often we will write xy for $x \cdot y$ when the context is clear.

From now on we will assume that all our rings are commutative (unless specified otherwise). An element $x \in R$ is said to be a *zero divisor* in R if there exists a nonzero element $y \in R$ such that $xy = 0$. If R is nonzero and has no zero divisors, except 0, we say that R is an *integral domain*. Following, we give an equivalent and useful definition.

Definition 2.2. *A commutative ring $R \neq 0$ is said to be an* ***integral domain*** *if for any elements $x, y, z \in R$, $xy = xz \implies y = z$.*

2.2 Integral Domains

For the remainder of this text, we will deal exclusiviely with integral domains. Therefore, it is useful to discuss various types of domains and their properties. We first give some basic definitions. Take x, y, z to be elements of the domain R:

(i) We say x is a *unit* if it is invertible with respect to multiplication;

(ii) We say x is *irreducible* (and we call it an *atom*) if it is nonzero, nonunit, and $x = yz$ implies either y or z is a unit;

(iii) We say x is *prime* if it is nonzero, nonunit, and whenever $x|yz$, then $x|y$ or $x|z$;

(iv) Two elements $x, y \in R$ are said to be *associates* if $x = uy$, where u is a unit; we then write $x \sim y$.

Furthermore, an integral domain R in which every nonzero element is a unit is called a *field*. Unless stated otherwise, we will consistently denote all fields by F.

Definition 2.3. *A* ***principal ideal domain*** *or* ***PID*** *is an integral domain in which every ideal is principal, i.e., for every ideal I there is an element a such that $I = (a)$.*

It is well known, that if one adjoins the variable X to F one obtains an integral domain, denoted $F[X]$, which is a principal ideal domain (in fact, $F[X]$ is a Euclidean domain). The elements of $F[X]$ are all polynomials $f(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$ where $a_0, a_1, a_2, \ldots, a_n$ are elements of the field and $n \geq 0$ a nonnegative integer. If $f \neq 0$, we say that the *degree of* $f(x)$ is equal to n and we write $\deg(f(X)) = n$. We then call a_nX^n the *leading term*. We define $\deg(0) = -\infty$. It is not difficult to show that the set of units in $F[X]$ is precisely the set of all zero-degree polynomials, i.e., nonzero elements of F.

It is well-known that every prime element is an atom. However, the converse is not true. For example, consider the integral domain $D = Z[\sqrt{-5}]$. The elements of this domain are of the form $\{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$, and it can be shown that in D the element 2 is an atom but not prime. However, for our purposes, it is more interesting to consider the domain $R = F[X^2, X^3]$ which consists of all polynomials over F whose coefficient by the variable X is zero. A simple degree argument shows that X^2 is an atom in R. However, $X^2 | X^6 = X^3X^3$, but $X^2 \nmid X^3$ in R; thus, it is not prime. Though irreducible does not always imply prime, there are domains in which the notions are equivalent. Consider the following examples:

Example 2.1. *(1) $\mathbb{Z}$ the ring of integers;*
(2) $\mathbb{Z}[X]$ the polynomial ring over $\mathbb{Z}$;
(3) $F[X_1, X_2, \ldots, X_n]$ where $n \geq 0$ is the polynomial ring over F with variables $X_1, X_2, \ldots, X_n$.

These examples, along with many others, motivate the following definition.

Definition 2.4. *The domain R is an* ***AP-domain*** *if the notions of an irreducible and a prime element are equivalent.*

One may wonder why we concern ourselves with the AP condition (that is, the atoms are prime condition). Consider the following scenario. Let x be a nonzero nonunit element of an integral domain D, and suppose that x can be factored as $x = p_1p_2 \ldots p_n$ where $n \geq 1$ and $p_1, p_2, \ldots, p_n$ are atoms. Suppose also that for some

$i \in \{1, 2, \ldots, n\}$, p_i is prime and consider another irreducible factorization of x, say $x = q_1 q_2 \ldots q_m$. Then, we can show that for some $j \in \{1, 2, \ldots, m\}$, $p_i \sim q_j$.

Proof. From above, we know that $p_1 p_2 \ldots p_i \ldots p_n = q_1 q_2 \ldots q_m$. Hence, p_i divides $q_1 q_2 \ldots q_m$, and because p_i is prime, it in fact divides at least one of the factors $q_1, q_2, \ldots, q_m$, say q_j. Thus, since q_j is irreducible and p_i is not a unit, $q_j \sim p_i$. □

Therefore, for every decomposition into atoms that x admits, there exists a factor which is an associate of p_i. Thus, in an AP-domain, every nonzero nonunit element x that admits some factorization into a finite number of irreducibles in fact admits an essentially unique factorization. That is, for any two irreducible factorizations of x, say $p_1 p_2 \ldots p_n$ and $q_1 q_2 \ldots q_m$, $n = m$ and there exists a permutation $\sigma \in S_n$ such that for each $i \in \{1, 2, \ldots, n\}$, $p_i = u_i q_{\sigma(i)}$ for some unit, u_i, in the integral domain.

Example 2.2. *In the AP-domain $\mathbb{Z}$, the essentially unique factorization of the element -156 into atoms is given by $-156 = (-1) \cdot 2 \cdot 2 \cdot 3 \cdot 13 = (-1) \cdot 2^2 \cdot 3 \cdot 13$.*

One may observe that in all of our examples, thus far, every nonzero nonunit element in the domain could be factored into a unit and a finite number of atoms. It should be noted this is not always the case. In fact, there are domains in which there are no atoms at all (consider any field). Domains of this type are called *antimatter domains*, however, in this text, we will not concern ourselves with such. Rather, many of the domains we will study are those in which every nonzero nonunit element admits at least one factorization into a finite number of irreducible elements, i.e., those domains which possess the *atomic* property.

Definition 2.5. *We say that a domain R is an* ***atomic domain*** *when every nonzero nonunit element can be factored into a finite number of atoms.*

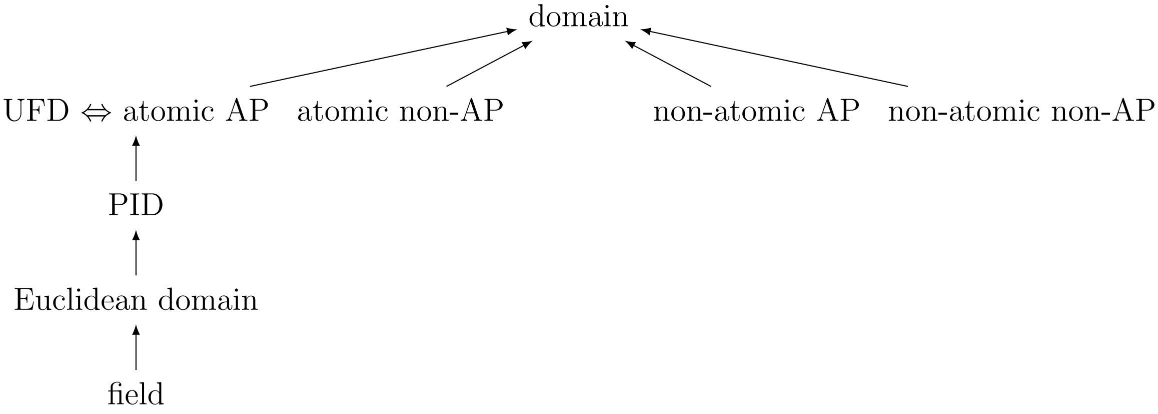
The domains we have discussed thus far (fields, Euclidean domains, and PIDs) are all atomic domains.

Definition 2.6. *We say that an integral domain R is a* ***unique factorization domain*** *(or* ***UFD****) if it is atomic and for every nonzero nonunit $x \in R$ the factorization of x into a product of atoms is unique up to the order and associates.*

2.3 Atomicity and AP Property and their Relations

The reader should note that UFDs satisfy both the atomic condition and the AP condition. It can be shown that the converse holds as well. Hence, UFDs can be characterized as atomic AP-domains. This leads us into our primary investigation: what is the precise relationship between the properties AP and atomic. One may reference the following implication diagram.

Figure 2.1: Atomic and AP Implication Diagram



Remark 2.1. *The only equivalence is between the notions of UFD and atomic AP. We will see that these implications are correct.*

2.4 Monoids and Monoid Domains

With these definitions and notions we will begin our investigation into the atomicity and AP property in integral domains. In doing so, we will focus much of our attention on a special class of domains called *monoid domains*, denoted $F[X; M]$.

Definition 2.7. *A* ***commutative monoid****, written additively, is a nonempty set* Γ *with a binary operation* $+$ *that is associative and has the identity element denoted by* 0 *(and called* ***zero****).*

We list some examples below.

Example 2.3. *(1)* $(\mathbb{N}_0, +)$*, the set of nonnegative integers, is a commutative monoid;*
(2) $(\mathbb{Q}_+, +)$*, the set of all non-negative rational numbers, is a commutative monoid;*
(3) Similarly, $(\mathbb{R}_+, +)$*, the set of all non-negative real numbers, is a commutative monoid;*
(4) Both $M = \{0, 2, 3, 4, 5, \dots\}$ *and* $M' = \{0, 2, 4, 6, 7, 8, 9, \dots\}$ *with addition are submonoids of* $(N_0, +)$*, and we say that they are generated by* $\{2, 3\}$ *and* $\{2, 5\}$*, respectively. That is, every element of* M *can be written as* $2s + 3t$ *and every element of* M' *can be written as* $2s' + 5t'$ *for nonnegative integers* s, t, s', t'*.*

Given a commutative monoid M, we may define the monoid ring $R = F[X; M]$, where F is a field and X is a variable. The elements of $F[X; M]$ are the polynomial expressions:

$$f(X) = a_1 X^{\alpha_1} + a_2 X^{\alpha_2} + \cdots + a_n X^{\alpha_n}$$

where $a_1, a_2, \dots, a_n$ are elements of the field and $\alpha_1, \alpha_2, \dots, \alpha_n$ are elements of the monoid. It is not difficult to verify that $F[X; M]$ is a commutative ring with the following natural operations: for nonzero elements $f, g \in F[X; M]$, written as

$$f(x) = a_1 X^{\alpha_1} + \cdots + a_n X^{\alpha_n},$$
$$g(x) = b_1 X^{\beta_1} + \cdots + b_m X^{\beta_m},$$

their product is written as $f(X)g(X) = a_1b_1X^{\alpha_1+\beta_1} + \cdots + a_nb_mX^{\alpha_n+\beta_m}$; under addition, we combine terms with equal exponents by adding their coefficients. If $f = 0$ or $g = 0$, then $fg = 0$. If $M \subseteq \mathbb{R}_+$ and if we assume the descending order of the exponents, then, we say that $\deg(f(X)) = \alpha_1$ (unless $f = 0$, in which case we define $\mathrm{def}(f) = -\infty$). Now, we will verify that $F[X; M]$ is indeed an integral domain, and by a simple degree argument, we will show that the set of units is precisely the set of nonzero constants.

Proposition 2.1. *If $M \subseteq \mathbb{R}_+$, then the commutative ring $R = F[X; M]$ is an integral domain.*

Proof. Let $f(X), g(X)$ be polynomials in R. We will first show that $\deg(f(X)g(X)) = \deg(f(X)) + \deg(g(X))$. Write $f(X) = a_1X^{\alpha_1} + a_2X^{\alpha_2} + \cdots + a_nX^{\alpha_n}$ and $g(X) = b_1X^{\beta_1} + b_2X^{\beta_2} + \cdots + b_nX^{\beta_m}$ assuming descending order on the exponents. Then $f(X)g(X) = a_1b_1X^{\alpha_1+\beta_1} + \cdots + a_nb_mX^{\alpha_n+\beta_m}$ which shows that $\deg(f(X)g(X)) = \alpha_1 + \beta_1 = \deg(f(X)) + \deg(g(X))$. This includes the possibility that $f = 0$ or $g = 0$, since we define $(-\infty) + (-\infty) = (-\infty)$ and $\alpha + (-\infty) = (-\infty) + \alpha = (-\infty)$ for $\alpha \geq 0$. Now, suppose that $f(X) \neq 0$ (i.e. $\deg(f(X)) \geq 0$), but $f(X)g(X) = 0$. Thus, we have $\deg(f(X)g(X)) = deg(0)$ which implies $\deg(f(X)) + \deg(g(X)) = -\infty$, so that $\deg(g(X)) \leq -\infty$. Hence, $g(X) = 0$ and R is an integral domain. □

Proposition 2.2. *The set of units of $R = F[X; M]$ is precisely the set of nonzero constant polynomials, i.e., the nonzero elements of the field.*

Proof. Let $\mathcal{U}(R)$ be the set of units of R. Because F is a field, every nonzero element of F is a unit, and, therefore, $F \setminus \{0\} \subseteq \mathcal{U}(R)$. Now, take the polynomial $f(X) \in \mathcal{U}(R)$. Then, there exists an element $g(X) \in R$ such that $f(X)g(X) = 1$. Hence, $\deg(f(X)) + \deg(g(X)) = \deg(1) = 0$. Since $f \neq 0$ and $g \neq 0$, we have f ≥ 0 and g ≥ 0; hence, $\deg(f(X)) = \deg(g(X)) = 0$ and so $f(X) \in F \setminus \{0\}$. Therefore, $\mathcal{U}(R) = F \setminus \{0\}$. □

EXAMPLE 2.4. *(1) Let $M = (\mathbb{Q}_+, +)$ and F be the field of real numbers; then the monoid domain $F[X; M] = \mathbb{R}[X; \mathbb{Q}_+]$ is the ring of polynomial expressions whose exponents are non-negative rational numbers and whose coefficients are real numbers. The units of $\mathbb{R}[X; \mathbb{Q}_+]$ are nonzero real numbers.*
(2) Recall our earlier example $R = F[X^2, X^3]$, the ring of polynomials over a field F whose coefficient by X is zero. The domain R is in fact a monoid domain. Indeed, let $M = \langle 2, 3\rangle$; then, $R = F[X; M]$.

Let M, M' be two monoids. A *monoid homomorphism* from M to M' is a map $\mu : M \to M'$ such that $\mu(x+y) = \mu(x)+\mu(y)$ for all $x, y \in M$ and $\mu(0_M) = 0_{M'}$. If $\mu : M \to M'$ is bijective, then we say that μ is a *monoid isomorphism.* For every monoid isomorphism μ, there is an associated ring isomorphism $\phi_\mu : F[X; M] \to F[X; M']$ defined by:

$$\phi_\mu(a_1X^{\alpha_1} + a_2X^{\alpha_2} + \cdots + a_nX^{\alpha_n}) = a_1X^{\mu(\alpha_1)} + a_2X^{\mu(\alpha_2)} + \cdots + a_nX^{\mu(\alpha_n)}.$$

It is easy to show that ϕ_μ is an isomorphism if and only if μ is an isomorphism.

EXAMPLE 2.5. *(1) Let M be a monoid and $\tau \in \mathbb{Q}_+ \setminus \{0\}$. Then $\tau M = \{\tau m : m \in M\}$ is a monoid and the map $\mu_\tau : M \to \tau M$ defined by $\mu_\tau(x) = \tau x$ for all $x \in M$ is a monoid isomorphism. Therefore, the naturally associated map $\phi_{\mu_\tau} : F[X; M] \to F[X; \tau M]$, defined by*

$$\phi_{\mu_\tau}(a_1X^{\alpha_1} + a_2X^{\alpha_2} + \cdots + a_nX^{\alpha_n}) = a_1X^{\tau\alpha_1} + a_2X^{\tau\alpha_2} + \cdots + a_nX^{\tau\alpha_n}$$

is a ring isomorphism.
(2) More concretely, define $M = \langle 2, 5\rangle = \{0, 2, 4, 5, 6, 7, \dots\}$, and suppose $\tau = \dfrac{1}{2}$. Then, the map $\mu_{1/2} : M \to \frac{1}{2}M$ defined by $\mu_{1/2}(x) = \frac{1}{2}x$ for all $x \in M$ is a monoid isomorphism from M to $\frac{1}{2}M = \left\langle 1, \dfrac{5}{2}\right\rangle$.

2.5 Factorization process of $f(X) \in F[X; M]$

Finally, to aid in our investigation, we will describe a factorization process of a nonzero nonunit element of an integral domain. Let R be an integral domain and $x \in R$ a nonzero nonunit. We describe a factorization process of x. If x is irreducible, we stop. If not, we decompose it as $x = x_0x_1$, where both x_0 and x_1 are nonzero nonunits. If both x_0, x_1 are irreducible, we stop. If not, we take the first from the left of the elements x_0, x_1 which is reducible and decompose it as a product of two nonzero nonunits. Say x_0 is reducible. We decompose it: $x_0 = x_{0,0}x_{0,1}$. Now we have $x = x_{0,0}x_{0,1}x_1$. If all of the $x_{0,0}$, $x_{0,1}$, x_1 are irreducible, we stop. If not, we take the first from the left of the elements $x_{0,0}$, $x_{0,1}$, x_1 which is reducible and decompose it as a product of two nonzero nonunits. Say $x_{0,1}$ is reducible: $x_{0,1} = x_{0,1,0}x_{0,1,1}$. Now we have $x = x_{0,0}x_{0,1,0}x_{0,1,1}x_1$, etc. We call this process a *factorization process* of x. If it stops after finitely many steps, we say that this is a *finite factorization process* of x. If it never stops, we say that this is an *infinite factorization process* of x.

To illustrate, we provide a brief example.

Example 2.6. *Consider the integral domain $R = \mathbb{Z}[X]$ and the polynomial*

$$f(X) = X^6 + 4X^5 + 5X^4 - 2X^3 - 4X^2 - 2X - 2.$$

In step 1 of the factorization process, we recognize that $f(X)$ is reducible and we factor it as

$$f(X) = (X^2 + X + 1)(X^4 + 3X^3 + X^2 - 3X - 2);$$

In step 2 of the factorization process, we see that $X^2 + X + 1$ is irreducible and that $X^4 + 3X^3 + X^2 - 3X - 2$ is reducible, so we further factor $f(X)$ as

$$f(X) = (X^2 + X + 1)(X^2 - 1)(X^2 + 3X + 2);$$

In step 3 we recognize that $X^2 - 1$, *so we factor it as* $(X-1)(X+1)$ *and get*

$$f(X) = (X^2 + X + 1)(X-1)(X+1)(X^2 + 3X + 2).$$

In step 4 we recognize that $X - 1$ *and* $X + 1$ *are irreducible and that* $X^2 + 3X + 2$ *is reducible, so we factor it as* $(X+1)(X+2)$ *and get*

$$f(X) = (X^2 + X + 1)(X-1)(X+1)(X+1)(X+2).$$

In step 5 we recognize that $X+1$ *and* $X+2$ *are irreducible, so we stop. Thus* $f(X)$ *has a finite factorization process.*

With these definitions and notions we have a firm foundation upon which we can approach the remaining chapters in confidence. In Chapter 3, we will introduce the *principal containment* property, by which we will provide a simple new characterization of principal ideal domains.

CHAPTER 3
A NEW CHARACTERIZATION OF PIDS

In this chapter, we present a simple new characterization of principal ideal domains. We introduce a new notion, namely, the *principal containment condition* for integral domains which successfully generalizes previous advancements heretofore. It is worth noting that it is in this context that we discovered our impetus to further investigate monoid domains; indeed, we will make significant use of these domains to prove that our classification is, in fact, more general. We will begin by highlighting relevant advances in PID classifications.

For $n \geq 1$, we say that an ideal I of a domain R is *n-generated* if there exist $x_1, x_2, \ldots, x_n \in R$ such that $I = (x_1, x_2, \ldots, x_n)$. Note: Every k-generated ideal, $k \geq 1$, is an l-generated ideal for all $l > k$. Of specific interest to this chapter are those domains whose every $2-$*generated* ideal is principal; we call these integral domains *Bézout domains.* The next two theorems are characterizations of PIDs. The first one (*Cohn's Theorem*) is Theorem 3.1 that was first stated in [3.1, Proposition 1.2]. Even though it is well-known and often used, we were not able to locate a proof in the literature. Cohn remarks in 3.1 that is is easy to prove that Bézout's domains which satisfy ACCP PIDs (however, ACCP is not equivalent to atomicity, as it was later shown). The second one is Theorem 3.2, proved in 2008 by Chinh and Nam in [4].

Theorem 3.1 (Cohn's Theorem)**.** *If R is an atomic Bézout domain, then R is a PID.*

Theorem 3.2 (Chinh-Nam Theorem). *If R is a UFD in which every maximal ideal is principal, then R is a PID.*

Our next theorem, presented in our paper [5], improves both of the above theorems. It weakens one of the conditions in Cohn's theorem and both conditions in Chinh and Nam's theorem.

Theorem 3.3. *Let R be an atomic domain which satisfies the PC condition. Then R is a PID.*

One may observe the striking similarities between Cohn's assertion and the characterization proved by Chinh and Nam. In both of their hypotheses, there are two restrictions to the given domain: 1) there is a restriction on the factorization and 2) a restriction on ideals that are principal. Strictly speaking, their choice of restrictions on the ideals cannot be compared; however, Cohn allows for a much more general factorization property than Chinh and Nam.

Our characterization of PIDs is achieved by weakening each of the hypotheses in Chinh and Nam's result. By doing so, we improve upon Cohn's assertion and show that atomic Bézout domains are indeed principal ideal domains. Inspired by these authors, we introduce a new condition concerning principal ideals of integral domains and we prove that this new condition is weaker than those utilized heretofore.

Definition 3.1. *We call the condition that every 2-generated ideal of a domain R is principal the* ***Bézout condition****.*

It is straightforward to see that every PID is a Bézout domain, but we will show that the opposite implication is not true. To do so, we will make use of a specific ring construction $R = D + XK[X]$. Given a UFD D, a subring of a field K, the construction $R = D+XK[X]$ is an integral domain consisting of all polynomials $a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$ where $a_0 \in D$ and $a_1, a_2, \ldots, a_n \in K$.

Proposition 3.1 ([8, 9.4, Exercise 5, pages 306-307])**.** *The Bézout condition for integral domains is strictly weaker than the PID condition. Our provided counter example is the domain $R = \mathbb{Z} + X\mathbb{Q}[X]$, a Bézout domain that is not a PID.*

Proof. By [8, Corollary 4.13], we know that R is a Bézout domain because $\mathbb{Z}$ is a Bézout domain. To show that R is not a PID, we consider the ideal $P = X\mathbb{Q}[X] \subseteq R$. We will show that P is not principal. In fact, we will show that P is not finitely generated. Suppose to the contrary, and let $P = (f_1, f_2, \ldots, f_k)$ for some $k \geq 1$. Each f_i has constant term zero. Let $q_{1,i}$ be the coefficient by X for each f_i, $i = 1, 2, \ldots, k$. Then, any element of P, say $g_1 f_1 + g_2 f_2 + \cdots + g_k f_k$, has the coefficient by X a member of the set $\mathbb{Z}q_{1,1} + \mathbb{Z}q_{1,2} + \cdots + \mathbb{Z}q_{1,k} \neq \mathbb{Q}$, because $\mathbb{Q}$ is not a finitely generated group. Thus, P is not finitely generated, and, therefore, is not principal. Thus, R is not a PID. □

Definition 3.2. *We call the* ***PIP condition*** *the condition for integral domains that every prime ideal is principal.*

Definition 3.3. *We call the* ***MIP condition*** *the condition for integral domains that every maximal ideal is principal.*

Clearly, the PID condition implies the PIP condition and the PIP condition implies the MIP condition. However, we can provide more precise relations as well.

Proposition 3.2 ([8, 8.2, Exercise 6, pages 283])**.** *The PID condition for integral domains is equivalent to the PIP condition.*

Proof. The forward direction is clear, so we only need to prove the backward direction. Suppose that every prime ideal of R is principal, however, suppose also that, to the contrary, R is not a PID, i.e., that the set $\mathcal{J}$ of all ideals of R that are not principal is nonempty. This set is partially ordered under inclusion. Let ϕ be a chain of ideals in $\mathcal{J}$ and let $J = \cup\{I : I \in \phi\}$. We claim that J is not principal.

Suppose to the contrary. Then $J = (a)$ for some $a \in R$. Then $a \in I$ for some $I \in \phi$. Hence, $J = (a) \subseteq I \subseteq J$, so that $I = J$, hence J is not principal, a contradiction. Thus, every chain in $\mathcal{J}$ has a majorant. Hence, by Zorn's Lemma, $\mathcal{J}$ has a maximal set.

Let $\mathcal{I}$ be a maximal element in $\mathcal{J}$, i.e., an ideal of R which is maximal with respect to the property of being non-principal. In particular, I is not prime. Hence, there are $a, b \in R$ such that $ab \in I$, but $a \notin I$ and $b \notin I$. Let $I_a = (I, a)$, the ideal generated by I and a, and let $I_b = (I, b)$ be the ideal generated by I and b. Since $I_a \supset I_b$, I_a is a principal ideal. Let $I_a = (\alpha)$. Let $J = (I : I_a) = \{r \in R : rI_a \subseteq I\}$. Then, $I \subsetneq I_b \subseteq J$; hence $(J) = (\beta)$ is also a principal ideal. Now, $I_a J = (a)(b) = (\alpha\beta) \subseteq I$, and since $J = (I : I_a)$, we have that for every $x \in I$, $x = sa$ for some $s \in J$. Hence, $I = I_a J$ and so I is principal, a contradiction. Thus R is a PID. □

Proposition 3.3. *The MIP condition for integral domains is strictly weaker than the PIP condition.*

Proof. Consider the Bézout domain $R = \mathbb{Z} + X\mathbb{Q}[X]$. We showed in Proposition 3.1 that R is not a PID, hence, by Proposition 3.2, it does not satisfy the PIP condition. Thus, we only need to justify that R satisfies the MIP condition. According to [6, Theorem 1.3], the maximal ideals of R are of the following types: (1) the contractions of the maximal ideals of $\mathbb{Q}[X]$ distinct from (X), and (2) the ideals $(p) + X\mathbb{Q}[X]$, where p is a prime number. Let $\mathfrak{m} = (f(X)) \cap R$ be a maximal ideal of the first type, where $f(X) = a_0 + a_1X + \cdots + a_nX^n$ is irreducible in $Q[X]$. Then, let $\widetilde{f}(X) = 1 + \frac{a_1}{a_0}X + \cdots + \frac{a_n}{a_0}X^n$, an element of R. Then, $\mathfrak{m}$ can be written as $\mathfrak{m} = (\widetilde{f}(X))R$ and $\mathfrak{m}$ is principal. Now, let $\mathfrak{m} = (p) + X\mathbb{Q}[X]$, an ideal of the second type. Then, $\mathfrak{m} = (p)R$. Hence, every maximal ideal of R is principal. Thus, we have provided a domain that satisfies the MIP condition but not the PIP condition. □

Now, we will introduce a new notion for an integral domain R concerning proper 2-generated ideals.

Definition 3.4. *We call the* ***principal containment condition*** *(PC) the condition for integral domains that every proper 2-generated ideal is contained in a proper principal ideal.*

It is easy to see that the Bézout condition implies the PC condition. By recalling Krull's Theorem, which states that every proper ideal I of a commutative ring R is contained in a maximal ideal of R, it is also clear that the MIP condition implies the PC condition. However, asserting that the PC condition is strictly weaker than the MIP and Bézout conditions requires justification. To do so, we will need to recall the definition of the localization of a ring at a prime ideal.

Definition 3.5. *Given a domain R and a prime ideal $\mathfrak{p}$ of R, the localization of R* ***at*** *$\mathfrak{p}$, denoted $R_{\mathfrak{p}}$, is the set of elements $\left\{\frac{m}{n} : m, n \in R \text{ and } n \notin \mathfrak{p}\right\}$. ($R_{\mathfrak{p}}$ is a local ring.)*

Note, that, because every maximal ideal is prime, we may consider the localization of a domain R at a maximal ideal $\mathfrak{m}$.

Proposition 3.4. *The PC condition is strictly weaker than the MIP condition.*

Proof. We will provide an example of a domain that satisfies the PC condition but not the MIP condition. We will begin with the monoid ring $R = F[X; \mathbb{Q}_+]$. Let $\mathfrak{m}$ be the maximal ideal of R consisting of all the polynomials in R whose constant term is zero. Consider, then, the local ring $D = R_{\mathfrak{m}}$. Note that every non-zero element of D has the form uX^{α}, where u is a unit in D and $\alpha \in \mathbb{Q}_+$. Indeed, every nonzero element of D is of the form:

$$f = \frac{a_0 + a_1 X^{\alpha_1} + \cdots + a_n X^{\alpha_n}}{b_0 + b_1 X^{\beta_1} + \cdots + b_m X^{\beta_m}}$$

where b_0 is nonzero, $0 < \alpha_1 < \alpha_2 < \cdots < \alpha_n$ and $0 < b_0 < \cdots < b_m$. If $a_0 \neq 0$, then f is a unit. If $a_0 = a_1 = \cdots = a_{i-1} = 0$, $i \geq 1$, then we can write

$$f = \frac{a_i + a_{i+1}X^{\alpha_{i+1}-\alpha_i} + \cdots + a_nX^{\alpha_n-\alpha_i}}{b_0 + b_1X^{\beta_1} + \cdots + b_mX^{\beta_m}} \cdot X^{\alpha_i},$$

and so f can be written in the form uX^α. Now, the maximal ideal $\mathfrak{m}R_\mathfrak{m}$ of D consists of all uX^α where $\alpha > 0$ and is not finitely generated. To show that $\mathfrak{m}R_\mathfrak{m}$ is not finitely generated, we need only suppose that it can be finitely generated, say $\mathfrak{m}R_\mathfrak{m} = (u_1X^{\gamma_1}, \ldots, u_kX^{\gamma_k})$, where $k \geq 1$, $r_1, \ldots, r_k > 0$, and u_i is a unit for $i = 1, 2, \ldots, k$. Suppose that γ_1 is the least exponent. Because $(u_1X^{\gamma_1}, \ldots, u_kX^{\gamma_k})$ generates $\mathfrak{m}R_\mathfrak{m}$, then, there exists $g_1, g_2, \ldots, g_k \in D$ such that:

$$\begin{aligned} X^{\frac{\gamma_1}{2}} &= g_1(u_1X^{\gamma_1}) + \cdots + g_k(u_kX^{\gamma_k}) \\ &= X^{\frac{\gamma_1}{2}}(g_1(u_1X^{\frac{\gamma_1}{2}}) + \cdots + g_k(u_kX^{\frac{\gamma_k}{2}})), \end{aligned}$$

and by cancellation, we get that $1 \in \mathfrak{m}R_\mathfrak{m}$, an impossibility. Thus, D does not satisfy the MIP condition.

Now, we show that D does satisfy the PC condition. For any two elements $uX^\alpha, vX^\beta \in D$, $\alpha \leq \beta$, we have that $uX^\alpha | vX^\beta$ and so (uX^α, vX^β), an arbitrary proper 2-generated ideal, is contained in (vX^β), a proper principal ideal. □

Proposition 3.5. *The PC condition is strictly weaker than the Bézout condition.*

Proof. We will provide an example of a domain that satisfies the PC condition but not the Bézout condition. First, consider the subring R of $\mathbb{R}[X; \mathbb{Q}_+]$, consisting of all the polynomial of the form: $f(X) = a_0 + a_1X^{\alpha_1} + \cdots + a_nX^{\alpha_n}$ where $a_0 \in \mathbb{Q}$, $a_1, \ldots, a_n \in \mathbb{R}$, and $0 < \alpha_1 < \cdots < \alpha_n$. Let $\mathfrak{m}$ be the maximal ideal of R consisting of all the polynomials in R whose constant term is 0. Consider the local ring $D = R_\mathfrak{m}$. The units of D are of the form

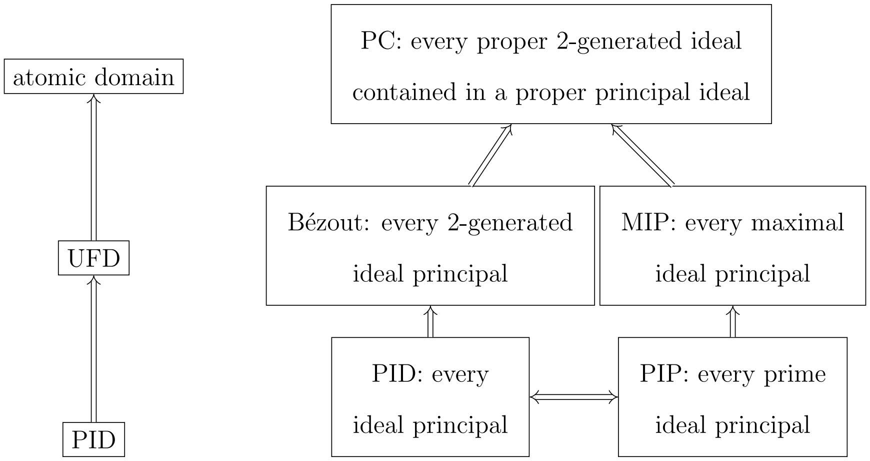
$$\frac{a_0 + a_1X^{\alpha_1} + \cdots + a_mX^{\alpha_m}}{b_0 + b_1X^{\beta_1} + \cdots + b_nX^{\beta_n}},$$

where a_0 and b_0 are nonzero rational numbers and the $a_i, b_j \in \mathbb{R}$ for all $i = 1, 2, \ldots, m$ and $j = 1, 2, \ldots, n$. Similar to Proposition 3.4, every nonzero element of D can be written as uaX^{α} where u is a unit in D, $\alpha \in \mathbb{Q}_{+}$, and a is a non-zero real number. Note, if $\alpha = 0$, then a is rational. Let $I = (aX^{\alpha}, bX^{b}),\ 0 < \alpha \leq \beta$, be a proper 2-generated ideal of D, and let γ be a rational number such that $0 < \gamma < \alpha$. Then, since X^{γ} divides both aX^{α} and bX^{β}, $I \subsetneq (X^{\gamma})$; hence D satisfies the PC condition.

We now show that D does not satisfy the Bézout condition. We accomplish that by considering the 2-generated ideal $J = (X, \sqrt{2}X)$ and supposing that there exists some element $aX^{\alpha} \in D$ such that $J = (aX^{\alpha})$. Then, α must be equal to one and from $aX|X$, we get that for some rational element $b \in D$, $(aX)(b) = X$, hence, $ab = 1$ and a must be rational. However, it cannot then be true that aX divides $\sqrt{2}X$, a contradiction. Thus, D does not satisfy the PC condition. Therefore, the PC condition is strictly weaker than the Bézout condition. □

Now, with these relations proved, we present the implication diagram in the figure on the next page.

Figure 3.1: Relations of Integral Domains and Domain Properties


atomic domain
UFD
PID
PC: every proper 2-generated ideal contained in a proper principal ideal
Bézout: every 2-generated ideal principal
MIP: every maximal ideal principal
PID: every ideal principal
PIP: every prime ideal principal

One may notice that there is only one equivalence in the diagram, the rest are strict implications. The higher one goes on each side of the diagram, the more general the statement one obtains. For example, factorization properties in atomic domains are weaker than those of UFD and PID. Also, the PC condition is more general than the Bézout and MIP conditions. Thus, to improve upon the results of Cohn and Chinh and Nam we will choose the most general conditions available; that is, the atomic and PC conditions. Now, we present our characterization of PIDs.

Theorem 3.4. *Let R be an atomic domain which satisfies the PC condition. Then R is a PID.*

Proof. It is enought to show that every prime ideal is principal. Let $P \neq 0$ be a prime ideal of R. Then, there exists a nonzero nonunit element $x \in P$, and since R is atomic, we may factor x into a finite number of atoms:

$$x = p_1 p_2 \dots p_k.$$

where $k \geq 1$. Because P is a prime ideal, for some $i \in \{1, 2, \dots, k\}$, $p_i \in P$. We will show that P is, in fact, equal to (p_i). Take y to be an element of P and consider the 2-generated ideal (p_i, y). Since (p_i, y) is contained in P, it must be a proper ideal of R; thus, by the PC condition, there is some element, say r, such that $(p_i, y) \subseteq (r) \subset R$. Therefore, r must divide both p_i and y; because p_i is an atom, $r \sim p_i$. Thus, $p_i | y$ and $P = (p_i)$. □

There we have a simple new characterization of PIDs. Take note that much of the labor was spent in proving that the PC condition was indeed strictly weaker than the Bézout and MIP conditions. In finding appropriate counter examples, we made use of specific monoid domains. These examples, together with a theorem by Daileda in [9], provided the proper impetus for our investigation into the atomicity and AP property in monoid domains which we discuss in the following chapter. There, we will introduce Daileda's theorem and improve upon our theory of monoid domains. (Remark: It happens that the PC condition implies the AP property; however, the converse does not hold. In the final chapter, we present two diagrams with all relevant implications from our work.)

CHAPTER 4
THE ATOMICITY AND AP PROPERTY OF $F[X;M]$

In the previous chapter, we discussed the context under which monoid domains initially became appealing in our study. In this chapter, and throughout the remainder of this dissertation, we will analyze monoid domains and the monoids which they are associated to uncovering sufficient conditions for the existence of ring-theoretic properties of particular interest, more specifically, the atomic and AP properties.

In 2008 Daileda showed in [7] that $F[X;M]$, where $M = (\mathbb{Q}_+, +)$, is AP. Also, it is common knowledge that the integral domain $F[X]$, which is, in fact, a monoid domain and can be written as $F[X;\mathbb{N}_0]$, is a UFD, i.e., an atomic AP domain. So it was natural to ask the question: for which submonoids M of $(\mathbb{Q}_+, +)$ is the monoid domain $F[X;M]$ AP? Moreover, what about atomicity? These questions are particular instances of Gilmer's "generic question" (Q_E) from [12]: *if R is a ring, Γ a monoid and E some ring-theoretic propery, under what conditions does the semigroup ring $R[X;\Gamma]$ have the property E?*

We will begin our analysis with some simple, yet quite usefull, notions and results.

4.1 Preliminary Notions and Results

Proposition 4.1. *If $f(X)$ is a divisor in $F[X;M]$ of an element X^{α}, $\alpha \in M$, then $f(X) = aX^{\beta}$ with $a \in F$, $\beta \in M$, and $\alpha - \beta \in M$.*

Proof. Let $f(X) = a_1X^{\alpha_1} + \cdots + a_nX^{\alpha_n} \in F[X;M]$, where $n \geq 1$ and $\alpha_1 < \alpha_2 < \cdots < \alpha_n$. Since $f(X)|X^\alpha$, there exists an element $g(X) = b_1X^{\beta_1} + \cdots + b_mX^{\beta_m} \in F[X;M]$, where $m \geq 1$ and $\beta_1 < \beta_2 < \cdots < \beta_m$, such that $f(X)g(X) = X^\alpha$. Hence, $m = 1$, $n = 1$, $g(X) = b_1X^{\beta_1}$ with $a_1b_1 = 1$ and $\alpha_1 + \beta_1 = \alpha$. This implies the statement. □

Definition 4.1. *We say that a fraction* $\frac{m}{n}$, $m \in \mathbb{N}_0$, $n \in \mathbb{N}$, *is (written) in* ***reduced form*** *if gcd(m,n)=1.*

Example 4.1. *1)* $\frac{0}{1}$, $\frac{3}{5}$, $2 = \frac{2}{1}$, *and* $\frac{17}{8}$ *are all written in reduced form;*
2) $\frac{0}{3}$, $\frac{3}{15}$ *are not written in reduced form, however.*

Lemma 4.1 (Reduced Form Lemma)**.** *Let* $\frac{k}{l}, \frac{m}{n} \in \mathbb{Q}_+$ *be two fractions in reduced form. Then,*

$$\frac{k}{l} = \frac{m}{n} \iff k = m \text{ and } l = n.$$

Proof. The equality $\frac{k}{l} = \frac{m}{n}$ is equivalent with $kn = ml$. Suppose that for some prime p, $0 \leq \beta < \alpha$ are such that p^α is the highest power of p as a factor of l and p^β is the highest power of p as a factor of n. By writing $l = p^\alpha l'$, $m = p^\beta n'$, we have $kn'p^\beta = ml'p^\alpha$, hence $kn' = ml'p^{\alpha-\beta}$, so that $p^{\alpha-\beta} \mid kn'$, a contradiction. Similarly, if we suppose that $0 \leq \beta < \alpha$ are such that p^α is the highest power of p as a factor of n and p^β is the highest power of p as a factor of l, we arrive at a contradiction. It follows then that $l = n$, and this implies that $m = n$. □

Having reviewed these definitions and results, we begin our study of monoid domains $F[X;M]$ by first analyzing the submonoids M of $(\mathbb{Q}_+, +)$. We do this by considering another familiar notion, that of, a monoid's *generators*.

4.2 Essential Generators

Let $A \subseteq \mathbb{Q}_+$ and let $\mathcal{A}$ be the (nonempty) set of all submonoids of $(\mathbb{Q}_+, +)$ that contain A. Now, consider the set

$$M = \bigcap_{A_i \in \mathcal{A}} A_i.$$

It is not difficult to show that M is a monoid, in fact, it is a submonoid of $(\mathbb{Q}_+, +)$. Indeed: each A_i contains 0, therefore, $0 \in M$; for elements $a, b \in M$, $a + b \in A_i$ for all i, and, hence, $a + b \in M$; finally, the operation $+$ maintains associativity seeing that it is induced from $(\mathbb{Q}_+, +)$. Furthermore, it happens that M is the smallest submonoid of $(\mathbb{Q}_+, +)$ containing A. We say that M is the *submonoid generated by* A and we write $M = \langle A \rangle$. The elements of $\langle A \rangle$ are of the form:

$$k_1 a_1 + k_2 a_2 + \cdots + k_n a_n$$

where $n \in \mathbb{N},\ a_i \in A,\ k_i \in \mathbb{N}_0\ \forall\ i = 1, 2, \ldots, n$. We call the elements of A *generators* of M, and if a monoid M can be generated by a finite set A, then we say that M is *finitely generated.* Otherwise, M is *infinitely generated.* Following are examples of submonoids of $(\mathbb{Q}_+, +)$ generated by finite and infinite sets.

Example 4.2. *(1)* $\mathbb{N}_0 = \langle 1 \rangle$*, and is, thus, finitely generated;*
(2) $\{0, 4, 6, 8, 10, \ldots\} = \langle 4, 6 \rangle$*, and is, thus, finitely generated;*
(3) $\mathbb{Q}_+$ *is infinitely generated.*

4.2.1 Essential Generators and the Monoid

All of the previous notions are well known. We now introduce a new notion that will aid in our investigation of monoid domains $F[X; M]$, where M is a submonoid of $(\mathbb{Q}_+, +)$.

Definition 4.2. *An element* $a \in M$ *is called an* ***essential generator*** *of* M *if* $\langle M \setminus \{a\} \rangle \neq M$.

A quick and useful deduction from the definition is that if a is an essential generator of a monoid M, then a cannot be a member of $\langle M \setminus \{a\} \rangle$. Therefore, if a is not an essential generator, $a \in \langle M \setminus \{a\} \rangle$, i.e., for a natural number n, there exist nonnegative integers $k_1, k_2, \ldots, k_n$ and elements of the monoid, $x_1, x_2, \ldots, x_n$, all different than a, such that a may be written as the sum

$$a = k_1 x_1 + k_2 x_2 + \cdots + k_n x_n.$$

This implies that there exists elements $\alpha, \beta \in M$ where $a = \alpha + \beta$. These implications prove particularly useful in later proofs. Below, we provide several examples of submonoids of $(\mathbb{Q}_+, +)$ and their essential generators (if they exist) and several propositions revealing the relationships between essential generators of M and generating sets of M.

Example 4.3. *(1) $M = \mathbb{N}_0 = \langle 1 \rangle$ is a finitely generated monoid and 1 is an essential generator of M;*

(2) $M = \langle 2, 5 \rangle$ is a finitely generated monoid and both 2 and 5 are essential generators of M;

(3) $M = \mathbb{Q}_+$ is an infinitely generated monoid with no essential generators;

(4) $M = \left\langle \frac{1}{2}, \frac{1}{2^2}, \frac{1}{2^3}, \ldots \right\rangle$ is an infinitely generated monoid with no essential generators;

(5) $M = \left\langle \frac{1}{2}, \frac{1}{2^2}, \frac{1}{2^3}, \ldots ; \frac{1}{5} \right\rangle$ is an infinitely generated monoid with one essential generator, namely $\frac{1}{5}$;

(6) $M = \left\langle \frac{1}{2}, \frac{1}{3}, \frac{1}{5}, \ldots \right\rangle$ is an infinitely generated monoid and each element $\frac{1}{2}, \frac{1}{3}, \frac{1}{5}, \ldots$ is an essential generator;

(7) $M = \langle 0 \rangle$ is a finitely generated monoid with no essential generators since $M = \langle \emptyset \rangle$.

Proposition 4.2. *Let $a \in M$ be an essential generator. If $A \subseteq M$ is a generating set of M, then $a \in A$.*

Proof. Suppose to the contrary; that is, $a \notin A$. Since $\langle A \rangle = M$, a can be written as the sum

$$a = k_1a_1 + k_2a_2 + \cdots + k_na_n,$$

where $n \geq 1$ is an integer, $k_1, k_2, \ldots, k_n \in \mathbb{N}_0$, and $a_1, a_2, \ldots, a_n \in A$. However, because $A \subset M \setminus \{a\}$, a is then a member of $\langle M \setminus \{a\} \rangle$, a contradiction since a is an essential generator. □

Proposition 4.3. *Let A be a generating set of M and let $a \in A$ such that $\langle A \setminus \{a\} \rangle \neq M$. Then a is an essential generator of M.*

Proof. Suppose to the contrary, that is, suppose that a is not an essential generator of M, i.e., $a \in \langle M \setminus \{a\} \rangle$. Then, a can be written as the sum

$$a = k_1x_1 + k_2x_2 + \cdots + k_nx_n,$$

where $n \geq 1$ is an integer, $k_1, k_2, \ldots, k_n \in \mathbb{N}_0$, and $x_1, x_2, \ldots, x_n \in M \setminus \{a\}$. At least one of the elements $x_1, x_2, \ldots, x_n$ cannot be generated by the elements of $A \setminus \{a\}$; otherwise, $a \in \langle A \setminus \{a\} \rangle$, a contradiction. Thus, for some $i \in \{1, 2, \ldots, n\}$, we will suppose that x_i cannot be written as a linear combination of elements from $A \setminus \{a\}$. We may assume that $k_i > 0$. Note also that if all k_jx_j $(j \neq i)$ are 0, then $k_i \geq 2$ (otherwise $x_i = a$). Hence,

$$x_i = l_1a_1 + l_2a_2 + \cdots + l_ma_m + la,$$

where $m \geq 1$ is an integer, $l_1, l_2, \ldots, l_m \in \mathbb{N}_0$, $l \in \mathbb{N}$, and $a_1, a_2, \ldots, a_m \in A$. By substitution, we then write

$$\begin{aligned} a &= k_1x_1 + k_2x_2 + \cdots + k_ix_i + \cdots + k_nx_n \\ &= k_1x_1 + k_2x_2 + \cdots + k_i(l_1a_1 + l_2a_2 + \cdots + l_ma_m + la) + \cdots + k_nx_n \\ &= k_ila + \Big[k_1x_1 + k_2x_2 + \cdots + k_i(l_1a_1 + l_2a_2 + \cdots + l_ma_m) + k_{i+1}x_{i+1} + \dots k_nx_n\Big], \end{aligned}$$

and since $x_i \neq a$, we have a false equality. The right-hand side of the equation is greater than the left-hand side as either $k_il \geq 2$ or at least one of k_jx_j $(j \neq i)$ is $\neq 0$. □

Proposition 4.4. *If $M = \langle A \rangle$, then we may remove from A any finite set consisting of nonessential generators of M and the set A' obtained in such a way still generates M.*

Proof. Let $n \in \mathbb{N}$ and $A \backslash A' = \{a_1, a_2, \ldots, a_n\}$. We will show by finite induction that we can remove the elements $a_1, a_2, \ldots, a_n$ from A and still have a set which generates M. The contrapositive of Proposition 4.3 asserts that $\langle A \setminus \{a_1\}\rangle = M$. Suppose that for $k > 1$, $k < n$, $\langle A \setminus \{a_1, a_2, \ldots, a_k\}\rangle = M$. Then, again, by utilizing the contrapositive of Proposition 4.3, we have that $\langle (A \backslash \{a_1, a_2, \ldots, a_k\}) \backslash \{a_{k+1}\}\rangle = M$, i.e., $\langle A \setminus \{a_1, a_2, \ldots, a_{k+1}\}\rangle = M$. Thus, by induction, $\langle A \setminus \{a_1, a_2, \ldots, a_n\}\rangle = M$. □

Proposition 4.5. *Let M and M' be two monoids, $\mu : M \to M'$ a monoid isomorphism, and let $a \in M$. Then a is an essential generator of M if and only if $\mu(a)$ is an essential generator of M'.*

Proof. It is enough to prove that if a is an essential generator of M, then $\mu(a)$ is an essential generator of M' as μ^{-1} is also an isomorphism of monoids. Suppose to the contrary; then, $\mu(a)$ is an element of the set generated by $M' \setminus \{\mu(a)\}$. Thus, for $n \geq 1$, a natural number, there are nonnegative integers $k_1, k_2, \ldots, k_n$ and elements of $M' \setminus \{\mu(a)\}$, $x_1, x_2, \ldots, x_n$, such that

$$\mu(a) = k_1x_1 + k_2x_2 + \cdots + k_nx_n.$$

Hence,

$$\mu^{-1}\big(\mu(a)\big) = \mu^{-1}\big(k_1x_1 + k_2x_2 + \cdots + k_nx_n\big),$$

i.e.,

$$\begin{aligned} a &= \mu^{-1}(k_1x_1) + \mu^{-1}(k_2x_2) + \cdots + \mu^{-1}(k_nx_n) \\ &= k_1\mu^{-1}(x_1) + k_2\mu^{-1}(x_2) + \cdots + k_n\mu^{-1}(x_n), \end{aligned}$$

where $\mu^{-1}(x_1), \mu^{-1}(x_2), \ldots, \mu^{-1}(x_n) \in M\backslash\{a\}$. Thus, $a \in \langle M\backslash\{a\}\rangle$, a contradiction since a is an essential generator. □

In order to facilitate instruction, we have provided an examples below.

Example 4.4. *Let M be a numerical monoid. That is, define M to be generated by the set $\{x_1, x_2, \ldots, x_k\}$, where $x_1, x_2, \ldots, x_k \in \mathbb{N}$ and gcd$(x_1, x_2, \ldots, x_k) = 1$. An example of such a monoid is $M = \langle 2, 3\rangle = \{0, 2, 3, 4, 5, 6, 7, \ldots\}$. Its associated monoid domain $F[X; M]$ is atomic since $F[X; M]$ is a subring of $F[X]$ which contains F. However, it is easy to show that $F[X; M]$ is not AP. Indeed, consider X^2 and X^3. We have already shown that any divisor of X^2 must be of the form $f(X) = a_1X^{\beta_1}$ where $a_1 \in F$ and $\beta_1 \in M$. Since $1 \notin M$, it follows that $X \notin F[X; M]$. Hence, $\beta_1 = 0$ or $\beta_1 = 2$, and so X^2 is irreducible. Similarly, if $g(X) = a_2X^{\beta_2}$ divides X^3 in $F[X; M]$, it must be that $\beta_2 = 0$ or $\beta_2 = 3$, and, therefore, X^3 is irreducible, as well. Notice that the element $X^6 \in F[X; M]$ may be factored in two ways: 1) $X^6 = X^2X^2X^2$ and 2) $X^6 = X^3X^3$. Thus, $X^2|X^3X^3$, and since we know that X^3 is irreducible, $X^2 \nmid X^3$. Hence, X^2 is not prime and $F[X; M]$ is not an AP domain.*

Now, 2 and 3 are essential generators of M. Under the monoid isomorphism $\mu_2 : M \to 2M$, the elements 4 and 6 are essential generators of the monoid $\langle 4, 6\rangle$. Moreover, the monoid domain $F[X; M]$ is isomorphic to $F[X; 2M]$ via the ring isomorphism $\phi_2 : F[X; M] \to F[X; 2M]$ defined by

$$\phi_2(a_0 + a_1X^{\alpha_1} + \cdots + a_nX^{\alpha_n}) = a_0 + a_1X^{\mu_2(\alpha_1)} + \cdots + a_nX^{\mu_2(\alpha_2)}.$$

Therefore, $F[X; 2M]$ is also an atomic non-AP domain. Note, however, that $2M$ is not a numerical monoid since $gcd(4, 6) \neq 1$.

We may arrive at a similar conclusion for any monoid of the form τM, where $\tau \in \mathbb{Q} \setminus \{0\}$, since $\mu_\tau : M \to \tau M$ is a monoid ismorphism. For example, the monoid $\left\langle 1, \frac{3}{2} \right\rangle$ is also an atomic non-AP domain, because $\mu_{1/2}$ is an isomorphism.

4.2.2 Essential Generators and the Monoid Domain

At this point, one may wonder why we are lending significant attention to particular elements of the monoid rather than to the elements of the associated monoid domain $F[X; M]$. The purpose of our investigation will become clear as we explore the implications that essential generators of M have on the irreducible elements of $F[X; M]$. We will see that not every generator is equal.

Proposition 4.6. *Suppose that a is an essential generator of the monoid M and $M \neq \langle a\rangle$. Then X^a is an irreducible non-prime element of $F[X; M]$.*

Proof. Suppose there is an element $b \in M$ such that $0 < b < a$. Let $a = \frac{p}{q}$ and $\frac{m}{n}$. Then

$$aq = p, \ nb = m;$$

hence,

$$a(mq) = pm,$$

$$b(np) = pm.$$

Hence,

$$X^a \mid \underbrace{X^a \cdot X^a \cdots X^a}_{mq\ times} = X^{pm} = \underbrace{X^b \cdot X^b \cdots X^b}_{np\ times},$$

however, $X^a \nmid X^b$. Hence, X^a is not prime.

The same argument holds if we don't have the condition $0 < b < a$, but the condition that b is another (different) essential generator instead.

The irreducibility of X^a follows from the fact that otherwise the relation $X^a = X^b \cdot X^c$, $b \neq 0$,$c \neq 0$, would imply $a = b + c$, which is not possible since a is an essential generator.

It remains to consider the option that a is the smallest non-zero element of M and the only essential generator of M. Consider the intervals $[a, 2a), [2a, 3a), [3a, 4a), \ldots,$ and let $(ma, (m + 1)a)$ be the first interval in which we have an element, say b, of $M \setminus \langle a \rangle$. Then, $b = b_1 + b_2$, where $b_1, b_2 \neq 0$, and at least one of them, say b_1, is from $M \setminus \langle a \rangle$. Then, $b_1 \in (ma, (m+1)a)$, which implies $b_1 \in (0, a)$, a contradiction. Thus, this option case cannot occur. □

Proposition 4.7. *The irreducible elements of $F[X; M]$ of the form X^a, $a \in M$, are precisely the elements X^a where a is an essential generator of M.*

Proof. Let $\mathcal{S}$ be the set of all elements $X^a \in F[X; M]$ such that X^a is irreducible. We will show that for all $X^a \in \mathcal{S}$, a is an essential generator of M. Suppose there exists some $X^{a'} \in \mathcal{S}$ such that $a' \in M$ is not an essential generator. Then, there exists $\alpha, \beta \in M$ such that $a' = \alpha + \beta$, $\alpha, \beta \neq 0$. Hence, we may factor X^a into two nonzero, nonunit factors, namely, $X^a = X^\alpha \cdot X^\beta$, a contradiction. Therefore, for every $X^a \in \mathcal{S}$, a is an essential generator of M. The opposite direction follows from Proposition 4.6 when $M \neq \langle a \rangle$ and it is clear when $M = \langle a \rangle$. □

Proposition 4.8. *If $M \neq \{0\}$ cannot be generated by essential generators, then $F[X; M]$ is not atomic.*

Proof. Suppose to the contrary, that is, suppose that $F[X;M]$ is atomic. Let A be the set of all essential generators of M. Since $M \neq \langle A \rangle$, there exists an element $a \in M \setminus \langle A \rangle$. Because $F[X;M]$ is atomic, X^a admits at least one factorization into a finite number (≥ 1) of atoms, say,

$$X^a = f_1(X) f_2(X) \ldots f_n(X),$$

and from Proposition 4.7 we know that for each $i = 1, 2, \ldots, n$, $f_i(X)$ is, up to associates, the monomial $X^{\alpha_i} \in F[X;M]$ where $\alpha_i \in M$ is an essential generator. Hence,

$$X^a = X^{\alpha_1} X^{\alpha_2} \cdots X^{\alpha_n},$$

so that $a = \alpha_1 + \alpha_2 + \cdots + \alpha_n$, i.e., $a \in \langle A \rangle$, a contradiction. □

The natural question to ask here is whether the converse of Proposition 4.8 holds. That is, if a monoid M can be generated by essential generators, is the associated monoid domain $F[X;M]$ necessarily atomic? As we seek to answer this question, we will begin by analyzing a particular case where the implication holds.

4.3 The Monoid $M = \left\langle \frac{1}{2}, \frac{1}{3}, \frac{1}{5}, \ldots \right\rangle$

In this section, we will assume that M always denotes the monoid $\left\langle \frac{1}{2}, \frac{1}{3}, \frac{1}{5}, \ldots \right\rangle$. In our analysis of M, we discover useful tools and develop an intuition that aid in further generalizations. We begin by supplying a unique representation for each element of M. Then, we will find essential generators of M by utilizing the unique representations of its elements.

Lemma 4.2. *Every element $\alpha \in M$ can be uniquely written in the form*

$$\alpha = k + \frac{a_1}{p_1} + \frac{a_2}{p_2} + \cdots + \frac{a_r}{p_r}, \tag{4.1}$$

where $k \in \mathbb{N}_0$, $r \geq 0$ an integer, and $p_1, p_2, p_3, \ldots, p_r$ are distinct primes and $a_1, a_2, \ldots, a_r$ are integers such that $1 \leq a_i < p_i$ for all $i = 1, 2, \ldots, r$. We call equation (4.1) the ***unique representation*** *of α. (We call k the* ***integer part of*** *α and $\dfrac{a_1}{p_1} + \dfrac{a_2}{p_2} + \cdots + \dfrac{a_r}{p_r}$ the* ***fractional part of*** *α.)*

Proof. Let $\alpha \in M$. Then

$$\alpha = \frac{b_{i_1}}{p_{i_1}} + \frac{b_{i_2}}{p_{i_2}} + \frac{b_{i_3}}{p_{i_3}} + \cdots + \frac{b_{i_n}}{p_{i_n}}$$

for some distinct primes $p_{i_1}, p_{i_2}, \ldots, p_{i_r}$ and integers $b_{i_1}, b_{i_2}, \ldots, b_{i_r} \geq 1$. For all $j = 1, 2, \ldots, r$, $\dfrac{b_{i_j}}{p_{i_j}}$ can be written as

$$\frac{b_{i_j}}{p_{i_j}} = k_{i_j} + \frac{a_{i_j}}{p_{i_j}}$$

where $k_{i_j} \geq 0$ is an integer and $0 \leq a_{i_j} < p_{i_j}$. By substituting k for the sum $k_{i_1} + k_{i_2} + \cdots + k_{i_r}$ and relabeling the denominators of each fraction $\dfrac{a_{i_j}}{p_{i_j}}$, in which $a_{i_j} \geq 1$, as $p_1, p_2, \ldots, p_r$ and each respective numerator as $a_1, a_2, \ldots, a_r$, we get

$$\alpha = k + \frac{a_1}{p_1} + \frac{a_2}{p_2} + \cdots + \frac{a_r}{p_r}.$$

Next, we will show that this representation is, in fact, unique. If we suppose the contrary, then

$$\alpha = k + \frac{a_1}{p_1} + \frac{a_2}{p_2} + \cdots + \frac{a_r}{p_r} = l + \frac{b_1}{q_1} + \frac{b_2}{q_2} + \cdots + \frac{b_s}{q_s}$$

are two representations of α of the form (4.1). By combining each side into one fraction, we get

$$\frac{kp_1 \cdots p_r + a_1\widehat{p_1} \cdots p_r + \cdots + a_r p_1 \cdots \widehat{p_r}}{p_1 \cdots p_r} = \frac{lq_1 \cdots q_s + b_1\widehat{q_1} \cdots q_s + \cdots + b_s q_1 \cdots \widehat{q_s}}{q_1 \cdots q_r}$$

where each fraction is in reduced form (with regard to notation, $\widehat{p_i}$ and $\widehat{q_j}$represents the absence of the respective prime in the product from which it comes). Now, by employing the Reduced Form Lemma, we have that $\{p_1, p_2, \ldots, p_r\} = \{q_1, q_2, \ldots, q_s\}$. Thus $r = s$, and after relabeling we have

$$k + \frac{a_1}{p_1} + \frac{a_2}{p_2} + \cdots + \frac{a_r}{p_r} = l + \frac{b_1}{p_1} + \frac{b_2}{p_2} + \cdots + \frac{b_r}{p_r}.$$

Now, if for some $i \in \{1, 2, \ldots, r\}$, $a_i > b_i$, we write:

$$k + \frac{a_1}{p_1} + \cdots + \frac{a_i - b_1}{p_i} + \cdots + \frac{a_r}{p_r} = l + \frac{b_1}{p_1} + \frac{b_2}{p_2} + \cdots + \frac{b_{i-1}}{p_{i-1}} + \frac{b_{i+1}}{p_{i+1}} + \cdots + \frac{b_r}{p_r}$$

and so the left-hand side of the equation has a term with denominator p_i while the right-hand side does not, which is not possible since the left hand side and the right hand side, when each is written as one fraction in reduced form, would have different denominators of those reduced forms. Hence, for all $i = 1, 2, \ldots, r$, $a_i = b_i$, and, thus, $k = l$. Therefore, the representation of α of the form (4.1) is unique. □

Lemma 4.3. *Let $\alpha, \beta, \gamma \in M$ be such that $\alpha = \beta + \gamma$. Then the sum of the integer parts of β and γ is less than or equal to the integer part of α. In particular, the integer parts of β and γ are less than or equal to the integer part of α.*

Proof. Since α, β, and γ are elements of M, each has a unique representation:

$$\alpha = k_\alpha + \frac{a_1}{p_1} + \cdots + \frac{a_l}{p_l};$$

$$\beta = k_\beta + \frac{b_1}{q_1} + \cdots + \frac{b_m}{q_m};$$

$$\gamma = k_\gamma + \frac{c_1}{r_1} + \cdots + \frac{c_n}{r_n}.$$

Then, by substitution $\alpha = \beta + \gamma$ becomes:

$$k_\alpha + \frac{a_1}{p_1} + \cdots + \frac{a_l}{p_l} = k_\beta + \frac{b_1}{q_1} + \cdots + \frac{b_m}{q_m} + k_\gamma + \frac{c_1}{r_1} + \cdots + \frac{c_n}{r_n}.$$

If for some $i \in \{1, 2, \ldots, m\}$, there exists $j \in \{1, 2, \ldots, n\}$ such that $q_i = r_j$, we combine the fractions by writing $\dfrac{b_i + c_j}{q_i}$. We then write:

$$\frac{b_i + c_j}{q_i} = k_{ij} + \frac{d_{ij}}{q_i}$$

where $0 \leq d_{ij} < q_i$ and $k_{ij} \in \{0, 1\}$. If $d_{ij} = 0$, we omit the fraction $\dfrac{d_{ij}}{q_i}$. After writing any applicable additions and omitions and after adding each k_{ij} to $k_\beta + k_\gamma$, the right-hand side of the equation is in unique representation form. Thus, when comparing integer parts of the left-hand side and right-hand side of the equation, we get:

$$k_\alpha = k_\beta + k_\gamma + \sum k_{i_j}.$$

Hence, $k_\alpha \geq k_\beta + k_\gamma$, and, in particular, $k_\alpha \geq k_\beta$ and $k_\alpha \geq k_\gamma$. □

Lemma 4.4. *The element $\dfrac{1}{p} \in M$, p prime, cannot be written as $\dfrac{1}{p} = \alpha + \beta$ for any $\alpha, \beta \in M \setminus \{0\}$.*

Proof. Suppose to the contrary, i.e., that for some prime number p we have $\dfrac{1}{p} = \alpha + \beta$,where $\alpha, \beta \in M \setminus \{0\}$. From Lemma 4.3, we know that the integer part of both α and β is zero; thus, their unique representations have the form

$$\alpha = \frac{a_1}{p_1} + \frac{a_2}{p_2} + \cdots + \frac{a_n}{p_n},$$

$$\beta = \frac{b_1}{q_1} + \frac{b_2}{q_2} + \cdots + \frac{b_m}{q_m}.$$

Clearly, for all $i = 1, 2, \ldots, n$ and $j = 1, 2, \ldots, m$, neither p_i nor q_j can be equal to p. Otherwise, the right-hand side of the equation would be greater than the left-hand side of the equation. By substitution, the equation $\dfrac{1}{p} = \alpha + \beta$ becomes

$$\frac{1}{p} = \frac{a_1}{p_1} + \frac{a_2}{p_2} + \cdots + \frac{a_n}{p_n} + \frac{b_1}{q_1} + \frac{b_2}{q_2} + \cdots + \frac{b_m}{q_m}.$$

If $p_i = q_j$, we combine $\dfrac{a_i}{p_i} + \dfrac{b_j}{q_j}$ into $\dfrac{a_i + b_j}{p_i}$. Note that we have $a_i + b_j < p_i$, otherwise we have a contradiction. After these combinings, on the right hand side we have a sum of fractions with different prime denominators, with all of the denominators $p_1, p_2, \ldots, p_n$ appearing there. Then we add the fractions on the right hand side, using the common denominator $p_1 p_2 \cdots p_n q_{i_1} \cdots q_{i_r}$, where $q_{i_1}, \ldots, q_{i_r}$ $(r \geq 0)$ are those of the elements $q_1, \ldots, q_n$ that were not equal to any p_i. We get then

$$\frac{1}{p} = \frac{k}{p_1 p_2 \cdots p_n q_{i_1} \cdots q_{i_r}}$$

where the fractions on each side are in reduced forms, a contradiction. □

Thus, we see that each element $\frac{1}{p} \in M$, p is prime, is an essential generator of M, i.e., M is an infinitely generated monoid whose every generator is essential. Clearly, these are then precisely all the essential generators of M. This fact, together with Proposition 4.7, gives us a particularly useful lemma for describing certain irreducible elements of the monoid domain $F[X; M]$, and, hence, factorization processes of polynomials in the same.

Lemma 4.5. *The irreducible elements of $F[X; M]$ of the form X^α, $\alpha \in M$, are precisely the elements $X^{1/p}$, where p is a prime number.*

Proof. Follows from above. □

Recall how we describe a factorization process of a nonzero nonunit element of an integral domain. Let R be an integral domain and $x \in R$ a nonzero nonunit. We describe a factorization process of x. If x is irreducible, we stop. If not, we decompose it as $x = x_0 x_1$, where both x_0 and x_1 are nonzero nonunits. If both x_0, x_1 are irreducible, we stop. If not, we take the first from the left of the elements x_0, x_1 which is reducible and decompose it as a product of two nonzero nonunits. Say x_0 is reducible. We decompose it: $x_0 = x_{0,0} x_{0,1}$. Now we have $x = x_{0,0} x_{0,1} x_1$. If all of the $x_{0,0}$, $x_{0,1}$, x_1 are irreducible, we stop. If not, we take the first from the left of the elements $x_{0,0}$, $x_{0,1}$, x_1 which is reducible and decompose it as a product of two nonzero nonunits. Say $x_{0,1}$ is reducible: $x_{0,1} = x_{0,1,0} x_{0,1,1}$. Now we have $x = x_{0,0} x_{0,1,0} x_{0,1,1} x_1$, etc. We call this process a *factorization process* of x. If it stops after finitely many steps, we say that this is a *finite factorization process* of x. If it never stops, we say that this is an *infinite factorization process* of x.

Example 4.5. *If R is a subring of the domain $F[X]$, F a field, and R contains F, then R is atomic. Indeed, by the degree argument any element $f \in R$ of degree $n \geq 1$ can be decomposed into at most n irreducible factors, so every factorization process of f is finite. (The elements of F are precisely the units of R.)*

Lemma 4.6. *If the unique representation of $\alpha \in M$ is $\alpha = \dfrac{a_1}{p_1} + \cdots + \dfrac{a_n}{p_n}$, then*

$$X^\alpha = \underbrace{X^{1/p_1} \cdots X^{1/p_1}}_{a_1} \cdot \cdots \cdot \underbrace{X^{1/p_n} \cdots X^{1/p_n}}_{a_n}$$

is, up to associates, the only decomposition of X^α into irreducibles. In particular, any factorization process of X^α has a (the same) finite number of steps.

Proof. By Proposition 4.1, we know that any divisor of X^α must be of the form aX^β, where $a \in F$, $\beta \in M$, and $\alpha - \beta \in M$. Since $\alpha \in M$, it may be uniquely written in the form:

$$\alpha = \frac{a_1}{p_1} + \cdots + \frac{a_n}{p_n}.$$

Thus, every factorization process of X^α will end in finitely many steps and be factored as:

$$X^\alpha = \underbrace{X^{1/p_1} \cdots X^{1/p_1}}_{a_1} \cdot \cdots \cdot \underbrace{X^{1/p_n} \cdots X^{1/p_n}}_{a_n}.$$

□

Lemma 4.7. *For every $\alpha \in M \setminus \{0\}$, X^α has every factorization process finite.*

Proof. The proof is by induction on the integer part of α. If the integer part of α is 0, the statement follows from Lemma 4.6. Suppose that for every $\alpha \in M \setminus \{0\}$ with integer part $< k$ all factorization processes of X^α are finite. Let $\alpha = k + \dfrac{a_1}{p_1} + \cdots + \dfrac{a_r}{p_r}$ be the unique representation of α. Let $X^\alpha = X^\beta \cdot X^\gamma$ be the first step of a fixed factorization process of X^α. If the integer parts of both β, γ are $< k$, then both β, γ have all factorization processes finite by the inductive hypothesis and so the factorization process of α is finite. Suppose that one of β, γ

has the integer part equal to k and (by Lemma 4.3) the other one to 0. We will assume that the integer part of β is k (it is not a big difference if we assume that γ has the integer part k. It follows that, after relabeling,

$$\beta = k + \frac{a_1}{p_1} + \cdots + \frac{a_m}{p_m} + \frac{b_{m+1}}{p_{m+1}} + \cdots + \frac{b_n}{p_n},$$
$$\gamma = \frac{c_{m+1}}{p_{m+1}} + \cdots + \frac{c_n}{p_n} + \frac{a_{n+1}}{p_{n+1}} + \cdots + \frac{a_r}{p_r},$$

where $m \geq 0$, $n \geq 0$, $b_i + c_i = a_i$ $(i = m+1, \ldots, n)$. Since γ has at least one addend in its unique representation, the fractional part of the unique representation of β is "smaller" than the fractional part of the unique representation of α. The next step in the factorization process of X^α would be a factorization of X^β, namely $X^\beta = X^\delta \cdot X^\varepsilon$. If both δ and ε have integer part $< k$, they have finite factorization processes and since X^γ also has a finite factorization process, then the factorization process of $X^\alpha = X^\delta X^\varepsilon X^\gamma$ is finite. If δ has the integer part equal to k (similarly if ε has the integer part equal to k), then the fractional part of δ would be "smaller" than the fractional part of β. There can be only finitely many steps in which the integer part of one of the factors stays k and the fractional part is "smaller" and "smaller", so after finitely many steps the integer parts of both factors become $< k$ and we can apply the inductive hypothesis. □

Theorem 4.1. *Let* $M = \left\langle \frac{1}{2}, \frac{1}{3}, \frac{1}{5}, \ldots \right\rangle$. *Then the associated monoid domain* $F[X; M]$ *is atomic and non-AP. Moreover, no nonzero nonunit element of* $F[X; M]$ *has an infinite factorization process.*

Proof. Let $f \in F[X; M]$ be a nonzero nonunit element. For atomicity of $F[X; M]$, we must show that f has at least one finite factorization process. We will show, in fact, that f has every factorization process finite. If we suppose that f actually has some infinite factorization process, then we may assume that it has the following form:

$$f = f_0 f_1 = f_0 f_{1,0} f_{1,1} = f_0 f_{1,0} f_{1,1,0} f_{1,1,1} = \ldots,$$

after relabeling factors after each step. Denote the leading monomials of $f, f_0, f_1, f_{1,0}, f_{1,1}, \ldots$ by $X^{\alpha}, X^{\alpha_0}, X^{\alpha_1}, X^{\alpha_{1,0}}, X^{\alpha_{1,1}}, \ldots$. Then

$$X^{\alpha} = X^{\alpha_0}X^{\alpha_1} = X^{\alpha_0}X^{\alpha_{1,0}}X^{\alpha_{1,1}} = X^{\alpha_0}X^{\alpha_{1,0}}X^{\alpha_{1,1,0}}X^{\alpha_{1,1,1}} = \ldots$$

is an infinite factorization process of X^{α}, which is a contradiction by Lemma 4.6. This is impossible, because by Lemma 4.7, X^{α_n} must have every factorization process finite. $F[X;M]$ is not AP since

$$X^{1/2} \mid X^{1/2}X^{1/2} = X = X^{1/3}X^{1/3}X^{1/3}$$

, however, $X^{1/2} \nmid X^{1/3}$. ($X^{1/2}$ is irreducible by Lemma 4.5.) □

We will now investigate the atomicity and the AP property of monoid domains $F[X;M]$ associated to submonoids M of $(\mathbb{Q}_+,+)$. We will first consider the monoid domains $F[X;M]$ associated to finitely generated submonoids M of $(\mathbb{Q}_+,+)$.

4.4 The Case of Finitely Generated Submonoids of $(\mathbb{Q}_+,+)$

In this section we asume that M is a submonoid of $(\mathbb{Q}_+,+)$.

Proposition 4.9. *If $M \neq \{0\}$ is a finitely generated monoid, then M has essential generators $a_1, \ldots, a_n$ such that $M = \langle a_1, \ldots, a_n \rangle$, i.e., every finitely generated monoid can be generated by essential generators.*

Proof. Let $A = \{b_1, \ldots, b_m\}$ be a finite generating set for M and suppose that $b_1 < \cdots < b_m$. Obviously b_1 cannot be generated by $\{b_2, \ldots, b_m\}$, hence b_1 is an essential generator for M (by Proposition 4.3). Let $a_1 = b_1$. Among the elements $b_2, \ldots, b_m$ we find the first one from the left which cannot be generated by $\{a_1\}$, say b_i. That element cannot be generated by $\{a_1, b_{i+1}, \ldots, b_m\}$, hence it cannot be generated by $\{b_1, \ldots, b_{i-1}, b_{i+1}, \ldots, b_m\}$. Hence it is an essential generator of M (by

Proposition 4.3). Denote $a_2 = b_i$. Among the elements $b_{i+1}, b_{i+2}, \ldots, b_m\}$ we find the first one from the left which cannot be generated by $\{a_1, a_2\}$, say b_j. That element cannot be generated by $\{a_1, a_2, b_{j+1}, \ldots, b_m\}$, hence it cannot be generated by $\{b_1, \ldots, b_{j-1}, b_{j+1}, \ldots, b_m\}$. Hence it is an essential generator of M (by Proposition 4.3). Continuing this process we get the elements $a_1, \ldots, a_n$ such that each of them is an essential generator of M and all of the elements $b_1, \ldots, b_m$ can be generated by $\{a_1, \ldots, a_n\}$. Hence $\langle a_1, \ldots, a_n \rangle = M$. □

Theorem 4.2. *Let M be a finitely generated monoid. Then precisely one of the following situations occurs:*

(i) $M = \{0\}$*; then* $F[X; M] = F$*, a field;*

(ii) $M = \langle a \rangle$, $a \neq 0$*; then* $F[X; M] \cong F[X]$*, a Euclidean domain;*

(iii) $M = \langle a_1, \ldots, a_n \rangle$, $n \geq 2$*, all* a_i *essential generators of* M*; then* $F[X; M]$ *is an atomic non-AP domain.*

Proof. The case (i) is clear. The case (ii) follows from Proposition 4.3 and from what we have previously stated about monoid isomorphism and their associated ring homomorphisms. By Proposition 4.9, we the case (iii) is the only remaining case. It follows from Proposition 4.6 that, in this case, $F[X; M]$ is non-AP. To show that $F[X; M]$ is also atomic, we use the monoid isomorphism $\mu_\tau : M = \langle a_1, \ldots, a_n \rangle \to M' = \langle \tau a_1, \ldots, \tau a_n \rangle \subseteq (\mathbb{N}_0, +)$. Since $F[X; M]$ is a subring of $F[X]$, containing F, then by Example 4.5, it is atomic. Hence, $F[X; M]$ is atomic too (since it is isomorphic to $F[X; M']$). □

4.5 The Case of Infinitely Generated Submonoids of $(\mathbb{Q}_+, +)$

In this section we assume that M is a submonoid of $(\mathbb{Q}_+, +)$.

Proposition 4.10. *Let $M \neq \{0\}$ and suppose M cannot be generated by essential generators. Then every generating set of M contains infinitely many nonessential generators.*

Proof. Suppose to the contrary. Let A be a generating set of M having only finitely many nonessential generators, say $a_1, \dots, a_n$. We may assume that all of them are $\neq 0$ and that $a_1 < \cdots < a_n$. Then the element $\frac{a_1}{2}$ can be generated by essential generators (since each of $a_1, \dots, a_n$ is $> \frac{a_1}{2}$). Hence a_1 can be generated by essential generators and so $A \setminus \{a_1\}$ is still generating set of M. Continuing this process we get that $A \setminus \{a_1, \dots, a_n\}$ is a generating set of M, a contradiction. □

Lemma 4.8. *Let $\frac{m_1}{n_1}, \dots, \frac{m_t}{n_t} \in M$, each in reduced form, at least one of them nonzero. Then gcd$(m_1, \dots, m_t)$ and lcm$(n_1, \dots, n_t)$ are relatively prime.*

Proof. Suppose to the contrary. Then there is a prime p which divides both $\gcd(m_1, \dots, m_t)$ and $\operatorname{lcm}(n_1, \dots, n_t)$. Hence

$$(\forall m_i)\ p \mid m_i,$$

$$(\exists n_j)\ p \mid n_j.$$

Hence $\frac{m_j}{n_j}$ is not in reduced form, a contradiction. □

Lemma 4.9. *Let $\frac{m_1}{n_1}, \dots, \frac{m_t}{n_t} \in M$, each in reduced form, at least one of them nonzero. Suppose that*

$$\frac{gcd(m_1, \dots, m_t)}{lcm(n_1, \dots, n_t)} \in M.$$

Then,

$$\tau = \frac{lcm(n_1, \dots, n_t)}{gcd(m_1, \dots, m_t)}$$

is an element of $\mathbb{Q}_+$, in reduced form, such that:

$$\tau \frac{m_i}{n_i} \in \mathbb{N}_0 \text{ for all } i;$$

$$\frac{1}{\tau} \in M.$$

Proof. From the previous lemma, it follows that τ is in reduced form. The first claim is clear, because τ is in reduced form. The second claim follows directly from the assumption. □

Our next theorem, introduced in [14], is a slight generalization of a theorem by R. Daileda from [7]. The proof follows Daileda's proof.

Theorem 4.3. *Let M be a monoid such that for any elements $\frac{m_1}{n_1}, \ldots, \frac{m_t}{n_t}$ from M, all in reduced form, at least one of which is nonzero, we have*

$$\frac{gcd(m_1, \ldots, m_t)}{lcm(n_1, \ldots, n_t)} \in M.$$

Then, $F[X; M]$ is AP.

Proof. Let $f(X) = a_1X^{\alpha_1} + \cdots + a_nX^{\alpha_n}$ be an irreducible element of $F[X; M]$. We will show that f is prime. Suppose that $f(X) \mid a(X)b(X)$, where $a(X), b(X) \in F[X; M]$. Then, there exists a polynomial $h(X) \in F[X; M]$ such that $f(X)h(X) = a(X)b(X)$. Define $E(a), E(b), E(f)$, and $E(h)$ to be the sets of the exponents of a, b, f, and h, respectively, and take E to be their union. Let $E = \left\{\frac{m_1}{n_1}, \ldots, \frac{m_t}{n_t}\right\}$, where each element is written in reduced form. Since f is irreducible, at least one of the elements in E must be nonzero. Now, let $\tau = \frac{\text{lcm}(n_1, \ldots, n_t)}{\text{gcd}(m_1, \ldots, m_t)}$. In the monoid domain $F[X; \tau M]$, we have the following relation:

$$\phi_\tau(a)\phi_\tau(b) = \phi_\tau(f)\phi_\tau(h)$$

and all the polynomials in this relation belong to $F[X]$, a UFD. Hence, $\phi_\tau(f)$ divides $\phi_\tau(a)\phi_\tau(b)$ in $F[X]$. Note that $\tau M \supseteq \mathbb{N}_0$ since $\frac{1}{\tau} \in M$; hence, $F[X; \tau M] \supseteq F[X]$. Because ϕ_τ is a ring isomorphism and f is irreducible in $F[X; M]$, $\phi_\tau(f)$ is irreducible in $F[X]$, and since the notions of irreducible and prime are equivalent in UFDs, $\phi_\tau(f)$ is prime as well in $F[X]$. Therefore, either $\phi_\tau(f) \mid \phi_\tau(a)$ or $\phi_\tau(f) \mid \phi_\tau(b)$. Without the loss of generality, we may assume that the former holds. Then, there exists an element, say $a'(X)$, in $F[X] \subseteq F[X;\tau M]$ such that $\phi_\tau(f) \cdot a'(X) = \phi_\tau(a)$. If we apply the inverse isomorphism $\phi_{1/\tau} : F[X;\tau M] \to F[X;M]$ and we get $a(X) = f(X) \cdot \phi_{1/\tau}(a')$, i.e., $f(X)$ divides $a(X)$. Thus, $f(X)$ is prime, and, hence, $F[X;M]$ is AP. □

Motivated by this proof, we present the following new notion and corollaries.

Definition 4.3. *We say that a monoid M has the* ***gcd/lcm property*** *if $\frac{m_1}{n_1}, \frac{m_2}{n_2}, \ldots, \frac{m_t}{n_t} \in M$, each in reduced form and at least one of which is nonzero, implies that*

$$\frac{gcd(m_1, \ldots, m_t)}{lcm(n_1, \ldots, n_t)} \in M.$$

Equivalently, we may say that a monoid M has the gcd/lcm property if for any two elements $\frac{m_1}{n_1}, \frac{m_2}{n_2} \in M$, both in reduced form and at least one is not zero,

$$\frac{gcd(m_1, m_2)}{lcm(n_1, n_2)} \in M.$$

We will prove this equivalence in Chapter 6.

Corollary 4.1 (Daileda, [9]). *$F[X;\mathbb{Q}_+]$ is a nonatomic AP domain.*

Proof. $F[X;\mathbb{Q}_+]$ is an AP domain by the previous theorem. It is nonatomic by Proposition 13. □

Corollary 4.2. *Let $M = \left\langle \frac{1}{2}, \frac{1}{2^2}, \frac{1}{2^3}, \ldots \right\rangle$. Then $F[X;M]$ is a nonatomic AP domain.*

Proof. $F[X;M]$ is an AP domain by the previous theorem. It is nonatomic by Proposition 4.6. □

Taking into account Corollaries 4.1 and 4.2, one may wonder if for any M without essential generators, $F[X;M]$ is AP. To answer this question, we considered monoids of a different sort. A relatively simple example of this sort is the monoid

$M = \left\langle \frac{1}{2}, \frac{1}{2^2}, \ldots; \frac{1}{5}, \frac{1}{5^2}, \ldots \right\rangle$. To see that M has no essential generators, one need only consider two elements of M: $\frac{1}{2^k}$ and $\frac{1}{5^l}$ where $k, l \geq 1$. We then see the following:

$$\frac{1}{2^k} = \frac{1}{2^{k+1}} + \frac{1}{2^{k+1}}$$

and

$$\frac{1}{5^l} = \frac{1}{5^{l+1}} + \frac{1}{5^{l+1}} + \frac{1}{5^{l+1}} + \frac{1}{5^{l+1}} + \frac{1}{5^{l+1}};$$

hence, neither $\frac{1}{2^k}$ nor $\frac{1}{5^l}$ is an essential generator for any positive integers k, l. Moreover, the gcd/lcm condition for it does not hold. Indeed, for $\frac{1}{2}, \frac{1}{5} \in M$, it is easy to show that $\frac{\gcd(1,1)}{\operatorname{lcm}(2,5)} = \frac{1}{10} \notin M$. So we cannot use Theorem 4.3 to prove that $F[X; M]$ is AP. One can wonder if it is then non-AP. We will prove later (Chapter 5, Proposition 5.2) that it indeed is.

Proposition 4.11. *For the submonoid $M = \left\langle \frac{1}{2}, \frac{1}{2^2}, \ldots; \frac{1}{5}, \frac{1}{5^2}, \ldots \right\rangle$ of $(\mathbb{Q}_+, +)$, the monoid domain $F[X; M]$ is a nonatomic non-AP domain.*

Proof. To show that $F[X; M]$ is non-AP, we need to provide an irreducible element of $F[X; M]$ that is not prime. The difficult part lies in finding an appropriate atom, however, one such atom is the binomial $X^{27/50} - 1$ (in Chapter 5, Proposition 5.2, we will prove that it is indeed irreducible). We now show that $X^{27/50} - 1$ is not prime.

First note that $(X^{27/50} - 1) \mid (X^{27/25} - 1)$, and $X^{27/25} - 1$ can be factored in the following way: $X^{27/25} - 1 {=} (X^{9/25} - 1)(X^{18/25} + X^{9/25} + 1)$. Hence, $X^{27/50} - 1$ divides the product $(X^{9/25} - 1)(X^{18/25} + X^{9/25} + 1)$. Now, since $\frac{9}{25} < \frac{27}{50}$, it is clear that $(X^{27/50} - 1) \nmid (X^{9/25} - 1)$. Next, to show that $(X^{27/50} - 1) \nmid (X^{18/25} + X^{9/25} + 1)$, we need only show that $\frac{9}{50} = \frac{18}{25} - \frac{27}{50}$ is not an element of M. Suppose to the contrary. Then $\frac{9}{50}$ may be uniquely written in the following way:

$$\frac{9}{50} = \frac{5^l m + 2^k n}{2^k 5^l}$$

where $m, n \geq 1$ are integers and the right hand side is in reduced form. Thus, $k = 1$ and $l = 2$, and, hence, $9 = 25m + 2n$, an impossibility. Thus, we have shown that the binomial $X^{27/50} - 1$ is indeed nonprime. Therefore, $F[X; M]$ is non-AP.

That $F[X; M]$ is nonatomic follows from Proposition 4.8. □

Theorem 4.4. *If M is an infinitely generated monoid, then precisely one of the following situations occurs:*

(i) M has no essential generators; then $F[X; M]$ is non-atomic; it can be AP and non-AP;

(ii) M has at least one essential generator but cannot be generated by essential generators; then $F[X; M]$ is non-atomic and non-AP;

(iii) M can be generated by essential generators; then $F[X; M]$ is non-AP; it can be atomic, but we do not know if it can be non-atomic.

Proof. (i) That $F[X; M]$ is nonatomic frollows from Proposition 4.8. Corollaries 4.1 and 4.2 are examples where $F[X; M]$ is AP and Proposition 4.11 gives an example where $F[X; M]$ is non-AP.

(ii) $F[X; M]$ is non-atomic by Proposition 4.8 and non-AP by Proposition 4.6. An example of a monoid of this type is

$$M = \left\langle \frac{1}{2}, \frac{1}{2^2}, \frac{1}{2^3}, \ldots ; \frac{1}{5} \right\rangle .$$

(iii) $F[X; M]$ is non-AP by Proposition 4.6. It can be atomic (by example from Section 4.2). □

CHAPTER 5
THE IRREDUCIBILITY OF $X^{\pi} - 1$ IN $F[X; M]$

5.1 Introduction and preliminaries for Chapter 5

In the previous chapter we conclusively showed that there is no relation between the notions AP and atomic. That is, we provided examples of domains which are atomic and AP, atomic and non-AP, non-atomic and AP, and, non-atomic and non-AP. Of course, it is well known that integral domains that are both atomic and AP are Unique Factorization Domains. To this end, we made significant use of *essential generators* of additive monoids, and we considered the question: if M has no essential generators, is the associated monoid domain $F[X; M]$ necessarily AP? We answered this question in the negative, by considering the monoid domain $F[X; M]$ with $M = \left\langle \frac{1}{2}, \frac{1}{2^2}, \frac{1}{2^3}, \ldots ; \frac{1}{5}, \frac{1}{5^2}, \frac{1}{5^3}, \ldots \right\rangle$ and providing an irreducible element of $F[X; M]$, namely $X^{27/50} - 1$, which is not prime. In the following pages, we will justify that $X^{27/50} - 1$ is indeed an atom of $F[X; M]$ and we will introduce a theorem which provides sufficient conditions for when the binomial $X^{\pi} - 1$ is irreducible in $F[X; M]$, but first we will provide necessary definitions and results.

We say that a monoid M is *cancellative*, and that it satisifes the *cancellative property*, if for any elements $\alpha, \beta, \gamma \in M$, $\alpha + \gamma = \beta + \gamma$ implies $\alpha = \beta$. Moreover, if M satisfies the condition that for any integer $n \geq 1$ and any elements $\alpha, \beta \in M$, $n\alpha = n\beta$ implies that $\alpha = \beta$, then M is said to be *torsion-free.* It's not difficult to show that if M is a torsion-free monoid, then it also satisfies the following weaker property: for any integer $n \geq 1$ and every $\alpha \in M$, $n\alpha = 0$ implies $\alpha = 0$. For groups, these properties are equivalent and the latter is the way how the notion of a torsion-free group is usually defined. Next, we will turn our attention to several notions in number theory which proved to be invaluable in the proof of our theorem.

Let F be a field, $k \in \mathbb{N}$, and $X_1, X_2, \ldots, X_k$ be variables over F. Then, the *elementary symmetric polynomials* in these variables are the polynomials from $F[X_1, X_2, \ldots, X_k]$ defined by the following:

$$\sigma_1 = \sum_{1 \leq i \leq k} X_i;$$

$$\sigma_2 = \sum_{1 \leq i < j \leq k} X_i X_j;$$

$$\vdots$$

$$\sigma_k = X_1 \cdots X_k;$$

and $\sigma_e = 0$ for all $e > k$. The *power sums* in the variables $X_1, X_2, \ldots, X_k$ are the polynomials from $F[X_1, X_2, \ldots, X_k]$ defined by the following:

$$\pi_e = \sum_{1 \leq i \leq k} X_i^e$$

for all $e \geq 1$. The following is a theorem presented in [1, page A.IV.70] giving the relations (called, the *Newton's relations*) between the elementary symmetric polynomials and the power sums in the variables $X_1, X_2, \ldots, X_k$ in the ring $F[X_1, X_2, \ldots, X_k]$.

THEOREM 5.1 (Newton's Relations). *For every integer $e \in \{1, 2, \ldots, k\}$, we have*

$$\pi_e = \sigma_1 \pi_{e-1} - \sigma_2 \pi_{e-2} + \cdots + (-1)^e \sigma_{e-1} \pi_1 + (-1)^{e+1} e \sigma_e.$$

Now, notice, if we replace the variables $X_1, X_2, \ldots, X_k$ with elements $x_1, x_2, \ldots, x_k$ of F, respectively, we obtain Newton's relations between the elementary symmetric polynomials and the power sums of the elements $x_1, x_2, \ldots, x_k$.

The next theorem, called *Lucas' Theorem*, was proven by É. Lucas in 1878. A simpler proof was given by N. J. Fine in [11].

Theorem 5.2 (Lucas' Theorem)**.** *Let p be a prime number and let*

$$M = M_t p^t + M_{t-1} p^{t-1} + \cdots + M_2 p^2 + M_1 p + M_0,$$
$$N = N_t p^t + N_{t-1} p^{t-1} + \cdots + N_2 p^2 + N_1 p + N_0$$

be the expansions of the nonnegative integers M and N in base p (so that $M_i, N_i \in \{0, 1, \ldots, p-1\}$). Then

$$\binom{M}{N} \equiv \binom{M_t}{N_t}\binom{M_{t-1}}{N_{t-1}} \cdots \binom{M_2}{N_2}\binom{M_1}{N_1}\binom{M_0}{N_0} \pmod{p},$$

where we assume that $\binom{M_i}{N_i} = 0$ if $M_i < N_i$.

The final preliminary result that we will present was given by T. Y. Lam and K. H. Leung in 2000 in [16], and it is worth noting that the result was previously an open problem in number theory. We call their theorem *Lam-Leung Theorem*. First, recall that for any integer $n \geq 1$, we say that z is an *n-th root of unity in R* if $z^n = 1$. Now, let n be a natural number with the prime-power factorization $n = p_1^{v_1} p_2^{v_2} \cdots p_r^{v_r}$, and consider the n-th roots of unity in the field of numbers, denoted $\mathbb{C}$. The *Lam-Leung Theorem* describes all natural numbers t such that there are t n-th roots of unity in $\mathbb{C}$ whose sum is 0.

Theorem 5.3 (Lam-Leung Theorem)**.** *The set of all numbers t such that there are t n-th roots of unity in $\mathbb{C}$ whose sum is 0 is equal to $\mathbb{N}_0 p_1 + \mathbb{N}_0 p_2 + \cdots + \mathbb{N}_0 p_r$.*

Along with these definitions and results, in the next section we will introduce the notion of *elements of height* $(0, 0, 0, \ldots)$ *in torsion-free monoids.*

5.2 Elements of Height $(0, 0, 0, \ldots)$ in Torsion-Free Monoids

For a torsion-free group G, the following notions are well-known. Let p be a prime number; then, the $p-$ *height*, $h_p(a)$, of an element $a \in G$ is defined in [4, p. 108] as the nonnegative integer r such that $a \in p^r G \setminus p^{r+1} G$ if such an integer exists and is defined as ∞ otherwise. The *height sequence of* a is the sequence $(h_2(a), h_3(a), h_5(a), \ldots)$ of p-heights of a as p increases through the prime numbers. Of particular interest in this chapter are elements of height $(0, 0, 0, \ldots)$; we will, more generally, consider such elements in torsion-free monoids instead of groups.

Definition 5.1. *We say that an element a of a torsion-free monoid Γ is of **height** $(0, 0, 0, \ldots)$ if for every prime number p the equation $a = px$ is unsolvable in Γ.*

Example 5.1. *(1) There are no elements of height $(0, 0, 0, \ldots)$ in the torsion-free monoids $\{0\}$, $(\mathbb{Q}_+, +)$, or $(\mathbb{R}_+, +)$.*
(2) The only element of height $(0, 0, 0, \ldots)$ in $(\mathbb{N}_0, +)$ is 1.
(3) The elements of height $(0, 0, 0, \ldots)$ in the monoid $\langle 2, 3\rangle = \mathbb{N}_0 \setminus \{1\}$ are precisely the prime numbers $2, 3, 5, \ldots$.
(4) In the monoid $\langle 2, 5\rangle = \{0, 2, 4, 5, 6, \ldots\}$ the elements of height $(0, 0, 0, \ldots)$ are the prime numbers 2,5,7,11,... and the composite number 9. In fact, it can be easily shown that for any submonoid M of $(\mathbb{N}_0, +)$ and any prime number $p \notin M$, the composite number p^2 is of height $(0, 0, 0, \ldots)$ in M if it is an element of M.
(5) In the submonoid $\left\langle \frac{1}{2}, \frac{1}{2^2}, \frac{1}{2^3}, \ldots; \frac{1}{5} \right\rangle$ of $(\mathbb{Q}_+, +)$, the only element of height $(0, 0, 0, \ldots)$ is $\frac{1}{5}$.
(6) There are infinitely many elements of height $(0, 0, 0, \ldots)$ in the submonoid $\left\langle \frac{1}{2}, \frac{1}{2^2}, \frac{1}{2^3}, \ldots; \frac{1}{5}, \frac{1}{5^2}, \frac{1}{5^3}, \ldots \right\rangle$ of $(\mathbb{Q}_+, +)$. To show this, consider the element $\frac{5^j + 2}{2 \cdot 5^j} = \frac{1}{2} + \frac{1}{5^j} \in M$, in reduced form and where $j \geq 1$. Supposing that this element is not of height $(0, 0, 0, \ldots)$, there is an element, say $\frac{m \cdot 5^l + n \cdot 2^k}{2^k \cdot 5^l}$ where $k, l, m, n \geq 1$

and in reduced form, of M such that for some prime number p,

$$\frac{5^j+2}{2\cdot 5^j} = p\cdot\frac{m\cdot 5^l + n\cdot 2^k}{2^k\cdot 5^l}.$$

We have three cases: 1) Let $p = 2$; then $k = 2$ and $l = j$, and, thus, we have that $5^j + 2 = m \cdot 5^j + n \cdot 2^2$, an impossibility; 2) Let $p = 5$; then $k = 1$ and $l = j + 1$, and, thus, we have that $5^{l-1} + 2 = m \cdot 5^l + n \cdot 2$, an impossibility; finally, 3) Let $p \neq 2, 5$; then $k = 1$ and $l = j$, and, thus, we have that $5^l + 2 = p(m \cdot 5^l + n \cdot 2)$, an impossibility.

Proposition 5.1. *Let $\mu : \Gamma \to \Gamma'$ be an isomorphism between two torsion-free monoids. For any $a \in \Gamma$, a is of height $(0, 0, 0, \dots)$ in Γ if and only if $\mu(a)$ is of height $(0, 0, 0, \dots)$ in Γ'.*

Proof. It is sufficient to prove the forward direction; that is, if $a \in \Gamma$ is of height $(0, 0, 0, \dots)$ in Γ, then $\mu(a)$ is of height $(0, 0, 0, \dots)$ in Γ'. Suppose not; then for some prime number p the equation $\mu(a) = px$ is solvable in Γ'. If we now apply μ^{-1} we get: $a = p \cdot \mu^{-1}(x)$, a contradiction. □

5.3 Matsuda's lemma and Matsuda's monoids

The next theorem is Lemma 2.2 in the paper [18] by R. Matsuda (we call it Matsuda's Lemma). For the sake of completeness we also include Matsuda's proof.

Theorem 5.4 (Matsuda's Lemma)**.** *Let F be a field, $G \neq 0$ a torsion-free group, and π an element of G of height $(0, 0, 0, \dots)$. Then $X^\pi - 1$ is an irreducible element of $F[G; X]$.*

Proof. Suppose $X^\pi - 1 = gh$, where $g, h \in F[G; X]$. Let H be the subgroup generated by π and the power exponents appearing in g and h. By [15, Lemma 2.1], $\mathbb{Z}\pi$ is a direct summand of H. Let $H = \mathbb{Z}\pi \oplus \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_n$, $X^\pi = Y$, and

$X^{e_i} = X_i$. The set $Y, X_1, \dots, X_n$ is algebraically independent over F. Hence $Y-1$ is irreducible in $F_{\mathbb{Z}}[Y, X_1, \dots, X_n]$. Here, $F_{\mathbb{Z}}[Y, X_1, \dots, X_n]$ denotes the quotient ring of $F[Y, X_1, \dots, X_n]$ by the multiplicative system generated by $Y, X_1, \dots, X_n$. □

Inspired by Matsuda's Lemma, we introduce the following notions relating elements of height $(0, 0, 0, \dots)$ in cancellative torsion-free monoids and their associated monoid domains.

Definition 5.2. *We call a cancellative torsion-free monoid Γ a **Matsuda's monoid** if for every element $\pi \in \Gamma$ of height $(0, 0, 0, \dots)$ the binomial $X^{\pi} - 1$ is irreducible in the associated monoid domain $F[X; \Gamma]$ for every field F.*

Definition 5.3. *We call a cancellative torsion-free monoid Γ a **Matsuda's monoid of type 0** (respectively, **p**) if for every element $\pi \in \Gamma$ of height $(0, 0, 0, \dots)$ the binomial $X^{\pi} - 1$ is irreducible in the associated monoid domain $F[X; \Gamma]$ for every field F of characteristic 0 (respectively, p).*

When a monoid Γ is, in fact, a group, we say a *Matsuda group*, a *Matsuda group of type 0*, and a *Matsuda group of type p*.

Below, we provide examples of various Matsuda monoids.

Example 5.2. *(1) Every torsion-free group G is a Matsuda group by Matsuda's Lemma.*

(2) The monoids $\{0\}$, $(\mathbb{Q}_+, +)$, and $(\mathbb{R}_+, +)$ have no elements of height $(0, 0, 0, \dots)$, and so they are Matsuda monoids.

(3) In the monoid $M = (\mathbb{N}_0, +)$, 1 is the only element of height $(0, 0, 0, \dots)$, and, since, $X^1 - 1$ is irreducible in $F[X; M]$ for every field F, M is a Matsuda monoid.

(4) In the monoid $M = \langle 2, 3 \rangle$, as we have shown already, the elements of height $(0, 0, 0, \dots)$ are precisely the prime numbers. We may see that M is not a Matsuda monoid of type 2 since $7 \in M$ is of height $(0, 0, 0, \dots)$ and in $\mathbb{F}_2[X; M]$, we have

the following factorization:

$$X^7 - 1 = (X^4 + X^3 + X^2 - 1)(X^3 + X^2 + 1).$$

Moreover, it happens that M is not a Matsuda monoid of type 3 since $11 \in M$ *is of height* $(0, 0, 0, \dots)$ *and in* $\mathbb{F}_3[X; M]$*, we have the following factorization:*

$$X^{11} - 1 = (X^6 - X^5 + 2X^4 - X^3 + X^2 - 1)(X^5 + X^4 + 2X^3 + X^2 + 2).$$

The last example, in particular, begs the question: is the monoid $M = \langle 2, 3 \rangle$ a Matsuda monoid of any finite type? We do not yet know the answer to this question. However, as a result of our Theorem 5.5, which is the first theorem in the next section, we may assert that M is a Matsuda monoid of type 0.

5.4 Submonoids of $(\mathbb{Q}_+, +)$ are Matsuda's monoids of type 0.

Theorem 5.5. *Every submonoid of* $(Q_+, +)$ *is a Matsuda monoid of type 0.*

Proof. We begin by proving the statement for the submonoids of $(\mathbb{N}_0, +)$ and then we extend that proof to submonoids of the nonnegative rationals.

By Example 5.2 (3), we know that $\mathbb{N}_0$ is a Matsuda monoid. Let us assume, then, that M is a proper submonoid of $(N_0, +)$, i.e. $1 \notin M$. Let $n \in M$ be of type $(0, 0, 0, \dots)$ with a prime factorization $n = p_1^{v_1} p_2^{v_2} \cdots p_r^{v_r}$. It is enough to show that $X^n - 1$ cannot be factored into a product of two polynomials of degree ≥ 1 in $F[X; M]$ for any algebraically closed field F of characteristic 0. So let F be an algebraically closed field of characteristic 0. We may assume that F contains the field $\mathbf{A}$ of algebraic numbers. Suppose to the contrary, that is, that the binomial $X^n - 1$ can be factored $F[X; M]$ as $g(X)h(X)$, where g and h are two monic polynomials of degree $k \geq 1$ and $l \geq 1$, respectively. Without the loss of generality, we will assume that $k \geq l$. In $F[X]$, the binomial $X^n - 1$ can be factored as a product of n monic linear polynomials $X - \zeta$, where ζ is an n-th root of unity (in $\mathbf{A}$). Therefore, we have $g(X) = (X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_k)$, where $\alpha_1, \alpha_2, \ldots, \alpha_k$ are n-th roots of unity (in $\mathbf{A}$). Now, let $\beta_i = \alpha_i^{-1}$ for $i = 1, 2, \ldots, k$, and note that β_i is an n-th root of unity (in $\mathbf{A}$) as well. Let us also write $g(X)$ as

$$g(X) = X^k + g_{k-1}X^{k-1} + \cdots + g_1 X + g_0,$$

where $g_0, g_1, \ldots, g_{k-1}$ are elements in F.

Claim 1: Let e be an element of $\mathbb{N}_0$ such that $e < k$ and $e \notin M$. Then

$$\sigma_e(\beta_1, \ldots, \beta_k) = 0,$$
$$\pi_e(\beta_1, \ldots, \beta_k) = 0.$$

Proof of Claim 1: Since $e \notin M$, the coefficient g_e by X^e in $g(X)$ is equal to 0. Thus

$$\sum \alpha_{i_1}\alpha_{i_2} \cdots \alpha_{i_{k-e}} = 0,$$

where the sum goes over all $(k-e)$-element subsets $\{i_1, \ldots, i_{k-e}\}$ of $\{1, 2, \ldots, k\}$. Hence,

$$\sum \beta_{j_1}\beta_{j_2} \cdots \beta_{j_e} = 0,$$

where the sum goes over all e-element subsets $\{j_1, \ldots, j_e\}$ of $\{1, 2, \ldots, k\}$. Therefore,

$$\sigma_e(\beta_1, \ldots, \beta_k) = 0.$$

Now, to prove the second relation, we use induction on e. For $e = 1$ we have

$$\pi_1(\beta_1, \ldots, \beta_k) = \sigma_1(\beta_1, \ldots, \beta_k) = 0.$$

Suppose that

$$\pi_f(\beta_1, \ldots, \beta_k) = 0$$

for all elements $f \in \mathbb{N}_0$ such that $f < e$ and $f \notin M$. We, then, have the Newton's relations

$$\pi_e = \sigma_1\pi_{e-1} - \sigma_2\pi_{e-2} + \cdots + (-1)^e\sigma_{e-1}\pi_1 + (-1)^{e+1}e\sigma_e, \tag{5.1}$$

where each of σ_i, π_i is a function of $\beta_1, \dots, \beta_k$. Since $e \notin M$, $\sigma_e = 0$ by the first relation. Also, in each of the sets $\{1, e-1\}, \{2, e-2\}, \dots, \{\left\lfloor \frac{e}{2} \right\rfloor, \left\lfloor \frac{e+1}{2} \right\rfloor\}$ at least one of the elements is not in M, otherwise their sum, which is e, would be in M. If in any of these sets $\{j, e-j\}$ say $j \notin M$, then $\sigma_j = 0$ by the first relation of this claim and $\pi_j = 0$ by the inductive hypothesis. Hence, $\sigma_j \pi_{e-j} = 0$ and $\sigma_{e-j}\pi_j = 0$, and, hence, all the addends on the right hand side of (5.1) are 0, i.e., $\pi_e(\beta_1, \dots, \beta_k) = 0$. Claim 1 is proved.

Claim 2: Let $d < n$ be a divisor of n. Let e be an element of $\mathbb{N}_0$ such that $ed \le k$ and $ed \notin M$. Then

$$\pi_e(\beta_1^d, \dots, \beta_k^d) = 0,$$
$$\sigma_e(\beta_1^d, \dots, \beta_k^d) = 0.$$

Proof of Claim 2: We have

$$\pi_e(\beta_1^d, \dots, \beta_k^d) = \pi_1(\beta_1^d, \dots, \beta_k^d) = 0$$

by Claim 1 as $ed \notin M$. We prove the second relation by induction on e. For $e = 1$ we have

$$\sigma_1(\beta_1^d, \dots, \beta_k^d) = \pi_d(\beta_1, \dots, \beta_k) = 0$$

by Claim 1 as $d \notin M$. Let e be an element of $\mathbb{N}_0$ such that $ed \le k$ and $ed \notin M$. Suppose that

$$\sigma_f(\beta_1^d, \dots, \beta_k^d) = 0$$

for all elements $f \in \mathbb{N}_0$ such that $f < e$ and $fd \notin M$. We have the Newton's relation

$$\sigma_e = \frac{(-1)^{e+1}}{e}[\pi_e - \sigma_1\pi_{e-1} + \sigma_2\pi_{e-2} - \cdots + (-1)^{e-1}\sigma_{e-1}\pi_1], \tag{5.2}$$

where each of σ_i, π_i is a function of $\beta_1^d, \dots, \beta_k^d$. Since $ed \notin M$, $\pi_e = 0$ by the first relation. Consider any of the sets $\{1, e-1\}, \{2, e-2\}, \dots, \{\left\lfloor \frac{e}{2} \right\rfloor, \left\lfloor \frac{e+1}{2} \right\rfloor\}$, say $\{j, e-j\}$. At least one of the elements jd, $(e-j)d$ is not in M, otherwise their sum, which is ed, would be in M. If say $jd \notin M$, then $\pi_j = 0$ by the first relation of this claim and $\sigma_j = 0$ by the inductive hypothesis. Hence, $\sigma_j \pi_{e-j} = 0$ and $\sigma_{e-j}\pi_j = 0$. Hence, all the addends on the right hand side of (5.2) are 0 and so $\sigma_e(\beta_1^d, \ldots, \beta_k^d) = 0$. Claim 2 is proved.

Let now $j \in \{1, 2, \ldots, r\}$. For $e = p_1^{v_1} \cdots \widehat{p_j^{v_j}} \cdots p_r^{v_r}$, by Claim 1,

$$\pi_e(\beta_1, \ldots, \beta_k) = \beta_1^e + \cdots + \beta_k^e = 0,$$

i.e.,

$$\sigma_1(\beta_1^e, \ldots, \beta_k^e) = 0.$$

Each of the elements $\beta_1^e, \ldots, \beta_k^e$ is a $p_j^{v_j}$-th root of unity, hence, by Lam-Leung Theorem,

$$k \in \mathbb{N}_0 p_j.$$

We will prove by induction on s that $k \in \mathbb{N}_0 p_j^s$ for every $s = 1, 2, \ldots, v_j$. For $s = 1$ we have already done that. Suppose that $k \in \mathbb{N}_0 p_j^{s-1}$ for some $s \in \{1, 2, \ldots, v_j\}$. We want to show that then $k \in \mathbb{N}_0 p_j^s$. Suppose to the contrary, i.e., that $k \notin \mathbb{N}_0 p_j^s$. Then k can be written as

$$k = k_t p_j^t + k_{t-1} p_j^{t-1} + \cdots + k_s p_j^s + k_{s-1} p_j^{s-1},$$

where t is some number, $k_t, k_{t-1}, \ldots, k_s, k_{s-1}$ are from $\{0, 1, \ldots, p-1\}$, and $k_{s-1} \neq 0$. Let $d = p_1^{v_1} \cdots \widehat{p_j^{v_j}} \cdots p_r^{v_r}$ and $e = p_j^{s-1}$. Then by Claim 2,

$$\sigma_e(\beta_1^d, \ldots, \beta_k^d) = 0.$$

Since each β_j^d is a $p_j^{v_j}$-th root of unity, the last equation is a vanishing sum of $\binom{k}{e} = \binom{k}{p_j^{s-1}}$ $p_j^{v_j}$-th roots of unity, hence, by Lam-Leung Theorem,

$$\binom{k}{p_j^{s-1}} \in \mathbb{N}_0 p_j.$$

However, by Lucas' Theorem,

$$\binom{k}{p_j^{s-1}} \equiv \binom{k_{s-1}}{1} = k_{s-1} \neq 0 \pmod{p_j},$$

a contradiction. Thus, $k \in \mathbb{N}_0 p_j^s$, and since this holds for any $s \leq v_j$, we have

$$k \in \mathbb{N}_0 p_j^{v_j}.$$

This holds for all $j = 1, 2, \ldots, r$; hence,

$$k \equiv 0 \pmod{n},$$

which is a contradiction with our starting hypothesis that $X^n - 1$ can be factored into two nonconstant polynomials, one of which is of degree k. Hence, $X^n - 1$ is an irreducible element of $\overline{F}[X; M]$ and, in particular, of $F[X; M]$. The statement is proved for submonoids of $(\mathbb{N}_0, +)$.

Now, let M be a submonoid of $(\mathbb{Q}_+, +)$. Let π be an element of M of height $(0, 0, 0, \ldots)$. Suppose to the contrary, i.e., that $X^\pi - 1 = g(X)h(X)$, where g and h are two elements of $\overline{F}[X; M]$ of degree $\neq 0$. Let N be the submonoid of M generated by π and the exponents of the polynomials of g and h. N is, therefore, a finitely generated submonoid of M in which π is also of height $(0, 0, 0, \ldots)$ and the factorization $X^\pi - 1 = g(X)h(X)$ is in $\overline{F}[X; N]$. Let d be the least common denominator of all the generators of N. Then $\mu_d : N \to dN$ is a monoid isomorphism betweeen N and the submonoid dN of $(\mathbb{N}_0, +)$. By Proposition 5.1, the element $d\pi$ is of height $(0, 0, 0, \ldots)$ in dN. The associated ring isomorphism $\phi_d : \overline{F}[X; N] \to \overline{F}[X; dN]$ transports the factorization $X^\pi - 1 = g(X)h(X)$ from $\overline{F}[X; N]$ into the factorization $X^{d\pi} - 1 = \phi_d(g)\phi_d(h)$ in $\overline{F}[X; dN]$, with both polynomials $\phi_d(g), \phi_d(h)$ nonconstant. We already proved that this is not possible for submonoids of $(\mathbb{N}_0, +)$, so we arrived at a contradiction, and the theorem is proved. □

5.5 An application: a submonoid M of $(\mathbb{Q}_+, +)$ without essential generators, such that $F[X;M]$ is not AP

In concluding this chapter, we will provide the reader with a useful application of our main theorem. Recall that in the previous chapter, we offered as an example of a nonatomic, non-AP domain the monoid domain $F[X;M]$ where $M = \left\langle \frac{1}{2}, \frac{1}{2^2}, \frac{1}{2^3}, \ldots; \frac{1}{5}, \frac{1}{5^2}, \frac{1}{5^3}, \ldots \right\rangle$. We proved that the element $X^{27/50} - 1$ is not prime in $F[X;M]$, however, we did not justify that it is an atom. We will now provide such a proof by applying our result.

Proposition 5.2. *Let $M = \left\langle \frac{1}{2}, \frac{1}{2^2}, \frac{1}{2^3}, \ldots; \frac{1}{5}, \frac{1}{5^2}, \frac{1}{5^3}, \ldots \right\rangle$ and let F be a field of characteristic 0. Then, the monoid domain $F[X;M]$ is not AP.*

Proof. We have shown in Example 5.1 (6) that the elements $\frac{1}{2} + \frac{1}{5^j}$ $(j \geq 1)$ are of height $(0, 0, 0, \ldots)$, so $\frac{1}{2} + \frac{1}{5^2}$ is of height $(0, 0, 0, \ldots)$ in M.

Hence, by Theorem 5.5, we have that the binomial $X^{27/50} - 1$ is irreducible in the domain $F[X;M]$. In Chapter 4, we showed that this same binomial is not prime; therefore, $F[X;M]$ is non-AP. □

CHAPTER 6
RELATIONS BETWEEN GCD/LCM PROPERTY OF M, AP PROPERTY OF $F[X;M]$, AND ELEMENTS OF HEIGHT $(0,0,0,\dots)$ IN M

In this chapter we always assume that M is a submonoid of $(\mathbb{Q}_+,+)$.

6.1 Preliminary discussion of the relations.

In this final chapter of analysis, we will devote our energies to the following properties of the monoid M and its associated domain $F[X;M]$:

(1) M has the gcd/lcm property;

(2) $F[X;M]$ is AP;

(3) M has no elements of height $(0,0,0,\dots)$;

and we will determine any relations that may exists between them.

For the case of M being finitely generated, we have the following cases: (1) $M=\{0\}$, (2) $M=\langle a\rangle$, $a\neq 0$, and (3) $M=\langle a_1,a_2,\dots,a_k\rangle$, $k\geq 2$, all a_i essential generators (by our discussion of monoid isomorphisms, Proposition 4.5, and Proposition 5.1 we may assume that M is a numerical semigroup).

1. In the first case, M satisfies the gcd/lcm property, M has no elements of height $(0,0,0,\dots)$, and $F[X;M]=F$ is AP.

2. In the next case, M satisfies the gcd/lcm property, M has exactly one element of height $(0,0,0,\dots)$, namely a, and $F[X;M]\cong F[X]$ is AP.

3. In the final case, M does not satisfy the gcd/lcm property, M has elements of height $(0,0,0,\dots)$, namely $a_1, a_2, \dots, a_k$ (and others), and $F[X;M]$ is non-AP.

For the case of M being infinitely generated, we have only two cases: (1) M has at least one essential generator and (2) M does not have any essential generators.

1. In the former case, $F[X;M]$ is non-AP, hence, M does not satisfy the gcd/lcm property (by Theorem 4.3), and M has elements of height $(0,0,0,\dots)$, e.g., every essential generator.

2. In the latter case, $F[X;M]$ can be AP and non-AP; M does not have to satisfy the gcd/lcm property (e.g., whenever $F[X;M]$ is non-AP), but it can (e.g., $M = \mathbb{Q}_+$ or $M = \left\langle \frac{1}{2}, \frac{1}{2^2}, \frac{1}{2^3}, \dots \right\rangle$). Thus, all options are possible in this second case.

We consider the diagram following only in the case where M is infinitely generated and without essential generators (note: $F[X;M]$ is non-atomic).

$$\begin{tikzcd}
& \text{M has the gcd/lcm property} \arrow[dl, Rightarrow] \arrow[dr, Rightarrow] & \\
\text{$F[X;M]$ has the AP property} & & \text{M has no elements of height $(0,0,0,\dots)$}
\end{tikzcd}$$

Figure 6.1: Relations of the properties: M has the gcd/lcm property, $F[X;M]$ is AP, and M has no elements of height $(0,0,0,\dots)$.

6.2 Some structural properties of submonoids of $(\mathbb{Q}_+, +)$

That M has the gcd/lcm property implies that $F[X; M]$ is AP follows from Theorem 4.3. To show that M has the gcd/lcm property implies that M has no elements of height $(0, 0, 0, \dots)$, we will prove that $F[X; M]$ is AP implies that M has no elements of height $(0, 0, 0, \dots)$. We begin by investigating some structural properties of M.

Proposition 6.1. *Let M and M' be submonoids of $(\mathbb{Q}_+, +)$ and let $\mu : M \to M'$ be a monoid isomorphism. Then $\mu = \mu_\tau$ where $\tau \in \mathbb{Q}_+ \setminus \{0\}$.*

Proof. If $M = \{0\}$, the satement is clearly true. Suppose $M \neq \{0\}$. Let $M = \langle A \rangle$ and let $\frac{a_1}{b_1} \neq 0$ and $\frac{a_2}{b_2}$ be two elements of A. Let

$$\mu\left(\frac{a_1}{b_1}\right) = \frac{c_1}{d_1}$$

and

$$\mu\left(\frac{a_2}{b_2}\right) = \frac{c_2}{d_2}.$$

Let $\tau = \frac{c_1 b_1}{d_1 a_1}$. Then

$$\frac{c_1}{d_1} = \tau \cdot \frac{a_1}{b_1}.$$

We have that

$$b_1 a_2 \cdot \frac{a_1}{b_1} = b_2 a_1 \cdot \frac{a_2}{b_2}.$$

Hence,

$$\mu\left(b_1 a_2 \cdot \frac{a_1}{b_1}\right) = \mu\left(b_2 a_1 \cdot \frac{a_2}{b_2}\right),$$

hence,

$$b_1 a_2 \cdot \mu\left(\frac{a_1}{b_1}\right) = b_2 a_1 \cdot \mu\left(\frac{a_2}{b_2}\right),$$

hence,

$$b_1 a_2 \cdot \frac{c_1}{d_1} = b_2 a_1 \cdot \frac{c_2}{d_2},$$

hence,

$$b_1a_2 \cdot \tau \cdot \frac{a_1}{b_1} = b_2a_1 \cdot \frac{c_2}{d_2},$$

and, thus,

$$\frac{c_2}{d_2} = \tau \cdot \frac{a_2}{b_2}.$$

Therefore, once we fix the unique rational number $\tau > 0$ such that $\mu\left(\frac{a_1}{b_1}\right) = \mu_\tau\left(\frac{a_1}{b_1}\right)$, then for any $\frac{a_2}{b_2} \in A$ we have

$$\mu\left(\frac{a_2}{b_2}\right) = \mu_\tau\left(\frac{a_2}{b_2}\right).$$

Hence, $\mu|_A = \mu_\tau|_A$. Now, for any $k_1a_1 + \cdots + k_ta_t \in M$ ($k_i \in \mathbb{N}$, $a_i \in A$) we have

$$\begin{aligned}
\mu(k_1a_1 + \cdots + k_ta_t) &= k_1\mu(a_1) + \cdots + k_t\mu(a_t) \\
&= k_1\mu_\tau(a_1) + \cdots + k_t\mu_\tau(a_t) \\
&= \tau(k_1a_1 + \cdots + k_ta_t) \\
&= \mu_\tau(k_1a_1 + \cdots + k_ta_t).
\end{aligned}$$

Thus, $\mu \equiv \mu_\tau$. □

Definition 6.1. *Let R be a commutative ring, $a_1, a_2, \ldots, a_n \in R$. An element $d \in R$ is called a* ***greatest common divisor*** *of $a_1, a_2, \ldots, a_n$, and denoted gcd$(a_1, a_2, \ldots, a_n)$ if the following hold:*

(i) $d \mid a_1$, $d \mid a_2$, $\ldots$, $d \mid a_n$;

(ii) if $c \mid a_1, c \mid a_2, \ldots, a \mid a_n$, then $c \mid d$.

Lemma 6.1. *Let R be a PID, $a_1, a_2, \ldots, a_n \in R$. Then $d =$ gcd$(a_1, a_2, \ldots, a_n)$ if and only if $(a_1, a_2, \ldots, a_n) = (d)$.*

Proof. Burton, A First Course in Rings and Ideals, Theorem 6-3. □

Lemma 6.2. *Let R be a PID, $n \geq 2$, $a_1, a_2, \ldots, a_n \in R$. Then gcd$(a_1, a_2, \ldots, a_n) =$ gcd(gcd$(a_1, a_2, \ldots, a_{n-1}), a_n)$.*

Proof. Using Lemma 6.1, we have the following:

$$\begin{aligned} d = \gcd(\gcd(a_1, a_2, \ldots, a_{n-1}), a_n) &\iff (d) = (\gcd(a_1, a_2, \ldots, a_{n-1}), a_n) \\ &\iff (d) = (\gcd(a_1, a_2, \ldots, a_{n-1})) + (a_n) \\ &\iff (d) = (a_1, a_2, \ldots, a_{n-1}) + (a_n) \\ &\iff (d) = (a_1, a_2, \ldots, a_n) \\ &\iff d = \gcd(a_1, a_2, \ldots, a_n). \end{aligned}$$

□

Definition 6.2. *Let R be a commutative ring, $a_1, a_2, \ldots, a_n \in R$. An element $m \in R$ is called a* ***least common multiple*** *of $a_1, a_2, \ldots, a_n$, and denoted by lcm$(a_1, a_2, \ldots, a_n)$ if the following hold:*

(i) $a_1 \mid m, a_2 \mid m, \ldots, a_n \mid m$;

(ii) *if* $a_1 \mid m', a_2 \mid m', \ldots, a_n \mid m'$, *then* $m \mid m'$.

Lemma 6.3. *Let R be a PID, $a_1, a_2, \ldots, a_n \in R$. Then $d =$ lcm$(a_1, a_2, \ldots, a_n)$ if and only if $(m) = (a_1) \cap (a_2) \cap \cdots \cap (a_n)$.*

Proof. Burton, A First Course in Rings and Ideals, Theorem 6-5. □

Lemma 6.4. *Let R be a PID, $n \geq 2$, $a_1, a_2, \ldots, a_n \in R$. Then lcm$(a_1, a_2, \ldots, a_n) =$ lcm(lcm$(a_1, a_2, \ldots, a_{n-1}), a_n)$.*

Proof. Using Lemma 6.3, we have the following:

$$\begin{aligned} m = \operatorname{lcm}(\operatorname{lcm}(a_1, a_2, \ldots, a_{n-1}), a_n) &\iff (m) = (\operatorname{lcm}(a_1, a_2, \ldots, a_{n-1})) \cap (a_n) \\ &\iff (m) = (a_1) \cap (a_2) \cap \cdots \cap (a_{n-1}) \cap (a_n). \end{aligned}$$

□

PROPOSITION 6.2. *The following are equivalent about any monoid $M \subseteq (\mathbb{Q}_+, +)$:*

(i) for any $t \geq 2$, $\frac{a_1}{b_1}, \ldots, \frac{a_t}{b_t} \in M$ in reduced form, at least one $\neq 0$,

$$\frac{gcd(a_1, \ldots, a_t)}{lcm(b_1, \ldots, b_t)} \in M;$$

(ii) for any $\frac{a_1}{b_1}, \frac{a_2}{b_2} \in M$ in reduced form, at least one $\neq 0$

$$\frac{gcd(a_1, a_2)}{lcm(b_1, b_2)} \in M.$$

Proof. Clearly, (i) $\Longrightarrow$ (ii).

Suppose (ii) holds and let $\frac{a_1}{b_1}, \ldots, \frac{a_t}{b_t} \in M$ where $t \geq 2$ is an integer. We have:

$$\frac{\gcd(a_1, \ldots, a_t)}{\operatorname{lcm}(b_1, \ldots, b_t)} = \frac{\gcd(\gcd(a_1, \ldots, a_{t-1}), a_t)}{\operatorname{lcm}(\operatorname{lcm}(b_1, \ldots, b_{t-1}), b_t)}$$

by Lemma 6.2 and 6.4. Now, by Lemma 4.8, $\frac{\gcd(a_1, \ldots, a_{t-1})}{\operatorname{lcm}(b_1, \ldots, b_{t-1})}$ is in reduced form. Hence, by (ii), $\frac{\gcd(\gcd(a_1, \ldots, a_{t-1}), a_t)}{\operatorname{lcm}(\operatorname{lcm}(b_1, \ldots, b_{t-1}), b_t)} \in M$, i.e., $\frac{\gcd(a_1, \ldots, a_t)}{\operatorname{lcm}(b_1, \ldots, b_t)} \in M$. □

DEFINITION 6.3. *We say that a mnoid M satisfies the* ***gcd/lcm property*** *if the equivalent conditions from Proposition 6.2 hold.*

THEOREM 6.1. *If M and M' are two isomorphic submonoids of $(\mathbb{Q}_+, +)$, then M has the gcd/lcm property if and only if M' has the same property.*

Proof. Let $\mu : M \to M'$ be a monoid isomorphism. From Proposition 6.1, we know that μ may be written as μ_τ where $\tau \in \mathbb{Q}_+ \setminus \{0\}$. Let $\tau = \frac{r}{s}$, in reduced form, and let $\frac{p_1}{q_1}, \frac{p_2}{q_2} \in M'$, in reduced form and at least one not zero. Note that $\frac{p_1}{q_1}$ and $\frac{p_2}{q_2}$ are images of elements from M, say $\frac{m_1}{n_1}$ and $\frac{m_2}{n_2}$, respectively, in reduced form, i.e.,

$$\mu_{r/s}\left(\frac{m_1}{n_1}\right) = \frac{p_1}{q_1}$$

and

$$\mu_{r/s}\left(\frac{m_2}{n_2}\right) = \frac{p_2}{q_2}.$$

In fact, one may note that $\frac{p_1}{q_1}$ and $\frac{p_2}{q_2}$ are reduced forms of $\frac{r}{s}\frac{m_1}{n_1}$ and $\frac{r}{s}\frac{m_2}{n_2}$ respectively. Thus, in order to prove our statement, we need to consider what these reduced forms look like. To this end, we will write $r = r'r_1r_2r_{1,2}$ where $r_{1,2}$ is the greatest factor that can be cancelled with factors in both n_1 and n_2, r_1 is the greatest factor from the remaining part that can be cancelled with factors from n_1, r_2 is the greatest remaining factor from the remaining part that can be cancelled with factors in n_2, and r' is the remaining factor after cancellation. We will also write $s = s's_1s_2s_{1,2}$, defined similarly, with respect to m_1 and m_2. Now, with respect to appropriate cancellations, we may define m_1, m_2, n_1, and n_2 in the following way:

$$m_1 = s_1s_{1,2}m_1'$$

$$m_2 = s_2s_{1,2}m_2'$$

$$n_1 = r_1r_{1,2}n_1'$$

$$n_2 = r_2r_{1,2}n_2'.$$

With these, we can see that $\gcd(s_1, s_2) = 1$, $\gcd(r', n_1) = 1$, $\gcd(s', m_1) = 1$, $\gcd(r_1, r_2) = 1$, $\gcd(r', n_2) = 1$, and $\gcd(s', m_2) = 1$. Therefe, we may write $\gcd(m_1, m_2)$ and $\operatorname{lcm}(n_1, n_2)$ in the following way:

$$\gcd(m_1, m_2) = s_{1,2} \cdot \gcd(s_1m_1', s_2m_2') = s_{1,2} \cdot \gcd(m_1', m_2'), \tag{6.1}$$

$$\operatorname{lcm}(n_1, n_2) = r_{1,2} \cdot \operatorname{lcm}(r_1n_1', r_2n_2') = r_{1,2}r_1r_2 \cdot \operatorname{lcm}(n_1', n_2'). \tag{6.2}$$

We may also write

$$\frac{r}{s}\frac{m_1}{n_1} = \frac{r'r_1r_2r_{1,2}}{s's_1s_2s_{1,2}} \cdot \frac{s_1s_{1,2}m_1'}{r_1r_{1,2}n_1'} = \frac{r'r_2m_1'}{s's_2n_1'},$$

in reduced form, and

$$\frac{r}{s}\frac{m_2}{n_2} = \frac{r'r_1r_2r_{1,2}}{s's_1s_2s_{1,2}} \cdot \frac{s_2s_{1,2}m_2'}{r_2r_{1,2}n_2'} = \frac{r'r_1m_2'}{s's_1n_2'},$$

also in reduced form. Thus, $p_1 = r'r_2m_1'$, $q_1 = s's_2n_1'$, $p_2 = r'r_1m_2'$, and $q_2 = s's_1n_2'$, and, hence,

$$\gcd(p_1, p_2) = r'\gcd(m_1', m_2') \tag{6.3}$$

and

$$\operatorname{lcm}(q_1, q_2) = s' s_1 s_2 \operatorname{lcm}(n_1', n_2'). \tag{6.4}$$

Now, since M satisfies the gcd/lcm property, from 6.1 that

$$\frac{s_{1,2}\gcd(m_1', m_2')}{r_{1,2} r_1 r_2 \operatorname{lcm}(n_1', n_2')} = \frac{\gcd(m_1, m_2)}{\operatorname{lcm}(n_1, n_2)} \in M.$$

Finally, from equations 6.3 and 6.4 we need to show that M' satisfies the gcd/lcm property, i.e., that

$$\frac{r'\gcd(m_1', m_2')}{s' s_1 s_2 \operatorname{lcm}(n_1', n_2')} \in M'.$$

Indeed, we have

$$\frac{r'\gcd(m_1', m_2')}{s' s_1 s_2 \operatorname{lcm}(n_1', n_2')} = \frac{r' r_1 r_2 r_{1,2}}{s' s_1 s_2 s_{1,2}} \cdot \frac{s_{1,2}\gcd(m_1', m_2')}{r_{1,2} r_1 r_2 \operatorname{lcm}(n_1', n_2')} = \frac{r}{s} \cdot \frac{\gcd(m_1, m_2)}{\operatorname{lcm}(n_1, n_2)} \in M'.$$

The other direction follows since $\mu^{-1} = \mu_{1/\tau} : M' \to M$ is also a monoid isomorphism. □

6.3 The case when M is infinitely generated and without essential generators

Theorem 6.2. *Let M be an infinitely generated submonoid of $(\mathbb{Q}_+, +)$ without essential generators. If $F[X; M]$, where F is of characteristic 0, is AP, then M has no elements of height $(0, 0, 0, \dots)$.*

Proof. Our proof will be by contrapositive, i.e., we will assume that M has an element of height $(0, 0, 0, \dots)$ and show that $F[X; M]$ is non-AP.

Let π be an element of M of height $(0, 0, 0, \dots)$. Since, by our hypothesis, π is not an essential generator, $\pi = \pi_1 + \pi_2$ for some elements $\pi_1 = \dfrac{m_1}{n_1}$ and $\pi_2 = \dfrac{m_2}{n_2}$ (both in reduced form) of the monoid. We will sow that the element $X^\pi - 1$ of $F[X; M]$ is irreducible, but not prime. Under the monoid isomorphism $\tau_{n_1 n_2} : M \to M' = n_1 n_2 M$, the element π is mapped to the element $\pi' = n_1 n_2 \pi = m_1 n_2 + n_1 m_2$.

The monoid M' is infinitely generated, without essential generators and π' is an element of M' of height $(0,0,0,\dots)$ which is a sum of two nonzero elements of M', namely $m_1n_2 + n_1m_2$. Moreover, $X^\pi - 1$ is irreducible and non-prime in $F[X;M]$ if and only if $X^{\pi'} - 1$ is irreducible and non prime in $F[X;M']$.

So it is enough to prove that if the monoid M in the statement of our theorem contains an elements π of height $(0,0,0,\dots)$ such that $\pi = m_1 + m_2$, where m_1, m_2 are relatively prime elements of $\mathbb{N}$, then $X^\pi - 1$ is irreducible but not prime. Note that $m_1 \neq 1$, $m_2 \neq 1$; otherwise π is not of height $(0,0,0,\dots)$. So m_1 has at least one prime factor, say p.

Under the monoid ismorphism $\tau_{1/m_2p} : M \to M' = \dfrac{1}{m_2p}M$, the element $\pi = m_1 + m_2$ is mapped to the element

$$\pi' = \frac{1}{m_2p}\pi = \frac{m_1'}{m_2} + \frac{1}{p},$$

where $m_1' = \dfrac{m_1}{p}$. The monoid M' is infinitely generated, without essential generators, and π' is an element of M' of height $(0,0,0,\dots)$ which is a sum of two nonzero elements of M', namely $\dfrac{m_1'}{m_2}$ and $\dfrac{1}{p}$ (both in reduced form). Moreover, $X^\pi - 1$ is irreducible and non-prime in $F[X;M]$ if and only if $X^{\pi'} - 1$ is irreducible and non-prime in $F[X;M']$.

So it is enough to prove that if the monoid M in the statement of our theorem contains an element π of height $(0,0,0,\dots)$ such that $\pi = \dfrac{m}{n} + \dfrac{1}{p}$, where $\gcd(m,n) = 1$, $\gcd(n,p)$, $n \neq 1$, then $X^\pi - 1$ is irreducible and non-prime.

So let's assume that we have this situation. Then, by Theorem 5.5, $X^\pi - 1$ is irreducible. We will show that it is not prime.

We have $\pi = \dfrac{mp+n}{pn}$. Hence, $X^\pi - 1 = (X^{\frac{mp+n}{pn}} - 1) \mid (X^{\frac{mp+n}{p}} - 1)$. We have, also:

$$\begin{aligned} X^{\frac{mp+n}{p}} - 1 &= (X^{\frac{1}{p}})^{mp+n} - 1 \\ &= (X^{\frac{1}{p}} - 1)(X^{\frac{mp+n-1}{p}} + X^{\frac{mp+n-2}{p}} + \cdots + X^{\frac{1}{p}} + 1). \end{aligned}$$

Since $\dfrac{1}{p} < \pi$, we have $X^{\pi} - 1 \nmid (X^{\frac{1}{p}} - 1)$.

Suppose that

$$(X^{\pi} - 1) \mid (X^{\frac{mp+n-1}{p}} + X^{\frac{mp+n-2}{p}} + \cdots + X^{\frac{1}{p}} + 1). \tag{6.5}$$

Then,

$$\begin{aligned} &X^{\frac{mp+n-1}{p}} + X^{\frac{mp+n-2}{p}} + \cdots + X^{\frac{1}{p}} + 1 \\ &= (X^{\frac{mp+n}{pn}} - 1)(X^{\alpha_1} + g_2 X^{\alpha_2} + \cdots + g_{k-1} X^{\alpha_{k-1}} - 1), \end{aligned} \tag{6.6}$$

where $\alpha_1 > \alpha_2 > \cdots > \alpha_{k-1} > 0$ and $g_2, g_3, \ldots g_{k-1}$ are coefficients.

It follows that

$$\alpha_1 = \frac{(mp+n)(n-1) - n}{pn}.$$

Note that $\alpha_1 \neq \dfrac{mp+n-i}{p}$ for all $i = 2, 3, \ldots, mp+n-1$, since, otherwise, we would get $(i-2)n = mp$, which is not possible since $\gcd(m,n) = 1$ and $\gcd(p,n) = 1$, one can calculate that $\alpha_1 < \dfrac{mp+n-2}{p}$.

Hence, the exponent $\dfrac{mp+n-2}{p}$ on the LHS of 6.6 has to be obtained from

$$X^{\frac{mp+n}{pn}} \cdot (X^{\alpha_1} + g_2 X^{\alpha_2} + \cdots + g_{k-1} X^{\alpha_{k-1}} - 1),$$

since it cannot be obtained from

$$(-1) \cdot (X^{\alpha_1} + g_2 X^{\alpha_2} + \cdots + g_{k-1} X^{\alpha_{k-1}} - 1)$$

(these two are parts of the LHS). But then it has to be either

$$\frac{mp+n}{pn} + \alpha_2 = \frac{mp+n-2}{p}, \tag{6.7}$$

or, if

$$\frac{mp+n}{pn} + \alpha_i = \frac{mp+n-2}{p}, \quad \text{for some } i \geq 3, \tag{6.8}$$

then the terms with the exponents $\dfrac{mp+n}{pn}+\alpha_2, \ldots, \dfrac{mp+n}{pn}+\alpha_{i-1}$ would have to be cancelled on the RHS, so that we would have

$$\begin{aligned}\frac{mp+n}{pn}+\alpha_2 &= \alpha_1,\\ \frac{mp+n}{pn}+\alpha_3 &= \alpha_2,\\ &\vdots\\ \frac{mp+n}{pn}+\alpha_{i-1} &= \alpha_{i-2}.\end{aligned}$$

Hence,

$$\begin{aligned}\alpha_2 &= \frac{(mp+n)(n-2)-n}{pn},\\ \alpha_2 &= \frac{(mp+n)(n-3)-n}{pn},\\ &\vdots\\ \alpha_{i-1} &= \frac{(mp+n)(n-i+1)-n}{pn},\end{aligned}$$

and from equation 6.8

$$\alpha_{i-1} = \frac{(mp+n)(n-i+1)-n}{pn} > \frac{(mp+n)(n-1)-2n}{pn} = \alpha_i,$$

which gives

$$n > (mp+n)(i-2), \quad i \geq 3,$$

which is not true. Hence, equation 6.7 holds. This gives

$$\alpha_2 = \frac{(mp+n)(n-1)-2n}{pn}. \tag{6.9}$$

Note that $\alpha_2 \neq \dfrac{mp+n-i}{p}$ for all $i = 3, 4, \ldots, mp+n-1$, since otherwise we would get $(i-3)n = mp$, which is not possible since $\gcd(m,n) = 1$ and $\gcd(p,n) = 1$. Also, note that

$$\alpha_2 < \frac{mp+n-3}{p}.$$

Hence, the exponent $\dfrac{mp+n-3}{p}$ on the LHS of equation 6.6 has to be obtained from

$$X^{\frac{mp+n}{pn}}(X^{\alpha_1}+g_2X^{\alpha_2}+\cdots+g_{k-1}X^{\alpha_{k-1}}-1)$$

(we noticed before that it cannot be equal to α_1). Reasoning in the same way as before we conclude that

$$\alpha_3=\frac{(mp+n)(n-1)-3n}{pn}, \tag{6.10}$$

and by induction we get

$$\alpha_i=\frac{(mp+n)(n-1)-in}{pn}, \tag{6.11}$$

for $i=2,3,\dots,r$, where r is the largest integer for which

$$\frac{mp+n}{pn}<\frac{mp+n-r}{p}. \tag{6.12}$$

From 6.12 we get

$$r<mp+n-1-\frac{mp}{n}.$$

Hence,

$$r\le mp+n-2.$$

However, then

$$\frac{mp+n-r}{p}\ge\frac{2}{p}, \tag{6.13}$$

so that all of the exponents $\dfrac{mp+n-i}{p}$ from the LHS are obtained as $\dfrac{mp+n}{pn}+\alpha_i$. As before, $\alpha_r=\dfrac{(mp+n)(n-1)-rn}{pn}$ cannot be equal to any $\dfrac{mp+n-i}{p}$, $i=r+1,r+2,\dots,mp+n-1$, otherwise we would get $n(i-r-1)=mp$, which is not possible as $\gcd(m,n)=1$ and $\gcd(p,n)=1$. Now note that

$$\alpha_r<\frac{mp+n-(r+1)}{p}. \tag{6.14}$$

It follows that the exponent $\dfrac{mp+n-(r+1)}{p}$ from the LHS cannot be obtained from

$$X^{\frac{mp+n}{pn}}(X^{\alpha_1}+g_2X^{\alpha_2}+\cdots+g_{k-1}X^{\alpha_{k-1}}-1)$$

since r was the largest integer for which 6.12 holds, nor from

$$(-1)(X^{\alpha_1}+g_2X^{\alpha_2}+\cdots+g_{k-1}X^{\alpha_{k-1}}-1)$$

since 6.14 holds and no α_i with $i<r$ can be equal to any $\dfrac{mp+n-i}{p}$, $i=r+1,r+2,\ldots,mp+n-1$. We got a contradiction, hence 6.6 does not hold, i.e., 6.5 does not hold. So $X^{\pi}-1$ is not prime. $\square$

Remark 6.1. *We had before that for any monoid $M\subseteq(\mathbb{Q}_+,+)$, if M has the gcd/lcm property, then $F[X;M]$ is AP. Therefore, for the case of infinitely generated monoid without essential generators, we have the following diagram:*

Figure 6.2: Relations of the properties: M has the gcd/lcm property, $F[X;M]$ is AP, and M has no elements of height $(0,0,0,\ldots)$.

$$\begin{tikzcd}
 & \begin{array}{c}M \text{ has the}\\ \text{gcd/lcm property}\end{array} \arrow[dl, Rightarrow] & \\
\begin{array}{c}F[X;M] \text{ has the}\\ \text{AP property}\end{array} \arrow[rr, Rightarrow] & & \begin{array}{c}M \text{ has no elements}\\ \text{of height } (0,0,0,\ldots)\end{array}
\end{tikzcd}$$

Note that if we only want to prove the implication "M has the gcd/lcm property" $\Longrightarrow$ "M has no elements of height $(0, 0, 0, \dots)$", we can do that in a simpler way, as follows.

PROPOSITION 6.3. *Let M be a nonmonogenerated monoid with the gcd/lcm property. Then M has no elements of height* $(0, 0, 0, \dots)$.

Proof. Suppose to the contrary, that is, that there is an element $\frac{m_1}{n_2} \in M$, in reduced form, of height $(0, 0, 0, \dots)$. Because M is not monogerated, there exists a second element, say $\frac{m_2}{n_2} \in M$, in reduced form, such that $\frac{m_2}{n_2} \notin \left\langle \frac{m_1}{n_1} \right\rangle$. Now, utilizing our assumption that M has the gcd/lcm property, we know that $\frac{\gcd(m_1, m_2)}{\operatorname{lcm}(n_1, n_2)}$ is a member of the monoid. Hence, there are positive integers x, y such that $m_1 = \gcd(m_1, m_2) \cdot x$ and $n_1 \cdot y = \operatorname{lcm}(n_1, n_2)$, and, therefore, we have that

$$\frac{m_1}{n_1} = \frac{\gcd(m_1, m_2) \cdot x}{\operatorname{lcm}(n_1, n_2)/y} = xy \cdot \frac{\gcd(m_1, m_2)}{\operatorname{lcm}(n_1, n_2)}$$

where $xy \geq 1$. If $xy = 1$, then $x = y = 1$. Hence, $m_1 \mid m_2$ and $n_2 \mid n_1$. Supposing $n_2 \cdot k = n_1$ and $m_1 \cdot l = m_2$, we get that $\frac{m_2}{n_2} = lk \cdot \frac{m_1}{n_1}$, a contradiction since $\frac{m_2}{n_2} \notin \left\langle \frac{m_1}{n_1} \right\rangle$. If $xy \neq 1$ we simply factor out a prime factor and we are finished. Thus, $\frac{m_1}{n_1}$ cannot be an element of height $(0, 0, 0, \dots)$. □

CHAPTER 7
REMARKS AND CONCLUSION

One of the main topics that we investigated are the properties of the monoid domain $F[X;M]$, where F is a field and M is a submonoid of $(\mathbb{Q}_+,+)$. We were particularly interested in the notions of atomicity and AP-ness of the domain $F[X;M]$ and we obtained several results relating these properties of $F[X;M]$ with the properties of the monoid M. For example, in Chapter 6 we proved that

$$F[X;M]\ AP \implies M \text{ has no elements of height } (0,0,0,\dots)$$

and that

$$M \text{ has the gcd/lcm property} \implies F[X;M] \text{ AP.}$$

Our main question, then, became the following: what is the precise property $P(M)$ of the monoids $M \subseteq (\mathbb{Q}_+,+)$ such that

$$P(M) \iff F[X;M] \text{ AP?}$$

From previous chapters, we have that

$$\text{gcd/lcm property} \implies P(M) \implies \text{no elements of height } (0,0,0,\dots).$$

However, more recent results show that these implications are, in fact, equivalences. Indeed, by considering other properties of the monoid $M \subseteq (\mathbb{Q}_+,+)$, we have the following results.

Theorem 7.1. *Let M be a submonoid of $(\mathbb{Q}_+,+)$ and F a field. The following are equivalent:*

(a) M is a ***Prüfer monoid*** *(i.e., a union of an increasing sequence of cyclic monoids);*

(b) M is a ***half-group monoid*** *(i.e., $M = G \cap \mathbb{Q}_+$, where G is a subgroup of $\mathbb{Q}$);*

(c) M is ***difference-closed****, (i.e., if $a, b \in M$ and $a \leq b$, then $b - a \in M$);*

(d) $M = Diff(M) \cap \mathbb{Q}_+$;

(e) M satisfies the gcd/lcm condition;

(f) $M \cong \mathbb{N}_0$ or M has no elements of height $(0, 0, 0, \dots)$;

(g) M is integrally closed.

Theorem 7.2. *Let M be a submonoid of $(\mathbb{Q}_+, +)$ and F a field.*

(i) The conditions (a)-(g) from Theorem 7.1 are equivalent and each of them implies that $F[X; M]$ is an AP-domain.

(ii) If F is of characteristic 0, then each of the conditions from Theorem 7.1 is equivalent with $F[X; M]$ being an AP-domain.

From the literature, when considering the monoid domains $F[X; M]$ where $M \subseteq (\mathbb{Q}_+, +)$, the following domains are equivalent: Euclidean domains, principal ideal domains, unique factorization domains, and Dedekind domains. Moreover, in the same context, Bézout domains, Prüfer domains, integrally closed domains, GCD domains, Schreier domains, and Pre-Schreier domains are also all equivalent. With our new results we have shown that AP-domains are equivalent to the latter. Moreover, we found that those domains which satisfy the PC condition are equivalent to the latter domains, as well. We display our findings in the figures following.

Figure 7.1: Implications Between Some Types of Domains

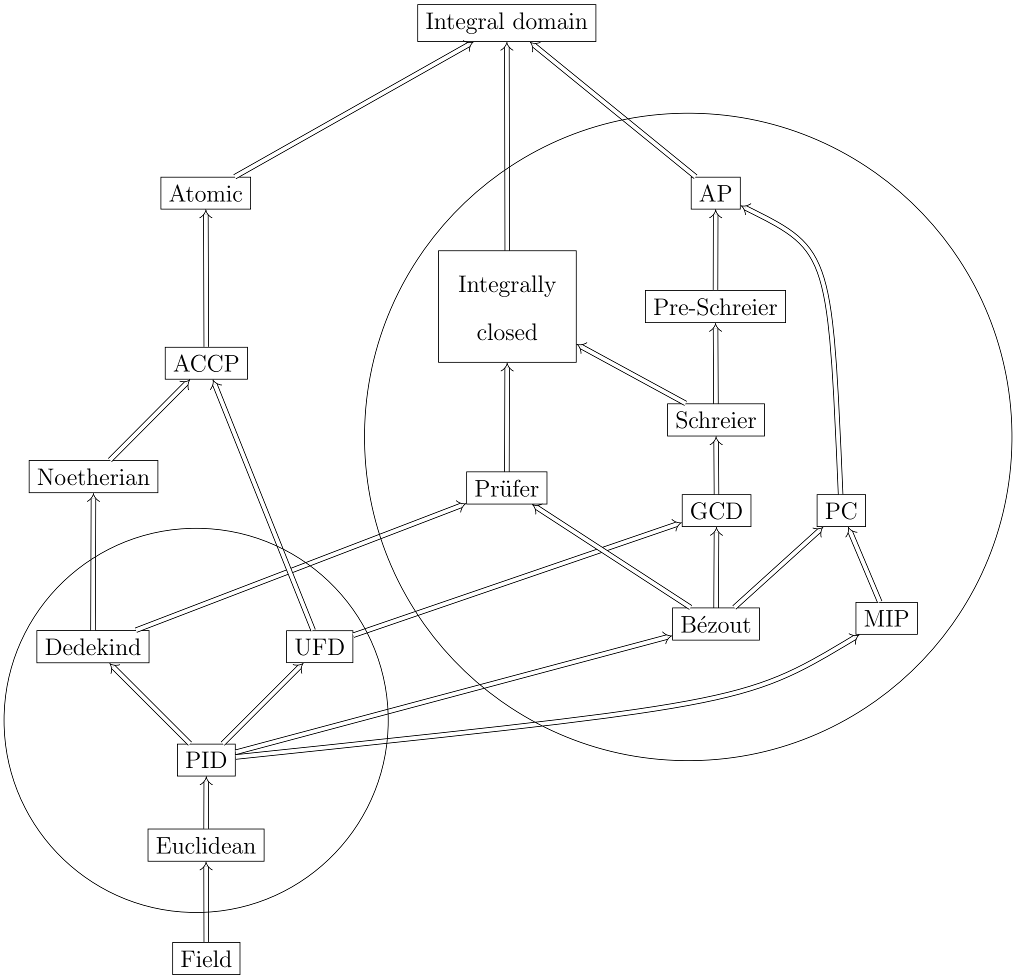
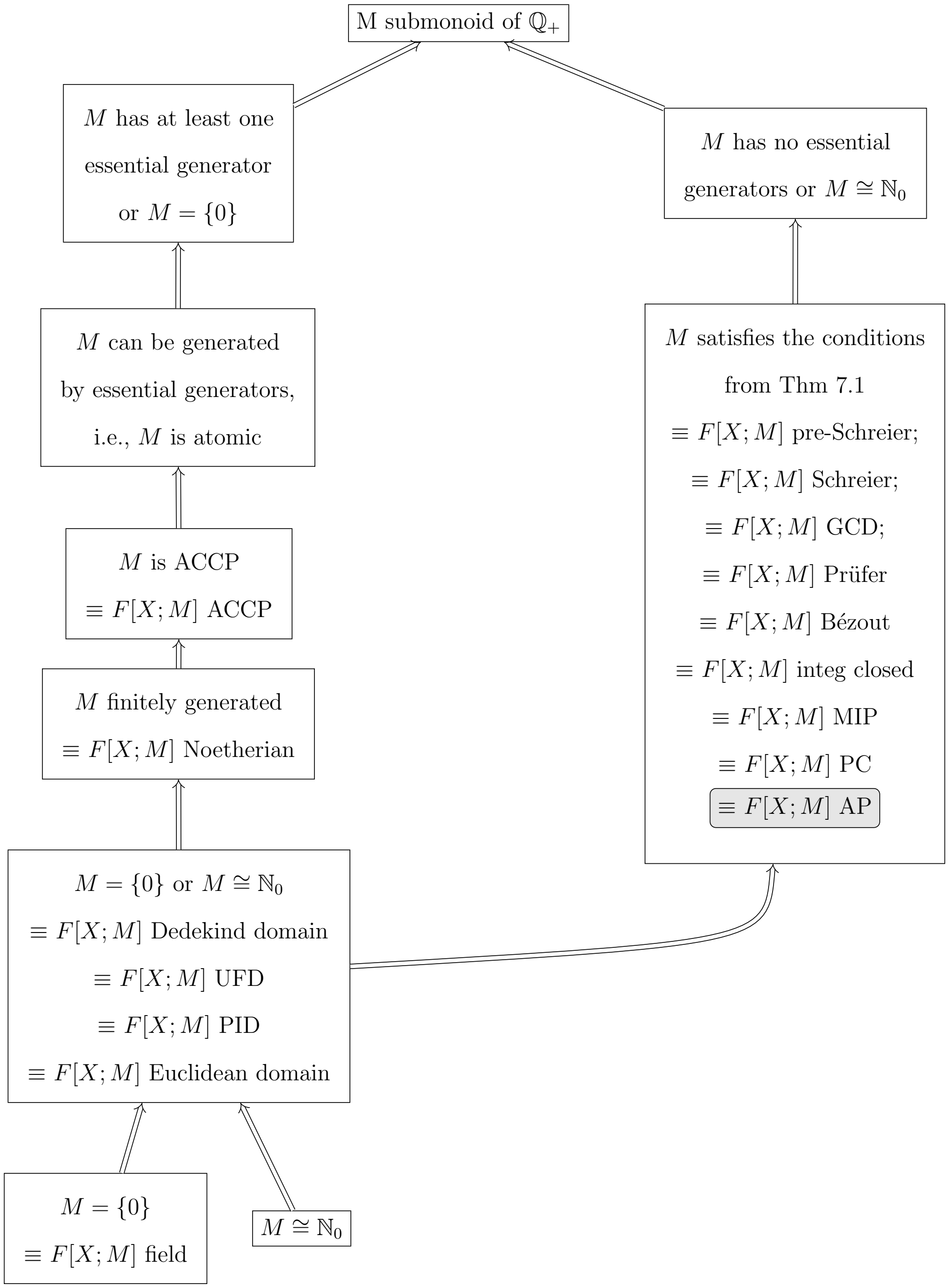


Diagram 1: Implications between some types of integral domains

The properties contained within their respective circles are equvialent in $F[X; M]$ where $M \subseteq (\mathbb{Q}_+, +)$. Related to this implication diagram, the next figure shows relations for various properties of the submonoids of nonnegative rational numbers.

Figure 7.2: Implications Between Some Types of Submonoids $M \subseteq (\mathbb{Q}_+, +)$


M submonoid of $\mathbb{Q}_+$
M has at least one essential generator or $M = \{0\}$
M has no essential generators or $M \cong \mathbb{N}_0$
M can be generated by essential generators, i.e., M is atomic
M satisfies the conditions from Thm 7.1
$\equiv F[X;M]$ pre-Schreier;
$\equiv F[X;M]$ Schreier;
$\equiv F[X;M]$ GCD;
$\equiv F[X;M]$ Prüfer
$\equiv F[X;M]$ Bézout
$\equiv F[X;M]$ integ closed
$\equiv F[X;M]$ MIP
$\equiv F[X;M]$ PC
$\equiv F[X;M]$ AP
M is ACCP
$\equiv F[X;M]$ ACCP
M finitely generated
$\equiv F[X;M]$ Noetherian
$M = \{0\}$ or $M \cong \mathbb{N}_0$
$\equiv F[X;M]$ Dedekind domain
$\equiv F[X;M]$ UFD
$\equiv F[X;M]$ PID
$\equiv F[X;M]$ Euclidean domain
$M = \{0\}$
$\equiv F[X;M]$ field
$M \cong \mathbb{N}_0$

Those properties contained within the larger rectangle on the left (respectively, right) correspond to the domain properties contained within the smaller circle (respectively, larger circle) in the previous figure. Notice, in the large rectangle on the right hand side of the diagram, we have highlighted our addition to the literature, that is, $F[X : M]$ being AP is equivalent to the other properties of the domain contained within the same rectangle when M is as assumed.

We have, therefore, answered our main question fully in the case that F is of characteristic 0. However, the question remains in the case where F is of finite characteristic > 0.

In Chapter 5 we introduced the notion of Matsuda monoids and showed that every monoid $M \subseteq (\mathbb{Q}_+, +)$ is a Matsuda monoid of type 0. In our paper [6] we raised the following questions:

(i) Is any proper submonoid of $(\mathbb{N}_0, +)$ a Matsuda monoid of any finite type?

(ii) Is every cancellative torsion-free monoid a Matsuda monoid of type 0?

Aside from these three questions we would like to work on the relations between properties of $M \subseteq (\mathbb{Q}_+, +)$ and various other properties of $F[X; M]$, including atomicity, ACCP, U-UFD, etc. (An integral domain R is *U-UFD* if for every nonzero nonunit $x \in R$ which has an irreducible factorization, that factorization is its unique irreducible factorization, up to associates.) We would be especially interested in studying the properties (of $F[X; M]$) introduced in the paper [1].

Furthermore, in [17], Lebowitz-Lockard classified various subatomic domains, e.g., Semi-Atomic, Almost atomic, Furstenberg, and Almost Furstenberg, etc. It would be interesting to extend our research to consider relations between the properties of the monoid $M \subseteq (\mathbb{Q}_+, +)$ and various subatomic properties of the domain $F[X; M]$.

REFERENCES

[1] D. D. ANDERSON, D. F. ANDERSON, and M. ZAFRULLAH, *Factorization in integral domains*, J. Pure Appl. Algebra **69** (1990), 1–19.

[2] D. M. BURTON, *A first course in rings and ideals*, Addison-Wesley Publishing Company, Inc., 1970.

[3] ———, *Abstract algebra*, Wm. C. Brown Publishers, Dubuque, IA, 1988.

[4] N. Q. CHINH and P. H. NAM, *New Characterization of Principal Ideal Domains*, East-West J. Math. **10** (2008), 149–152.

[5] K. CHRISTENSEN, R. GIPSON, and H. KULOSMAN, *A new characterization of principal ideal domains*, Sarajevo J. Math., accepted.

[6] ———, *Irreducibility of certain binomials in semigroup rings for nonnegative rational monoids*, Intern, Electr. J. Algebra **42** (2018), to appear.

[7] P. M. COHN, *Bézout rings and their subrings*, Proc. Camb. Phil. Soc. **64** (1968), 251–264.

[8] D. COSTA, J. MOTT, and M. ZAFRULLAH, *The Construction of $D + XD_S[X]$*, J. Algebra **53** (1978), 423–439.

[9] R. DAILEDA, *A Non-UFD Integral Domains in Which Irreducibles are Prime*, preprint.

[10] D. S. DUMMIT and R. M. FOOTE, *Abstract algebra*, 3 ed., John Wiley and Sons, Inc., 2004.

[11] N. J. FINE, *Binomial Coefficients Modulo a Prime*, Amer. Math. Monthly **54** (1947), 589–592.

[12] R. GILMER, *Commutative semigroup rings*, 1 ed., The University of Chicago Press, Chicago, 1984.

[13] ______, *Property E in commutative monoid rings*, Group and semigroup rings (G. Karpilovsky (Ed.)), Elsevier Science Publishers, B.V. (North-Holland) (1986), 13–18.

[14] R. GIPSON and H. KULOSMAN, *Atomic and AP semigroup rings $F[X;M]$, where M is a submonoid of the additive monoid of nonnegative rational numbers*, Intern. Electr. J. Algebra **22** (2017), 133–146.

[15] A. GRAMS, *Atomic rings and the ascending chain condition for principal ideals*, Mathematical Proceedings of the Cambridge Philosophical Society **75** (1974), 321–329.

[16] T. Y. LAM and K. H. LEUNG, *On Vanishing Sums of Roots of Unity*, J. Algebra **224** (2000), 91–109.

[17] N. LEBOWITZ-LOCKARD, *Classifying Subatomic Domains*, arXiv:1610.05874v1 (2016).

[18] R. MATSUDA, *On Algebraic Properties of Infinite Group Rings*, Bull. Fac. Sci. Ibaraki Univ. **7** (1975), 29–37.

[19] D. G. NORTHCOTT, *Lessons on rings, modules and multiplicities*, Cambridge University Press, 1968.

CURRICULUM VITAE

Ryan H. Gipson
124 Cherrywood Dr.
Frankfort, KY 40601
r0gips01@louisville.edu
(502) 229-4000

EDUCATION

University of Louisville, Louisville, KY
Ph.D. in Applied and Industrial Mathematics **Expected August 2018**
Areas of Concentration: Commutative Algebra and Factorization Theory
Title of Dissertation: “Factorization in Integral Domains.”
Advisor: Dr. Hamid Kulosman

University of Louisville, Louisville, KY
M.A. Mathematics **May 2015**

Murray State University, Murray, KY
B.S. Mathematics **May 2012**

TEACHING EXPERIENCE

University of Louisville, Louisville, KY

Graduate Teaching Assistant **August 2013-Present**

Primary Instructor:	Semester(s) Taught:
Math 205- Calculus I: Early Transcendentals	Spring17, Fall17
Math 190- Precalculus	Fall15, Fall16
Math 180- Elements of Calculus	Summer14, Summer16
Math 111- College Algebra	Fall14, Spring16, Summer17

Teaching Assistant:	Semester(s) Taught:
Math 109- Elementary Statistics	Spring15
Math 105- Contemporary Mathematics	Fall13, Spring14

RELATED EXPERIENCE

Private Tutor, Louisville, KY

Tutor **August 2014-Present**

Tutored middle school, high school, and undergraduate students in Geometry, Precalculus, College Algebra, Introduction to Higher Mathematics, and Abstract Algebra. These tutoring sessions included homework help, in-class test prep, standardized test prep, and/or proof strategies.

With multiple students, I provided additional take-home problems, as well as, diagnostic quizzes throughout our meetings to measure progress.

PAPERS AND PUBLICATIONS

CHRISTENSEN, K., GIPSON, R., KULOSMAN, H.: *A new characterization of integral domains*, submitted.

CHRISTENSEN, K., GIPSON, R., KULOSMAN, H.: *Irreducibility of certain binomials* $X^\pi - 1$ *in the semigroup rings* $F[X;M]$*, where* M *is a submonoid of* $(\mathbb{Q}_+, +)$ *and* F *is a field*, submitted.

GIPSON, R., KULOSMAN, H.: *Atomic and AP semigroup rings* $F[X;M]$*, where* M *is a submonoid of the additive monoid of nonnegative rational numbers*, Intern. Electr. J. Algebra, **22**(2017), 133-146.

CARTOR, R., GIPSON, R., SMITH-TONE, D., VATES, J.: *On the Differential Security of the HFEv- Signature Primitive.* 7th International Workshop, PQCrypto 2016, Fukuoka, Japan, February 24-26, 2016, Proceedings, Springer (2016)

PRESENTATIONS

“Differential Security of the HFEv$^-$ Signature Primitive, Algebra & Combinatorics Seminar, University of Louisville, Louisville, KY, 2015.

“New Characterizations of Principal Ideal Domains, Graduate Student Seminar, University of Louisville, Louisville, KY, 2016.

“Atomic and AP Semigroupg Rings $F[X;M]$, where $(M,+)$ is a subset of the Additive Monoid of Non-negative Rationals,” KYMAA 2017 Sectional Meeting, Berea College, Berea, KY, 2017.

“Factorization in Integral Domains,” Candidacy Exam, University of Louisville, Louisville, KY, May 15, 2017.

“A New Characterization of Principal Ideal Domains,”37th Annual Mathematics Symposium, Western Kentucky University, Bowling Green, KY, 2017.

“Essential Generators of the Monoid $M \subseteq (\mathbb{Q}_+, +)$ and their effects on the domain $F[X; M]$,”AMS Graduate Student Chapter Seminar, University of Louisville, Louisville, KY, 2018.

AWARDS

Presidential Scholar	**2008-2012**
Robert Byrd Scholarship	**2008-2011**
Alpha Chi Honors Society	**2008**