On the IV-equivalence of subsets E and $f(E)$ of $\mathbb{Z}$

Robert Gilmer*

Department of Mathematics, Florida State University
Tallahassee, Florida 32306-4250

AND

William W. Smith†

Department of Mathematics, University of North Carolina
Chapel Hill, North Carolina 27599-3250

* email: gilmer@math.fsu.edu
† email: wwsmith@math.unc.edu

Abstract: For a subset E of an integral domain D and an integer-valued polynomial f over D, we investigate conditions under which the subsets E and $f(E)$ of D determine the same integer- valued polynomials on D (this is the definition of IV-equivalence of E and $f(E)$). Our primary interest in this problem lies in the case where D is the ring of rational integers. Using work of McQuillan, the case where E is finite is resolved completely in Section 3. For E infinite we show in several cases that IV-equivalence of E and $f(E)$ implies that f is linear, but whether this is true in general for, say, $D = \mathbb{Z}$ is an open question.

1. INTRODUCTION

Let D be an integral domain with quotient field K and let E be a subset of D. We denote by $\mathrm{Int}(E, D)$ the subset of $K[t]$ consisting of all polynomials $f(t)$ such that $f(E) \subseteq D$; we write $\mathrm{Int}(D)$ in place of $\mathrm{Int}(D, D)$. $\mathrm{Int}(E, D)$ is called the *ring of integer-valued polynomial on E.* The rings $\mathrm{Int}(D)$ have been actively investigated by commutative ring theorists for at least twenty-five years, but the more general rings $\mathrm{Int}(E, D)$ are a relatively recent focal point of research in the area (see [M3], [CC, Chap. IV]). We mention a few papers that are relevant to our work here. McQuillan made a definitive study of the rings $\mathrm{Int}(E, D)$, for E finite, in [M1]. For a Dedekind domain D with finite residue fields, Gilmer in [G1] determined those subsets E of D such that $\mathrm{Int}(E, D) = \mathrm{Int}(D)$, and this work of Gilmer was extended by McQuillan in [M2]. Recently Chabert, Chapman and Smith have investigated various properties of the ring $\mathrm{Int}(\mathbb{P}, \mathbb{Z})$, where $\mathbb{P}$ is the set of prime integers [Ch1], [CCS1], [CCS2].

Our work in this paper is in somewhat the same vein as that of [G1] and [M2]. Specifically, we say that subsets E_1 and E_2 of D are *IV-equivalent* if E_1 and E_2 determine the same integer-valued polynomials on D — that is, if $\mathrm{Int}(E_1, D) = \mathrm{Int}(E_2, D)$. Our primary interest lies in the IV-equivalence of E and $f(E)$ for a subset E of $\mathbb{Z}$ and a polynomial $f \in \mathrm{Int}(\mathbb{Z})$. In Sections 4 and 5 our main considerations are in the concrete setting of $\mathbb{Z}$; in Sections 2 and 3 we work in the greater generality of a Dedekind domain D with the finite norm property (that is, D/I is finite for each nonzero ideal I of D or, equivalently, for each maximal ideal I of D).

For subsets E_1, E_2 of a Dedekind domain D with finite residue fields, Theorem 2.2 gives equivalent conditions for the IV-equivalence of E_1 and E_2. These conditions are different from, but closely related to, conditions given by McQuillan in Theorem 1 of [M2]. We indicate how the two sets of conditions are related. In Section 3 we consider IV-equivalence of E and $f(E)$ in the case where E is finite. McQuillan has shown that E and $f(E)$ are IV-equivalent only if f induces a permutation on E, so our emphasis in Section 3 is on determining (Corollary 3.2) the set of polynomials f in $\mathrm{Int}(D)$ such that $f(E) = E$.

In Theorem 4.2 we show that if E is an almost prime-power complete subset of $\mathbb{Z}$ (defined in Section 4), then E and $f(E)$ are IV-equivalent only if $f = a \pm t$ for some $a \in A$. Section 5 treats IV-equivalence of E and $f(E)$ for some subsets E of $\mathbb{Z}$ that have arisen in various contexts in the study of $\mathrm{Int}(\mathbb{Z})$. In particular, if E is either the set of prime integers, an infinite set whose elements are factorials, or an infinite set all of whose elements are powers of a fixed integer $n > 1$, we show that t is the only polynomial f in $\mathrm{Int}(\mathbb{Z})$ such that E and $f(E)$ are IV-equivalent.

2. IV-EQUIVALENCE

Our purpose in this section is to derive (Theorem 2.2) a new criterion for *IV*-equivalence of subsets E_1, E_2 of a Dedekind domain with the finite norm property (henceforth abbreviated FNP) that is more useful for our purposes than criteria given by McQuillan [M2, Th.1]. The proof of our first result, Lemma 2.1, requires only a slight extension of the proof of Theorem 8 of [G1].

LEMMA 2.1. *Let P be a maximal ideal of a Dedekind domain R such that R/P is finite. Let k be a positive integer, let $d \in R$, and let $S = \{x \in R \mid x \not\equiv d \pmod{P^k}\}$. Then there exists $f \in \mathrm{Int}(S, R)$ such that $f(d) \notin R$.*

Proof. The second paragraph of the proof of Theorem 8 of [G1] exhibits a polynomial $D(X) \in \mathrm{Int}(S, R)$ and an element u in R such that $u \equiv d \pmod{P^k}$ and $D(u) \notin R$. (In the notation of [G1], $u = t^k + s_j$, where $d \equiv s_j \pmod{P^k}$.) Let $f = D(X - d + u)$. Then $f(d) = D(u) \notin R$, but $f \in \mathrm{Int}(S, R)$ because $S + (u - d) = S$ since $u - d \in P^k$. □

If I is an ideal of the domain D and E is a subset of D, we denote by E mod I the image of E in D/I. Hence $E \bmod I = \{x + I \mid x \in E\}$; if $I = dD$ is principal, we write $E \pmod{d}$ in place of E mod I or E mod dD.

THEOREM 2.2. *Let D be a Dedekind domain with FNP and let E_1 and E_2 be subsets of D.*

(1) $\mathrm{Int}(E, D) \subseteq \mathrm{Int}(E_2, D)$ if and only if $E_2 \bmod Q \subseteq E_1 \bmod Q$ for each nonzero prime-power ideal Q of D.

(2) E_1 and E_2 are IV-equivalent if and only if $E_1 \bmod Q = E_2 \bmod Q$ for each Q as in (1).

Proof. We need only prove (1). Assume first that $E_2 \bmod Q \subseteq E_1 \bmod Q$ for each Q. Let $f \in \mathrm{Int}(E_1, D)$ and write $f = g/d$, where $g \in D[t]$ and $d \in D - \{0\}$. Then $g(E_1) \subseteq dD$ and we wish to show that $g(E_2) \subseteq dD$. It suffices to show that $g(E_2) \subseteq Q$ for each prime-power ideal Q containing dD. Thus, take $v \in E_2$. There exists $w \in E_1$ such that $v \equiv w \pmod{Q}$, and hence $g(v) \equiv g(w) \equiv 0 \pmod{Q}$. Therefore $g(E_2) \subseteq Q$ as we wished to show.

Conversely, if there exists $i \in E_2$ such that $i + Q$ is not in E_1 mod Q for some nonzero prime-power ideal Q of D, then Lemma 2.1 shows that there exists $f \in \mathrm{Int}(D - (i + Q), D)$ such that $f(i) \notin D$. Since $E_1 \subseteq D - (i + Q)$ and $i \in E_2$, it follows that $f \in \mathrm{Int}(E_1, D)$ but $f \notin \mathrm{Int}(E_2, D)$. □

COROLLARY 2.3. *Let D, E_1, and E_2 be as in the statement of Theorem 2.2, let $\{M_\alpha\}_{\alpha\in A}$ be the set of maximal ideals of D, and for $\alpha \in A$ denote by V_α the completion of the valuation domain D_{M_α}. Then E_1 and E_2 are IV-equivalent as subsets of D if and only if they are IV-equivalent as subsets of V_α for each $\alpha \in A$.*

Proof. Suppose E_1 and E_2 are IV-equivalent as subsets of D. Let $\alpha \in A$, let P_α be the maximal ideal of V_α, and let k be a positive integer. Since $P_\alpha^k \cap D = M_\alpha^k$ and since $V_\alpha = D + P_\alpha^k$, the equality $E_1 \bmod M_\alpha^k = E_2 \bmod M_\alpha^k$ implies that $E_1 \bmod P_\alpha^k = E_2 \bmod P_\alpha^k$. Therefore $\mathrm{Int}(E_1, V_\alpha) = \mathrm{Int}(E_2, V_\alpha)$.

Reversal of the argument just given yields the converse. □

Let D be a Dedekind domain with FNP and with quotient field K. For a subset S of K, McQuillan in [M2] defines the D-closure of S, denoted $\mathrm{cl}(S)$, to be $\{a \in K \mid f(a) \in D$ for each $f \in \mathrm{Int}(S, D)\}$ [1]. Thus $\mathrm{cl}(S)$ is the unique largest subset T of K such that $\mathrm{Int}(S, D) = \mathrm{Int}(T, D)$, and subsets S_1 and S_2 are IV-equivalent if and only if these sets have the same closure. For a D-fractional subset[2] S of K, McQuillan gives in Theorem 1 of [M2] a set-theoretic description of the D-closure of S, as follows. For a maximal ideal P of D, denote by ${}_PK$ the P-adic completion of K and by ${}_PS$ the topological closure of S in ${}_PK$ under the P-adic topology. Then $\mathrm{cl}(S) = \cap_P({}_PS \cap K)$. For our purposes we have found the conditions of Theorem 2.2 to be easier to apply in checking IV-equivalence of E_1 and E_2 than the condition that $\cap_P({}_PE_1 \cap K) = \cap_P({}_PE_2 \cap K)$ or that ${}_PE_1 = {}_PE_2$ for all P. However, the difference in the two criteria is merely point of view; Theorem 2.2 could have been obtained from results of [M2], while Theorem 1 (for subsets of D) and Lemma 2 of [M2] can be derived from our (2.2) and (2.3). To clarify these connections a bit, we prove a result that is of interest for us in its own right.

PROPOSITION 2.4. *Let D be a Dedekind domain with FNP and with quotient field K. Let E be a subset of D and let $x \in K$.*

(1) For a fixed prime P of D, $x \in \cap_{n=1}^\infty(E + P^nD_P)$ if and only if x belongs to the P-adic closure ${}_PE^*$ of E in K. (Note that ${}_PE^* = {}_PE \cap K$.)

(2) $\mathrm{cl}(E) = \{x \in D \mid x \in (E + Q)$ for each nonzero prime-power ideal Q of $D\} = \cap_P({}_PE^*)$.

[1] $\mathrm{Int}(S, D)$ is defined in the obvious way.

[2] *D-fractional* means $dS \subseteq D$ for some $d \in D - (0)$.

Proof. (1) is immediate from the definition of the P-adic topology on K.

The first equality in (2) follows from the fact that E and $\mathrm{cl}(E)$ are IV-equivalent, Theorem 2.2, and the fact that any $x \in E$ mod Q for all Q belongs to $\cap_P D_P = D$. The second equality in (2) follows from the first and from (1); the equality $\mathrm{cl}(E) = \cap_P({}_P E^*)$ is, of course, McQuillan's description of $\mathrm{cl}(E)$. □

We remark that, for a general domain D, equivalent conditions for the IV-equivalence of subsets E_1 and E_2 are not known (see [N, p. 20]).

3. THE CASE WHERE E IS FINITE

Suppose D is an integral domain with quotient field K. We turn our attention to the question of IV-equivalence of E and $f(E)$. In this section we consider the case where $E = \{a_i\}_{i=1}^n \subseteq D$ is finite. An argument of McQuillan's shows that E is closed; it goes as follows: if $b \in D - E$, if $c = \prod_{i=1}^n (b - a_i)$, and if $k \in K - D$, then $g = kc^{-1}\prod_1^n (t - a_i)$ is in $\mathrm{Int}(E, D)$, but $g(b) = k \notin D$. It follows that E and $f(E)$ are IV-equivalent if and only if f induces a permutation on E. There is, of course, at least one polynomial f in $\mathrm{Int}(D)$ such that $f(E) = E$, namely $f = t$. To determine the set of all such polynomials in some cases, we need to examine, for $a \in D$, the ideals $I_a = (t - a)K[t] \cap \mathrm{Int}(D) = \{f \in \mathrm{Int}(D) \mid f(a) = 0\}$. Proposition 3.1 is a basic result concerning these ideals.

PROPOSITION 3.1. *Let D be an integral domain with quotient field K. The following conditions are equivalent.*

(1) For all $a, b \in D$ with $a \neq b$, the ideals I_a and I_b are comaximal.

(2) Any mapping from a finite subset of D into D is induced by an element of $\mathrm{Int}(D)$.

(3) For each finite subset E of D, all permutations of E are induced by elements of $\mathrm{Int}(D)$.

Proof. If (1) is satisfied and if $\varphi : E \to D$ is a mapping, where $E = \{x_i\}_{i=1}^n$ is finite, comaximality of the ideals I_{x_i} in $\mathrm{Int}(D)$ implies that there exists $f \in \mathrm{Int}(D)$ such that $f \equiv \varphi(x_i) \pmod{I_{x_i}}$. For such an f we have $f(x_i) = \varphi(x_i)$ for each i.

Clearly (2) implies (3). If (3) is satisfied and if a, b are distinct elements of D, there is a permutation σ of $\{a, b, 0, 1\}$ such that $\sigma(a) = 0$ and $\sigma(b) = 1$. If $f \in \mathrm{Int}(D)$ induces the permutation σ, then $f \in I_a$ and $1 - f \in I_b$. Therefore I_a and I_b are comaximal. □.

COROLLARY 3.2. *Assume the domain D satisfies the equivalent conditions of Proposition 3.1. If $E = \{a_i\}_{i=1}^n$ is a finite subset of D, if σ is a permutation of E, and if $f \in$* $\mathrm{Int}(D)$

induces σ, then $f + \cap_{i=1}^n I_{a_i} = f + \prod_{i=1}^n I_{a_i}$ is the set of all polynomials g in $\mathrm{Int}(D)$ that induce the permutation σ on E. Moreover, $\cap_{i=1}^n I_{a_i} = \prod_1^n (t-a_i)K[t] \cap \mathrm{Int}(D)$.

Proof. The polynomial $g \in \mathrm{Int}(D)$ induces σ if and only if $g(a_i) = f(a_i)$ for each i, hence if and only if $g - f \in \cap_1^n I_{a_i}$, or equivalently, $g \in f + \cap_1^n I_{a_i}$. The equality $\cap_1^n I_{a_i} = \prod_1^n I_{a_i}$ follow from comaximality of the ideals I_{a_i}, and the equality in the last sentence follows because $\prod_1^n (t-a_i)K[t] = \cap_1^n (t-a_i)K[t]$. □

We have no characterization of domains D satisfying the conditions of Proposition 3.1. It is easy to see that the conditions are satisfied if and only if, for all $a, b \in D$ with $a \neq b$, there exists $f \in \mathrm{Int}(D)$ such that $f(a) = 0$ and $f(b) = 1$. Moreover, since the substitution $t \to t - a$ induces an automorphism of $\mathrm{Int}(D)$, there is no loss of generality in taking $a = 0$ in checking this criterion. Proposition 3.3 shows that a Dedekind domain with FNP satisfies the conditions of (3.1).

PROPOSITION 3.3. *A Dedekind domain D with FNP satisfies the equivalent conditions of Proposition 3.1.*

Proof. Let $a \in D - \{0\}$. We show that the ideals I_0 and I_a of $\mathrm{Int}(D)$ are comaximal. Suppose not, and let M be a maximal ideal of $\mathrm{Int}(D)$ containing $I_0 + I_a$. Then $t-(t-a) = a$ is a nonzero element of $M \cap D = P$, a maximal ideal of D. Passing to $\mathrm{Int}(D_P) = [\mathrm{Int}(D)]_{D-P}$ [CC, Prop. I.2.7], we assume without loss of generality that D is a DVR with maximal ideal P and with finite residue field. If $(\widehat{D}, \widehat{P})$ denotes the completion of (D, P), it is known that $M = \{f \in \mathrm{Int}(D) \mid f(c) \in \widehat{P}\}$ for some $c \in \widehat{D}$ [CC, Prop. V.2.3]. Moreover, the inclusions $I_0 \subseteq M$ and $I_a \subseteq M$ show that $0 = c = a$ [CC, Prop. V.2.5], a contradiction. Hence I_0 and I_a are comaximal. □

Suppose D is a domain, not a field, such that $\mathrm{Int}(D) = D[t]$. Then D does not satisfy the conditions of (3.1), for if d is a nonunit of D, there is no polynomial $f \in D[t]$ such that $f(0) = 0$ and $f(d) = 1$. Sufficient conditions for the equality $\mathrm{Int}(D) = D[t]$ are that D is the intersection of a family $\{D_{P_a}\}_{a \in A}$ of localizations, where $|D/P_a|$ is infinite for each $a \in A$ [CC, Lemma I.3.6]. Hence, for example, any Krull domain of dimension greater than 1 is a domain not satisfying the conditions of (3.1).

If D satisfies the conditions of (3.1) and if φ is a mapping of a finite subset $\{a_i\}_1^n$ of D into D, the degree of each $f \in \mathrm{Int}(D)$ that induces φ may be arbitrarily large in relation to n. For example, if $D = \mathbb{Z}$ and p is prime, then p is the minimum of the degrees of the polynomials $f \in \mathrm{Int}(\mathbb{Z})$ that induce the map $0 \to 0$, $p \to 1$ of $\{0, p\}$ into $\mathbb{Z}$.

4. ALMOST PRIME-POWER COMPLETE SUBSETS OF $\mathbb{Z}$

According to the terminology of [G1], a subset E of $\mathbb{Z}$ is *prime-power complete* if E contains a complete set of residues modulo q for each prime power q in $\mathbb{Z}$. In the notation of Section 2, E is prime-power complete if $E(\text{mod } q) = \mathbb{Z}(\text{mod } q)$ for each prime-power q of $\mathbb{Z}$. Thus in accord with Theorem 2.2 (and [G1, Th. 2]) the prime-power complete subsets are precisely the subsets E of $\mathbb{Z}$ such that $\mathrm{Int}(E, \mathbb{Z}) = \mathrm{Int}(\mathbb{Z})$. Cahen and Chabert [CC, p. 74] use the term *polynomially dense* for this concept. Narkiewicz uses the term *arithmetically dense* [N, p. 20]. Narkiewicz attributes this term to Rauzy in [R], but to Rauzy E is arithmetically dense if it contains a complete set of residues modulo n for each positive integer n, and this concept is strictly stronger than that of being arithmetically dense; for example, $6\mathbb{Z} \cup (1+6\mathbb{Z}) \cup (2+6\mathbb{Z})$ is prime-power complete, but does not satisfy Rauzy's condition.

We originally proved that if E is a prime-power complete subset of $\mathbb{Z}$, then a polynomial $f \in \mathrm{Int}(\mathbb{Z})$ such that E and $f(E)$ are IV-equivalent must be of the form $a \pm t$ for some $a \in \mathbb{Z}$. We were subsequently able to generalize to the case where E is *almost prime-power complete*, defined to mean that E contains a complete set of residues modulo q for each prime power relatively prime to each of a finite set $\{p_i\}_{i=1}^{n}$ of primes. We call $p_1, \dots, p_n$ *exceptional primes* for E; if E has no exceptional primes, then E is prime-power complete. Our first result is a lemma.

LEMMA 4.1. *Suppose E is a nonempty subset of $\mathbb{Z}$ and $a, b \in \mathbb{Z}$. Suppose p is a prime divisor of b. If $E(\text{mod } p^k) = [a + bE](\text{mod } p^k)$ for each positive integer k, then $|E| = 1$.*

Proof. Let $e \in E$. There exists $e_1 \in E$ such that $e \equiv a + be_1 (\text{mod } p^k)$, and $e_1 \equiv a + be_2 (\text{mod } p^k)$ for some $e_2 \in E$. Hence $e \equiv a + ab + b^2 e_2 \,(\text{mod } p^k)$. Continuing in this fashion, it follows that $e \equiv a + ab + \ldots + ab^{k-1}(\text{ mod } p^k)$; this congruence holds for each $e \in E$ and for each $k \in \mathbb{Z}^+$. Consequently, if $e' \in E$ then $e \equiv e' \ (\text{mod } p^k)$ for all k, so $e = e'$. $\square$

If $f \in \mathrm{Int}(\mathbb{Z})$ and n is a positive integer, it is known that f has positive period s modulo n, this is defined to mean that $\{i \in \mathbb{Z} \mid f(a) \equiv f(a+i)(\text{mod } n) \text{ for each } a \in \mathbb{Z}\} = s\mathbb{Z}$. Following [GS, p. 153], we use $\pi_n(f)$ to denote the period of f modulo n. Proposition 2.7 and Theorem 2.8 of [GS] show that if p is prime and the degree of f is less than p, then for any positive integer k, $\pi_{p^k}(f)$ is a divisor of p^k.

THEOREM 4.2. *If E is an almost prime-power complete subset of $\mathbb{Z}$ and $f \in \mathrm{Int}(\mathbb{Z})$ is such that E and $f(E)$ are IV-equivalent, then $f = a \pm t$ for some integer a.*

Proof. Write $f = g/d$, where $g \in \mathbb{Z}[t]$ and $d \in \mathbb{Z}^+$. Let m be the degree of g, and suppose $m > 1$. Then the derivative g' of g is nonconstant, so there exist infinitely many prime integers p such that (1) p is not one of the exceptional primes of E, (2) $p > \max\{m, d\}$, and (3) g' has a root modulo p. Suppose p is a prime satisfying (1)–(3). Since $p > m$, the result of Gilmer and Smith cited above shows that, for any positive integer k, $\pi_{p^k}(f)$ is a divisor of p^k. It follows that f induces a well-defined function $f_k : \mathbb{Z}_{p^k} \to \mathbb{Z}_{p^k}$ defined by $f_k(i + p^k\mathbb{Z}) = f(i) + p^k\mathbb{Z}$. Moreover, because $f(E)(\bmod p^k) = \mathbb{Z}_{p^k}$, f_k is surjective, and hence is a permutation on $\mathbb{Z}_{p^k}$. Since the congruence $df(i) \equiv df(j)(\mathrm{mod}\ p^k)$ is equivalent to the congruence $f(i) \equiv f(j)(\mathrm{mod}\ p^k)$, the polynomial g induces a permutation g_k of $\mathbb{Z}_{p^k}$ in the same manner. But this leads to a contradiction, for if a is a root of g' modulo p, then for any integer s, $g(a+sp) = g(a) + g'(a)(sp) + (sp)^2y$ for some integer y, and hence $g(a+sp) \equiv g(a)(\bmod p^2)$. In particular, $g_2(a + p^2\mathbb{Z}) = g_2(a + p + p^2\mathbb{Z})$. We conclude that $m \leq 1$, and it is clear that $m = 0$ is impossible.

Let $g = a + bt$, where $a, b \in \mathbb{Z}$. Since $g/d \in \mathrm{Int}(\mathbb{Z})$, we may assume without loss of generality that $d = 1$. We show that $b = \pm 1$ by showing that no prime q divides b. If $q \neq p_i$ for each i, this follows because $[a + bE](\mathrm{mod}\ q) = \mathbb{Z}_q$. If $q = p_i$ for some i, then Theorem 3.2 shows that $E(\mathrm{mod}\ h) = [a + bE](\mathrm{mod}\ h)$ for each power h of q. Since E is infinite, Lemma 4.1 shows that q does not divide b. Consequently, $b = \pm 1$ and $f = a \pm t$, as asserted. □

We consider the converse of Theorem 4.2. Clearly a polynomial $f = a \pm t$ induces a permutation of $\mathbb{Z}_n$ for each $n \in \mathbb{Z}^+$. Therefore $|E(\mathrm{mod}\ n)| = |f(E)(\mathrm{mod}\ n)|$ for each subset E of $\mathbb{Z}$, and it follows that E and $f(E)$ are IV-equivalent if E is prime-power complete. On the other hand, f need not induce a permutation of E itself. If $E = \mathbb{Z}^+$, for example, the images of E under all such polynomials f are the subsets of $\mathbb{Z}$ of the form $\{x \in \mathbb{Z} \mid x > a\}$ or $\{x \in \mathbb{Z} \mid x < a\}$ for some $a \in \mathbb{Z}$. If E is almost prime-power complete with exceptional primes $p_1, \ldots, p_n$, then again $E(\mathrm{mod}\ q) = f(E)(\mathrm{mod}\ q)$ for each prime power q such that $|E(\mathrm{mod}\ q)| = q$, and in particular this equality holds if q is relatively prime to each p_i. Thus E and $f(E)$ are IV-equivalent if and only if $E(\mathrm{mod}\ q) = f(E)(\mathrm{mod}\ q)$ for each q that is a power of some p_i. For a polynomial of the form $a + t$, there is nice criterion for determining whether this equality holds.

PROPOSITION 4.3. *Suppose $n > 1$, E is a subset of $\mathbb{Z}_n$, and $a \in \mathbb{Z}_n$. Let $f =$*

$a+t \in \mathbb{Z}_n[t]$ and denote by $\langle a \rangle$ the additive subgroup of $\mathbb{Z}_n$ generated by a. Then $E = f(E) = a+E$ if and only if E is a union of cosets of $\langle a \rangle$ in $\mathbb{Z}_n$.

The proof of Proposition 4.3 is routine, and hence is omitted.

COROLLARY 4.4. *Suppose $E \subseteq \mathbb{Z}$ and $q = p^k$ is a prime power such that $E(\text{mod } q) \neq \mathbb{Z}_q$. If $f = a+t \in \mathbb{Z}[t]$ is such that $E(\text{mod } q) = f(E)(\text{mod } q)$, then p divides a and $|E(\text{mod } q)|$ is a multiple of p^{k-i}, where $p^i = \gcd(a, p^k)$.*

For any subset E of $\mathbb{Z}_n$, there is at least one element a in $\mathbb{Z}_n$ such that $E = a+E$, but there may be no element $b \in \mathbb{Z}_n$ such that $E = b - E$. For example, the subset $\{0,1,3\}$ of $\mathbb{Z}_7$ has this property. If $E = \{e_i\}_{i=1}^k$, where $0 \leq e_1 < e_2 < \ldots, e_k \leq n-1$, if $d_i = e_i - e_{i-1}$ for $2 \leq i \leq k$, and if $d_1 = e_1 - e_k + n$, it is straightforward to show that $E = b - E$ for some b if and only if, as ordered k-tuples, $(d_1, \ldots, d_k) = (d_i, d_{i-1}, \ldots, d_1, d_k, \ldots, d_{i+1})$ for some i.

Particular examples of subsets of $\mathbb{Z}$ that are almost prime-power complete are the *homogeneous sets* of McQuillan [M2, p. 248], defined as sets of the form $\cup_{i=1}^r (a_i + n\mathbb{Z})$ for some $n \in \mathbb{Z}^+$. The Chinese Remainder Theorem implies that these subsets are almost prime-power complete and that any exceptional prime of such a subset is a divisor of n. Proposition 4.5 deals with the case of homogeneous sets.

PROPOSITION 4.5. *Suppose $n > 1$ is an integer and $E = \cup_{i=1}^r (a_i + n\mathbb{Z})$ is a subset of $\mathbb{Z}$. Then E is almost prime-power complete. If $n = q_1 q_2 \cdots q_k$ is the factorization of n into pairwise comaximal prime powers and if $f = a \pm t \in \mathbb{Z}[t]$, then E and $f(E)$ are IV-equivalent if and only if $E(\text{ mod } q_i) = f(E)(\text{ mod } q_i)$ for $1 \leq i \leq k$. If $r = 1$, E and $f(E)$ are IV-equivalent if and only if $E = f(E)$.*

Proof. The first assertion in the statement of Proposition 4.5 has already been noted. Observe that $f(E) = \cup_{i=1}^r (a \pm a_i + n\mathbb{Z})$. Hence if $q_j = p_j^{e_j}$, if $q = p_j^e$, and if $m = \min\{e_j, e\}$, then $E(\text{ mod } q) = \cup_{i=1}^r (a_i + p_j^m \mathbb{Z})$ and $f(E)(\text{ mod } q) = \cup_{i=1}^r (a \pm a_i + p_j^m \mathbb{Z})$. Since the equality $\cup_{i=1}^r (a_i + p_j^{e_i}\mathbb{Z}) = \cup_{i=1}^r (a \pm a_i + p_j^{e_i}\mathbb{Z})$ implies the corresponding equality for $1 \leq m \leq e_i$, it follows that E and $f(E)$ are equal modulo each power of p_j for $1 \leq j \leq k$ if and only if $E(\text{mod } q_j) = f(E)(\text{mod } q_j)$. Because the Chinese Remainder Theorem implies that E and $f(E)$ are equal modulo any prime power that is relatively prime to n, it follows that E and $f(E)$ are IV-equivalent if and only if $E(\text{ mod } q_i) = f(E)(\text{mod } q_i)$ for $1 \leq i \leq k$.

If $E = a_1 + n\mathbb{Z}$, the equality $a + a_1 + q_i\mathbb{Z} = a_1 + q_i\mathbb{Z}$ for each i implies that

$a \in \cap_{i=1}^k q_i\mathbb{Z} = n\mathbb{Z}$, and hence $f(E) = E$ if $f = a + t$. Similarly, the equalities $a_1 + q_i\mathbb{Z} = a - a_1 + q_i\mathbb{Z}$, $1 \le i \le k$, imply that $a_1 + n\mathbb{Z} = a - a_1 + n\mathbb{Z}$, and hence $f(E) = E$ if $f = a - t$. □

We record one consequence of the proof of Proposition 4.5 as a formal corollary.

COROLLARY 4.6. *Suppose $E = a_1 + n\mathbb{Z}$, where $n > 1$. Then E and $f(E)$ are IV-equivalent if and only if either $f = a + t$ for some $a \in n\mathbb{Z}$, or else $f = b - t$ for some $b \in 2a_1 + n\mathbb{Z}$.*

If the homogeneous set E consists of more than one residue class of $n\mathbb{Z}$ in $\mathbb{Z}$, then IV-equivalence of E and $f(E)$ need not imply equality of these two sets. To indicate some of the possibilities, we consider three examples of homogeneous sets $E = \cup_{i=1}^r (a_i + 60\mathbb{Z})$.

(1) If $r = 5$ and $\{a_i\} = \{0, 1, 2, 3, 4\}$, then E is prime-power complete and E and $f(E)$ are IV-equivalent if and only if $f = a \pm t$ for some $a \in \mathbb{Z}$.

(2) If $r = 4$ and $\{a_i\} = \{0, 1, 2, 3\}$, then $E(\text{mod } 4) = \mathbb{Z}_4$, $E(\text{mod } 3) = \mathbb{Z}_3$, and $|E(\text{mod } 5)| = 4$. Hence if $f = a + t$, Proposition 4.3 shows that E and $f(E)$ are IV-equivalent if and only if $a \in 5\mathbb{Z}$; if $g = b - t$, the criterion in the paragraph following Corollary 4.4 can be used to show that E and $g(E)$ are IV-equivalent if and only if $b \in 3 + 5\mathbb{Z}$.

(3) If $r = 4$ and $\{a_i\} = \{18, 28, 38, 48\}$, then $E(\text{ mod } 4) = \{0 + 4\mathbb{Z}, 2 + 4\mathbb{Z}\}$, $E(\text{mod } 3) = \{0 + 3\mathbb{Z}, 1 + 3\mathbb{Z}\}$, and $E(\text{mod } 5) = \{3 + 5\mathbb{Z}\}$. For $a \in \mathbb{Z}$, equality of the sets E and $a + E$ modulo 4, 3, and 5, respectively, is equivalent, respectively, to $a \equiv 0$ or $2 \pmod 4$, $a \equiv 0 \pmod 3$, and $a \equiv 0 \pmod 5$. Hence E and $f(E)$ are IV-equivalent for $f = a + t$ exactly when $a \equiv 0$ or $30 \pmod{60}$. A similar analysis for $g = b - t$ shows that E and $g(E)$ are equivalent if and only if $b \equiv 16$ or $46 \pmod{60}$.

As noted earlier, a given subset of $\mathbb{Z}_n$ need not be permuted by any polynomial of the form $b - t$. The subset $\{0, 1, 3\}$ of $\mathbb{Z}_7$ has this property, and hence the homogeneous set $E = 7\mathbb{Z} \cup (1 + 7\mathbb{Z}) \cup (3 + 7\mathbb{Z})$ is not IV-equivalent to $g(E)$ for any polynomial $g = b - t$ in $\mathbb{Z}[t]$.

5. SOME EXAMPLES

In this section we continue the study of IV-equivalence for infinite sets E. As established in Theorem 4.2, the only polynomials for which E and $f(E)$ are IV-equivalent when E is an almost a prime-power complete subset of $\mathbb{Z}$ are linear. Ultimately in this section, we explore the same questions for infinite sets which do not satisfy the denseness property of the prime-power complete subsets and produce a similar result. The question of whether there exists an infinite subset E of $\mathbb{Z}$ and a nonlinear polynomial f for which E and $f(E)$ are IV-equivalent remains open.

It is of interest to consider this problem in light of a property of fields described in [N, p.69]. In the terminology of Narkiewicz, a field K *has property (P)* if the polynomials $f(t)$ in $K[t]$ for which $f(E) = E$ for some infinite set E must be linear. It is known [N, Thm. 9.3] that the field of rational numbers has this property. For the IV-equivalence problem, the condition $E = f(E)$ is replaced by the condition $E(\text{mod } p^k) = f(E)(\text{mod } p^k)$ for every prime power p^k.

We begin our discussion in the more general context of a Dedekind domain D with FNP. In Section 3 we observed for a finite set E that E and $f(E)$ are IV-equivelent if and only if f induces a permutation on E. There is a concept of "isolated point" (defined below) which leads to a generalization of this result.

For $E \subseteq D$, an element a of E is called an *isolated point* of E if $Int(E, D) < Int(E \backslash \{a\}, D)$ [CCS3]. This terminology is used because the condition for IV-equivalence given in Theorem 2.2 yields, for an isolated point a of E, that there is a prime power Q of D for which $a + Q \neq b + Q$ for any $b \neq a$ in E. In terms of McQuillan's topological notion, this is stating that a is an isolated point of E in the P-adic completion for some prime ideal P. If E is finite, every a in E is an isolated point of E.

THEOREM 5.1. *Let D be a Dedekind domain with FNP and let I be the set of isolated points of $E \subseteq D$ If $f \in Int(D)$ is such that $f(E) \subseteq E$ and if E and $f(E)$ are IV-equivalent, then $I \subseteq f(I)$.*

Proof. We first observe that $I \subseteq f(E)$, since existence of an element $c \in I \backslash f(E)$ would yield $Int(E, D) \not\subseteq Int(E) \backslash \{a\}, D) \subseteq Int(f(E), D)$, contradicting the assumption that E and $f(E)$ are IV-equivalent. For $a \in I$, write $a = f(b)$ for some $b \in E$. We show that, in fact, $b \in I$. If b is not in I, then for each prime power P^k there exists b_k in E, $b_k \neq b$, for which $b_k \equiv b \pmod{P^k}$. Under the P-adic topology on D, integer-valued polynomials are continuous [CC, Section III.2]; hence, there exists an integer $h \geq 1$ for which $r \equiv s$ (mod P^{k+h}) implies $f(r) \equiv f(s) \pmod{P^k}$. Applied to the sequence b_k above, we have for each prime power P^k an element $f(b_{k+h})$ in E such that $f(b_{k+h}) \equiv f(b) \equiv a \pmod{P^k}$. Since infinitely many of the elements $f(b_{k+h})$ must be distinct from a, it follows that a is not an isolated point of E. Therefore, $b \in I$ and $I \subseteq f(I)$. □

EXAMPLE 5.2. Let $\mathbb{P}$ be the set of prime integers. The ring of integer-valued polynomials $Int(\mathbb{P}, \mathbb{Z})$ has been the center of study in two recent papers [CCS1] and [CCS2]. In

[CCS2] the authors show that $Int(E, \mathbb{Z}) = Int(\mathbb{P}, \mathbb{Z})$ if and only if $\mathbb{P} \subseteq E \subseteq \mathbb{P} \cup \{-1, +1\}$. Thus, if $f \in Int(\mathbb{Z})$ is such that $\mathbb{P}$ and $f(\mathbb{P})$ are IV-equivalent, then $f(\mathbb{P}) \subseteq \mathbb{P} \cup \{-1, +1\}$. Hence, for p sufficiently large, $f(p) \in \mathbb{P}$. According to the terminology of [S] this means that f is *prime mapping*, and hence $f = t$ by [S, Cor., p.391]. □

Before considering other examples, we prove a general result related to IV-equivalence in a discrete valuation domain (DVR). We note that the hypothesis of Theorem 5.3 implies that each element of the set E_1 is isolated.

THEOREM 5.3. *Suppose E_1 and E_2 are subsets of a DVR V with maximal ideal M such that E_1 mod $M^k = E_2$ mod M^k for each k in $\mathbb{Z}^+$. Let v be a normed valuation associated with V and assume that for each x in E_1, the set $A_x = \{y \in E_1 \mid v(y) = v(x)\}$ is finite. Then:*

(1) $E_2 \setminus \{0\} \subseteq E_1$.

(2) For each u in E_2, the set $B_u = \{w \in E_2 \mid v(w) = v(u)\}$ is finite.

(3) $(E_1 \setminus E_2) \cup (E_2 \setminus E_1) \subseteq \{0\}$.

Proof. For (1), choose b in $E_2 \setminus \{0\}$ and set $v(b) = c \geq 0$. For k in $\mathbb{Z}^+$ with $k > c$, each element of $b + M^k$ has v-value c. Under the assumption E_1 mod $M^k = E_2$ mod M^k, there exists an element x in E_1 such that $v(x) = c$ and $A_x = \{x_1, \ldots, x_t\}$ is finite. For each $k > c, b \equiv x_{j_k} \pmod{M^k}$ for some j_k with $1 \leq j_k \leq t$. Hence, there is an integer j, $1 \leq j \leq t$, such that $b \equiv x_j \pmod{M^k}$ for infinitely many integers k. It follows that $b = x_j$, and hence $b \in E_1$.

To establish (2) we assume there is a u in E_2 with $v(u) = c$ such that the set B_u contains infinitely many elements $u_1, u_2, \ldots$ of E_2. For any positive integer k there exists an integer $n_k > c$ such that $u_1, u_2, \ldots, u_k$ are distinct modulo M^{n_k}. Since E_1 mod $M^{n_k} = E_2$ mod M^{n_k}, there exist elements $x_1, \ldots, x_k$ in E_1 such that $x_1 \equiv u_i \pmod{M^{n_k}}$ for each i, $1 \leq i \leq k$. Thus, $v(x_i) = c$ and $x_i \neq x_j$ when $i \neq j$ since $x_i \not\equiv x_j \pmod{M^{n_k}}$. We conclude that $\mid A_{x_1} \mid \geq k$ for each k in $\mathbb{Z}^+$, a contradiction.

The inclusion given in (3) follows since (2) establishes that the set E_2 must satisfy the initial hypothesis on the set E_1, hence (1) can be applied to both sets. □

In the notation of Theorem 5.3 we remark that it is possible to have $E_1 = E_2 \cup \{0\}$. This occurs, for example, if V is $\mathbb{Z}$ localized at the prime $2\mathbb{Z}$ and $E_2 = \{2^i\}_{i=1}^{\infty}$.

The finiteness condition on the set E_1 in the case of a DVR is related to the concept of isolated points used earlier in this section. In fact, it is easily observed that the condition implies every x in E_1 is an isolated point. For a Dedekind domain with FNP the IV-equivalence conditions localizes (that is, $Int(E_1, D) = Int(E_2, D)$ implies $Int(E_1, D_P) = Int(E_2, D_P)$ [CC, Prop.I.2.7]). However, care must be taken in that every element of a set E may be an isolated point when considered in the setting of the domain D, but not in the local setting of the DVR D_P. This is illustrated by Example 5.2. To wit, if $\mathbb{P}$ is the set of prime integers, then as a subset of $\mathbb{Z}$, every point is isolated, but as a subset of $\mathbb{Z}_{(p)}$ for a fixed prime p, only the element p of $\mathbb{P}$ is isolated. This fact is an easy consequence of Dirichlet's Theorem, which yields for each prime q different from p an infinite sequence of distinct primes q_k such that $q_k \equiv q \pmod{p^k}$. However, there are subsets E of a domain D for which we can apply the results of Theorem 5.3. The proof of our next result uses a basic lemma.

LEMMA 5.4. *Suppose K is a field with property (P), E is an infinite subset of K, and $f \in K[t]$ is such that $E \subseteq f(E)$. Then f is linear.*

Proof. If $E^* = E \cup f(E) \cup f(f(E)) \cup ...$, the hypothesis implies that $f(E^*) = E^*$. Since E^* is infinite and K has property (P), we conclude that f is linear. □

THEOREM 5.5. *Suppose D is a Dedekind domain with quotient field K satisfying property (P). Assume that E is an infinite subset of D which does not contain 0 and which satisfies the hypothesis of Theorem 5.3 in the DVR D_P for some prime ideal P of D. If $f \in Int(D)$ is such that E and $f(E)$ are IV-equivalent, then f is a linear polynomial.*

Proof. The hypothesis implies that $Int(E, D_P) = Int(f(E), D_P)$, where $f \in Int(D_P)$ [CC, p. 7]. Thus, Theorem 5.3 implies that $E = f(E)$ or $f(E) = E \cup \{0\}$. In either case, $E \subseteq f(E)$, so Lemma 5.4 shows that f is linear. □

EXAMPLE 5.6. Let $E = \{n^{k_i}\}_{i=1}^{\infty}$, where $n \geq 2$ is an integer and $\{k_i\}_1^{\infty}$ is a strictly increasing sequence of positive integers. The set E satisfies the hypothesis of Theorem 5.5 by choosing for P the ideal $p\mathbb{Z}$, where p is any prime divisor of n. Hence (5.5) shows that if $f \in Int(\mathbb{Z})$ is such that E and $f(E)$ are IV-equivalent, then f is linear — say $f(t) = at + b$ for some $a, b \in \mathbb{Z}$. In fact, $a = 1$ and $b = 0$ by the following argument. Theorem 5.3 shows that $f(E) = E$ or $f(E) = E \cup \{0\}$, so $a > 0$. Hence, $\lim_{m \to \infty} f(m) = \infty$. If $s \in \mathbb{Z}^+$, there exists $N \in \mathbb{Z}^+$ such that $f(m) > n^s$ for $m > N$. It follows that n^s divides $f(m)$ for $m > N$. If $i \in \mathbb{Z}^+$ is such that $k_i > s$ and $n^{k_i} > N$, then n^s divides

$f(n^{k_i}) = an^{k_i} + b$. Therefore, n^s divides b, and because s is arbitrary, $b = 0$. If $a > 1$ we obtain the contradiction that each element x of $f(E)$ satisfies $x \geq an^{k_1} > n^{k_1}$, and hence $E \not\subseteq f(E)$. $\square$

EXAMPLE 5.7. Let $E = \{n_i!\}_{i=1}^{\infty}$, where $\{n_i\}_{i=1}^{\infty}$ is a strictly increasing sequence of nonnegative integers. For each prime ideal $p\mathbb{Z}$ of $\mathbb{Z}$, the set E satisfies the hypothesis of Theorem 5.5. Thus, if $f \in Int(\mathbb{Z})$ is such that E and $f(E)$ are IV-equivalent, then $f(t) = at + b$ is linear; here a and b are integers. It follows from Theorem 5.3 that for i sufficiently large, $f(n_i!) = M_i! \in E$. Thus, $a > 0$ and $\lim_{i\to\infty} M_i! = \infty$. Let p be a positive prime. There exists $i \in \mathbb{Z}^+$ such that $p < n_i$ and $p \mid M_i$. Thus, p divides $M_i! - a(n_i!) = b$, and hence $b = 0$. If $a > 1$, then $M_i! = a(n_i!) > n_i!$, so $(n_i + 1)!$ divides $a(n_i!)$ and $n_i + 1$ divides a. This contradiction shows that $a = 1$, and $f(t) = t$, as asserted. $\square$

REFERENCES

[C] P.-J. CAHEN, Parties pleines d'un anneaux noethérien, *J. Algebra* 157 (1993), 199–212.

[CC] P.-J. CAHEN and J.-L. CHABERT, "Integer-Valued Polynomials", Math. Surveys and Monographs Vol. 48, Amer. Math. Soc., Providence, RI, 1997.

[Ch1] J.-L. CHABERT, Une caractérisation des polynômes prenant des valeurs entières sur tous les nombres premiers, *Canad. Math. Bull.* 39 (1996), 402–407.

[Ch2] J.-L. CHABERT, Anneaux de "Polynomes à valeurs entières et anneaux de Fatou", *Bull. Soc. Math. France* 99 (1971), 273–282.

[CCS1] J.-L. CHABERT, S. CHAPMAN, and W.W. SMITH, A basis for the ring of polynomials integer-valued on prime numbers, Lecture Notes in Pure and Appl. Math. Vol. 189, Marcel-Dekker, New York, 1997, pp. 271–284.

[CCS2] J.-L. CHABERT, S. CHAPMAN, and W.W. SMITH, Algebraic properties of the ring of integer-valued polynomials on prime numbers, *Comm. Algebra* 25 (1997), 1947–1959.

[CCS3] J.-L. CHABERT, S. CHAPMAN, and W.W. SMITH, The Skolem property in rings of integer-valued polynomials, Proc. Amer. Math. Soc. (to appear).

[G1] R. GILMER, Sets that determine integer-valued polynomials, *J. Number Theory* 33 (1989), 95–100.

[G2] R. GILMER, Prüfer domains and rings of integer-valued polynomials, *J. Algebra* 129 (1990), 502–517.

[GM] H. GUNJI and D.L. MCQUILLAN, On a class of ideals in an algebraic number field

J. Number Theory 2 (1970), 207–222.

[M1] D.L. MCQUILLAN, Rings of integer-valued polynomials determined by finite sets, *Proc. Roy. Irish Acad. Sect. A* 85 (1985), 177–184.

[M2] D.L. MCQUILLAN, On a theorem of R. Gilmer, *J. Number Theory* 39 (1991), 245–250.

[M3] D.L. MCQUILLAN, On Prüfer domains of polynomials, *J. Reine Angew. Math.* 358 (1985), 162–178.

[N] W. NARKIEWICZ, "Polynomial Mappings", Lecture Notes in Math, Vol. 1600, Springer, Berlin-Heidelberg, 1995.

[R] G. RAUZY, Ensembles arithmétiquement denses, *C.R. Acad. Sci. Paris* 265 (1967), 37–38.

[S] E.G. STRAUSS, Functions periodic modulo each of a sequence of integers, *Duke Math. J.* 19 (1952), 379–395.