

---

# Robert Gilmer's Contributions to the Theory of Integer-Valued Polynomials

Scott T. Chapman<sup>1\*</sup>, Vadim Ponomarenko<sup>2</sup> and William W. Smith<sup>3</sup>

<sup>1</sup> Trinity University, Department of Mathematics, One Trinity Place, San Antonio, TX 78212-7200, [schapman@trinity.edu](mailto:schapman@trinity.edu)

<sup>2</sup> Trinity University, Department of Mathematics, One Trinity Place, San Antonio, TX 78212-7200, [vadim123@gmail.com](mailto:vadim123@gmail.com)

<sup>3</sup> The University of North Carolina at Chapel Hill, Department of Mathematics, Chapel Hill, North Carolina 27599-3250, [wsmith@email.unc.edu](mailto:wsmith@email.unc.edu)

## 1 Robert Gilmer and $\text{Int}(E, D)$

It is fitting in a volume dedicated to Robert Gilmer's work in commutative algebra that special mention be made of his contributions to the theory of integer-valued polynomials. To remind the reader, if  $D$  is an integral domain with quotient field  $K$  and  $E \subseteq D$  a subset of  $D$ , then let

$$\text{Int}(E, D) = \{f(X) \in K[X] \mid f(a) \in D \text{ for every } a \in E\}$$

denote the ring of integer-valued polynomials on  $D$  with respect to the subset  $E$  (for ease of notation, if  $E = D$ , then set  $\text{Int}(D, D) = \text{Int}(D)$ ). Gilmer's work in this area (with the assistance of various co-authors) was truly groundbreaking and led to numerous extensions and generalizations by authors such as J. L. Chabert, P. J. Cahen, D. McQuillan and A. Loper. In this paper, we will review Gilmer's papers dedicated to this subject. We close with an elementary analysis of polynomial closure in integral domains, a topic which Gilmer motivated with a characterization of which subsets  $S$  of  $\mathbb{Z}$  define the ring  $\text{Int}(\mathbb{Z})$  in [18]. Before proceeding, please note that we use  $\mathbb{Q}$  to represent the rationals,  $\mathbb{Z}$  the integers,  $\mathbb{N}$  the natural numbers and  $\mathbb{P}$  the primes in  $\mathbb{Z}$ .

It is clear that Gilmer's interest in the rings  $\text{Int}(E, D)$  was motivated by his early work on multiplicative ideal theory and the theory of Prüfer domains. In particular, there was a problem open in the early 60's regarding the number of required generators for a finitely generated ideal of a Prüfer domain. It was at the time well known in the Noetherian case (i.e., for a Dedekind domain) that every ideal could be generated by two elements, one of which could be chosen to be an arbitrary non-zero element of the ideal.

---

\* Part of this work was completed while the first author was on an Academic Leave granted by the Trinity University Faculty Development Committee.

Whether or not this property extended to the finitely generated ideals of a Prüfer domain (the non-Noetherian case) was the subject of much inquiry for over two decades. Evidence of this work, often determining cases where the property held, can be found in a 1970 paper of Gilmer and Heinzer [20]. There was much work on this problem during the subsequent years. Notable results were those by Sally and Vasconcelos [42] where it was established that for a one-dimensional Prüfer domain, every finitely generated ideal could be generated by two elements, with one chosen arbitrarily. Later, Heitman and Levy [27] gave an example of a Prüfer domain where the finitely generated ideals were 2-generated, yet one generator could not be chosen arbitrarily. About the same time, Heitman [26] extended the Sally and Vasconcelos results by showing in an  $n$ -dimensional Prüfer domain every finitely generated ideal could be generated by  $n + 1$  elements. Schulting [43] gave the first example of an invertible ideal in a Prüfer domain which required more than 2-generators. Finally, Swan [44] provided a construction for each positive integer  $n > 1$  of a Prüfer domain of dimension  $n$  which contains a finitely generated ideal requiring  $n + 1$  generators. In the examples just mentioned, the Prüfer domains are described as intersections of valuation domains and the reasoning used involved geometric techniques beyond those of basic commutative ideal theory. Hence, even after the basic question of generators of finitely generated ideals in Prüfer domains was answered, there were two very general problems of interest to ideal theorists. These were described in the recent work “Non-Noetherian Commutative Ring Theory” [13] [14] and formulated based on work in a paper of Loper [33] as follows:

- (A) [14, Problem 76] Let  $K$  be a field, and let  $\{V_i\}$  be a set of valuation domains all of which have quotient fields equal to  $K$ . Give necessary and sufficient conditions on the set  $\{V_i\}$ , so that  $\bigcap V_i$  is a Prüfer domain with quotient field  $K$ .
- (B) [14, Problem 77] The proof of Swan’s result cited above [44] uses tools outside ring theory. Give a construction which yields, for each positive integer  $n$ , a Prüfer domain containing a finitely generated ideal requiring  $n$  generators, such that the proof of the necessity of  $n$  generators can be carried out using elementary ring theoretical techniques without any reliance on geometry.

During the same period that the above work was taking place, considerable work was in progress on rings of integer-valued polynomials. Notable in this regard were the works of Brizolis, Cahen, Chabert and McQuillan. A good general reference for these works can be found in [5]. In particular, it was established in the late 70’s that  $\text{Int}(\mathbb{Z})$  is a two-dimensional Prüfer domain (for example, see [1]). In particular, in light of the Schulting example and Problem (B) described above, the question arose as to whether or not the simple domain  $\text{Int}(\mathbb{Z})$  might represent an example of a Prüfer domain where the finitely generated ideals were not two-generated. Gilmer and Smith considered this problem which resulted in two publications, [23] and [24]. In

the first publication, they established the following Theorem (an ideal  $I$  in  $\text{Int}(\mathbb{Z})$  is called *unitary* if  $I \cap \mathbb{Z} \neq 0$ ).

**Theorem 1.1 (Gilmer-Smith [23]).**  *$\text{Int}(\mathbb{Z})$  has the two-generator property on finitely generated ideals. Moreover, if  $I$  is a finitely generated unitary ideal of  $\text{Int}(\mathbb{Z})$  and  $0 \neq n \in I \cap \mathbb{Z}$ , then there exists  $f(X) \in I$  such that  $I = (n, f(X))$ .*

The main technique in the proof of Theorem 1.1 considers the periodic behavior of the sequence of ideals

$$I(0) + n\mathbb{Z}, I(1) + n\mathbb{Z}, I(2) + n\mathbb{Z}, \dots$$

where  $n$  is a positive integer,  $I$  a finitely generated unitary ideal of  $\text{Int}(\mathbb{Z})$  and

$$I(a) = \{f(a) \mid f \in I\}.$$

This result was extended to  $\text{Int}(E, D)$  where  $D$  is a Dedekind domain with finite residue fields and  $E$  is a “ $D$ -fractional” subset of  $K$  (i.e., there exists a  $d \in D$  such that  $dE \subseteq D$ ) by McQuillan [34, Theorem 5.5] (see also [7]).

Although the above Theorem answered the question regarding the existence of two generators for every finitely generated ideal of  $\text{Int}(\mathbb{Z})$ , it left open the additional question about the arbitrary choice of one of the two generators. The common terminology used is an ideal  $I$  is called *strongly two-generated* if it can be generated by two elements and the first of the two generators can be chosen at random from the nonzero elements of  $I$ . A ring where every finitely generated ideal is strongly two-generated is said to have the *strong two-generator property*. Finally, an element  $\alpha$  of a domain  $R$  which can be chosen as one of two generators for every two-generated ideal  $I$  in which it is contained is called a *strong two-generator of  $R$* . We note a result of Lantz and Martin [28] yields that the set of strongly two-generated ideals of  $R$  forms a subgroup of the set of invertible ideals of  $R$ . Hence, we set  $G_2$  to be the subgroup of the class group  $G$  of  $R$  which is given by the strongly two-generated ideals.

Using the above terminology, Gilmer-Smith established in Theorem 1.1 that every integer  $n \neq 0$  is a strong two-generator in  $\text{Int}(\mathbb{Z})$ . However, in a subsequent paper [24], they established that  $\text{Int}(\mathbb{Z})$  did not have the strong two-generator property. In that paper the following results were established on the presence of elements that were not strong two-generators as well as a description of some elements other than  $0 \neq n \in \mathbb{Z}$  which were strong two-generators.

**Theorem 1.2.** [24] *For  $\text{Int}(\mathbb{Z})$ ,*

1. *If  $d$  is a square free integer and the class group of  $\mathbb{Q}(\sqrt{d})$  is not an elementary abelian 2-group, then  $X^2 - d$  is not a strong two-generator of  $\text{Int}(\mathbb{Z})$ .*

2. For an odd prime  $p$ , the ideal  $(p, X)$  is not a strongly two-generated ideal of  $\text{Int}(\mathbb{Z})$ .
3. If  $n$  and  $a$  are non-zero elements of  $\mathbb{Z}$ , and  $b, c$  elements of  $\mathbb{Z}$  with  $c \geq 0$ , then every element of the form  $n(aX + b)^c$  is a strong two-generator of  $\text{Int}(\mathbb{Z})$ .

Hence, it was established in  $\text{Int}(\mathbb{Z})$  that  $G_2 \subsetneq G$  (i.e.,  $\text{Int}(\mathbb{Z})$  does not have the strong two-generator property). We outline the main tool used in the proof of Theorem 1.2. Let  $f(X) \in \text{Int}(\mathbb{Z})$  be an irreducible polynomial in  $\mathbb{Q}[X]$  with root  $\theta$ . Set  $K = \mathbb{Q}(\theta)$  and define the map

$$\varphi : \text{Int}(\mathbb{Z}) \rightarrow \mathbb{Q}(\theta)$$

by

$$g(X) \mapsto g(\theta).$$

Now, if

$$\tilde{f} = \text{Ker}(\varphi) = f(X)\mathbb{Q}[X] \cap \text{Int}(\mathbb{Z}),$$

then

$$\text{Int}(\mathbb{Z})/\tilde{f} \cong \{g(\theta) \mid g(X) \in \text{Int}(\mathbb{Z})\}.$$

Set  $J(f) = \text{Int}(\mathbb{Z})/\tilde{f}$ .  $J(f)$  is the homomorphic image of a Prüfer domain and is hence integrally closed. Clearly  $J(f) \subseteq \mathbb{Q}(\theta)$  and since  $\mathbb{Z} \subseteq J(f)$ , we have that  $\mathbb{Z}^* \subseteq J(f)$  where  $\mathbb{Z}^*$  is the ring of integers of  $\mathbb{Q}(\theta)$  over  $\mathbb{Z}$ .  $J(f)$  is an overring of  $\mathbb{Z}^*$  and is thus itself a Dedekind domain. Thus, we have a set  $S = \{p_\alpha\}_{\alpha \in \mathcal{A}}$  of prime ideals of  $\mathbb{Z}^*$  so that

$$J(f) = \bigcap_{p_\alpha \in S} \mathbb{Z}_{p_\alpha}^*.$$

In [24], the authors argue that a nonzero  $f \in \text{Int}(\mathbb{Z})$  is a strong two-generator in  $\text{Int}(\mathbb{Z})$  if and only if  $J(f)$  is a principal ideal domain. These ideas were extended in a subsequent paper by McQuillan [37].

It remains open to determine the following:

1. Does there exist a non-principal ideal of  $\text{Int}(\mathbb{Z})$  which is strongly two-generated?
2. A characterization of all the strong two-generators of  $\text{Int}(\mathbb{Z})$ .

Recalling that  $\text{Int}(\mathbb{Z}) = \text{Int}(\mathbb{Z}, \mathbb{Z})$ , we summarize the above problems in the context of a general domain  $D$  and non-empty subset  $E \subseteq D$ . Let  $\mathcal{R} = \text{Int}(E, D)$ ,  $G$  be the class group of  $\mathcal{R}$  and  $G_2$  the subgroup of  $G$  represented by the strongly two-generated ideals of  $\mathcal{R}$ .

#### General Problems:

1. For a given  $\mathcal{R}$ , describe  $G$  and  $G_2$  (or  $G/G_2$ ).
2. Describe the strong two-generators of  $\mathcal{R}$ .

3. Determine those  $\mathcal{R}$  for which  $G_2 = G$  (that is,  $\mathcal{R}$  is strongly two-generated).

We note some additional work of Gilmer in this direction. In [22], Gilmer-Henizer-Lantz-Smith determined the structure of  $G$  for  $\text{Int}(\mathbb{Z})$  as a free abelian group on a countably infinite basis. Additional descriptions of  $G$  can be found in [5, Chapter VIII].

Less is known about the subgroup  $G_2$ , in particular the strongly two-generated ideals. For the general case  $\text{Int}(E, D)$ , we note that the situation where  $E$  is a finite set is very special. A simple description of the domain  $\text{Int}(E, D)$  where  $|E| < \infty$  was given by McQuillan [35]. Using this characterization of  $\text{Int}(E, D)$ , Chapman-Loper-Smith were able to establish the following in [15] and [16].

**Theorem 1.3.** *Let  $D$  be an integral domain and  $E = \{e_1, \dots, e_k\}$  a finite nonempty subset of  $D$ . Then  $\text{Int}(E, D)$  has the strong two-generator property if and only if  $D$  is a Bezout domain.*

**Theorem 1.4.** *If  $D$  is a Dedekind domain which is not a principal ideal domain and  $E = \{e_1, \dots, e_k\}$  is a finite nonempty subset of  $D$ , then  $f(X)$  is a strong two-generator in  $\text{Int}(E, D)$  if and only if  $f(e_i) \neq 0$  for every  $1 \leq i \leq k$ .*

Theorem 1.3 is of interest, since there is no example in the literature of the form  $R = \text{Int}(E, D)$  with the strong two-generator property where the Jacobson radical of  $R$  is zero (for other examples of rings of form  $\text{Int}(E, D)$  with the strong two-generator property, see Rush [41] or Brewer and Klingler [2] [3]). In light of Theorem 1.3, the current authors are unaware of a domain of the form  $\text{Int}(E, D)$  with zero Jacobson radical with the strong two-generator property where  $E$  is infinite. Additional information on the strong two-generator property in  $\text{Int}(E, D)$  can be found in [5, Chapter VIII].

We briefly mention two other papers of Gilmer on integer-valued polynomials. Following the early observation that  $\text{Int}(\mathbb{Z})$  was a Prüfer domain, a basic question was raised.

**Question:** What are necessary and sufficient conditions on a domain  $D$  in order that  $\text{Int}(D)$  be a Prüfer domain?

A necessary condition is that  $D$  be an almost Dedekind domain with finite residue fields. In the Noetherian case (for instance when  $D$  is a Dedekind domain with finite residue fields) then this condition is also sufficient. In [19] Gilmer considered two related questions:

**Q1** If  $\text{Int}(D)$  is Prüfer, must  $D$  be Noetherian?

**Q2** Does  $D$  almost Dedekind with finite residue fields imply  $\text{Int}(D)$  is Prüfer?

Exploiting previous work (some joint work with others) Gilmer provides constructions yielding a negative answer to both questions. Additional work on this problem was done by Chabert [7] [8] [9] and Loper [29] [30] [31] and necessary and sufficient conditions were finally given by Loper in [32].

In [21], Gilmer-Heinzer-Lantz discuss the Noetherian properties in the ring  $\text{Int}(D)$  and in the prime spectrum of  $\text{Int}(D)$ . A summary of the results of that work and of subsequent work can be found in [5, Chapter VI].

Finally, there are two other papers of Gilmer regarding a different aspect of study for integer-valued polynomials. In [23], the authors give an argument that if  $E$  is a subset of  $\mathbb{Z}$  that includes all except a finite number of positive integers, then  $f(a) \in \mathbb{Z}$  for all  $a$  in  $E$  implies  $f(b) \in \mathbb{Z}$  for all  $b \in \mathbb{Z}$ . That is,  $\text{Int}(E, \mathbb{Z}) = \text{Int}(\mathbb{Z})$ . A question was raised as to exactly what subsets  $E$  of  $\mathbb{Z}$  have this property. Gilmer answered this question in [18], both for  $\mathbb{Z}$  and also in the setting of a Dedekind domain  $D$  with finite residue fields. McQuillan [36] extended the Gilmer result describing when  $\text{Int}(E_1, D) = \text{Int}(E_2, D)$  in terms of the closures of  $E_1$  and  $E_2$  in the  $p$ -adic completions of  $D$ . Gilmer's description was more in terms of basic number theory (especially in the case  $D = \mathbb{Z}$ ) and is described as follows in terms of  $\mathbb{Z}$  (where the extension to the Dedekind case is straight forward). We require a definition.

**Definition 1.5.** For  $E \subseteq \mathbb{Z}$  and a prime power  $p^k$  where  $k \geq 1$ ,

$$E \bmod p^k = \{x + (p^k) \mid x \in E\}.$$

Although basically established in [18], the following result is stated in a later Gilmer-Smith paper [25, Theorem 2.2].

**Theorem 1.6.** Let  $E_1$  and  $E_2$  be nonempty subsets of  $\mathbb{Z}$ . Then  $\text{Int}(E_1, \mathbb{Z}) = \text{Int}(E_2, \mathbb{Z})$  if and only if  $E_1 \bmod p^k = E_2 \bmod p^k$  for every prime  $p$  and every integer  $k \geq 1$ .

The terminology now used for the property  $\text{Int}(E_1, D) = \text{Int}(E_2, D)$  is that  $E_1$  and  $E_2$  are *polynomially equivalent*. Additional work on the notion of polynomial equivalence can be found in [5, Chapter IV].

In this spirit, Gilmer-Smith in [25] consider the following problem:

**Question:** For  $E \subseteq \mathbb{Z}$  and  $f(X) \in \text{Int}(\mathbb{Z})$ , under what conditions are  $E$  and  $f(E)$  polynomially equivalent?

In [25], the answer is provided when  $E$  is finite and for several special cases when  $E$  is infinite. In every case considered where  $E$  is infinite, it was shown that  $E$  and  $f(E)$  polynomially equivalent implied  $f(X)$  must be linear (in some cases linear of a special form). These results are of interest in connection with some terminology and questions raised by Narkiewicz. In [39], Narkiewicz defines a property **(P)** for a field as follows.

**Definition 1.7.** A field  $K$  has property **(P)** if the polynomials  $f(t)$  in  $K[t]$  for which  $f(E) = E$  for some infinite set  $E$  of  $K$ , must be linear.

Narkiewicz provides several results about property **(P)**, including that  $\mathbb{Q}$  has the property and poses several interesting questions. Note the problem posed by Gilmer-Smith in [25] is related in that it asked if  $f(X)$  must be linear when

“ $f(E) = E$ ” is replaced by “ $E \bmod p^k = f(E) \bmod p^k$ ” (that is,  $E$  and  $f(E)$  are polynomially equivalent) where  $E$  is an infinite subset of  $\mathbb{Z}$  and  $f(X)$  is in  $\text{Int}(\mathbb{Z})$ . We note that the Gilmer-Smith question on polynomially equivalence of  $E$  and  $f(E)$  has been recently answered in the affirmative by Fares [17]. A more general result has been offered by Mulay [38].

All of the above is directly related to the concept of *polynomial closure* of a set  $E$  (see [4]). More precisely, if  $D$  is a domain and  $E \subseteq D$  define

$$\overline{E} = \{d \in D \mid f(d) \in D \text{ for all } f(X) \in \text{Int}(E, D)\}.$$

That is,  $\overline{E}$  is the largest subset of  $E$  such that  $\text{Int}(\overline{E}, D) = \text{Int}(E, D)$ . We provide in the next section an alternate description to that given in [36] of  $\overline{E}$  using only elementary arithmetical tools available in the domain  $D$ .

## 2 A New Approach to Polynomial Closure

The work in this section is sparked by the papers [10], [11] and [12] which study the ring  $\text{Int}(\mathbb{P}, \mathbb{Z})$ . In [12, Proposition 2.1] (which is actually a restatement of [11, Propositions 5.1 and 5.2]), the authors argue that  $\overline{\mathbb{P}} = \mathbb{P} \cup \{\pm 1\}$  with respect to  $\mathbb{Z}$ . To show that a polynomial  $f(X) \in \text{Int}(\mathbb{P}, \mathbb{Z})$  has the property  $f(\pm 1) \in \mathbb{Z}$ , they appeal to localizations. In fact, their argument is based on the following result: for any prime  $p$ ,  $\text{Int}(\mathbb{P}, \mathbb{Z})_{(p)} = \text{Int}(X_p, \mathbb{Z}_{(p)})$  where  $X_p = (\mathbb{Z} \setminus p\mathbb{Z}) \cup \{p\}$  ([10, Corollaire 3]). We present an elementary proof of this fact which does not rely on localizations or topological closures (see [12, Proposition 2.2]). Our primary result is Proposition 2.5, where we give a new characterization of  $\overline{S}$ . We then apply this result to give an elementary description of the closure of the set of natural prime integers  $\mathbb{P}$  in both  $\mathbb{Z}$  and in the larger domain  $\mathbb{Z}[i]$ . We close by applying our method to the set of prime numbers contained in arithmetic sequence in  $\mathbb{Z}$ . Proposition 2.11 computes the polynomial closure of any such set.

In the following, let  $S$  be a subset of  $D$ ,  $a \neq 0$  an element of  $D$  and  $g(X) \in D[X]$ .

- Definition 2.1.** 1. We say that  $g(S) \equiv 0 \pmod{a}$  if  $s \in S$  implies that  $g(s) \equiv 0 \pmod{a}$ .
2. We say that  $g(S) \not\equiv 0 \pmod{a}$  if  $s \in S$  implies that  $g(s) \not\equiv 0 \pmod{a}$ .

Let  $S_1$  and  $S_2$  be subsets of  $D$ .

- Definition 2.2.** 1. We say that  $(a, g(X))$  separates  $S_1$  from  $S_2$  if  $g(S_1) \equiv 0 \pmod{a}$  and  $g(S_2) \not\equiv 0 \pmod{a}$ .
2. We say that  $a$  separates  $S_1$  from  $S_2$  if there exists a  $g(X) \in D[X]$  such that  $(a, g(X))$  separates  $S_1$  from  $S_2$ .

In the latter case, we call  $a$  a *separator*. Clearly a separator is never a unit of  $D$ . We say that  $S_1$  and  $S_2$  are *separable* if there is a separator  $a$  separating  $S_1$

from  $S_2$  or  $S_2$  from  $S_1$ . We say that  $S_1$  and  $S_2$  are *fully separable* if there is a separator  $a_1$  separating  $S_1$  from  $S_2$  and a separator  $a_2$  separating  $S_2$  from  $S_1$ . We note that our definition of *separates* differs sharply from the notion of  $\text{Int}(D)$  *separating points* in the completion  $\hat{D}$  of  $D$  as illustrated in [5, Chapter III.4].

**Comments.**

- (1) If there exists  $s_1 \in S_1$ ,  $s_2 \in S_2$  and  $a \in D$  with  $s_1 \equiv s_2 \pmod{a}$ , then  $a$  cannot separate  $S_1$  from  $S_2$ . This clearly holds for all  $a$  if  $S_1 \cap S_2 \neq \emptyset$ .
- (2) Set  $D = \mathbb{Z}$ . If  $S_1$  and  $S_2$  are disjoint and both finite, then  $S_1$  and  $S_2$  are fully separable. To see this, let  $p \in \mathbb{P}$  with

$$p > \left( \prod_{s_1 \in S_1} s_1 \right)^{|S_2|} \left( \prod_{s_2 \in S_2} s_2 \right)^{|S_1|}$$

and set  $g(X) = \prod_{s \in S_1} (X - s)$ . Clearly  $g(S_1) \equiv 0 \pmod{p}$ . If  $s_2 \in S_2$ , then  $g(s_2) = \prod_{s \in S_1} (s_2 - s) \not\equiv 0 \pmod{p}$  and so  $g(S_2) \not\equiv 0 \pmod{p}$ . Similarly, setting  $f(X) = \prod_{s \in S_2} (X - s)$  yields that  $p$  also separates  $S_2$  from  $S_1$ .

- (3) If  $a$  separates  $S_1$  from  $S_2$  and  $0 \neq b \in D$ , then  $ab$  also separates  $S_1$  from  $S_2$ . To see this, suppose  $(a, g_1(X))$  separates  $S_1$  from  $S_2$ . Set  $g(X) = bg_1(X)$ . Clearly  $g(S_1) \equiv 0 \pmod{ab}$ . Suppose for some  $s_2 \in S_2$  that  $g(s_2) = kab = bg_1(s_2)$  for  $0 \neq k \in D$ . But then  $g_1(s_2) = ka$ , so  $g_1(s_2) \equiv 0 \pmod{a}$ , which is impossible. So  $g(S_2) \not\equiv 0 \pmod{ab}$ .
- (4) Suppose  $S_1$  and  $S_2$  are subsets in  $D$  with  $S_2 = \{\alpha\}$  a singleton. If we can separate  $S_1$  from  $S_2$ , then a separator can be chosen of the form  $p^k$  where  $p$  is a prime in  $D$ . To see this, suppose  $(a, g(X))$  separates  $S_1$  from  $S_2$ . Write  $a = p_1^{m_1} \cdots p_k^{m_k}$ . Now,  $g(S_1) \equiv 0 \pmod{a}$ , hence  $g(S_1) \equiv 0 \pmod{p_i^{m_i}}$  for  $1 \leq i \leq k$ . We cannot have  $g(S_2) \equiv 0 \pmod{p_i^{m_i}}$  for  $1 \leq i \leq k$ , since in that case  $g(S_2) \equiv 0 \pmod{a}$ . Therefore, one of the  $p_i^{m_i}$  must separate  $S_1$  and  $S_2$ , using the same  $g(X)$ .

*Example 2.3.* If  $S_1$  and  $S_2$  are separable, they may not be fully separable. Let  $D = \mathbb{Z}$  and set

$$S_1 = \bigcup_{i=1}^5 \{i + 6k \mid k \in \mathbb{N} \cup \{0\}\} \text{ and } S_2 = \{0\}.$$

We have  $(6, X)$  separating  $S_2$  from  $S_1$ . Suppose that  $(m, g(X))$  separates  $S_1$  from  $\{0\}$ . From Comment (4), we may assume  $m$  is a prime power  $p^k$ ,  $k > 0$ . Whatever this prime power,  $p^k \not\equiv 0 \pmod{6}$ , thus  $p^k \in S_1$ . As clearly  $p^k \equiv 0 \pmod{p^k}$ , we reach a contradiction by Comment (1).

We also find points which cannot be separated from  $S$  of interest.



**Definition 2.4.** Let  $S$  be a nonempty subset of an integral domain  $D$ . We say that  $x \in D$  sticks to  $S$  if there does not exist an  $a \in D$  which separates  $S$  from  $\{x\}$ . We denote the set of elements in  $D$  which stick to  $S$  by  $\tilde{S}$ .

Clearly  $x$  sticks to  $S$  if and only if

$$\forall a \in D, a \neq 0, g(S) \equiv 0 \pmod{a} \text{ implies } g(x) \equiv 0 \pmod{a}.$$

**Proposition 2.5.** Let  $S$  be a nonempty subset of the domain  $D$ . Then  $\tilde{S}$  is equal to the polynomial closure  $\overline{S}$  of  $S$ .

*Proof.* Note that a polynomial  $q[X] \in K[X]$  can be written  $q = \frac{f}{a}$ , with  $f \in D[X]$  and  $a \in D \neq 0$ . With this in mind for  $\alpha \in D$ , the following assertions are equivalent.

- $\alpha \notin \overline{S}$ ,
- there exists a polynomial  $q[X] \in K[X]$  such that  $q(S) \subseteq D$ , but  $q(\alpha) \notin D$ ,
- there exists  $a \in D, a \neq 0$ , and  $f(X) \in D[X]$  such that  $f(S) \equiv 0 \pmod{a}$ , but  $f(\alpha) \not\equiv 0 \pmod{a}$ ,
- $\alpha \notin \tilde{S}$ . □

Notice that our separation method makes verification of the basic properties related to closure relatively simple (see [5, Proposition IV.1.5]). We list these properties here for the convenience of the reader.

**Basic Facts:** Let  $D$  be an integral domain.

- (i) If  $\emptyset \neq S \subseteq D$ , then  $\overline{\overline{S}} = \overline{S}$ .
- (ii) If  $\emptyset \neq S \subseteq T \subseteq D$ , then  $\overline{S} \subseteq \overline{T}$ .
- (iii) If  $\{S_i\}$  is a family of nonempty subsets of  $D$ , then

$$\overline{\bigcap_i S_i} \subseteq \bigcap_i \overline{S_i} \text{ and } \bigcup_i \overline{S_i} \subseteq \overline{\bigcup_i S_i}.$$

We now offer the promised applications.

*Example 2.6.* Let  $D$  be any integral domain and  $b, c$  nonzero elements of  $D$ . If  $S = \{b + cz \mid z \in D\}$ , then every  $\alpha \notin S$  is separated from  $S$  by  $(c, X - b)$ . Thus  $\overline{S} = S$  and in general a set which is equal to its closure is called *polynomially closed*. In the above construction, set  $D = \mathbb{Z}$  and suppose both  $b$  and  $c$  are positive integers. If  $S_1$  is a subset of  $S$  with  $S \setminus S_1$  bounded above or below (or both), then  $\overline{S_1} = S$ . To see this, first consider  $s_2 \not\equiv b \pmod{c}$ . Then  $(c, X - b)$  separates  $S_1$  from  $\{s_2\}$ . Now, let  $s_2 \equiv b \pmod{c}$ . Suppose  $(a, g(X))$  separates  $S_1$  from  $\{s_2\}$ . Now,  $s_2 = mc + b$  for some  $m \in \mathbb{Z}$  and by hypothesis,  $nmc + b \in S_1$  for all  $n$  sufficiently large (or small). Choose one such  $n \equiv 1 \pmod{a}$ . Then  $s_2 = mc + b \equiv nmc + b \pmod{a}$ . This contradicts the supposition that  $a$  separates  $S_1$  from  $\{s_2\}$ . Therefore,  $s_2 \in \overline{S_1}$ .

*Example 2.7.* Let  $\mathcal{SF}$  be the set of squarefree integers. Using Theorem 1.6, one can argue that  $\mathcal{SF}$  is its own closure. We show how to obtain this result using Proposition 2.5. It suffices to separate  $\mathcal{SF}$  from each  $y \in \mathbb{Z} \setminus \mathcal{SF}$ . Suppose that  $p^2 \mid y$  for some prime  $p$ . Set  $f_1(X) = (X - p)(X - 2p) \cdots (X - (p - 1)p)$ . Set  $f_2(X) = (X - 1)(X - 2) \cdots (X - (p - 1))$ . Set  $f(X) = f_1(X)f_2(X)^p$ . Now, consider the pair  $(p^p, f(X))$ . We claim that this separates  $\mathcal{SF}$  from  $y$ .

If  $X \not\equiv 0 \pmod{p}$ , then  $f_2(X) \equiv 0 \pmod{p}$ , and hence  $f(X) \equiv 0 \pmod{p^p}$ . If  $X \equiv 0 \pmod{p}$ , then write  $X = kp$ . Note that  $f_2(X) \not\equiv 0 \pmod{p}$ , and hence  $v_p(f(X)) = v_p(f_1(X))$ . Now,  $f_1(X) = (kp - p)(kp - 2p) \cdots (kp - (p - 1)p) = p^{p-1}(k - 1)(k - 2) \cdots (k - (p - 1))$ . If  $p \nmid k$ , then  $k \not\equiv 0 \pmod{p}$  and therefore  $p^p \mid f_1(X)$  so  $f(X) \equiv 0 \pmod{p^p}$ . Therefore, if  $p \nmid k$ , then  $f(\mathcal{SF}) \equiv 0 \pmod{p^p}$ . However, if  $p \mid k$  then  $v_p(f_1(X)) = p - 1$  and  $f(X) \not\equiv 0 \pmod{p^p}$ . Since  $p^2 \mid y$  we write  $y = pk$ , with  $p \mid k$ . Hence,  $f(y) \not\equiv 0 \pmod{p^p}$ .

**Proposition 2.8.** *Let  $\mathbb{P}$  be the set of prime numbers. Then  $\overline{\mathbb{P}} = \mathbb{P} \cup \{\pm 1\}$ .*

*Proof.* If  $x = \pm 1$ , then, by Dirichlet's Theorem, for each  $a \neq 0$  which is not a unit in  $\mathbb{Z}$ , there is a prime  $p$  congruent to  $x \pmod{a}$ , hence  $\mathbb{P}$  cannot be separated from  $\{1\}$  and  $\{-1\}$  by Comment (1).

If  $x \notin \mathbb{P} \cup \{\pm 1\}$ , choose a prime  $p$  dividing  $x$  and let  $r = v_p(x - p)$  (where  $v_p(y)$  is the  $p$ -adic valuation of  $y$ ), then  $\mathbb{P}$  is separated from  $\{x\}$  by

$$(p^{r+1}, (X - p)[(X - 1) \cdots (X - p + 1)]^{r+1}),$$

completing the argument.  $\square$

We further demonstrate the versatility of our method by computing  $\overline{\mathbb{P}}$  with respect to  $\mathbb{Z}[i]$ . The proof requires a lemma.

**Lemma 2.9.** *Let  $D = \mathbb{Z}[i]$ .*

- (1) *The closure  $\overline{S}$  of a subset  $S$  of  $D$  such that  $S \subseteq \mathbb{Z}$  is itself such that  $\overline{S} \subseteq \mathbb{Z}$ .*
- (2) *If two subsets of  $D$  are separable, then a separator  $m$  can be chosen in  $\mathbb{Z}$ .*

*Proof.* (1) Suppose that  $\alpha$  sticks to  $S$  (i.e., suppose that  $\alpha \in \overline{S}$ ). Pick a prime  $p$  such that  $p \equiv 3 \pmod{4}$ . Set

$$g(X) = X(X - 1)(X - 2) \cdots (X - p + 1).$$

Then  $g(S) \equiv 0 \pmod{p}$  and hence,  $g(\alpha) \equiv 0 \pmod{p}$ . As  $p$  is prime in  $D$  it divides some  $\alpha - j$ ,  $0 \leq j \leq p - 1$ , in  $D$ , and thus clearly divides the imaginary part of  $\alpha$  in  $\mathbb{Z}$ . As there are infinitely many such primes  $p$ , it follows that  $\alpha$  is real.

- (2) If  $z$  is a separator, then  $m = z\bar{z}$  (where  $\bar{z}$  is the conjugate of  $z$ ) is an integer and, by Comment (3), another separator.  $\square$

From the lemma follows this result about the polynomial closure of subsets of  $\mathbb{Z}$  in  $\mathbb{Z}[i]$ .

**Proposition 2.10.** *Let  $S$  be a subset of  $D = \mathbb{Z}[i]$  such that  $S \subseteq \mathbb{Z}$ , then its polynomial closure  $D$  is the same as in  $\mathbb{Z}$ . In particular,  $\overline{\mathbb{P}} = \mathbb{P} \cup \{\pm 1\}$ .*

*Proof.* From Lemma 2.9, both closures are contained in  $\mathbb{Z}$ . Considering  $\alpha \in \mathbb{Z}$ , we show that it can be separated from  $S$  in  $D$  if and only if it can be so in  $\mathbb{Z}$ . Note that if  $a, b$  are integers, then  $a$  divides  $b$  in  $\mathbb{Z}$  if and only if this is so in  $D$ .

- Suppose  $\alpha$  can be separated from  $S$  in  $\mathbb{Z}$ : there exists  $(a, g(X))$ , with  $a \in \mathbb{Z}$ , and  $g(X) \in \mathbb{Z}[X]$  such that,  $\forall s \in S$ ,  $a$  divides  $g(s)$  but not  $g(\alpha)$  in  $\mathbb{Z}$ . As  $a$ ,  $g(s)$ , and  $g(\alpha)$  are integers, the same division properties hold in  $D$ . Hence  $\alpha$  can be separated from  $S$  in  $D$ .
- Suppose  $\alpha$  can be separated from  $S$  in  $D$ : From Lemma 2.9, the separated  $a$  can be chosen in  $\mathbb{Z}$ , and there is  $g(X) \in D[X]$  such that,  $\forall s \in S$ ,  $a$  divides  $g(s)$  but not  $g(\alpha)$  in  $D$ . Write  $g(X) = g_1(X) + ig_2(X)$ , where both  $g_1(X)$  and  $g_2(X)$  have their coefficients in  $\mathbb{Z}$ . Then, for  $i = 1$  or  $i = 2$ ,  $a$  does not divide both  $g_1(s)$  and  $g_2(s)$  in  $D$  and hence also in  $\mathbb{Z}$ . Therefore  $(a, g_i(X))$  separates  $\alpha$  from  $S$  in  $\mathbb{Z}$ .  $\square$

Let  $a$  and  $b$  be relatively prime natural numbers with  $1 \leq a < b$  and  $b \geq 2$ . Further, let  $\mathbb{P}_{a,b}$  represent the prime numbers in the arithmetic sequence  $A_{a,b} = \{a + bk \mid k \in \mathbb{N} \cup \{0\}\}$ . The method we have developed allows us to determine the polynomial closure of the sets  $\mathbb{P}_{a,b}$  in  $\mathbb{Z}$ .

**Proposition 2.11.** *Let  $a$ ,  $b$  and  $\mathbb{P}_{a,b}$  be as above.*

1.  $\overline{\mathbb{P}_{1,2}} = \mathbb{P}_{1,2} \cup \{\pm 1\}$ .
2. *Suppose that  $b > 2$ .*
  - a) *If  $a \neq 1$  or  $b - 1$ , then  $\overline{\mathbb{P}_{a,b}} = \mathbb{P}_{a,b}$ .*
  - b) *If  $a = 1$ , then  $\overline{\mathbb{P}_{a,b}} = \mathbb{P}_{a,b} \cup \{1\}$ .*
  - c) *If  $a = b - 1$ , then  $\overline{\mathbb{P}_{a,b}} = \mathbb{P}_{a,b} \cup \{-1\}$ .*

*Proof.* Note that  $\mathbb{P}_{a,b} = \mathbb{P} \cap A_{a,b}$ . By Basic Fact (ii) above,  $\overline{\mathbb{P}_{a,b}} \subseteq \overline{\mathbb{P}} \cap \overline{A_{a,b}}$ . The results follow immediately taking into account Example 2.6.  $\square$

We close with a generalization of the last result.

**Corollary 2.12.** *Let  $a_1, a_2, \dots, a_k, b \in \mathbb{Z}$  with  $1 \leq a_1 < a_2 < \dots < a_k < b$  and  $k > 1$ . Suppose that  $\gcd(b, a_i) = 1$  for each  $i$  and set  $X = \mathbb{P}_{a_1,b} \cup \mathbb{P}_{a_2,b} \cup \dots \cup \mathbb{P}_{a_k,b}$ . Then:*

1.  $(\overline{X} - X) \subseteq \{-1, 1\}$ .
2.  $1$  is in  $(\overline{X} - X)$  if and only if  $a_1 = 1$ .
3.  $-1$  is in  $(\overline{X} - X)$  if and only if  $a_k = b - 1$ .

*Proof.* By our hypothesis,  $b > 2$ . (2) and (3) follow from the previous proof. Using an argument similar to that used in Example 2.6, the set

$$Y = A_{a_1,b} \cup A_{a_2,b} \cup \dots \cup A_{a_k,b}$$

is closed. From Basic Fact (iii),

$$\overline{\mathbb{P}_{a_1,b}} \cup \overline{\mathbb{P}_{a_2,b}} \cup \cdots \cup \overline{\mathbb{P}_{a_k,b}} \subseteq \overline{X} \subseteq \overline{Y} = Y.$$

The result now follows immediately.  $\square$

## Acknowledgement

The authors would like to thank the referee for suggestions which substantially improved the paper.

## References

1. Brizolis, D.: A theorem on ideals in Prüfer rings of integer-valued polynomials. *Comm. Algebra*, **7**, 1065–1077 (1979)
2. Brewer, J. and Klinger, L.: The ring of integer-valued polynomials of a semi-local principal-ideal domain. *Linear Algebra Appl.*, **157**, 141–145 (1991)
3. Brewer, J. and Klinger, L.: Rings of integer-valued polynomials and the bcs-property, Commutative ring theory and applications. *Lecture Notes in Pure and Appl. Math.*, **231**, 65–75 (2003)
4. Cahen, P.-J.: Polynomial closure. *J. Number Theory*, **61**, 226–247 (1996)
5. Cahen, P.-J. and Chabert, J.-L.: Integer Valued-Polynomials, *Amer. Math. Soc. Surveys and Monographs* **58**, American Mathematical Society, Providence, (1997)
6. Cahen, P.-J. and Chabert, J.-L.: What’s new about integer-valued polynomials on a subset? In: Chapman, S. T. and Glaz, S. (eds) *Non-Noetherian Commutative Ring Theory*, Kluwer Academic Publishers, Boston, 75–96 (2000).
7. Chabert, J.-L.: Un anneau de Prüfer. *J. Algebra*, **107**, 1–16 (1987)
8. Chabert, J.-L.: Anneaux de polynômes à valeurs entières et anneaux de Prüfer. *C. R. Acad. Sci. Paris Sr. I Math.*, **312**, 715–720 (1991)
9. Chabert, J.-L.: Integer-valued polynomials, Prüfer domains, and localization. *Proc. Amer. Math. Soc.*, **118**, 1061–1073 (1993)
10. Chabert, J.-L.: Une caractérisation des polynômes prenant des valeurs entières sur tous les nombres premiers. *Canad. Math. Bull.*, **99**, 273–282 (1996)
11. Chabert, J.-L., Chapman, S. T. and Smith, W. W.: A basis for the ring of polynomials integer-valued on prime numbers. *Lecture Notes in Pure and Applied Mathematics*, **189**, 271–284 (1997)
12. Chabert, J.-L., Chapman, S. T. and Smith, W. W.: Algebraic properties of the ring of integer-valued polynomials on prime numbers. *Comm. Algebra*, **25**, 1947–1959 (1997)
13. Chapman, S. T. and Glaz, S. (eds): *Non-noetherian commutative ring theory*. Kluwer Academic Publishers, Boston (2000)
14. Chapman, S. T. and Glaz, S.: One hundred problems in commutative ring theory. In: Chapman, S. T. and Glaz, S. (eds) *Non-Noetherian Commutative Ring Theory*, Kluwer Academic Publishers, Boston, 459–476 (2000)

15. Chapman, S. T., Loper, K. A. and Smith, W. W.: The strong two-generator property in rings of integer-valued polynomials determined by finite sets. *Arch. Math.*, **78**, 372-377 (2002)
16. Chapman, S. T., Loper, K. A. and Smith, W. W.: Strongly two-generated ideals in rings of integer-valued polynomials determined by finite sets, *C. R. Math. Rep. Acad. Sci. Canada*, **26**, 33-38 (2004)
17. Fares, Y.: Factorial Preservation. *Arch. Math. (Basel)*, **83**, 497-506 (2004)
18. Gilmer, R.: Sets that determine integer-valued polynomials. *J. Number Theory*, **33**, 95-100 (1989)
19. Gilmer, R.: Prüfer domains and rings of integer-valued polynomials. *J. Algebra*, **129**, 502-517 (1990)
20. Gilmer R. and Heinzer, W.: On the number of generators for an invertible ideal. *J. Algebra*, **14**, 139-151 (1970)
21. Gilmer, R., Heinzer, W. and Lantz, D.: The noetherian property in rings of integer-valued polynomials. *Trans. Amer. Math. Soc.*, **338**, 187-199 (1993)
22. Gilmer, R., Heinzer, W., Lantz, D. and Smith, W. W.: The ring of integer-valued polynomials of Dedekind domain. *Proc. Amer. Math. Soc.*, **108**, 673-681 (1990)
23. Gilmer, R. and Smith, W.W.: Finitely generated ideals of the ring of integer-valued polynomials. *J. Algebra*, **81**, 150-164 (1983)
24. Gilmer, R. and Smith, W.W.: Integer-valued polynomials and the strong two-generator property. *Houston J. Math.*, **11**, 65-74 (1985)
25. Gilmer, R. and Smith, W. W.: On the polynomial equivalence of subsets  $E$  and  $f(E)$  of  $\mathbb{Z}$ . *Arch. Math. (Basel)*, **73**, 355-365 (1999)
26. Heitmann, R. C.: Generating ideals in Prüfer domains. *Pacific J. Math.*, **62**, 117-126 (1976)
27. Heitman, R. C. and Levy, L. S.:  $1\frac{1}{2}$  and 2-generator ideals in Prüfer domains. *Rocky Mountain J. Math.*, **5**, 361-373 (1975)
28. Lantz, D. and Martin, M.: Strongly two-generated ideals. *Comm. Algebra*, **16**, 1759-1777 (1988)
29. Loper, K. A.: More almost Dedekind domains and Prüfer domains of polynomials. *Lecture Notes in Pure and Appl. Math.* **171**, 287-298 (1995)
30. Loper, K. A.: Another Prüfer ring of integer-valued polynomials. *J. Algebra*, **187**, 1-6 (1997)
31. Loper, K. A.: Ideals of integer-valued polynomial rings. *Comm. Algebra*, **25**, 833-845 (1997)
32. Loper, K. A.: A classification of all  $D$  such that  $\text{Int}(D)$  is a Prüfer domain. *Proc. Amer. Math. Soc.*, **126**, 657-660 (1998)
33. Loper, K. A.: Constructing examples of integral domains by intersection valuation domains. In: Chapman, S. T. and Glaz, S. (eds) *Non-Noetherian Commutative Ring Theory*, Kluwer Academic Publishers, Boston, 325-340 (2000)
34. McQuillan, D.L.: On Prüfer domains of polynomials. *J. Reine Angew. Math.*, **358**, 162-178 (1985)
35. McQuillan, D. L.: Rings of integer-valued polynomials determined by finite sets. *Proc. Royal Irish Acad.*, **85A**, 177-184 (1985)
36. McQuillan, D. L.: On a theorem of R. Gilmer. *J. Number Theory*, **39**, 245-250 (1991)
37. McQuillan, D. L.: Split Primes and Integer-Valued Polynomials. *J. Number Theory*, **43**, 216-219 (1993)
38. Mulay, S. B.: Polynomial-mappings and  $M$ -equivalence. preprint

39. Narkiewicz, W.: Polynomial mappings. Lecture Notes in Mathematics, Springer-Verlag, Berlin, No. 1600 (1995)
40. Rose, H. E.: A Course in Number Theory. Clarendon Press, Oxford (1994)
41. Rush, D.: Generating ideals in rings of integer-valued polynomials. *J. Algebra*, **92**, 389–394 (1985)
42. Sally, J. and Vasconcelos, W.: Stable rings. *J. Pure Appl. Algebra*, **4**, 319–336 (1974)
43. Schülting, H-W.: Über die Erzeugendenanzahl invertierbarer Ideale in Prüferingen. *Comm. Algebra*, **7**, 1331–1349 (1979)
44. Swan, R.:  $n$ -generator ideals in Prüfer domains. *Pacific J. Math.*, **111**, 433–446 (1984)