PRUFER DOMAINS, THE STRONG 2-GENERATOR PROPERTY, AND INTEGER-VALUED POLYNOMIALS

HEATHER ROTH

PRÜFER DOMAINS, THE STRONG 2-GENERATOR PROPERTY, AND INTEGER-VALUED POLYNOMIALS

by

Heather Roth

A Thesis Submitted to the Faculty of

The Charles E. Schmidt College of Science

in Partial Fulfillment of the Requirements for the degree of

Master of Science

Florida Atlantic University

Boca Raton, Florida

August 2004

PRÜFER DOMAINS, THE STRONG 2-GENERATOR PROPERTY, AND INTEGER-VALUED POLYNOMIALS

by

Heather Roth

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

SUPERVISORY COMMITTEE:

Lee Klingler
Thesis Advisor

James W. Brewer

Paul Yiu

Chairman, Department of Mathematical Sciences

Dean, The Charles E. Schmidt College of Science

Vice President for Research and Graduate Studies

Jun 29, 2004
Date

Abstract

Author:	Heather Roth
Title:	Prüfer Domains, the Strong 2-Generator Property, and Integer-Valued Polynomials
Institution:	Florida Atlantic University
Thesis Advisor:	Dr. Lee Klingler
Degree:	Master of Science
Year:	2004

We present several results involving three concepts: Prüfer domains, the strong 2-generator property, and integer-valued polynomials. An integral domain D is called a *Prüfer domain* if every nonzero finitely generated ideal of D is invertible. When each 2-generated ideal of D has the property that one of its generators can be any arbitrary selected nonzero element of the ideal, we say D has the *strong 2-generator property*. We note that, if D has the strong 2-generator property, then D is a Prüfer domain. If Q is the field of fractions of D, and E is a finite nonempty subset of D; we define $\text{Int}(E, D) = \{f(X) \in Q[X] \mid f(a) \in D \text{ for every } a \in E\}$ to be the ring of *integer-valued polynomials* on D with respect to the subset E. We show that D is a Prüfer domain if and only if $\text{Int}(E, D)$ is a Prüfer domain. Our main theorem is that $\text{Int}(E, D)$ has the strong 2-generator property if and only if D is a Bezout domain (that is, every finitely generated ideal of D is principal).

Acknowledgments

In honor and in loving memory of my grandpa, Stanley Hymowitz.
May 9, 1927 - January 8, 2000

I would like to thank those people who made this work possible. First, special thanks to my Mom and Dad, Ronni and Jeff Roth, for their love and support. It is because of them that I am the person that I am today. Next, many thanks to my thesis advisor, Dr. Lee Klingler, for his assistance and guidance. Words cannot express my appreciation to him. Finally, many thanks to my committee members Dr. James Brewer and Dr. Paul Yiu.

Contents

1 Introduction

In this thesis, we make a connection between two interesting structures, Prüfer domains and integer-valued polynomials. We begin this introduction by looking at each one from a historical perspective.

For Prüfer domains, we begin in the middle of the 19th century, when Ernst Eduard Kummer contributed a large amount of work in attempting to prove Fermat's Last Theorem, that is, that the equation $x^n + y^n = z^n$ has no nonzero integer solutions for x, y, and z when $n > 2$. In trying to prove Fermat's Last Theorem, he introduced the notion of "ideal numbers" in rings of integers in algebraic number fields. He was able to prove Fermat's Last Theorem for a large class of prime exponents n, namely, those exponents which are "regular."

At the end of the 19th century, Richard Dedekind showed that the ideal elements of Kummer could be reinterpreted as certain subsets of a ring, satisfying closure under both addition and multiplication by ring elements; he called these sets "ideals." One of the highlights of Dedekind's theory is a unique factorization theorem for ideals in rings of integers in algebraic number fields. He gave several proofs of this fundamental result, one of which involved showing that all nonzero ideals in such rings are "invertible," one of the key concepts in this thesis.

In the early 20th century, Emmy Noether axiomatized the rings D for which this unique factorization of ideals holds in terms of three properties which they must satisfy: (i) D must be integrally closed in its field of fractions; (ii) nonzero prime ideals of D must be maximal; and (iii) every ideal of D must be finitely generated. Such rings are now called *Dedekind domains*, although in this thesis, we use the (equivalent) definition as an integral domain in which all nonzero ideals are invertible. Rings satisfying condition (iii), studied extensively by Noether in the first part of the 20th century, are now known as *Noetherian rings.*

Also in the early 20th century, Ernst Paul Heinz Prüfer studied integral domains in which every nonzero *finitely generated* ideal is invertible; not surprisingly, such rings are now called *Prüfer domains.* From the definitions, it follows that D is a Dedekind domain if and only if D is a Noetherian Prüfer domain (Corollary 30).

One can show that, in a Dedekind domain, each ideal I can be generated by two elements, where one of the two elements is an arbitrary nonzero element of I. Such an ideal is called *strongly 2-generated*; as we shall see, nonzero strongly 2-generated ideals must be invertible (Theorem 34). A ring in which every 2-generated ideal is strongly 2-generated is said to have the *strong 2-generator property*, also an important concept in this thesis.

For the second key algebraic structure, integer-valued polynomials, we begin in the 17th century, when polynomials of the form $\binom{X}{n} = \frac{X(X-1)\ldots(X-n+1)}{n!}$, where n is a positive integer, first appeared in interpolation formulas. Although the coefficients of these polynomials are not integers when $n \geqslant 2$, these polynomials take on integer values for all integers. It has been known for a long time that these polynomials form an additive basis for the additive group of all integer-valued polynomials in $\mathbb{Q}[X]$.

More generally, for any integral domain D with field of fractions Q, if $E \subseteq D$ is a nonempty subset, we define the set of *integer-valued polynomials on* E to be $\text{Int}(E, D) = \{f(X) \in Q[X] \mid f(a) \in D$ for every $a \in E\}$. In the beginning of the 20th century, Georg Pólya and Alexander Ostrowski studied $\text{Int}(E, D)$ when D is the ring of integers in an arbitrary algebraic number field Q. In the middle of the 20th century, Thoralf Skolem studied the set $\text{Int}(D, D)$ as a ring, rather than as a D-module. In 1979, Demetrios Brizolis showed that $\text{Int}(\mathbb{Z}, \mathbb{Z})$ is a Prüfer domain, leading to an interest in studying integer-valued polynomial rings as a source of examples of Prüfer domains. For example, if E is a *finite* nonempty subset of D, then D is a Prüfer domain if and only if $\text{Int}(E, D)$ is a Prüfer domain (Theorem 49). Thus, the $\text{Int}(E, D)$ construction gives a method for building new Prüfer domains from old.

Throughout this thesis, we restrict our attention to a nonempty finite subset $E \subseteq D$. The theme of this thesis is the relationship between the structure of finitely generated ideals of D and those of $\text{Int}(E, D)$. The main result (Theorem 51) is that, if D is a Prüfer domain, then $\text{Int}(E, D)$ has the strong 2-generator property if and only if D satisfies an even stronger property, namely, that all finitely generated ideals of D are principal. (Such rings are called *Bézout domains.*) We show that an integral domain with the strong 2-generator property is a Prüfer domain (Corollary 35). Also, a Bézout domain is a Prüfer domain. Thus, the assumption that D be a Prüfer domain can be omitted in the main theorem.

The content of this thesis is as follows. Chapter 2 consists of background material on fractional ideals, including operations on fractional ideals, invertibility, and cancellation. Chapter 3 focuses on the strong 2-generator property. For integral domain D, let $\mathcal{I}(D)$ denote the set of invertible fractional ideals of D, and $\mathcal{P}(D)$ denote the set of nonzero principal fractional ideals of D. We note that the quotient group $\mathcal{I}(D)/\mathcal{P}(D)$ is called the *ideal class group* (or *Picard group*) of D. A prime n is called *regular* (and, as noted above, Kummer's proof of Fermat's Last Theorem holds for n), if n does not divide the order of the ideal class group of the ring of algebraic integers in $\mathbb{Q}[\zeta_n]$, where ζ_n is a primitive n-th root of unity.

In Chapter 4, we turn our attention to integer-valued polynomials, and we begin by recalling a few elementary facts about polynomials with coefficients in a field. Our main tool is Proposition 46, which characterizes ideals of $\mathrm{Int}(E, D)$ having nonzero intersection with D. (Such ideals are called *unitary ideals.*) This characterization shows that $\mathrm{Int}(E, D)$ has the *almost-strong Skolem property* (Corollary 48), that is, two finitely generated unitary ideals I and J of $\mathrm{Int}(E, D)$ are equal if and only if, for each element $a \in E$, the set of values $I(a)$ of the polynomials in I evaluated at a equals the set of values $J(a)$. Finally, in Chapter 5, we prove the main theorem mentioned above.

2 Preliminaries

Throughout this thesis, D always denotes an integral domain with field of fractions Q.

Theorem 1 *The following conditions are equivalent for a commutative ring R.*

(i) R has the Ascending Chain Condition: Every increasing sequence of ideals $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$ eventually stabilizes; that is, for some positive integer n, $I_n = I_{n+1} = I_{n+2} = \ldots$.

(ii) R satisfies the maximum condition: Every nonempty set X of ideals of R has a maximal element; that is, there exists some $I \in X$ such that, for all $J \in X$, if $I \subseteq J$, then $I = J$.

(iii) Every ideal of R is finitely generated.

Proof. For *(i)* $\Longrightarrow$ *(ii)*, suppose that X is a nonempty set of ideals with no maximal element. Then we need to show that some increasing sequence of ideals does not eventually stabilize. Choose an ideal $I_1 \in X$. I_1 is not maximal in X by assumption, so there must be $I_2 \in X$ such that $I_1 \subsetneq I_2$. But I_2 is not maximal in X by assumption, so there must be $I_3 \in X$ such that $I_2 \subsetneq I_3$. And so on. By induction, we get an ascending chain $I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \ldots$ which never stabilizes. Therefore, some increasing sequence of ideals does not eventually stabilize.

For *(ii)* $\Longrightarrow$ *(iii)*, let I be an ideal of R. Let $X = \{\text{ideals } J \mid J \subseteq I \text{ and } J \text{ is finitely generated}\}$. Now (0) is finitely generated and $(0) \subseteq I$, $(0) \in X$, so X is nonempty. By *(ii)*, X has a maximal element J. Now $J \subseteq I$ and $J = Ra_1 + \ldots + Ra_n$ for some $a_1, \ldots, a_n \in J$. Then we need to show that $J = I$. Suppose that $J \neq I$, so $J \subsetneq I$. Choose $b \in I - J$. Then $Ra_1 + \ldots + Ra_n + Rb \subseteq I$, so $Ra_1 + \ldots + Ra_n + Rb \in X$. But $J \subsetneq Ra_1 + \ldots + Ra_n + Rb$ because $b \notin J$. This is impossible since J is maximal in X. So, $J = I$. Therefore, every ideal of R is finitely generated.

For *(iii)* $\Longrightarrow$ *(i)*, let $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$ be ascending chain of ideals of R, and let $I = \cup_{n=1}^{\infty} I_n$. Since $(0) \subseteq I$, I is closed under addition, and I preserves scalar multiplication, then I is an ideal. Since I is finitely generated by assumption, then $I = Ra_1 + \ldots + Ra_t$ for some $a_1, \ldots, a_t \in I$. For each i, $a_i \in I_{n_i}$ for some n_i. Choose $N = \max\{n_1, \ldots, n_t\}$, then $a_1, \ldots, a_t \in I_N$. So, $I = Ra_1 + \ldots + Ra_t \subseteq I_N \subseteq I$ which implies $I = I_N = I_{N+1} = \ldots$. Therefore, R has the ascending chain condition. ■

We characterize the property specified by these conditions in the following definition.

Definition 2 *A commutative ring R is called* ***noetherian*** *if it satisfies the equivalent conditions of Theorem 1.*

Many of the definitions and results in the remainder of this chapter can be found in [7]. The following definition is a fundamental concept in this thesis.

Definition 3 *A* ***fractional ideal*** *of D is a D-submodule J of Q such that $dJ \subseteq D$ for some nonzero $d \in D$.*

Example 4 *Let $D = \mathbb{Z}$, $Q = \mathbb{Q}$, and $J = \{\frac{a}{2} \mid a \in \mathbb{Z}\}$. Then $J \subseteq \mathbb{Q}$ is a $\mathbb{Z}$-submodule, and $2J \subseteq D$ so that J is a fractional $\mathbb{Z}$-ideal.*

The following proposition answers the question of when two D-submodules are isomorphic.

Proposition 5 *If $M, N \subseteq Q$ are D-submodules, then $M \cong N$ if and only if $M = \alpha N$ for some nonzero $\alpha \in Q$.*

Proof. Suppose that $M, N \subseteq Q$ are D-submodules.

($\Longrightarrow$) Suppose that $\theta : N \longrightarrow M$ is a D-module isomorphism. If $N = \{0\}$, then $M = \theta(N) = \{0\}$ also, so α can be any nonzero element of Q. So, we can suppose that $N \neq \{0\}$. Fix $0 \neq n \in N$. For each $n' \in N$, let $0 \neq d \in D$ be a common denominator for n and n', so that $dn, dn' \in D$. Now, $dn\theta(n') = \theta(dnn') = dn'\theta(n)$. Since $dn \neq 0$, then $\theta(n') = \frac{dn'\theta(n)}{dn} = \frac{\theta(n)}{n}n' = \alpha n'$ where $\alpha = \frac{\theta(n)}{n}$. Therefore, $M = \theta(N) = \alpha N$.

($\Longleftarrow$) Suppose that $M = \alpha N$ for some $0 \neq \alpha \in Q$. We need to show that $\theta : N \longrightarrow M$ defined by $\theta(n) = \alpha n$ is a D-module homomorphism, one-to-one, and onto. So, for all $n, n' \in N$ and for all $\beta \in Q$, $\theta(n + n') = \alpha(n + n') = \alpha n + \alpha n' = \theta(n) + \theta(n')$ and $\theta(\beta n) = \alpha(\beta n) = (\alpha\beta)n = (\beta\alpha)n = \beta(\alpha n) = \beta\theta(n)$, so that θ is a D-module homomorphism. By the First Isomorphism Theorem, N / ker $\theta \cong$ im θ. Since if $\theta(n) = \theta(n')$, then $\alpha n = \alpha n'$ implies that $n = n'$ (because $\alpha \neq 0$). So, θ is one-to-one. Since by assumption $M = \alpha N$, then $M = \alpha N = \theta(N)$, so θ is onto. ■

Applying Proposition 5 to fractional ideals, we obtain the following consequence.

Corollary 6 *If $M \subseteq Q$ is a D-submodule, then M is a fractional D-ideal if and only if $M \cong I$ for some ideal $I \subseteq D$.*

Proof. Suppose that $M \subseteq Q$ is a D-submodule.

($\Longrightarrow$) Suppose that M is a fractional D-ideal. Then this implies that $\alpha M \subseteq D$ for some $0 \neq \alpha \in D$, where αM is an ideal in D, and $M \cong \alpha M$ by Proposition 5.

($\Longleftarrow$) Suppose that $M \cong I$ for some ideal $I \subseteq D$. By Proposition 5, this implies that $M = \alpha I$ for some $0 \neq \alpha \in Q$, where $\alpha = \frac{a}{b}$ for some $0 \neq a, b \in D$. Then $bM = b\alpha I = aI \subseteq D$. Therefore, M is a fractional D-ideal. ■

The example given in Example 4 is a special case of the following much more general class of examples.

Proposition 7 *A finitely generated D-submodule J of Q is a fractional D-ideal.*

Proof. Suppose that J is a finitely generated D-submodule of Q. If $x_1 = a_1/b_1, \ldots, x_n = a_n/b_n$ generate J and $b = b_1 \cdot \ldots \cdot b_n$, then $bJ \subseteq D$. Therefore, J is a fractional D-ideal. ■

For the converse of Proposition 7, we require the additional condition that every ideal be finitely generated.

Proposition 8 *If D is noetherian, then a fractional D-ideal J of D is a finitely generated D-submodule of Q.*

Proof. Suppose that D is noetherian, and suppose that J is a fractional D-ideal of D. Then J is isomorphic to an ideal of D, by Proposition 6. By assumption, every ideal of D is finitely generated, so J must be finitely generated as well. ■

Certain operations on fractional ideals (or, more generally, submodules of Q) are important for this thesis.

Definition 9 *For submodules I and J of Q, recall the usual binary operations of sum $I + J$ and intersection $I \cap J$ and define two more binary operations called the* **product** *$IJ = \{\Sigma_{i=1}^{n} a_i b_i \mid a_i \in I, b_i \in J, n < \omega\}$ and the* **residual** *$I : J = \{q \in Q \mid qJ \subseteq I\}$. The sum, intersection, product, and residual of I and J are again submodules.*

Example 10 *Let $I = \frac{1}{2}\mathbb{Z}$ and $J = \frac{3}{5}\mathbb{Z}$. Then $I : J = \{q \in Q \mid qJ \subseteq I\} = \frac{5}{6}\mathbb{Z}$.*

Let $\mathcal{F}(D)$ denote the set of nonzero fractional D-ideals.

Theorem 11 *$\mathcal{F}(D)$ is closed under finite sums, intersections, products, and residuals.*

Proof. Let I and J be fractional D-ideals of $\mathcal{F}(D)$. Then I is a D-submodule of Q such that $dI \subseteq D$ for some nonzero $d \in D$ and J is a D-submodule of Q such that $eJ \subseteq D$ for some nonzero $e \in D$. For the sum, we have that $de(I+J) \subseteq dI + eJ \subseteq D$ so $I+J$ is a fractional D-ideal. For the intersection, we have that $d(I \cap J) \subseteq dI \subseteq D$ so that $I \cap J$ is a fractional D-ideal. For the product, we have that $deIJ = (dI)(eJ) \subseteq D$ so that IJ is a fractional D-ideal. For the residual, $J(I:J) \subseteq I$ by definition, and then multiplying both sides by d, we have $dJ(I:J) \subseteq dI \subseteq D$. So, for any nonzero $c \in dJ$, $c(I:J) \subseteq D$. But c may not be an element of D, so we multiply by e since $eJ \subseteq D$. We have that ce is a nonzero element of D such that $ce(I:J) \subseteq eD \subseteq D$, so $(I:J)$ is a fractional D-ideal.

By induction, $\mathcal{F}(D)$ is closed under finite sums, intersections, products, and residuals. ■

We record some useful properties of these operations on fractional ideals in the following theorem.

Theorem 12 *Let I, J and K be submodules of Q; then:*

(i) $I(J+K) = IJ + IK$;

(ii) $I:(J+K) = (I:J) \cap (I:K)$;

(iii) $(I \cap J) : K = (I:K) \cap (J:K)$;

(iv)a $(I:J):K = I:JK$;

(iv)b $I:JK = (I:K):J$;

(v) $I(IJ:I) = IJ$;

(vi) $(I \cap J) + (I \cap K) \subseteq I \cap (J+K)$;

(vii) $I(J \cap K) \subseteq IJ \cap IK$;

(viii) $(I:K) + (J:K) \subseteq (I+J):K$.

Proof. For *(i)*, first, to show that $I(J+K) \subseteq IJ + IK$, take $a \in I$ and $b + c \in J + K$ where $b \in J$ and $c \in K$. Since $a \in I$ and $b \in J$, then $ab \in IJ$ and since $a \in I$ and $c \in K$, then $ac \in IK$. So, now $ab \in IJ$ and $ac \in IK$ implies that $ab + ac \in IJ + IK$. Now, to show that $IJ + IK \subseteq I(J+K)$, take $ab + a'c \in IJ + IK$ where $ab \in IJ$ and $a'c \in IK$. So, $ab \in IJ$ implies that $ab \in I(J+K)$ because $a \in I$ and $b \in J$ and $a'c \in IK$ implies that $a'c \in I(J+K)$ because $a' \in I$ and $c \in K$. So, $ab + a'c \in I(J+K)$. Therefore, $I(J+K) = IJ + IK$.

For *(ii)*, first, to show that $(I:(J+K)) \subseteq ((I:J) \cap (I:K))$, first take $a \in (I:(J+K))$. Then $a(J+K) \subseteq I$. Take any $b \in J$. Then $b \in J \subseteq J+K$. So, $ab \in aJ \subseteq a(J+K) \subseteq I$ so $aJ \subseteq I$ so $a \in (I:J)$. Now take any $b \in K$. Then $b \in K \subseteq J+K$. So, $ab \in aK \subseteq a(J+K) \subseteq I$ so $aK \subseteq I$

so $a \in (I : K)$. So, $a \in ((I : J) \cap (I : K))$. Now, to show that $((I : J) \cap (I : K)) \subseteq I : (J + K)$, take $a \in ((I : J) \cap (I : K))$. Then $a \in (I : J)$ and $a \in (I : K)$ so $aJ \subseteq I$ and $aK \subseteq I$. Now $aJ + aK = a(J + K) \subseteq I$ so $a \in (I : (J + K))$. Therefore, $I : (J + K) = (I : J) \cap (I : K)$.

For *(iii)*, first, to show that $((I \cap J) : K) \subseteq ((I : K) \cap (J : K))$, take $a \in ((I \cap J) : K)$ so $aK \subseteq (I \cap J)$ so $aK \subseteq I$ and $aK \subseteq J$. Then we have that $a \in (I : K)$ and $a \in (J : K)$ which implies that $a \in ((I : K) \cap (J : K))$. Now, to show that $((I : K) \cap (J : K)) \subseteq ((I \cap J) : K)$, take $a \in ((I : K) \cap (J : K))$. Then, $a \in (I : K)$ and $a \in (J : K)$ so $aK \subseteq I$ and $aK \subseteq J$ so $aK \subseteq (I \cap J)$ so $a \in ((I \cap J) : K)$. Therefore, $(I \cap J) : K = (I : K) \cap (J : K)$.

For *(iv)a*, first, to show that $((I : J) : K) \subseteq (I : JK)$, take $a \in ((I : J) : K)$ so $aK \subseteq (I : J)$. Then $aKJ \subseteq I$ so $aJK \subseteq I$ so $a \in (I : JK)$. Now, to show that $I : JK \subseteq (I : J) : K$, take $a \in (I : JK)$ so $aJK \subseteq I$ and then $aKJ \subseteq I$ so $aK \subseteq (I : J)$ so $a \in ((I : J) : K)$. Therefore, $(I : J) : K = I : JK$.

For *(iv)b*, first, to show that $(I : JK) \subseteq ((I : K) : J)$, take $a \in (I : JK)$. Then $aJK \subseteq I$ so $aJ \subseteq (I : K)$ so $a \in ((I : K) : J)$. Now, to show that $((I : K) : J) \subseteq (I : JK)$, take $a \in ((I : K) : J)$. Then $aJ \subseteq (I : K)$ so $aJK \subseteq I$ so $a \in (I : JK)$. Therefore, $I : JK = (I : K) : J$.

For *(v)*, first, to show that $I(IJ : I) \subseteq IJ$, take $a \in I$ and $b \in (IJ : I)$. Since $b \in (IJ : I)$, then $bI \subseteq IJ$. Since $a \in I$, then $ba = ab \in IJ$. Now, to show that $IJ \subseteq I(IJ : I)$, take $a \in I$ and $b \in J$ so that $ab \in IJ$. Since $b \in J$, then $bI \subseteq JI = IJ$, so $b \in (IJ : I)$, so $ab \in I(IJ : I)$. Therefore, $I(IJ : I) = IJ$.

For *(vi)*, to show that $((I \cap J) + (I \cap K)) \subseteq (I \cap (J + K))$, take $a + b \in ((I \cap J) + (I \cap K))$ where $a \in (I \cap J)$ and $b \in (I \cap K)$. So, $a \in I$ and $a \in J$ and $b \in I$ and $b \in K$. So, $a + b \in I$ and $a + b \in (J + K)$. Therefore, $a + b \in (I \cap (J + K))$.

For *(vii)*, to show that $I(J \cap K) \subseteq (IJ \cap IK)$, take $a \in I$ and $b \in (J \cap K)$. Then $b \in J$ and $b \in K$. Since $a \in I$ and $b \in J$, then $ab \in IJ$, and since $a \in I$ and $b \in K$, then $ab \in IK$. So, $ab \in (IJ \cap IK)$. Therefore, $I(J \cap K) \subseteq (IJ \cap IK)$.

For *(viii)*, to show that $((I : K) + (J : K)) \subseteq ((I + J) : K)$, take $a + b \in ((I : K) + (J : K))$ where $a \in (I : K)$ and $b \in (J : K)$. Then $aK \subseteq I$ and $bK \subseteq J$. So, $(a + b)K \subseteq aK + bK \subseteq I + J$ so $a + b \in ((I + J) : K)$. Therefore, $(I : K) + (J : K) \subseteq (I + J) : K$. ■

Two of the four operations mentioned previously, namely, the sum and product, yield finitely generated ideals when applied to finitely generated fractional ideals.

Proposition 13 *If I and J are finitely generated fractional ideals, then $I+J$ and IJ are finitely generated fractional ideals.*

Proof. Suppose that $I = Di_1 + \ldots + Di_n$ and $J = Dj_1 + \ldots + Dj_m$ are finitely generated fractional ideals. Then by Theorem 11, $I+J$ and IJ are fractional ideals. So, it is sufficient to show then that $I+J$ and IJ are finitely generated. But $I + J = Di_1 + \ldots + Di_n + Dj_1 + \ldots + Dj_m$ is finitely generated, and one easily checks that $IJ = \Sigma_{\substack{1 \leqslant k \leqslant n, \\ 1 \leqslant l \leqslant m}} Di_kj_l$, so that IJ is finitely generated as well. Therefore, $I+J$ and IJ are finitely generated fractional ideals. ■

Another fundamental concept in this thesis is the following.

Definition 14 *A nonzero fractional ideal I of D is called* ***invertible*** *if there exists a $J \in \mathcal{F}(D)$ such that $IJ = D$. This fractional ideal J, if it exists, is uniquely determined by I and is called the* ***inverse*** *of I, denoted by I^{-1}.*

The following example shows that nonzero principal fractional ideals are invertible.

Example 15 *If $I = Da$ is a nonzero principal fractional ideal, then $I^{-1} = Da^{-1}$.*

Lemma 16 *If I and J are fractional ideals, then IJ is invertible if and only if both I and J are invertible.*

Proof. Suppose that I and J are fractional ideals of D.

($\Longrightarrow$) Suppose that IJ is invertible. Then $(IJ)K = D$ for some $K \subseteq D$. Now, $I(JK) = D$ implies that I is invertible. Similarly, $J(IK) = D$ implies that J is invertible. Therefore, both I and J are invertible.

($\Longleftarrow$) Suppose that both I and J are invertible. Then $IK = D$ and $JL = D$ for some $K, L \subseteq D$. So, $IJ(KL) = D$. Therefore, IJ is invertible. ■

For fractional ideals, the following property is also an object of study but will not play a major role in this thesis.

Definition 17 *A fractional ideal I is said to be* **cancellative** *if for $J, L \in \mathcal{F}(D)$, $IJ = IL$ implies that $J = L$.*

This next example shows that invertible fractional ideals are cancellative.

Example 18 *If $IJ = IL$ and I is invertible, then multiplying both sides by I^{-1} gives $J = L$, so I is cancellative.*

Combining Example 15 and Example 18 we get the following.

Example 19 *Nonzero principal fractional ideals are cancellative.*

The equivalence given in Lemma 16 holds also for the cancellative property.

Proposition 20 *If I and J are fractional ideals, then IJ is cancellative if and only if I and J are cancellative.*

Proof. Let I and J be fractional ideals.

($\Longrightarrow$) Suppose that IJ is cancellative. Then $IJK = IJL$ implies $K = L$. So, now suppose that $IK = IL$. Then $IKJ = ILJ$ and so $IJK = IJL$ so $K = L$. Similarly, if $JK = JL$, then $IJK = IJL$ so $K = L$. Therefore, I and J are cancellative.

($\Longleftarrow$) Suppose that I and J are cancellative, and suppose that $(IJ)K = (IJ)L$. Then $I(JK) = I(JL)$ which implies that $JK = JL$ since I is cancellative which implies $K = L$ since J is cancellative. Therefore, IJ is cancellative. ∎

We now note three equivalent characterizations of cancellability.

Proposition 21 *For a nonzero fractional ideal I, TFAE:*

(i) I is cancellative;

(ii) $IJ : I = J$ for all fractional ideals J;

(iii) for $J, K \in F(D)$, $IJ \subseteq IK$ implies $J \subseteq K$.

Proof. *(i)* $\Longrightarrow$ *(ii)* Suppose that I is cancellative. By property *(v)* of Theorem 12, $I(IJ : I) = IJ$. By assumption, I is cancellative. Therefore, $IJ : I = J$ for all fractional ideals J.

(ii) $\Longrightarrow$ *(iii)* Suppose that $IJ : I = J$ for all fractional ideals J. If $IJ \subseteq IK$, then $J = IJ : I \subseteq IK : I = K$. Therefore, for $J, K \in \mathcal{F}(D)$, $IJ \subseteq IK$ implies $J \subseteq K$.

(iii) $\Longrightarrow$ *(i)* Suppose that for $J, K \in \mathcal{F}(D)$, $IJ \subseteq IK$ implies $J \subseteq K$. If $IJ = IK$, then $IJ \subseteq IK$, so $J \subseteq K$, and $IK \subseteq IJ$, so $K \subseteq J$. So, $J = K$. Therefore, I is cancellative. ∎

The next few results contain technical facts needed in what follows.

Proposition 22 *If I is a cancellative fractional ideal of D, and $P_1, \ldots, P_n$ are distinct maximal ideals of D, then $\cup_{i=1}^{n} IP_i \subsetneq I$.*

Proof. Suppose that $P \subseteq D$ is a maximal ideal, and suppose that $I, J \subseteq D$ are ideals.

We claim that, if $IJ \subseteq P$, then $I \subseteq P$ or $J \subseteq P$. To prove this claim, suppose that $I \nsubseteq P$ and $J \nsubseteq P$. Then there are $a \in I - P$ and $b \in J - P$. So, $ab \notin P$ because P is prime. $ab \in IJ - P$, so $IJ \nsubseteq P$.

Now, $P_1 \cdot \ldots \cdot P_{j-1} P_{j+1} \cdot \ldots \cdot P_n \subseteq P_1 \cap \ldots \cap P_{j-1} \cap P_{j+1} \cap \ldots \cap P_n$. Suppose that $P_1 \cap \ldots \cap P_{j-1} \cap P_{j+1} \cap \ldots \cap P_n \subseteq P_j$. Using induction and the argument in the previous paragraph, this implies that $P_i \subseteq P_j$ for some $i \neq j$. But P_i is maximal by assumption (and P_j proper), which forces $P_i = P_j$, impossible.

Since I is cancellative, then by Proposition 21 $I(\cap_{i \neq j} P_i) \nsubseteq IP_j$ (because cancellation of I would yield $\cap_{i \neq j} P_i \subseteq P_j$ again, which we showed is impossible). For each j, choose an $a_j \in I(\cap_{i \neq j} P_i) \setminus IP_j$. Then $a = a_1 + \ldots + a_n \in I$. We claim that $a \notin IP_i$ for each i. This is because of the following. If $j \neq i$, then $a_j \in I(\cap_{k \neq j} P_k) \subseteq IP_i$. From $a_j \in I(\cap_{i \neq j} P_i) \setminus IP_j$, we have that $a_i \notin IP_i$. Therefore, $a = a_i + a_1 + \ldots + a_{i-1} + a_{i+1} + \ldots + a_n \notin IP_i$ for all i. ■

Lemma 23 *(i) Let $J_1, \ldots, J_n$ be a finite collection of ideals of D, and I an ideal of D such that $I \subseteq \cup_{i=1}^{n} J_i$. If at most two of the ideals J_i are not prime, then $I \subseteq J_j$ for some j.*
(ii) If $J_1, \ldots, J_n$ are incomparable prime ideals (e.g., different maximal ideals), then $J_i \nsubseteq \cup_{j \neq i} J_j$ for $i = 1, \ldots, n$.

Proof. For *(i)*, we use induction on n. First, for $n = 1$, the claim is trivial. For $n = 2$, suppose that $I \subseteq J_1 \cup J_2$. Then it is sufficient to show that $I \subseteq J_1$ or $I \subseteq J_2$. By way of contradiction, suppose that $I \nsubseteq J_1$ and $I \nsubseteq J_2$. Pick $x_1 \in I - J_1$ and $x_2 \in I - J_2$. Then $x_1 + x_2 \in I$ because $x_1, x_2 \in I$, an ideal. So, $x_1 + x_2 \in I \subseteq J_1 \cup J_2$ by assumption, say $x_1 + x_2 \in J_1$ (similarly for J_2). But $x_1 \notin J_1$ by choice which implies that $x_2 \notin J_1$. This is because if we write $x_1 = (x_1 + x_2) - x_2$, since $x_1 + x_2 \in J_1$ and $x_1 \notin J_1$, then $x_2 \notin J_1$. But this is a contradiction because $x_2 \in I \subseteq J_1 \cup J_2$. Now, for $n \geqslant 3$, assume true for $n - 1$. Suppose that $I \subseteq J_1 \cup \ldots \cup J_n$. We can assume J_n is prime. If $I \subseteq J_1 \cup \ldots \cup J_{n-1}$, then we are done by induction, so suppose that $I \nsubseteq J_1 \cup \ldots \cup J_{n-1}$, and pick $x_1 \in I - (J_1 \cup \ldots \cup J_{n-1})$. If $J_k \subseteq J_n$ for k, $1 \leqslant k \leqslant n-1$, then $I \subseteq J_1 \cup \ldots \cup J_{k-1} \cup J_{k+1} \cup \ldots \cup J_n$, so again we are done by induction, so suppose that $J_k \nsubseteq J_n$ for all k, $1 \leqslant k \leqslant n-1$. If $I \subseteq J_n$, then we are done, so suppose $I \nsubseteq J_n$. Then $I \cdot J_1 \cdot \ldots \cdot J_{n-1} \nsubseteq J_n$ because J_n is prime and $I \nsubseteq J_n$ and $J_k \nsubseteq J_n$ for $k = 1, \ldots, n-1$. Pick $x_2 \in I \cdot J_1 \cdot \ldots \cdot J_{n-1} - J_n$. Since $x_1 \in I$, $x_2 \in I \cdot J_1 \cdot \ldots \cdot J_{n-1} \subseteq I$, and I is an ideal, then $x_1 + x_2 \in I$. If $1 \leqslant k \leqslant n-1$, then $x_1 \notin J_1 \cup \ldots \cup J_{n-1}$ which implies that $x_1 \notin J_k$, but $x_2 \in I \cdot J_1 \cdot \ldots \cdot J_{n-1} \subseteq J_k$. Then $x_1 + x_2 \notin J_k$. Since $x_1 \in I \subseteq J_1 \cup \ldots \cup J_n$, then

$x_1 \in J_n$, but $x_1 \notin J_1 \cup \ldots \cup J_{n-1}$. Now since $x_2 \notin J_n$ by choice, then $x_1 + x_2 \notin J_n$. This is a contradiction since $x_1 + x_2 \in I$, but $x_1 + x_2 \notin J_1 \cup \ldots \cup J_n$.

For *(ii)*, by part *(i)* and assuming that $J_1, \ldots, J_n$ are incomparable prime ideals, then $J_i \nsubseteq \cup_{j \neq i} J_j$ for $i = 1, \ldots, n$. ■

Definition 24 *D is called* ***semilocal*** *if D has only finitely many maximal ideals. D is called* **local** *if D has a unique maximal ideal.*

Proposition 25 *Let I be an invertible fractional ideal of D. Then:*

(i) $I^{-1} = D : I$;

(ii) I is finitely generated;

(iii) if D is semilocal, then I is a principal fractional ideal; if D is local, then every generating set of I contains an element generating I;

(iv) if I is an integral ideal and there is an $a \in I$ *contained in only finitely many maximal ideals, then* $I = Da + Db$ *for some* $b \in D$.

Proof. For *(i)*, suppose that $IJ = D$. Then J is cancellative. Therefore, part *(ii)* of Proposition 21 implies that $J = IJ : I = D : I$.

For *(ii)*, since I is an invertible fractional ideal, then $IJ = D$ for some fractional ideal J. Now $1 \in D$, so we can write $1 = a_1b_1 + \ldots + a_nb_n$ for some $a_1, \ldots, a_n \in I$ and $b_1, \ldots, b_n \in J$. We need to show that $I = Da_1 + \ldots + Da_n$. First, the containment $Da_1 + \ldots + Da_n \subseteq I$ is clear since $a_1, \ldots, a_n \in I$, a fractional ideal. For the containment $I \subseteq Da_1 + \ldots + Da_n$, choose $w \in I$, then $w = (wb_1)a_1 + \ldots + (wb_n)a_n \in Da_1 + \ldots + Da_n$ since $wb_i \in IJ$ for each i. Therefore, $I = Da_1 + \ldots + Da_n$, so I is finitely generated.

For *(iii)*, assume that D is semilocal, namely, that D has finitely many maximal ideals. So, let $\{P_1, \ldots, P_n\}$ be the set of maximal ideals of D. Proposition 22 ensures that $I \supsetneq \cup_{i=1}^n IP_i$. It is sufficient to verify that any $a \in I \setminus \cup_{i=1}^n IP_i$ satisfies $I = Da$. So, $Da \subseteq I$ and multiplying both sides by I^{-1} yields $aI^{-1} \subseteq D$.

We claim that, from $Da \nsubseteq \cup_{i=1}^n IP_i$, we obtain $aI^{-1} \nsubseteq \cup_{i=1}^n P_i$. To prove this claim, suppose that $aI^{-1} \subseteq \cup_{i=1}^n P_i$. Then Lemma 23 implies that $aI^{-1} \subseteq P_i$ for some i. Then $aI^{-1}I \subseteq IP_i$ and so $Da \subseteq IP_i \subseteq \cup_{i=1}^n IP_i$ which is a contradiction. So, we do obtain $aI^{-1} \nsubseteq \cup_{i=1}^n P_i$ from $Da \nsubseteq \cup_{i=1}^n IP_i$.

Now aI^{-1} is an integral ideal not contained in any maximal ideal of D, so $aI^{-1} = D$. Multiplying by I yields $Da = I$. Therefore, I is a principal fractional ideal.

Assume now that D is local, namely, that D has a unique maximal ideal, and also assume that $I = \Sigma_{i=1}^{n} Da_i = Da$. Then, for each $i \leqslant n$, $a_i = d_i a$ and $a = \Sigma_{i=1}^{n} e_i a_i$ for suitable $d_i, e_i \in D$. Then $1 = \Sigma_{i=1}^{n} d_i e_i$. Since every nonunit lies in some maximal ideal and there is only one maximal ideal, then all of the nonunits are in this maximal ideal. But since maximal ideals are proper, then d_i is a unit for some i, so $I = Da_i$ for such an i.

For *(iv)*, if $a = 0$, then D is semilocal, and the claim is a consequence of *(iii)*. So, suppose that $a \neq 0$. If $I = Da$, then we are done; so let $Da \subset I$. Then aI^{-1} is a proper ideal of D and $Da = II^{-1}a \subseteq I^{-1}a$. Let $P_1, \ldots, P_n$ denote the maximal ideals containing $I^{-1}a$. By Proposition 22, there exists a $b \in I \setminus \cup_{i=1}^{n} IP_i$. Such a b satisfies $I^{-1}b \subseteq D$ and $I^{-1}b \nsubseteq P_i$ for all $i \leqslant n$, thus $I^{-1}a + I^{-1}b$ is not contained in P_i for any $i \leqslant n$, neither is in any other maximal ideal of D. Therefore, $I^{-1}a + I^{-1}b = D$, and so $Da + Db = I$ after multiplying both sides by I. ∎

Definition 26 *An ideal which can be generated by two elements is called **2-generated**.*

An important fact is that, in a sense, the 2-generated ideals determine the behavior of all finitely generated ideals. The key is the following interesting fact.

Lemma 27 *For fractional ideals I, J, K, $(I + J)(J + K)(K + I) = (I + J + K)(IJ + JK + KI)$.*

Proof. Multiplying out the left-hand side gives $(I+J)(J+K)(K+I) = (IJ+IK+JJ+JK)(K+I) = IJK+IJI+IKK+IKI+JJK+JJI+JKK+JKI = IJK+IIJ+IIK+JJI+JJK+KKI+KKJ$. On the right-hand side, $(I + J + K)(IJ + JK + KI) = IIJ + IJK + IKI + JIJ + JJK + JKI + KIJ + KJK + KKI = IIJ + IKI + JIJ + JJK + IJK + KJK + KKI$. Therefore, since D is commutative, then $(I + J)(J + K)(K + I) = (I + J + K)(IJ + JK + KI)$. ∎

Theorem 28 *The invertibility of all 2-generated fractional ideals of D implies that all finitely generated fractional ideals of D are invertible.*

Proof. By induction.

For $n = 1$, since principal ideals are invertible, then true.

For $n = 2$, true by assumption.

For $n \geqslant 3$, let $I = Da_1 + \ldots + Da_{n-2}$, $J = Da_{n-1}$, and $K = Da_n$. Then we have that $((Da_1+\ldots+Da_{n-2})+Da_{n-1})(Da_{n-1}+Da_n)(Da_n+(Da_1+\ldots+Da_{n-2})) = ((Da_1+\ldots+Da_{n-2})+ Da_{n-1} + Da_n)((Da_1 + \ldots + Da_{n-2})(Da_{n-1}) + ((Da_{n-1})(Da_n)) + ((Da_n)(Da_1 + \ldots + Da_{n-2})))$.

This equality follows immediately from Lemma 27. Since we have invertibility up to $n-1$ and, by Lemma 16, the product of invertibles is invertible, then the invertibility of the left-hand side implies invertibility of the right-hand side. Therefore, $((Da_1 + \ldots + Da_{n-2}) + Da_{n-1} + Da_n)$ is invertible by Lemma 16, completing the induction. ■

We conclude this chapter by defining one of the main objects of study of this thesis, Prüfer domains, and note two special cases.

Definition 29 *An integral domain in which every nonzero finitely generated ideal is invertible is called a* ***Prüfer domain****. An integral domain in which every finitely generated ideal is principal is called a* ***Bézout domain****. Since principal ideals are invertible by Example 15, then a Bézout domain is a Prüfer domain. An integral domain in which every nonzero ideal is invertible is called a* ***Dedekind domain****.*

Corollary 30 *D is a Dedekind domain if and only if D is a Noetherian Prüfer domain.*

Proof. ($\Longrightarrow$) Suppose that D is a Dedekind domain. Then every nonzero ideal of D is invertible, making D a Prüfer domain. Also, since invertible ideals are finitely generated by part *(ii)* of Proposition 25, then D is Noetherian. Therefore, D is a Noetherian Prüfer domain.

($\Longleftarrow$) Suppose that D is a Noetherian Prüfer domain. Then every ideal of D is finitely generated and so invertible. This is exactly the definition we give for Dedekind domain in Definition 29. Therefore, D is a Dedekind domain. ■

3 The strong 2-generator property

The following definition plays a major role in the remainder of this thesis.

Definition 31 *A 2-generated fractional ideal I is* ***strongly 2-generated*** *if one of the two generators can be chosen as an arbitrary nonzero element in I. A ring in which each 2-generated ideal is strongly 2-generated is said to have the* ***strong 2-generator property****.*

We show now that, in the definition of the strong 2-generator property, we could have equivalently required that all finitely generated ideals be strongly 2-generated.

Proposition 32 *If D has the strong 2-generator property, then every finitely generated ideal of D is strongly 2-generated.*

Proof. By induction on the number of generators. For $n = 1$, the result is trivial. Suppose true for n, and let $I = Db_1 + ... + Db_n + Db_{n+1}$ for some $b_1, \ldots, b_n, b_{n+1} \in I$. Now $Db_1 + ... + Db_n = Dc + Dd$ for some $c, d \in I$ by induction so that $I = Dc + Dd + Db_{n+1}$. If $b_{n+1} = 0$, then $I = Dc + Dd$ is strongly 2-generated by assumption. Similarly, if $c = 0$, then I is strongly 2-generated. So, we can suppose that $c, b_{n+1} \neq 0$. Now $0 \neq cb_{n+1} \in Dc + Dd$ where $Dc + Dd$ is 2-generated which implies that $Dc + Dd$ is strongly 2-generated by assumption, so that $Dc + Dd = Dcb_{n+1} + Da$ for some a. Now $Dc + Dd + Db_{n+1} = Dcb_{n+1} + Da + Db_{n+1}$, but $Dcb_{n+1} \subseteq Db_{n+1}$. So, $Dcb_{n+1} + Da + Db_{n+1} = Da + Db_{n+1}$ is 2-generated and so is strongly 2-generated by assumption. This completes the induction. ∎

Proposition 33 *If I is a strongly 2-generated cancellative fractional ideal of D, then $I \ / \ IJ \cong D \ / \ J$ for any nonzero ideal J.*

Proof. Suppose that I is a strongly 2-generated cancellative fractional ideal of D. Pick any $0 \neq a \in IJ \subseteq I$. I strongly 2-generated means that $I = Da + Db$ for some $b \in I$. Define $\varphi : D \longrightarrow I \ / \ IJ$ by $\varphi(d) = d(b + IJ)$. φ is well-defined since an element of D is being mapped to its coset. φ is a D-homomorphism because for all $d, e \in D$, $\varphi(d + e) = (d + e)(b + IJ) =$

$((d+e)b)+IJ = (db+IJ)+(eb+IJ) = d(b+IJ)+e(b+IJ) = \varphi(d)+\varphi(e)$ and $\varphi(de) = (de)(b+IJ) = d(eb+IJ) = d(e(b+IJ)) = d\varphi(e)$. For any $c \in I$, $c = da+eb$ for some $d, e \in D$ because $I = (a, b)$. So, $c + IJ = da + eb + IJ = e(b + IJ) = \varphi(e) \in \text{im}(\varphi)$. So, φ is onto. Next, to show $\ker(\varphi) = J$, first to show $\ker(\varphi) \subseteq J$. Choose $d \in \ker(\varphi)$. Then $\varphi(d) = db + IJ = IJ$ implies that $db \in IJ$. But $a \in IJ$ by assumption, so $da \in IJ$, and so $dI \subseteq IJ$. Therefore, $d \in (IJ : I)$. Since $(IJ : I) = J$ by part *(ii)* of Proposition 21 (because I is assumed to be cancellative), then $\ker(\varphi) \subseteq J$. Next, to show that $J \subseteq \ker(\varphi)$, take $d \in J$, so $\varphi(d) = db + IJ = IJ$. Therefore, $d \in \ker(\varphi)$. By the First Isomorphism Theorem, $D \,/\, \ker(\varphi) \cong \text{im}(\varphi) = I \,/\, IJ$. Therefore, $I \,/\, IJ \cong D \,/\, J$ for any nonzero ideal J. ■

We will now see from the following result that, for an ideal, there is a connection between being strongly 2-generated and being invertible.

Theorem 34 *(Lantz and Martin, Theorem 1, [8]) Suppose that $I \subseteq D$ is a nonzero strongly 2-generated ideal. Then I is invertible.*

Proof. It is sufficient to show that $(D : I)I = D$. First, for the containment $(D : I)I \subseteq D$, recall that by definition, $D : I = \{q \in Q \mid qI \subseteq D\}$, so then $(D : I)I \subseteq D$ is clear. For the other containment $D \subseteq (D : I)I$, it is sufficient to show that, for each maximal ideal $M \subseteq D$, $(D : I)I \nsubseteq M$. For a given maximal ideal M, $MI \neq \{0\}$, so choose $0 \neq a \in MI$. Since I is strongly 2-generated, then $I = Da + Db$ for some $0 \neq b \in I$. Since $a \in MI$, then $I = Da + Db \subseteq MI + Db \subseteq I$, so $I = MI + Db$. So, we can write $a = ra + sb + tb$ for some $r, s \in M$ and $t \in D$. So, from $a = ra + sb + tb$, we have that $(1-r)a = (s+t)b$, where $r \in M$ which implies that $1 - r \notin M$. Then $a\frac{1-r}{b} = s + t \in D$ since $s \in M$ and $t \in D$ and M is an ideal. Also, $b\frac{1-r}{b} = 1 - r \in D$. So, $\frac{1-r}{b} \in (D : I)$. But $b\frac{1-r}{b} = 1 - r \notin M$, so $(D : I)I \nsubseteq M$. So, $D \subseteq (D : I)I$. Therefore, $(D : I)I = D$, I has an inverse, so I is invertible. ■

There is a connection between having the strong 2-generator property and being a Prüfer domain.

Corollary 35 *If D is an integral domain satisfying the strong 2-generator property, then D is a Prüfer domain.*

Proof. Suppose that $I \subseteq D$ is a 2-generated ideal. Then by assumption, I is strongly 2-generated, so by Theorem 34 I is invertible. Since all 2-generated ideals of D are invertible, then by Theorem 28 all finitely generated ideals of D are invertible. Therefore, D is a Prüfer domain. ■

Recall that $\mathcal{F}(D)$ is the set of nonzero fractional D-ideals. This set $\mathcal{F}(D)$ forms a multiplicative semigroup with identity D. The set $\mathcal{I}(D)$ consisting of all invertible fractional ideals of D is a multiplicative group and is the largest subgroup of $\mathcal{F}(D)$ whose identity is D. Furthermore, the set $\mathcal{P}(D)$ consisting of the nonzero principal fractional ideals is a multiplicative subgroup of $\mathcal{I}(D)$. Note that $I, J \in \mathcal{F}(D)$ are congruent modulo $\mathcal{P}(D)$ if and only if $J = IK$ for some $K \in \mathcal{P}(D)$ if and only if $J = \alpha I$ for some $0 \neq \alpha \in Q$ if and only if $I \cong J$ (by Proposition 5). Since $\mathcal{P}(D)$ is a normal subgroup of $\mathcal{F}(D)$, then $\mathcal{F}(D)$ modulo $\mathcal{P}(D)$ is a quotient semigroup, called the *class semigroup* of D. Furthermore, the class semigroup of D can be thought of as the semigroup of the isomorphy classes $[I] = \mathcal{P}(D)\cdot I = \{\alpha I \mid 0 \neq \alpha \in Q\} = \{J \in \mathcal{F}(D) \mid J \cong I\}$ of the fractional ideals $I \neq 0$ of D, where multiplication is induced by ideal multiplication: $[I]\cdot[J] = [I\cdot J]$. Since $\mathcal{P}(D)$ is a normal subgroup of $\mathcal{I}(D)$, then $\mathcal{I}(D)$ modulo $\mathcal{P}(D)$ is a quotient group. We call this quotient group the *(ideal) class group* (or the *Picard group*) of D.

4 Integer-valued polynomials

We begin this chapter by recalling three elementary facts about polynomials and their roots.

Theorem 36 *(Root Theorem) If $f(X)$ is a polynomial with coefficients in a field F, and $a \in F$, then $f(a) = 0$ if and only if $X - a$ divides $f(X)$.*

Proof. ($\Longrightarrow$) Suppose that $f(a) = 0$, so a is a root of $f(X)$. By the Division Algorithm. $f(X) = (X - a)\cdot q(X) + r(X)$, where $q(X), r(X) \in F[X]$, and $\deg(r(X)) < \deg(X - a) = 1$. So, $r(X)$ is a constant polynomial $r \in F$. Evaluating at a, $f(a) = (a - a)\cdot q(a) + r$. From this together with the assumption that $f(a) = 0$, we have that $0 = 0 + r = r$, so $f(X) = (X - a)\cdot q(X)$. Therefore, $X - a$ is a factor of $f(X)$, so $X - a$ divides $f(X)$.

($\Longleftarrow$) Suppose that $X - a$ divides $f(X)$, so $X - a$ is a factor of $f(X)$. Then $f(X) = (X - a)\cdot q(X)$ for some $q(X)$ with coefficients in F. Evaluating at a, $f(a) = (a - a)\cdot q(a) = 0$. Therefore, a is a root of $f(X)$, so $f(a) = 0$. ∎

Corollary 37 *(D'Alembert) A nonzero polynomial $f(X)$ of degree n in $F[X]$, F a field, has at most n distinct roots in F.*

Proof. By induction on n, the degree of $f(X)$. If $\deg(f(X)) = 0$, then f is a nonzero constant polynomial, so $f(X)$ has no roots in F. Suppose that $f(X)$ is a polynomial of degree $n > 0$, and suppose that $f(X)$ has r distinct roots $a_1, \ldots, a_r$ in F. It is sufficient to show that $r \leqslant n$. Since $f(X)$ has r distinct roots $a_1, \ldots, a_r$, then $f(a_r) = 0$, so by Theorem 36, $f(X) = (X - a_r)\cdot g(X)$, where $g(X)$ has degree $n - 1$. For each i, $1 \leqslant i \leqslant r - 1$, $f(a_i) = (a_i - a_r)\cdot g(a_i)$ in F. Since $f(a_i) = 0$ and the a_i's are distinct so that $a_i \neq a_r$, then $g(a_i) = 0$. So, $g(X)$ has roots $a_1, \ldots, a_{r-1}$. By induction, $r - 1 \leqslant n - 1 = \deg(g(X))$. Therefore, $r \leqslant n = \deg f(X)$. ∎

We will find the following consequence of D'Alembert's Theorem extremely useful in this thesis.

Corollary 38 *If $f(X)$ and $g(X)$ are polynomials with coefficients in a field F where $deg(f(X))$, $deg(g(X)) < n$ and if $f(a_i) = g(a_i)$ for n distinct elements $a_1, \ldots, a_n \in F$, then $f(X) = g(X)$ as polynomials.*

Proof. Suppose that $f(X)$ and $g(X)$ are polynomials with coefficients in F where $\deg(f(X))$, $\deg(g(X)) < n$ but $f(a_i) = g(a_i)$ for n distinct elements $a_1, \ldots, a_n \in F$. Then $\deg(f(X) - g(X)) < n$ but $f(X) - g(X)$ has n roots, so it must be the zero polynomial. Therefore, $f(X) = g(X)$ as polynomials. ■

We now define the other main object of study of this thesis, polynomials which take on restricted values on some subset of the domain. For the remainder of this thesis, we fix $E = \{a_1, \ldots, a_r\}$, a finite nonempty subset of D.

Definition 39 *Let $Int(E, D) = \{f(X) \in Q[X] \mid f(a) \in D$ for every $a \in E\}$, called* ***the set of integer-valued polynomials on D with respect to the subset E.*** *One easily checks that $Int(E, D)$ is a subring of $Q[X]$, containing $D[X]$.*

Definition 40 *Let I be an ideal of $Int(E, D)$, and let $a \in E$. We denote by $I(a) = \{f(a) \mid f(X) \in I\}$. One easily checks that $I(a)$ is an ideal of D, called the* ***ideal of values of I at a.***

We begin with a result relating the ideal structure of $\mathrm{Int}(E, D)$ to the ideal structure of D.

Proposition 41 *If $Int(E, D)$ has the strong 2-generator property, then D has the strong 2-generator property.*

Proof. Let d be a nonzero element of a 2-generated ideal I of D. Set $J = \mathrm{Int}(E, D) \cdot I$. By assumption, J is strongly 2-generated and $d \in J$, so there exists $g(X) \in J$ with $J = \mathrm{Int}(E, D) \cdot d + \mathrm{Int}(E, D) \cdot g(X)$. Evaluating at a_i for some $a_i \in E$, we get $J(a_i) = Dd + Dg(a_i)$. However, $J = \mathrm{Int}(E, D) \cdot I$ implies that $J(a_i) = I$ since elements of $\mathrm{Int}(E, D)$ evaluated at a_i are in D. Therefore, I is strongly 2-generated, so D has the strong 2-generator property. ■

Corollary 42 *If $Int(E, D)$ has the strong 2-generator property, then both $Int(E, D)$ and D are Prüfer domains.*

Proof. Follows from Proposition 41 and Corollary 35. ■

Definition 43 *An ideal I of $Int(E, D)$ is called* ***unitary*** *if $I \cap D \neq \{0\}$; that is, I contains a nonzero constant polynomial.*

We shall find the following technical fact quite useful.

Lemma 44 *(McQuillan, Lemma 2.2, [9]) Let $(0) \neq I \subsetneq Int(E, D)$ be a finitely generated non-unitary ideal. Then there are $0 \neq r \in D$, $g \in Int(E, D)$, and a unitary ideal $I_1 \subsetneq Int(E, D)$ such that $r \cdot I = g \cdot I_1$.*

Proof. Let $I = \operatorname{Int}(E, D) \cdot f_1 + \ldots + \operatorname{Int}(E, D) \cdot f_t$ (i.e., $f_1, \ldots, f_t$ generators of I as ideal of $\operatorname{Int}(E, D)$). Now $D[X] \subseteq \operatorname{Int}(E, D) \subseteq Q[X]$, where $Q[X]$ is a PID. Let $g_1 \in Q[X]$ be a gcd of $f_1, \ldots, f_t$ in $Q[X]$. Then $g_1 \cdot Q[X] = f_1 \cdot Q[X] + \ldots + f_t \cdot Q[X]$. We need an element of $D[X]$ that is a gcd of $f_1, \ldots, f_t$ in $Q[X]$. Let $0 \neq d \in D$ be a common denominator for all of the coefficients of g_1, and let $g = d \cdot g_1$. Then $g \cdot Q[X] = d \cdot g_1 \cdot Q[X] = d \cdot f_1 \cdot Q[X] + \ldots + d \cdot f_t \cdot Q[X] = f_1 \cdot Q[X] + \ldots + f_t \cdot Q[X]$. Write $f_i = g \cdot h_i$ for some $h_i \in Q[X]$. for all i. Let $0 \neq r \in D$ be a common denominator for all coefficients of all of $h_1, \ldots, h_t$. So, $r \cdot f_i = g \cdot r \cdot h_i$ where $r \cdot f_i, g, r \cdot h_i \in \operatorname{Int}(E, D)$. Now, let $I_1 = \operatorname{Int}(E, D) \cdot r \cdot h_1 + \ldots + \operatorname{Int}(E, D) \cdot r \cdot h_t \subseteq \operatorname{Int}(E, D)$. From these equations, $r \cdot I = g \cdot I_1$.

Lastly, we need to show that I_1 is unitary. For this, we will use the equations $g \cdot h_i = f_i$ for all i and $g \cdot Q[X] = f_1 \cdot Q[X] + \ldots + f_t \cdot Q[X]$. Now $g \in g \cdot Q[X]$ implies that $g = f_1 \cdot b_1 + \ldots + f_t \cdot b_t$ for some $b_1, \ldots, b_t \in Q[X]$. So, we have that $g = g \cdot h_1 \cdot b_1 + \ldots + g \cdot h_t \cdot b_t$ which implies that $1 = h_1 \cdot b_1 + \ldots + h_t \cdot b_t$. Now multiplying through by $r \cdot s$, where s is a common denominator for all of the coefficients of all of $b_1, \ldots, b_t$, we have that $0 \neq r \cdot s = (r \cdot h_1)(s \cdot b_1) + \ldots + (r h_t)(s \cdot b_t)$. Recall $I_1 = \operatorname{Int}(E, D) \cdot r \cdot h_1 + \ldots + \operatorname{Int}(E, D) \cdot r \cdot h_t \subseteq \operatorname{Int}(E, D)$, so we now have that $I_1 \cap D \neq \{0\}$. ■

Lemma 45 *The following statements are equivalent.*

(i) $Int(E, D)$ has the strong 2-generator property.

(ii) The 2-generated unitary ideals of $Int(E, D)$ are strongly 2-generated.

(iii) The 2-generated non-unitary ideals of $Int(E, D)$ are strongly 2-generated.

Proof. Clearly *(i)* is equivalent to the combination of *(ii)* and *(iii)*. We claim that *(ii)* implies *(iii)* which will then show that *(ii)* implies *(i)*. Suppose that *(ii)* holds and that I is a 2-generated non-unitary ideal of $\operatorname{Int}(E, D)$. By Lemma 44 and Proposition 5, $I \cong I_1$ for some unitary ideal I_1. Therefore, I_1 is also 2-generated. *(ii)* says I_1 is strongly 2-generated. Therefore, since $I \cong I_1$, then I is strongly 2-generated so the claim is proven.

Next, we claim that *(iii)* implies *(ii)* which will then show that *(iii)* implies *(i)*. Suppose that *(iii)* holds and that I is a 2-generated unitary ideal of $\operatorname{Int}(E, D)$. Take $f(X) \in D[X]$ with $\deg(f(X)) > 0$, and let $I_1 = f(X) \cdot I$. Then I_1 is non-unitary. Since I is 2-generated, then I_1 is also 2-generated, so *(iii)* says I_1 is strongly 2-generated. Therefore, since $I \cong I_1$, then I is strongly 2-generated so the claim is proven. This completes the proof. ■

The following is an exercise in [3] P. 90, and it gives several very useful facts about unitary ideals.

Proposition 46 *Set* $f = \Pi_{1\leqslant i\leqslant r}(X - a_i)$ *and, for* $1 \leqslant j \leqslant r$, *let* $\varphi_j = \Pi_{i\neq j}(X - a_i) \;/\; (a_j - a_i)$. *Then:*

(i) If g *is a polynomial with coefficients in* Q *and* h *is the remainder of the Euclidean division of* g *by* f, *then* $g \in Int(E, D)$ *if and only if* $h \in Int(E, D)$.

(ii) $Int(E, D) = f{\cdot}Q[X] + D\varphi_1 + \ldots + D\varphi_r$.

(iii) If $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ *are nonzero ideals of* D, *then* $I = f{\cdot}Q[X] + \mathfrak{a}_1\varphi_1 + \ldots + \mathfrak{a}_r\varphi_r$ *is an ideal of* $Int(E, D)$ *such that* $I \cap D = \cap_{1\leqslant j\leqslant r}\mathfrak{a}_j$.

(iv) Each unitary ideal I *of* $Int(E, D)$ *may be uniquely written* $I = f{\cdot}Q[X] + \mathfrak{a}_1\varphi_1 + \ldots + \mathfrak{a}_r\varphi_r$, *where* $\mathfrak{a}_j$ *are nonzero ideals of* D.

Proof. For *(i)*, suppose that $g \in Q[X]$, $g = f{\cdot}q + h$ for some $q, h \in Q[X]$, $\deg(h) < \deg(f) = r$. First, suppose that $g \in \text{Int}(E, D)$. Since $g \in \text{Int}(E, D)$, then $g(a_1), \ldots, g(a_r) \in D$. The equation now gives $g(a_i) = f(a_i){\cdot}q(a_i) + h(a_i)$ for all i. But $f(a_i) = 0$ for all i so $g(a_i) = h(a_i)$ for all i. Since $g \in \text{Int}(E, D)$ and $g(a_i) = h(a_i)$ for all i, then $h \in \text{Int}(E, D)$. Conversely, suppose that $h \in \text{Int}(E, D)$. Then $h(a_1), \ldots, h(a_r) \in D$. The equation now gives $h(a_i) = g(a_i) - f(a_i){\cdot}q(a_i)$ for all i. But $f(a_i) = 0$ for all i so $h(a_i) = g(a_i)$ for all i. Since $h \in \text{Int}(E, D)$ and $h(a_i) = g(a_i)$ for all i, then $g \in \text{Int}(E, D)$.

For *(ii)*, first, we will show that $f{\cdot}Q[X] + D\varphi_1 + \ldots + D\varphi_r \subseteq \text{Int}(E, D)$. If $f{\cdot}q \in f{\cdot}Q[X]$, $q \in Q[X]$, then $(f{\cdot}q)(a_i) = f(a_i){\cdot}q(a_i) = 0 \in D$ for all i, so $f{\cdot}q \in \text{Int}(E, D)$ meaning $f{\cdot}Q[X] \subseteq \text{Int}(E, D)$. Now given $d{\cdot}\varphi_j \in D{\cdot}\varphi_j$ for $1 \leqslant j \leqslant r$, and $d \in D$. Then $(d{\cdot}\varphi_j)(a_i) = d{\cdot}\varphi_j(a_i) = \left\{\begin{smallmatrix} 0\in D & \text{if } i\neq j \\ d\in D & \text{if } i=j \end{smallmatrix}\right.$. So, $d{\cdot}\varphi_j \in \text{Int}(E, D)$, so $D{\cdot}\varphi_j \subseteq \text{Int}(E, D)$. Therefore, $f{\cdot}Q[X] + D\varphi_1 + \ldots + D\varphi_r \subseteq \text{Int}(E, D)$. For the other containment, take $g \in \text{Int}(E, D)$. Then write $g = f{\cdot}q + h$ for some $q, h \in Q[X]$, $\deg(h) < \deg(f) = r$. Now $h \in \text{Int}(E, D)$ (by part *(i)*), and $f{\cdot}q \in Q[X]$. It is sufficient to show that $h = d_1\varphi_1 + \ldots + d_r\varphi_r$ for some $d_1, \ldots, d_r \in D$. Note that, for $d_1, \ldots, d_r \in D$, $(d_1\varphi_1 + \ldots + d_r\varphi_r)(a_i) = d_1{\cdot}\varphi_1(a_i) + \ldots + d_r{\cdot}\varphi_r(a_i) = d_i$ for each i. So, let $d_i = h(a_i) \in D$ for each i. Since both h and the φ_i's have degree at most $r - 1$, then by Corollary 38, $h = d_1\varphi_1 + \ldots + d_r\varphi_r \in D\varphi_1 + \ldots + D\varphi_r$.

For *(iii)*, suppose that $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ are nonzero ideals of D and $g \in Q[X]$.

Claim. $g \in f{\cdot}Q[X]$ if and only if $g(a_i) = 0$ for all i, $1 \leqslant i \leqslant r$. To prove the claim, first suppose that $g \in f{\cdot}Q[X]$. Then since $g = f{\cdot}h$ for some $h \in Q[X]$ and $f = \Pi_{1 \leqslant i \leqslant r}(X - a_i)$, then $g(a_i) = 0$ for all i, $1 \leqslant i \leqslant r$. For the converse, suppose that $g(a_i) = 0$ for all i, $1 \leqslant i \leqslant r$. Then we can write $g = f{\cdot}q + h$ for some $q \in Q[X]$ and $\deg(h) < \deg(f) = r$. Now evaluating at a_i, we have that $g(a_i) = f(a_i){\cdot}q(a_i) + h(a_i)$. Since $g(a_i) = 0$ and $f(a_i) = 0$ for each i, then $h(a_i) = 0$ for all i. Now by Corollary 37, h must be the zero polynomial.

I is an additive group since both $f{\cdot}Q[X]$ and $\mathfrak{a}_1\varphi_1 + \ldots + \mathfrak{a}_r\varphi_r$ are closed under sums. Now, for each j, $\varphi_j^2 - \varphi_j \in f{\cdot}Q[X]$ by the above claim, since for $i \neq j$, $\varphi_j^2(a_i) - \varphi_j(a_i) = 0 - 0 = 0$, and $\varphi_j^2(a_j) - \varphi_j(a_j) = 1 - 1 = 0$. Also, for each $i \neq j$, $\varphi_i\varphi_j \in f{\cdot}Q[X]$ since for each $i \neq j$, $(\varphi_i\varphi_j)(a_k) = 0$ for all k, $1 \leqslant k \leqslant r$. This is because if $k \neq i$, then $\varphi_i(a_k) = 0$ and if $k = i$, then $\varphi_j(a_k) = 0$. Now to show that I is closed under scalar multiplication, take $t \in \operatorname{Int}(E, D)$ and $s \in I$. By (part *(ii)*) we can write $t = f{\cdot}g + \Sigma_{j=1}^r d_j\varphi_j$, $g \in f{\cdot}Q[X]$, $d_1, \ldots, d_r \in D$ and by definition of I, $s = f{\cdot}h + \Sigma_{i=1}^r c_i\varphi_i$, $h \in f{\cdot}Q[X]$, $c_1, \ldots, c_r \in \mathfrak{a}_i$ for all i. Now $t{\cdot}s = f(fgh + g{\cdot}\Sigma_{i=1}^r c_i\varphi_i + h{\cdot}\Sigma_{j=1}^r d_j\varphi_j) + (\Sigma_{i,j} c_i d_j \varphi_i \varphi j)$. As just noted, $c_i d_j \varphi_i \varphi_j \in f{\cdot}Q[X]$ for $i \neq j$. For $i = j$, write $c_i d_i \varphi_i^2 = c_i d_i(\varphi_i^2 - \varphi_i) + c_i d_i \varphi_i$. Since $(\varphi_i^2 - \varphi_i) \in f{\cdot}Q[X]$, then $c_i d_i(\varphi_i^2 - \varphi_i) \in f{\cdot}Q[X]$ and since $c_i{\cdot}\varphi_i \in \mathfrak{a}_i{\cdot}\varphi_i$, then $c_i d_i \varphi_i \in \mathfrak{a}_1\varphi_1 + \ldots + \mathfrak{a}_r\varphi_r$. So, $c_i d_i \varphi_i^2 \in I$. Therefore, I is closed under scalar multiplication and hence an ideal.

Lastly, we claim $I \cap D = \cap_{1 \leqslant j \leqslant r}\mathfrak{a}_j$. First, take $b \in I \cap D$. Then b is a constant polynomial. Also, we can write $b = f{\cdot}g + c_1\varphi_1 + \ldots + c_r\varphi_r$ for some $g \in Q[X]$, $c_i \in \mathfrak{a}_i$ for each i by definition of I. It is sufficient to show that $b \in \mathfrak{a}_i$ for all i. Evaluating at a_i, we have that $b = 0{\cdot}g(a_i) + c_1{\cdot}0 + \ldots + c_i{\cdot}1 + \ldots + c_i{\cdot}0 = c_i$ which implies that $b = c_i \in \mathfrak{a}_i$. Lastly, for the other containment, take $a \in \cap_{1 \leqslant j \leqslant r}\mathfrak{a}_j$. Then $a = a\varphi_1 + \ldots + a\varphi_r$. This is because, by Corollary 38, since both a and $a\varphi_1 + \ldots + a\varphi_r$ are polynomials, $\deg(a) \leqslant 0$ and $\deg(a\varphi_1 + \ldots + a\varphi_r) \leqslant r - 1$ (so both have degree less than r), then evaluating both a and $a\varphi_1 + \ldots + a\varphi_r$ at a_i, we get a on the left-hand side and a on the right-hand side. Now $a \in I$ because, using the fact that for each $a \in \cap_{1 \leqslant j \leqslant r}\mathfrak{a}_j$, $a = a\varphi_1 + \ldots + a\varphi_r$, $a \in \mathfrak{a}_1\varphi_1 + \ldots + \mathfrak{a}_r\varphi_r$ and $a \in D$ because $a \in \cap_{1 \leqslant j \leqslant r}\mathfrak{a}_j$, so $a \in I \cap D$. Therefore, $I \cap D = \cap_{1 \leqslant j \leqslant r}\mathfrak{a}_j$.

For *(iv)*, let $I \subseteq \operatorname{Int}(E, D)$ be a unitary ideal. Let $\mathfrak{a}_j = I(a_j) = \{g(a_j) \mid g \in I\} \subseteq D$ ($g(a_j) \in D$ for $g \in I$ because $I \subseteq \operatorname{Int}(E, D)$). We now show that $\mathfrak{a}_j \neq (0)$ is an ideal of D. First, this is because $\mathfrak{a}_j$ is nonempty since, by definition, I is nonempty being an ideal. Also, $\mathfrak{a}_j$ is closed under addition, because, given $b, c \in \mathfrak{a}_j$, there is $g, h \in I$ such that $g(a_j) = b$ and $h(a_j) = c$ so that

$b + c = (g + h)(a_j) \in \mathfrak{a}_j$ because $g + h \in I$. Similarly, for negatives, given $d \in \mathfrak{a}_j$, there is $m \in I$ such that $m(a_j) = d$ so that $-d = (-m)(a_j) \in \mathfrak{a}_j$ because $-m \in I$. So, $\mathfrak{a}_j$ is nonempty and closed under addition and negatives. For scalar multiplication, take $d \in D$ and $b \in \mathfrak{a}_j$ so $b = g(a_j)$ some $g \in I$. We want to look at $d{\cdot}g$. Now $d{\cdot}g \in I$ because $d \in \text{Int}(E, D)$, $g \in I$, and I is an ideal. So, $(d{\cdot}g)(a_j) = d{\cdot}g(a_j) = d{\cdot}b$ and so $(d{\cdot}g)(a_j) \in \mathfrak{a}_j$. Next, we show that $\mathfrak{a}_j \neq (0)$. Since $I \cap D \neq (0)$, then let $0 \neq c \in I \cap D$. Now $c = c(a_j) \in \mathfrak{a}_j$, so $\mathfrak{a}_j \neq (0)$. Therefore, $\mathfrak{a}_j \neq (0)$ is an ideal of D. Given I, form the sum $f{\cdot}Q[X] + \mathfrak{a}_1\varphi_1 + \ldots + \mathfrak{a}_r\varphi_r$ which is an ideal in $\text{Int}(E, D)$ by part *(iii)*.

Next, for the existence, we show that $I = f{\cdot}Q[X] + \mathfrak{a}_1\varphi_1 + \ldots + \mathfrak{a}_r\varphi_r$. For this, we claim that $f{\cdot}Q[X] \subseteq I$. Note that $f{\cdot}Q[X] \subseteq \text{Int}(E, D)$ because $(f{\cdot}q)(a_j) = (f(a_j)){\cdot}(q(a_j)) = 0 \in D$ for all j. $I \cap D \neq (0)$, so take $0 \neq c \in I \cap D$. So, $\frac{1}{c} \in Q$. Then for any $q \in Q[X]$, $f{\cdot}q = c{\cdot}\frac{1}{c}{\cdot}f{\cdot}q = c{\cdot}f{\cdot}(\frac{1}{c}{\cdot}q) \in I$ because I is an ideal. Now it is sufficient to show that $\mathfrak{a}_1\varphi_1 + \ldots + \mathfrak{a}_r\varphi_r \subseteq I$ for each i. For this, let $c \in \mathfrak{a}_i$. There is $g \in I$ such that $g(a_i) = c$. Then $g{\cdot}\varphi_i \in I$. Dividing $g{\cdot}\varphi_i$ by f, we have that $g{\cdot}\varphi_i = f{\cdot}q + h$ where $\deg(h) < \deg(f) = r$. Note that $h \in I$ because $g{\cdot}\varphi_i, f{\cdot}q \in I$. Now $h(a_j) = 0$ if $j \neq i$ and $h(a_j) = c$ if $j = i$. Also note that $c{\cdot}\varphi_i(a_j) = 0$ if $j \neq i$ and $c{\cdot}\varphi_i(a_j) = c$ if $j = i$. Comparing h and $c{\cdot}\varphi_i$, we see that $h = c{\cdot}\varphi_i$ by Corollary 38, because $\deg(h)$, $\deg(c{\cdot}\varphi_i) \leqslant r - 1$ but agree on $a_1, \ldots, a_r$. So, $c{\cdot}\varphi_i \in I$ for each i as desired, and hence $\mathfrak{a}_1\varphi_1 + \ldots + \mathfrak{a}_r\varphi_r \subseteq I$. For the other containment, take a polynomial $g \in I$. Again, dividing g by f, we have that $g = f{\cdot}q + h$ where $\deg(h) < \deg(f) = r$. We need to show that $h \in \mathfrak{a}_1\varphi_1 + \ldots + \mathfrak{a}_r\varphi_r$. Let $c_i = g(a_i)$ for each i. Then $c_i \in \mathfrak{a}_i$, and we have that $h(a_i) = (g - f{\cdot}q)(a_i) = g(a_i) = c_i$ and $(c_1\varphi_1 + \ldots + c_r\varphi_r)(a_i) = c_i\varphi_i(a_i) = c_i$. This implies that $h = c_1\varphi_1 + \ldots + c_r\varphi_r$ by Corollary 38.

For uniqueness, suppose that $I = f{\cdot}Q[X] + \Sigma_{j=1}^{r}\mathfrak{B}_j\varphi_j$ for some ideals $\mathfrak{B}_1, \ldots, \mathfrak{B}_r \subseteq D$. Recall I is an ideal of $\text{Int}(E, D)$ and $I \cap D \neq (0)$. It is sufficient to show that $\mathfrak{B}_j = I(a_j)$ for all j. First, take $c \in \mathfrak{B}_j$. Then $c{\cdot}\varphi_j \in I$ and $(c{\cdot}\varphi_j)(a_j) = c{\cdot}1 = c$, so $c \in I(a_j)$. For the other containment, take $c \in I(a_j)$. Then $c = g(a_j)$ for some $g \in I$. Now write $g = f{\cdot}q + c_1{\cdot}\varphi_1 + \ldots + c_r{\cdot}\varphi_r$ for some $q \in Q[X]$, $c_i \in \mathfrak{B}_i$ for each i. So, $c = g(a_j) = f(a_j){\cdot}q(a_j) + c_1{\cdot}\varphi_1(a_j) + \ldots + c_r{\cdot}\varphi_r(a_j) = c_j \in \mathfrak{B}_j$. Therefore, $\mathfrak{B}_j = I(a_j)$ for all j. ■

We now characterize the property specified by the last part of this proposition in the following definition.

Definition 47 *Int(E, D) is said to have the* ***almost strong Skolem property*** *if whenever I and J are finitely generated unitary ideals of Int(E, D) such that $I(a) = J(a)$ for every $a \in E$, then*

$I = J$.

As a result of Proposition 46, we have the following corollary.

Corollary 48 *Int(E, D) has the almost strong Skolem property.*

Using Proposition 46, we can show that the idea of integer-valued polynomials gives us a method for constructing new Prüfer domains from old ones.

Theorem 49 *If E is a finite nonempty subset of D, then D is a Prüfer domain if and only if Int(E, D) is a Prüfer domain.*

Proof. ($\Rightarrow$) Suppose that D is a Prüfer domain. Let I be a nonzero, finitely generated ideal of $\mathrm{Int}(E, D)$. Since I is isomorphic to a unitary ideal by Proposition 5 and Lemma 44, then it is sufficient to show that I is invertible if I is unitary. Then $I = f{\cdot}Q[X] + \Sigma_{i=1}^{r} I(a_i)\varphi_i$ (from Proposition 46*(iii)*). Each $I(a_i)$ is a finitely generated nonzero ideal of D. Since D is a Prüfer domain by assumption, then $I(a_i)$ is invertible. Recall that, by Proposition 46*(ii)*, $f{\cdot}Q[X] \subseteq \mathrm{Int}(E, D)$. Also, since $I{\cdot}Q[X] \subseteq Q[X]$, then $I{\cdot}f{\cdot}Q[X] \subseteq f{\cdot}Q[X]$. So, we have that $I{\cdot}f{\cdot}Q[X] \subseteq f{\cdot}Q[X] \subseteq \mathrm{Int}(E, D)$. Using this and that $I = f{\cdot}Q[X] + \Sigma_{i=1}^{r} I(a_i)\varphi_i$, we now have that, for each index i, $I{\cdot}I(a_i)^{-1}{\cdot}\varphi_i \subseteq f{\cdot}Q[X] + I(a_i){\cdot}I(a_i)^{-1}{\cdot}\varphi_i^2 \subseteq \mathrm{Int}(E, D)$.

So, $f{\cdot}Q[X] + \Sigma_{i=1}^{r} I(a_i)^{-1}\varphi_i \subseteq I^{-1}$. Using that $\Sigma_{i=1}^{r} I(a_i)^{-1}\varphi_i \subseteq I^{-1}$ and that, by Corollary 38, $1 = \Sigma_{i=1}^{r}\varphi_i$, it is sufficient to show that, for each i, $\varphi_i \in II^{-1}$. Since $\varphi_i^2 \in I(a_i)\varphi_i{\cdot}I(a_i)^{-1}\varphi_i \subseteq II^{-1}$, then $\varphi_i^2 \in II^{-1}$. In addition, recall from the proof of Proposition 46*(iii)*, that $\varphi_i^2 - \varphi_i \in f{\cdot}Q[X]$, so it is sufficient to show that $f{\cdot}Q[X] \subseteq II^{-1}$. For $q \in Q[X]$, $fq = \Sigma_{i=1}^{r} fq{\cdot}\varphi_i = \Sigma_{i=1}^{r} b_i\varphi_i(b_i^{-1}{\cdot}fq) \in II^{-1}$, where $0 \neq b_i \in I(a_i)$ for each i, since $b_i\varphi_i \in I(a_i){\cdot}\varphi_i \subseteq I$ and $b_i^{-1}{\cdot}fq \in f{\cdot}Q[X] \subseteq I^{-1}$. So, $f{\cdot}Q[X] \subseteq II^{-1}$. Therefore, I is invertible, so $\mathrm{Int}(E, D)$ is a Prüfer domain.

($\Leftarrow$) Suppose that $\mathrm{Int}(E, D)$ is a Prüfer domain. Let $I = Db_1 + \ldots + Db_n$ be a nonzero ideal of D, and set $J = \mathrm{Int}(E, D){\cdot}b_1 + \ldots + \mathrm{Int}(E, D){\cdot}b_n$. Since $\mathrm{Int}(E, D)$ is a Prüfer domain by assumption, then J is invertible, so $JJ^{-1} = \mathrm{Int}(E, D)$. Therefore, we have $1 = g_1h_1 + \ldots + g_th_t$ for some $g_1, \ldots, g_t \in J$, $h_1, \ldots, h_t \in J^{-1}$. Since we set $J = \mathrm{Int}(E, D){\cdot}b_1 + \ldots + \mathrm{Int}(E, D){\cdot}b_n$, then we have that, for each index i, $g_i = k_1b_1 + \ldots + k_nb_n$ for some $k_1, \ldots, k_n \in \mathrm{Int}(E, D)$. Evaluating at a_1, we have that $g_i(a_1) = k_1(a_1){\cdot}b_1 + \ldots + k_n(a_1){\cdot}b_n \in I$. Since $h_1, \ldots, h_t \in J^{-1}$, then $h_iJ \subseteq \mathrm{Int}(E, D)$. Again since we set $J = \mathrm{Int}(E, D){\cdot}b_1 + \ldots + \mathrm{Int}(E, D){\cdot}b_n$, then we now have that $h_ib_1 \in \mathrm{Int}(E, D) \subseteq Q[X]$, so $h_i \in Q[X]$. Also, for all indices j, $h_ib_j \in \mathrm{Int}(E, D)$, and evaluating at

a_1, we have that, for all indices j, $h_i(a_1)\cdot b_j \in D$. Then we have $h_i(a_1) \in I^{-1}$. Plugging a_1 into the equation $1 = g_1h_1 + \ldots + g_th_t$, we get that $1 = g_1(a_1)h_1(a_1) + \ldots + g_t(a_1)h_t(a_1)$, where $g_1(a_1), \ldots, g_t(a_1) \in I$ and $h_1(a_1), \ldots, h_t(a_1) \in I^{-1}$. Therefore, I is invertible, so D is a Prüfer domain. ■

Making use of the almost strong Skolem property, we can take Proposition 41 a step further.

Proposition 50 *(i) If Int(E, D) has the 2-generator property, then D has the 2-generator property. (ii) If D has the strong 2-generator property, then Int(E, D) has the 2-generator property.*

Proof. For *(i)*, let $I = D\cdot c_1 + \ldots + D\cdot c_n$ for some $c_1, \ldots, c_n \in I$. Let $J = \text{Int}(E, D)\cdot I = \text{Int}(E, D)\cdot c_1 + \ldots + \text{Int}(E, D)\cdot c_n$. So, $J = \text{Int}(E, D)\cdot g(X) + \text{Int}(E, D)\cdot j(X)$ for some $g(X), j(X) \in J$. Now $J(a_1) = \{h(a_1) \mid h \in J\}$. We need to show that $I = J(a_1) = D\cdot g(a_1) + D\cdot j(a_1)$. For the first equality, take $w \in I$. Then $w = d_1\cdot c_1 + \ldots + d_n\cdot c_n$ for some $d_1, \ldots, d_n \in D$. But $c_1, \ldots, c_n \in J$ by definition, and $d_1, \ldots, d_n \in D \subseteq \text{Int}(E, D)$, so $w = d_1\cdot c_1 + \ldots + d_n\cdot c_n \in J$, where $w = w(a_1) \in J(a_1)$. For the other containment, take $h(a_1) \in J(a_1)$, where $h \in J$. So, $h(X) = b_1(X)c_1 + \ldots + b_n(X)c_n$ for some $b_1, \ldots, b_n \in \text{Int}(E, D)$. Now $h(a_1) = b_1(a_1)c_1 + \ldots + b_n(a_1)c_n \in I$ since $b_1(a_1), \ldots, b_n(a_1) \in D$ and $c_1, \ldots, c_n \in I$. Therefore, $I = J(a_1)$. For the second equality, take $h(a_1) \in J(a_1)$, where $h \in J$, so that $h = r\cdot g + s\cdot j$ for some $r, s \in \text{Int}(E, D)$. Then $h(a_1) = r(a_1)\cdot g(a_1) + s(a_1)\cdot j(a_1) \in D\cdot g(a_1) + D\cdot j(a_1)$. For the other containment, take $d_1\cdot g(a_1) + d_2\cdot j(a_1)$ for some $d_1, d_2 \in D \subseteq \text{Int}(E, D)$. Now $d_1\cdot g(X) + d_2\cdot j(X) \in J$ so that $d_1\cdot g(a_1) + d_2\cdot j(a_1) \in J(a_1)$. Therefore, $J(a_1) = D\cdot g(a_1) + D\cdot j(a_1)$, so D has the 2-generator property.

For *(ii)*, suppose that D has the strong 2-generator property. Let $I \subseteq \text{Int}(E, D)$ be a finitely generated ideal. By Lemma 44 and Proposition 5, $I \cong I_1$ for some unitary ideal $I_1 \subseteq \text{Int}(E, D)$. It is sufficient to show that I_1 is 2-generated. Recall $f = \Pi_{1 \leqslant i \leqslant r}(X - a_i)$ and, for $1 \leqslant j \leqslant r$, $\varphi_j = \Pi_{i \neq j}(X - a_i)/(a_j - a_i)$, from Proposition 46. If $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ are nonzero ideals of D, then $I_1 = f\cdot Q[X] + \Sigma_{i=1}^r \mathfrak{a}_i\cdot\varphi_i$ is an ideal of $\text{Int}(E, D)$ such that $I_1 \cap D = \mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_r \neq \{0\}$ where $\mathfrak{a}_i = I_1(a_i)$ for each i (by part *(iii)* of Proposition 46). I_1 is a finitely generated (because I is finitely generated and $I \cong I_1$) $\text{Int}(E, D)$-ideal so $\mathfrak{a}_i = I_1(a_i)$ for each i is a finitely generated D-ideal. Since D has the strong 2-generator property, then by Proposition 32 every finitely generated ideal of D is strongly 2-generated. So, each $\mathfrak{a}_i$ is strongly 2-generated. Since $\{0\} \neq I_1 \cap D = \mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_r \subseteq \mathfrak{a}_i$, then choose $0 \neq b \in \mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_r \subseteq \mathfrak{a}_i$. Then $\mathfrak{a}_i = D\cdot b + D\cdot c_i$ for some $c_i \in \mathfrak{a}_i$ for each i. Let $J = \text{Int}(E, D)\cdot b + \text{Int}(E, D)\cdot(\Sigma_{i=1}^r c_i\varphi_i)$. J is unitary because $0 \neq b \in J \cap D$. It is sufficient to show that $J(a_i) = I_1(a_i)$ for each i because then $J = I_1$ (by the almost strong Skolem property) which implies that I_1 is also 2-generated. For this, since $\mathfrak{a}_i = I_1(a_i)$ for each i, then it is sufficient to show that $\mathfrak{a}_i = J(a_i)$ for each i. For the containment $\mathfrak{a}_i \subseteq J(a_i)$, take $d_1 \cdot b + d_2 \cdot c_i \in \mathfrak{a}_i$ for some $d_1, d_2 \in D$. Since $d_1, d_2 \in \text{Int}(E, D)$, then $d_1 \cdot b + d_2 \cdot (\Sigma_{i=1}^{r} c_i \varphi_i) \in J$. After plugging in a_i, we have that $d_1 \cdot b + d_2 \cdot c_i \in J(a_i)$. For the containment $J(a_i) \subseteq \mathfrak{a}_i$, take $g \cdot b + h \cdot (\Sigma_{i=1}^{r} c_i \varphi_i) \in J$ for some $g, h \in \text{Int}(E, D)$. Then $g(a_i) \cdot b + h(a_i) \cdot (\Sigma_{i=1}^{r} c_i \varphi_i(a_i)) = g(a_i) \cdot b + h(a_i) \cdot c_i \in \mathfrak{a}_i$ since $g(a_i), h(a_i) \in D$. So, $\mathfrak{a}_i = J(a_i)$ for each i, so $J(a_i) = I_1(a_i)$ for each i. Therefore, $J = I_1$ (by the almost strong Skolem property) which implies that I_1 is also 2-generated. ■

5 The main theorem

The main theorem further connects the ideal structure of $\mathrm{Int}(E, D)$ with the ideal structure of D.

Theorem 51 *(Chapman, Loper, and Smith, [5]) Let D be an integral domain and $E = \{a_1, \ldots, a_r\}$ a finite nonempty subset of D. Then $\mathrm{Int}(E, D)$ has the strong 2-generator property if and only if D is a Bézout domain.*

Proof. ($\Rightarrow$) Suppose that $\mathrm{Int}(E, D)$ has the strong 2-generator property. Recall from Proposition 46, the polynomial $f(X) = (X - a_1)\cdot(X - a_2)\cdots(X - a_r)$. If $r(X)$ is a polynomial in $Q[X]$, then $r(X)\cdot f(X) \in I$ for every unitary ideal $I \subseteq \mathrm{Int}(E, D)$, by Proposition 46*(iv)*. In particular, $f(X)$ is in each unitary ideal of $\mathrm{Int}(E, D)$.

Note that, by a straightforward induction, if all 2-generated ideals of D are principal, then all finitely generated ideals of D are principal. So, it is sufficient to show that all 2-generated ideals of D are principal. Let $\{0\} \neq J = Dd_1 + Dd_2 \subseteq D$ be a 2-generated ideal of D, and set $J_1 = \mathrm{Int}(E, D)\cdot J = \mathrm{Int}(E, D)\cdot d_1 + \mathrm{Int}(E, D)\cdot d_2$. Then J_1 is a finitely generated unitary ideal because $J \subseteq J_1$. So, $f(X) \in J_1$, and so $J_1 = \mathrm{Int}(E, D)\cdot f + \mathrm{Int}(E, D)\cdot g$ for some $g \in J_1$ since $\mathrm{Int}(E, D)$ has the strong 2-generator property by assumption. Fix an index i. Now, $J = J_1(a_i) = D\cdot f(a_i) + D\cdot g(a_i) = D\cdot g(a_i)$ (since $f(a_i) = 0$). So, J is principal. Therefore, all 2-generated ideals of D are principal so that all finitely generated ideals of D are principal.

($\Leftarrow$) Suppose that D is a Bézout domain. Let J be a 2-generated unitary ideal of $\mathrm{Int}(E, D)$. For each $1 \leqslant i \leqslant r$, let b_i be an element of D such that $Db_i = J(a_i)$ (using the assumption that D is a Bézout domain). Since J is unitary, then $b_i \neq 0$ for each i by part *(iv)* of Proposition 46. Choose a nonzero polynomial $s(X) \in J$. Recall that from Proposition 46, for each $1 \leqslant j \leqslant r$, $\varphi_j(X) = \Pi_{i \neq j}(X - a_i) \ / \ (a_j - a_i)$ and $\varphi_j(a_j) = 1$ and $\varphi_j(a_i) = 0$ when $i \neq j$, hence each $\varphi_j(X) \in \mathrm{Int}(E, D)$. If $t(X) = \Sigma_{i=1}^{r} b_i \cdot \varphi_i(X)$, then $t(X) \in \mathrm{Int}(E, D)$ and $t(a_i) = b_i$ for each $1 \leqslant i \leqslant r$. We have two cases to consider.

<u>Case 1</u>: Suppose that $t(X)$ is relatively prime to $s(X)$ over $Q[X]$. We claim that $J = \mathrm{Int}(E, D)\cdot s + \mathrm{Int}(E, D)\cdot t$. Now $s(X)\cdot u(X) + t(X)\cdot v(X) = 1$ for some $u, v \in Q[X]$. Let $0 \neq d \in D$ be

a common denominator for all of the coefficients of u and v. Let $I = \text{Int}(E, D)\cdot s+ \text{Int}(E, D)\cdot t$. Multiplying through by d, we have that $s(X)\cdot d\cdot u(X) + t(X)\cdot d\cdot v(X) = d$ and $d\cdot u(X), d\cdot v(X) \in D[X] \subseteq \text{Int}(E, D)$ so that $s(X)\cdot d\cdot u(X) + t(X)\cdot d\cdot v(X) \in I$. Since $s(X)\cdot d\cdot u(X) + t(X)\cdot d\cdot v(X) \in I$ and $s(X)\cdot d\cdot u(X) + t(X)\cdot d\cdot v(X) = d$, then $d \in I$. Since $d \in D$ and $d \in I$, then $0 \neq d \in I \cap D$, so I is unitary. It is sufficient to show that $I(a_i) = J(a_i)$ for each $1 \leqslant i \leqslant r$ for then the almost strong Skolem property gives $I = J$. For this, note that $J(a_i) = D\cdot b_i$ for each i by definition so it is now sufficient to show that $I(a_i) = D\cdot b_i$ for each i. First, for the containment $I(a_i) \subseteq D\cdot b_i$, using $I = \text{Int}(E, D)\cdot s+ \text{Int}(E, D)\cdot t$, $I(a_i) = D\cdot s(a_i) + D\cdot t(a_i) \subseteq D\cdot b_i$ because $s(a_i) \in J(a_i)$ and $t(a_i) = b_i$. For the containment $D\cdot b_i \subseteq I(a_i)$, $I(a_i) = D\cdot s(a_i) + D\cdot t(a_i) \supseteq D\cdot b_i$ because $t(a_i) = b_i$. Now by the almost strong Skolem property, $I = J$.

Case 2: Suppose that $t(X)$ is not relatively prime to $s(X)$ over $Q[X]$. We claim that $J = \text{Int}(E, D)\cdot s+ \text{Int}(E, D)\cdot t_1$ for some polynomial $t_1 \in J$. Let $u(X)$ be a greatest common divisor of $s(X)$ and $t(X)$ over $Q[X]$. Let $s(X) = s_1(X)\cdot s_2(X)$ be a factorization in $Q[X]$ such that $\gcd(s_1(X), s_2(X)) = 1$ and $s_1(X)$ has exactly the same irreducible factors that $u(X)$ does. For all irreducible $\pi(X) \in Q[X]$, if $\pi(X) \mid t(X)$ and $\pi(X) \mid s(X)$, then $\pi(X) \mid u(X)$ because $u(X)$ is the greatest common divisor of $s(X)$ and $t(X)$. Then $\pi(X) \mid s_1(X)$ because $\pi(X)$ is irreducible and $s_1(X)$ has exactly the same irreducible factors that $u(X)$ has, so $\pi(X) \nmid s_2(X)$. On the other hand, if $\pi(X) \mid t(X)$ but $\pi(X) \nmid s(X)$, then $\pi(X) \nmid s_2(X)$. So, $\gcd(t(X), s_2(X)) = 1$ in $Q[X]$. Since $t(a_i) \neq 0$ for each i, then by Theorem 36 $(X - a_i) \nmid t(X)$. Recall that $f(X) = (X - a_1)\cdot(X - a_2)\cdots(X - a_r)$. So, it follows that $\gcd(t(X), f(X)) = 1$. Now, let $t_1(X) = t(X) + s_2(X)\cdot f(X)$. Ultimately, we want to show that $\gcd(t_1(X), s(X)) = 1$. Since $t(X) \in \text{Int}(E, D)$ and $s_2(X)\cdot f(X) \in \text{Int}(E, D)$, then $t_1(X) \in \text{Int}(E, D)$. Suppose that $\pi(X)$ is an irreducible factor of $s(X)$ over $Q[X]$. Then we have two subcases because, by how $s(X)$ is defined, either $\pi(X) \mid s_1(X)$ or $\pi(X) \mid s_2(X)$.

Subcase 1: $\pi(X) \mid s_1(X)$. Then $\pi(X) \mid t(X)$ because $s_1(X)$ has exactly the same irreducible factors that $u(X)$ has, and $u(X) \mid t(X)$. But $\pi(X) \nmid s_2(X)$ and $\pi(X) \nmid f(X)$ because $\gcd(t(X), f(X)) = 1$. Therefore, $\pi(X) \nmid t(X) + s_2(X)\cdot f(X)$.

Subcase 2: $\pi(X) \mid s_2(X)$. Since $\gcd(t(X), s_2(X)) = 1$, then $\pi(X) \nmid t(X)$. Therefore, $\pi(X) \nmid t(X) + s_2(X)\cdot f(X)$ here as well.

But $t_1(a_i) = t(a_i) + s_2(a_i)\cdot f(a_i) = t(a_i)$ for each i since $f(a_i) = 0$ for each i. Now as in Case 1, except using $t_1(X)$ in place of $t(X)$, $I = \text{Int}(E, D)\cdot t_1+ \text{Int}(E, D)\cdot s$ is a unitary ideal of $\text{Int}(E, D)$ for which $I(a_i) = J(a_i)$ for each $1 \leqslant i \leqslant r$. So, again $I = J$ by the almost strong Skolem property.

Therefore, the 2-generated unitary ideals of $\text{Int}(E, D)$ are strongly 2-generated. By Lemma 45, all the 2-generated ideals of $\text{Int}(E, D)$ are strongly 2-generated. ■

References

[1] A. Aczel, Fermat's Last Theorem. Four Walls Eight Windows, New York, NY (1996).

[2] D. Brizolis, "A theorem on ideals in Prüfer rings of integer-valued polynomials." Comm. in Algebra 7, 1065-1077 (1979).

[3] P.-J. Cahen and J.-L. Chabert, Integer-Valued Polynomials. Amer. Math Soc. Surveys and Monographs 48, Providence 1997.

[4] H. Cartan and S. Eilenberg, Homological Algebra. Princeton University Press, Princeton, NJ (1956).

[5] S. T. Chapman, A. Loper, and W. W. Smith, "The strong 2-generator property in rings of integer-valued polynomials determined by finite sets." Arch. Math. 78, 373-377 (2002).

[6] A. Clark, Elements of Abstract Algebra. Wadsworth Publishing Company, Inc., Belmont, CA (1971).

[7] L. Fuchs and L. Salce, Modules over Non-Noetherian Domains. Amer. Math. Soc., Providence, RI (2001).

[8] D. Lantz and M. Martin, "Strongly 2-generated ideals." Comm. Algebra 16, 1759-1777 (1988).

[9] D. L. McQuillan,"On Prüfer domains of polynomials." J. Reine Angew. Math. 358, 162-178 (1985).

[10] E. Noether, "Abstrakter Aufbau der Idealtheorie in algebraischen Zahl-und Funktionenkörpern." Math. Ann. 96, 26-61 (1927).

[11] A. Ostrowski, "Über ganzwertige Polynome in algebraischen Zahlkörpern." J. reine angew. Math 149, 117-124 (1919).

[12] G. Polya, "Über ganzwertige Polynome in algebraischen Zahlkörpern." J. reine angew. Math 149, 97-116 (1919).

[13] H. Prüfer, "Untersuchungen über die Teilbzurkeitseigenschaften in Körpern." J. Reine Angew Math 168, 1-36 (1932).

[14] Th. Skolem, "Ein Satz über ganzwertige Polynome." Det Kongelige Norske Videnskabers Selskab (Trondheim) 9, 111-113 (1936).