RELATIVE POLYNOMIAL CLOSURE AND MONADICALLY KRULL MONOIDS OF INTEGER-VALUED POLYNOMIALS

SOPHIE FRISCH

Abstract. Let D be a Krull domain and $\mathrm{Int}(D)$ the ring of integer-valued polynomials on D. For any $f \in \mathrm{Int}(D)$, we explicitly construct a divisor homomorphism from $[\![f]\!]$, the divisor-closed submonoid of $\mathrm{Int}(D)$ generated by f, to a finite sum of copies of $(\mathbb{N}_0, +)$. This implies that $[\![f]\!]$ is a Krull monoid.

For V a discrete valuation domain, we give explicit divisor theories of various submonoids of $\mathrm{Int}(V)$. In the process, we modify the concept of polynomial closure in such a way that every subset of D has a finite polynomially dense subset. The results generalize to $\mathrm{Int}(S, V)$, the ring of integer-valued polynomials on a subset, provided S doesn't have isolated points in v-adic topology.

1. Introduction

The ring of integer-valued polynomials $\mathrm{Int}(\mathbb{Z})$ enjoys quite chaotic non-unique factorization: given any finite list of natural numbers $1 < n_1 \leq n_2 \leq \ldots \leq n_k$, one can find a polynomial $f \in \mathrm{Int}(\mathbb{Z})$ that has exactly k essentially different factorizations into irreducible elements of $\mathrm{Int}(\mathbb{Z})$, namely, one with n_1 irreducible factors, one with n_2, etc. [4]. In contrast to this, A. Reinhart [9] has shown for any unique factorization domain D that $\mathrm{Int}(D)$ is monadically Krull, i.e., that the divisor-closed submonoid $[\![f]\!]$ generated by any single polynomial $f \in \mathrm{Int}(D)$ (the monoid consisting of all divisors in $\mathrm{Int}(D)$ of powers of f) is a Krull monoid. So we have here an interesting case of Krull monoids with rather wild factorization properties.

In this paper we find divisor homomorphisms and, in some cases, divisor theories for the divisor closed submonoids generated by single polynomials $f \in \mathrm{Int}(S, D)$, the ring of integer-valued polynomials on a subset of a Krull domain. If S doesn't have any isolated points in any of the topologies given by essential valuations of D, we can construct a divisor homomorphism from $[\![f]\!]$ to a finite direct sum of copies of $(\mathbb{N}_0, +)$ [Theorem 5.4]. This implies that $[\![f]\!]$ is a Krull monoid, and hence, that $\mathrm{Int}(S, D)$ is monadically Krull.

2000 *Mathematics Subject Classification.* Primary 13F20; Secondary 20M13, 13A05, 13B25, 11C08, 11R09.

Key words and phrases. monoid, factorization, monadically Krull, divisor homomorphism, divisor theory, integer-valued polynomial, polynomial closure.

This publication was supported by the Austrian Science Fund FWF, grant P23245-N18.

In the special case of D being a discrete valuation domain, we can determine explicitly the divisor theories of certain submonoids of $\mathrm{Int}(S, D)$ [Theorem 4.2 and Theorem 5.3].

As a tool for constructing divisor homomorphisms on monoids of integer-valued polynomials, we introduce "relative" polynomial closure, that is, polynomial closure with respect to a subset of $K[x]$, in section 2. This modification of the concept of polynomial closure makes it possible to find finite polynomially dense subsets of arbitrary sets in section 3. Equipped with these finite polynomially dense sets we construct the actual divisor homomorphisms and, in some cases, divisor theories, to finite sums of copies of $(\mathbb{N}_0, +)$ in sections 4 and 5.

The remainder of this introduction contains a short review of concepts and notation related to integer-valued polynomials.

Definition 1.1. Let D be a domain with quotient field K and $f \in K[x]$. f is called integer-valued if $f(D) \subseteq D$. For a subset $S \subseteq K$, $f \in K[x]$ is called integer-valued on S if $f(S) \subseteq D$. When there are several possibilities for D, we say D-valued on S instead of integer-valued on S.

The ring of integer-valued polynomials on D is written $\mathrm{Int}(D)$, and the ring of integer-valued polynomials on a subset S of the quotient field of D is denoted by $\mathrm{Int}(S, D)$:

$$\mathrm{Int}(S, D) = \{f \in K[x] \mid f(S) \subseteq D\}, \quad \mathrm{Int}(D) = \mathrm{Int}(D, D).$$

Definition 1.2. Let D be a domain with quotient field K, $S \subseteq D$ and $f \in \mathrm{Int}(S, D)$. The divisor-closed submonoid of $\mathrm{Int}(S, D)$ generated by f, which we write $[\![f]\!]$, is the multiplicative monoid consisting of all $g \in \mathrm{Int}(S, D)$ for which there exists $m \in \mathbb{N}$ and $h \in \mathrm{Int}(S, D)$, such that $g \cdot h = f^m$.

Keep in mind that an element of $[\![f]\!]$ is not just a polynomial $g \in \mathrm{Int}(S, D)$ that divides some power of f in $K[x]$. The co-factor $h = f^m/g$ is also required to be in $\mathrm{Int}(S, D)$. Take for example $\binom{x}{2}$ in $\mathrm{Int}(\mathbb{Z})$. Here x divides f in $K[x]$, but $x \notin [\![f]\!]$.

We will frequently use the following divisibility criterion for $[\![f]\!]$.

Remark 1.3. Let $[\![f]\!]$ be the divisor closed submonoid of $\mathrm{Int}(S, D)$ as in Definition 1.2 and $g, h \in [\![f]\!]$. Then g divides h in $[\![f]\!]$ if and only if g divides h in $K[x]$ and the cofactor h/g is in $\mathrm{Int}(S, D)$.

Multiplying a polynomial in $[\![f]\!]$ by a constant in D does not in general result in an element of $[\![f]\!]$. We can multiply elements of $[\![f]\!]$ by some suitable constants, though, see Lemma 1.4 below.

Regarding valuation terminology: we use additive valuations, that is, a valuation is a map $v\colon K \setminus \{0\} \to \Gamma$, where $(\Gamma, +)$ is a totally ordered group, satisfying

(1) $v(ab) = v(a) + v(b)$
(2) $v(a + b) \geq \min(v(a), v(b))$

and we set $v(0) = \infty$. The valuation domain of a valuation v on a field K is $V = \{k \in K \mid v(k) \geq 0\}$ and the valuation group is the image of v in Γ.

Lemma 1.4. *Let V be the valuation domain of a valuation v on K, $S \subseteq V$, $f \in \mathrm{Int}(S,V)$ and $[\![f]\!]$ the divisor-closed submonoid of $\mathrm{Int}(S,V)$ generated by f. Let $g \in [\![f]\!]$ and $a \in K$. If $-\min_{s\in S} v(g(s)) \leq v(a) \leq 0$ then $ag \in [\![f]\!]$.*

Proof. Let $g, h \in \mathrm{Int}(S,V)$ and $m \in \mathbb{N}$ such that $gh = f^m$. Then both ag and $a^{-1}h$ are in $\mathrm{Int}(S,V)$, and $ag \cdot a^{-1}h = f^m$. □

We recall the definitions of ideal content and fixed divisor, whose interplay will be an important ingredient of proofs. Let R be a domain and $f \in R[x]$. The content of f, denoted $c(f)$, is the fractional ideal generated by the coefficients of f. If R is a principal ideal domain, we identify, by abuse of notation, ideals by their generators and say that $c(f)$ is the gcd of the coefficients of f. A polynomial $f \in R[x]$ is called primitive if $c(f) = R$, that is, in the case of a PID, if $c(f) = 1$.

Definition 1.5. Let D be a domain with quotient field K, $S \subseteq D$ and $f \in K[x] \setminus \{0\}$. The *fixed divisor of f on S*, denoted $\mathrm{d_S}(f)$, is the D-submodule of K generated by the image $f(S)$. Note that $\mathrm{d_S}(f)$ is a fractional ideal. If $S = D$, we write $\mathrm{d}(f)$ for $\mathrm{d_D}(f)$. If D is a PID, we will, by abuse of notation, sometimes write a generator to stand for the ideal, e.g., $\mathrm{d_S}(f) = 1$ for $\mathrm{d_S}(f) = D$. A polynomial $f \in \mathrm{Int}(S,D)$ is called *image-primitive* if $\mathrm{d_S}(f) = D$.

For polynomials in $D[x]$, image-primitive implies primitive, but not vice versa. One difference between ideal content and fixed divisor is that the ideal content is multiplicative for sufficiently nice rings - called Gaussian rings - including principal ideal rings, whereas the fixed divisor is not multiplicative. $\mathrm{d_S}(f)\,\mathrm{d_S}(g)$ contains $\mathrm{d_S}(fg)$, but the containment is often strict.

Remark 1.6. Two easy but useful facts:

1. If $f \in \mathrm{Int}(S,D)$ is image-primitive then f^n is image-primitive for all $n \in \mathbb{N}$.
2. If $f \in \mathrm{Int}(S,D)$ is image-primitive then all divisors in $\mathrm{Int}(S,D)$ of f are also image-primitive.

Remark 1.7. In case D is an intersection of valuation rings, then every $f \in \mathrm{Int}(S,D)$ is also in $\mathrm{Int}(S,V)$ for all these valuation rings, and f may be image-primitive as an element of $\mathrm{Int}(S,V)$, but not as an element of $\mathrm{Int}(S,D)$. In this case, we write

$$v(f(S)) := \min_{s\in S} v(f(s))$$

and write $v(f(S)) = 0$ to express that f is image-primitive when regarded as an element of $\mathrm{Int}(S,V)$.

2. Relative polynomial closure

Definition 2.1 (relative polynomial closure)**.** Fix a domain D with quotient field K. Let $T \subseteq K$ and $\mathcal{F} \subseteq K[x]$.

The polynomial closure of T relative to $\mathcal{F}$ is

$$C_{\mathcal{F}}(T) = \{s \in K \mid \forall f \in \mathcal{F} \cap \mathrm{Int}(T, D): \; f(s) \in D\}.$$

If $T \subseteq S \subseteq K$, and $C_{\mathcal{F}}(T) \supseteq S$ we call T polynomially dense in S relative to $\mathcal{F}$.

The definition of polynomial closure and polynomial density depends on the choice of D. If there is any doubt about D, we say D-polynomial closure and D-polynomially dense.

Polynomial closure relative to $K[x]$ is the "usual" polynomial closure, introduced by Gilmer [6] and studied by McQuillan [7], the present author [3], Cahen [1], Park and Tartarone [8] and Chabert [2], among others. The reason why we generalize the well-known concept of polynomial closure will become apparent in the next section: when we consider polynomial closure relative to a set of polynomials whose irreducible factors are restricted to a finite set, it becomes possible to find finite polynomially dense subsets of any fractional set.

Remark 2.2. The following properties of polynomial closure relative to a subset $\mathcal{F}$ of $K[x]$ are easy to check.

(1) $C_{\mathcal{F}}(T) = \bigcap_{f \in \mathcal{F} \cap \mathrm{Int}(T,D)} f^{-1}(D)$
(2) Polynomial closure relative to $\mathcal{F}$ is a closure operator, in the sense that
  (a) $T \subseteq C_{\mathcal{F}}(T)$
  (b) $C_{\mathcal{F}}(C_{\mathcal{F}}(T)) = C_{\mathcal{F}}(T)$
  (c) $T \subseteq S \Longrightarrow C_{\mathcal{F}}(T) \subseteq C_{\mathcal{F}}(S)$
(3) Polynomial closure relative to $\mathcal{F}$ is the closure given by a Galois correspondence that maps every subset T of K to a subset of $\mathcal{F}$, and every subset G of $\mathcal{F}$ to a subset of K, namely,

$$T \mapsto \mathcal{F} \cap \mathrm{Int}(T, D) \quad \text{and} \quad G \mapsto \bigcap_{f \in G} f^{-1}(D).$$

(4) If $\mathcal{F}_0 \subseteq \mathcal{F}_1 \subseteq K[x]$ then $C_{\mathcal{F}_1}(T) \subseteq C_{\mathcal{F}_0}(T)$.
(5) If T is polynomially dense in S relative to $\mathcal{F}_1$, and $\mathcal{F}_0 \subseteq \mathcal{F}_1$, then T is polynomially dense in S relative to $\mathcal{F}_0$.

When D is a valuation domain, then polynomially dense subsets of S relative to $\mathcal{F}$ are easily characterized (subject to a weak condition on $\mathcal{F}$): they are the subsets T such that, for each $f \in \mathcal{F}$, $\min_{s \in S} v(f(s))$ is attained by some $s \in T$.

Lemma 2.3. *Let v be a valuation on a field K, V its valuation ring, $T \subseteq S \subseteq K$ and $\mathcal{F} \subseteq K[x]$. Consider*

(1) $\forall f \in \mathcal{F} \;\; \min_{s \in S} v(f(s)) = \min_{t \in T} v(f(t))$
(2) *T is V-polynomially dense in S relative to $\mathcal{F}$.*

(1) *implies* (2). *If $\mathcal{F}$ is closed under multiplication by non-zero constants in K then* (2) *implies* (1).

Proof. (1 $\Rightarrow$ 2) For every polynomial $f \in \mathcal{F} \cap \mathrm{Int}(T, V)$, $\min_{t\in T} v(f(t)) \geq 0$. Therefore, by (1), $\min_{s\in S} v(f(s)) \geq 0$ and hence $f \in \mathrm{Int}(S, V)$.

(2 $\Rightarrow$ 1) For every $f \in \mathcal{F}$, $\min_{t\in T} v(f(t)) \geq \min_{s\in S} v(f(s))$, since $T \subseteq S$. If $f \in \mathcal{F}$ and $\alpha \in \mathbb{Z}$ are such that $\min_{t\in T} v(f(t)) \geq \alpha > \min_{s\in S} v(f(s))$, pick $a \in K$ with $v(a) = -\alpha$. Then $af \in \mathcal{F} \cap \mathrm{Int}(T, V)$, but $af \notin \mathrm{Int}(S, V)$, so T is not V-polynomially dense in S relative to $\mathcal{F}$. □

3. Finite polynomially dense subsets

Let F be a finite set of irreducible polynomials in $K[x]$ and $\mathcal{F}$ the multiplicative submonoid of $K[x]$ generated by F and the non-zero constants of K. That is, $\mathcal{F}$ consists of all non-zero polynomials in $K[x]$ whose irreducible factors in $K[x]$ are (up to multiplication by non-zero constants) in F.

We will now construct, for every subset S of a discrete valuation ring V, a finite polynomially dense subset of S relative to $\mathcal{F}$. It is possible to admit fractional subsets of K, but for simplicity's sake we restrict ourselves to subsets of V.

By discrete valuation, we mean, more precisely, a discrete rank 1 valuation, that is, a valuation v whose value group is isomorphic to $\mathbb{Z}$. A normalized discrete valuation is one whose value group is actually equal to $\mathbb{Z}$. The valuation ring of a discrete valuation is called discrete valuation ring, abbreviated DVR. As we all know, a DVR is a local principal ideal domain.

Remark 3.1. Let v be a discrete valuation on K with valuation ring V, $f \in K[x]$, and $L \supseteq K$ a finite-dimensional field extension over which f splits. Let w be an extension of v to L ($w\mid_K = v$), W the valuation ring of w and P its maximal ideal. Say f splits as $f(x) = c\prod_{j=1}^{k}(x - b_j)\prod_{j=1}^{m}(x - a_j)$ with $w(b_j) < 0$ for $1 \leq j \leq k$ and $w(a_j) \geq 0$ for $1 \leq j \leq m$ over L.

Then for all $s \in V$,

$$v(f(s)) = w(c) + \sum_{j=1}^{k} w(b_j) + \sum_{j=1}^{m} w(s - a_j)$$

Proof. This follows from the fact that $w(s \pm b) = w(b)$ whenever $w(b) < w(s)$. □

Definition 3.2. Let X be a topological space and $S \subseteq X$. An isolated point of S is an element $s \in X$ having a neighborhood U such that $U \cap S = \{s\}$.

Proposition 3.3. *Let v be a discrete valuation on K and V its valuation ring. Let $F \neq \emptyset$ be a finite set of monic irreducible polynomials in $K[x]$ and $\mathcal{F}$ the set of those polynomials in $K[x]$ whose monic irreducible factors are all in F. Let $S \subseteq V$.*

(1) *Then there exists a finite subset $T \subseteq S$ such that*
$$\forall f \in \mathcal{F}\ \min_{t\in T} v(f(t)) = \min_{s\in S}(v(f(s)))$$
and every such $T \subseteq S$ is, in particular, a finite set that is polynomially dense in S relative to $\mathcal{F}$.

(2) *If no root of any $f \in F$ is an isolated point of S in v-adic topology, then the above set T can be chosen such as not to contain any root of any $f \in F$.*

(3) *Let L be the splitting field of F over K, w an extension of v to L and W the valuation ring of w. Let A be the set of distinct roots of polynomials of F in W. Then T in (1) and (2) can be chosen with $|T| \leq \max(1, |A|)$.*

Proof. Let L, w, W, and A as in (3). Let P be the maximal ideal of W. We call the elements of A "the roots". We may assume $S \neq \emptyset$ and $A \neq \emptyset$ (otherwise the claimed facts are trivial). In view of Remark 3.1, to show (1) it suffices to construct a finite set $T \subseteq S$ such that, for every finite sequence $(a_i)_{i=1}^m$ in A,

$$\min_{t \in T} \sum_{i=1}^{m} w(t - a_i) = \min_{s \in S} \sum_{i=1}^{m} w(s - a_i)$$

We will do this by constructing a finite covering $\mathcal{C}$ of S by disjoint sets $C \subseteq W$ and for each $C \in \mathcal{C}$ choosing a representative $t \in C \cap S$ such that $w(t - a) \leq w(s - a)$ for every $a \in A$ and every $s \in C \cap S$. This representative $t \in C \cap S$ then satisfies $\forall f \in \mathcal{F}\ v(f(t)) = \min_{s \in C \cap S} v(f(s))$, by Remark 3.1. If we take T to be the set of representatives of covering sets $C \in \mathcal{C}$ then for every $f \in \mathcal{F}$, $\min_{s \in S} v(f(s))$ is realized by some $s \in T$. By Lemma 2.3, this makes T polynomially dense in S relative to $\mathcal{F}$.

For any ideal I of W, we call a residue class $r + I$ "relevant" if $S \cap (r + I) \neq \emptyset$.

We construct $\mathcal{C}$, $\mathcal{C}_n$ ($n \geq 0$) and T inductively. Before step 0, initialize $T = \emptyset$, $\mathcal{C} = \emptyset$, $\mathcal{C}_0 = \{W\}$.

At the beginning of step n, $\mathcal{C}$ is a finite set of relevant residue classes of various P^k with $k < n$ while $\mathcal{C}_n$ is a finite set of relevant residue classes of P^n each containing at least one root. In step n, initialize $\mathcal{C}_{n+1} = \emptyset$; then go through each $C \in \mathcal{C}_n$ and process it as follows:

(1) If $C \cap S = \{c\}$ with $c \in A$ then put c in T and C in $\mathcal{C}$. Note that in this case $C \cap V$ is a v-adic neighborhood of c whose intersection with S is $\{c\}$, and that therefore $c \in A$ is an isolated point of S.

(2) Else, if C contains a relevant residue class D of P^{n+1} which doesn't contain a root, pick such a D, add a representative of $D \cap S$ to T; then put C in $\mathcal{C}$.

(3) Else place all relevant residue classes of P^{n+1} contained in C (each containing a root, by construction) in $\mathcal{C}_{n+1}$.

If $\mathcal{C}_{n+1}$ is empty at the end of step n, stop. Otherwise proceed to step $n + 1$.

Note that after each step n, $\mathcal{C} \cup \mathcal{C}_{n+1}$ is a covering of S. When the algorithm terminates with $\mathcal{C}_{n+1} = \emptyset$, then $\mathcal{C}$ is a covering of S and T contains for each $C \in \mathcal{C}$ a representative $t \in C \cap S$ satisfying $w(t - a) = \min_{s \in C \cap S} w(s - a)$ for all $a \in A$. Therefore $v(f(t)) = \min_{s \in C \cap S} v(f(s))$ for all $f \in \mathcal{F}$ by Remark 3.1.

The algorithm terminates when no root is left in $\bigcup \mathcal{C}_{n+1}$. For each root $a \in A$, one can give an upper bound on n such that a is no longer in $\mathcal{C}_{n+1}$. Namely, let n such that $w(a - a') < n$ for all roots $a \neq a'$. If $(a + P^{n+1}) \cap S = \emptyset$ then a residue class containing a has been dropped as not relevant at or before step n, so $a + P^{n+1} \notin \mathcal{C}_{n+1}$. If $(a + P^{n+1}) \cap S = \{a\}$, then a residue class containing a is placed in $\mathcal{C}$ at step $n + 1$ or earlier. Otherwise, $a + P^{n+1}$ contains an element of S other than a. Let $s \in (a + P^{n+1}) \cap S$, with $w(s - a) = m$ minimal. Then $a + P^m$ will be placed in $\mathcal{C}$ by step m.

This shows (1). For (2), note that the set T thus constructed contains no root of any $f \in F$ except such as are isolated points of S in v-adic topology. For (3), note that every time an element is added to T, a set containing at least one root is transferred from $\mathcal{C}_n$ to $\mathcal{C}$ and the number of roots in $\bigcup_{C \in \mathcal{C}_n} C$ decreases. □

Remark 3.4. Thanks to the anonymous referee for pointing out that parts (1) and (2) of Proposition 3.3 can be show more quickly by applying Dickson's theorem [5][Thm. 1.5.3], which says that the set of minimal elements of any subset N of $\mathbb{N}_0^m$ is finite and that for every $a \in N$ there exists a minimal element $b \in N$ with $b \leq a$, to the subset $N = \{(w(s - a))_{a \in A} \mid s \in S\}$ of $\mathbb{N}_0^A$.

4. Divisor theories for monoids of integer-valued polynomials on discrete valuation rings

We are going to construct divisor homomorphisms from submonoids of $\mathrm{Int}(S, D)$, where D is a Krull domain, to finite sums of copies of $(\mathbb{N}_0, +)$. The idea is to gain insight into divisibility in $\mathrm{Int}(S, D)$ by relating it to divisibility in a finitely generated free commutative monoid. In this section, we assume V to be a discrete valuation domain and determine the divisor theory of the submonoid consisting of all elements of $\mathrm{Int}(S, V)$ whose irreducible factors in $K[x]$ come from a fixed finite set.

By *monoid* we mean a semigroup that has a neutral element. All monoids that we examine here are cancellative, that is, whenever $ab = cb$ or $ba = bc$, it follows that $a = c$. Also, all our monoids will be commutative.

A short review of divisibility terminology, in the perhaps less familiar additive form: Let $(M, +)$ be a commutative monoid, written additively, and $a, b \in M$.

(1) We say that a *divides* b in M and write $a \mid b$, whenever there exists $c \in M$ such that $a + c = b$.
(2) We call an element $d \in M$ a *greatest common divisor*, abbreviated gcd, of a subset $A \subseteq M$, if
   (a) $d \mid a$ for all $a \in A$
   (b) for all $c \in M$: if $c \mid a$ for all $a \in A$ then $c \mid d$.

If $(M, +)$ is a direct sum of k copies of $(\mathbb{N}_0, +)$, then the divisibility relation in M is just the partial order given by the order relations on each component: Let $a, b \in M = \sum_{i=1}^{k} (\mathbb{N}_0, +)$ with $a = (a_1, \ldots, a_k)$ and $b = (b_1, \ldots, b_k)$. Then $a \mid b$ in M is equivalent to $a_i \leq b_i$ for all $1 \leq i \leq k$. Therefore, any set $\{(m_{i1}, m_{i2}, \ldots, m_{ik}) \mid i \in I\}$ of elements of M has a unique gcd, namely, $d = (\min_i(m_{i1}), \min_i(m_{i2}), \ldots, \min_i(m_{ik}))$.

Definition 4.1. A monoid homomorphism $\varphi\colon G \to H$ is called a divisor homomorphism if $\varphi(a) \mid \varphi(b)$ in H implies $a \mid b$ in G. (Note that the reverse implication holds for every monoid homomorphism).

A divisor homomorphism $\varphi\colon G \to \sum_{i=1}^{n}(\mathbb{N}_0, +)$ is called a divisor theory if each of the unit vectors e_i (having 1 in the i-th coordinate and zeros elsewhere) occurs as gcd of a finite set of images of elements of G.

In what follows, we denote the normalized discrete valuation on $K(x)$ corresponding to an irreducible polynomial $h \in K[x]$ by v_h; that is, for $g \in K[x]$, $v_h(g)$ is the exponent to which h occurs in the essentially unique factorization of g in $K[x]$ into irreducible polynomials, and for $g_1/g_2 \in K(x)$, $v_h(g_1/g_2) = v_h(g_1) - v_h(g_2)$.

In this section we examine the special case $\mathrm{Int}(S, V)$, where V is a discrete valuation ring (DVR).

Theorem 4.2. *Let v be a normalized discrete valuation on K and V its valuation ring. Let H be a finite set of pairwise non-associated irreducible polynomials in $K[x]$ and $\mathcal{H}$ the multiplicative submonoid of $K[x]$ generated by H and the non-zero constants in K. Let $S \subseteq V$ such that no root of any $h \in H$ is an isolated point of S in v-adic topology. Let $\mathcal{F} = \mathcal{H} \cap \mathrm{Int}(S, V)$.*

There exists a finite subset T of S that is polynomially dense in S relative to $\mathcal{H}$ and contains no root of any $h \in H$; and for every such T

$$\varphi\colon \mathcal{F} \to \sum_{h\in H}(\mathbb{N}_0, +) \oplus \sum_{t\in T}(\mathbb{N}_0, +), \quad \varphi(g) = ((v_h(g) \mid h \in H), (v(g(t)) \mid t \in T)),$$

is a divisor homomorphism. If T is chosen minimal, φ is a divisor theory.

Proof. The existence of a finite polynomially dense subset T containing no root of any $h \in H$ is Proposition 3.3. Once we have a finite dense set, a minimal dense set can be obtained by removing redundant elements.

φ is well defined, because T contains no root of any $h \in H$. Once φ is a well-defined function, it clearly is a monoid homomorphism. Now suppose $a, b \in \mathcal{F}$ such that $\varphi(a) \mid \varphi(b)$, and set $c = b/a$. We must show $c \in \mathrm{Int}(S, V)$.

$\varphi(a) \mid \varphi(b)$ means $v_h(a) \leq v_h(b)$ for all $h \in H$ and $v(a(t)) \leq v(b(t))$ for all $t \in T$. The first shows $c \in K[x]$, and therefore $c \in \mathcal{H}$, and the second shows that $c(t) \in V$ for all $t \in T$. Since T is polynomially dense in S relative to $\mathcal{H}$, it follows that $c \in \mathrm{Int}(S, V)$. We have shown φ to be a divisor homomorphism.

It remains to show that every e_h for any $h \in H$ and every e_t for any $t \in T$ occurs as the gcd of a finite set of images of elements of $\mathcal{F}$, provided T is minimal.

We may assume, without changing $\mathcal{H}$, $\mathcal{F}$ or φ in any way, that the elements of H are in $V[x]$ and primitive.

First, let p be a generator of the maximal ideal of V. The constant polynomial p is an element of $\mathcal{F}$ satisfying $v_h(p) = 0$ for all $h \in H$ and $v(p(t)) = 1$ for all $t \in T$.

Second, we note that every polynomial $h \in H$ is an element of $\mathcal{F}$ satisfying $v_h(h) = 1$ and $v_l(h) = 0$ for every $l \in H \setminus \{h\}$.

Third, we show that for every $t \in T$, there exists $g_t \in \mathcal{F}$ such that $v(g_t(t)) = 0$ and $v(g_t(r)) > 0$ for all $r \in T \setminus \{t\}$. We use the minimality of T and Lemma 2.3: Since T is polynomially dense in S relative to $\mathcal{H}$, but $T \setminus \{t\}$ is not, there exists a polynomial $k \in \mathcal{H}$ with $v(k(t)) = \min_{s\in S} v(k(s))$ and $v(k(r)) > \min_{s\in S} v(k(s))$ for all $r \in T\setminus\{t\}$. Let k be such a polynomial and $\alpha = v(k(t))$. Then $g_t(x) = p^{-\alpha}k(x)$ has the desired properties.

Fourth, we show that for every $t \in T$ and $h \in H$ there exists $g_{th} \in \mathcal{F}$ such that $v(g_{th}(t)) = 0$ and $v_h(g_{th}) > 0$. Let k be any polynomial in $\mathcal{F}$ with $v_h(k) > 0$. If $v(k(t)) = \alpha > 0$, set $g_{th}(x) = p^{-\alpha}k(x)g_t(x)^{\alpha}$.

Now for any $h \in H$ and $t \in T$,

$$e_h = \gcd\big(\{\varphi(g_{th}) \mid t \in T\} \cup \{\varphi(h)\}\big) \quad \text{and} \quad e_t = \gcd\big(\{\varphi(g_r) \mid r \neq t\} \cup \{\varphi(p)\}\big).$$

$\square$

5. Divisor homomorphisms on monadic monoids of integer-valued polynomials

What we have found out about the submonoid of $\mathrm{Int}(S, V)$ consisting of polynomials whose irreducible factors in $K[x]$ come from a fixed finite set, we now apply to the divisor closed submonoid of $\mathrm{Int}(S, V)$ generated by a single polynomial. We consider discrete valuation domains first and afterwards generalize to Krull domains.

Recall from Definition 1.2 that $[\![f]\!]$, the divisor-closed submonoid of $\mathrm{Int}(S, D)$ generated by f, is the multiplicative monoid consisting of all those $g \in \mathrm{Int}(S, D)$ which divide some power of f in $\mathrm{Int}(S, D)$. Also, recall the definition of image-primitive, and of $\mathrm{d_S}(f)$, the fixed divisor of f on S from Definition 1.5.

First, let us get a trivial case out of the way:

Lemma 5.1. *Let V be a DVR, $S \subseteq V$ and $f \in V[x]$ with $\mathrm{d_S}(f) = V$. Let $F \subseteq V[x]$ be a set of primitive polynomials in $V[x]$ representing the different irreducible factors of f in $K[x]$. Let $\mathcal{F}_0$ be the multiplicative submonoid of $V[x]$ generated by F and the units of V. Then*

(1) $[\![f]\!] = \mathcal{F}_0$
(2) *Every element g of $[\![f]\!]$ is in $V[x]$, is primitive, and satisfies $\mathrm{d_S}(g) = V$.*
(3) *If $g, h \in [\![f]\!]$, then g divides h in $[\![f]\!]$ if and only if g divides h in $K[x]$.*
(4) $\varphi\colon [\![f]\!] \to \sum_{h\in F}(\mathbb{N}_0, +), \quad \varphi(g) = (v_h(g) \mid h \in F)$, *is a divisor theory.*

Proof. We will show (1) and (2). The remaining statements follow.

$f \in V[x]$ is image-primitive on S and hence primitive. The same holds for all powers of f and for all divisors in $V[x]$ of any power of f by Remark 1.6.

Clearly, every element of $\mathcal{F}_0$ divides in $V[x]$ some power of f. Therefore $\mathcal{F}_0 \subseteq [\![f]\!]$, and every element of $\mathcal{F}_0$ is image-primitive on S.

Now let $g \in [\![f]\!]$. Let $m \in \mathbb{N}$ and $h \in \mathrm{Int}(S, V)$ with $hg = f^m$. Then $h = c\tilde{h}$ and $g = d\tilde{g}$ with $\tilde{g}, \tilde{h} \in \mathcal{F}_0$ and $c, d \in K$. Since $\tilde{g}$ and $\tilde{h}$ are image-primitive on S, we must have $v(c) \geq 0$ and $v(d) \geq 0$. Since f^m is primitive, $v(c) = -v(d)$. It follows that $v(c) = v(d) = 0$ and therefore $g, h \in \mathcal{F}_0$. □

Let D be a domain with quotient field K, S a subset of D, and $f \in \mathrm{Int}(S, D)$. Let H be a set of representatives (up to multiplication by a non-zero constant) of the irreducible factors of f in $K[x]$. For instance, H could be the set of monic irreducible factors of f in $K[x]$. Or, in case that D is a principal ideal domain, such as, for instance, a discrete valuation domain, H can be chosen to be a set of primitive irreducible polynomials in $D[x]$. By $\mathcal{H}$ we denote the multiplicative submonoid of $K[x] \setminus \{0\}$ generated by H and the constants in $K \setminus \{0\}$. (Note that $\mathcal{H}$ depends only on f, not on the choice of H). Obviously $[\![f]\!] \subseteq \mathcal{H} \cap \mathrm{Int}(S, D)$. We now examine when equality holds. In this case we can give a divisor theory of $[\![f]\!]$ [Theorem 5.3]. Otherwise, we have to be content with a divisor homomorphism [Theorem 5.4].

Theorem 5.2. *Let V be a discrete valuation domain with quotient field K, $S \subseteq V$ and $f \in \mathrm{Int}(S, V) \setminus \{0\}$. Let $\mathcal{H}$ be the multiplicative submonoid of $K[x]$ generated by the monic irreducible factors of f in $K[x]$ and the non-zero constants in K. If $\mathrm{d_S}(f) \neq V$ then*

$$[\![f]\!] = \mathcal{H} \cap \mathrm{Int}(S, V).$$

Proof. Clearly, $[\![f]\!] \subseteq \mathcal{H} \cap \mathrm{Int}(S, V)$. For the reverse inclusion, let $f = c\tilde{f}$ with $c \in K \setminus \{0\}$ and $\tilde{f} \in V[x]$ primitive. We wlll first show that $b\tilde{f} \in [\![f]\!]$, for arbitrary $b \in V \setminus \{0\}$:

Since $\mathrm{d_S}(f) \neq V$, $v(\mathrm{d_S}(f)) > 0$, and we may apply the Archimedean axiom. Let $m \in \mathbb{N}$ such that $mv(\mathrm{d_S}(f)) \geq v(b) - v(c)$. Then $f^{m+1} = (f^m cb^{-1})b\tilde{f}$, and both $(f^m cb^{-1})$ and $b\tilde{f}$ are in $\mathrm{Int}(S, V)$. Therefore $b\tilde{f} \in [\![f]\!]$.

Furthermore, for arbitrary $b \in V \setminus \{0\}$, all divisors in $V[x]$ of $b\tilde{f} \in [\![f]\!]$ are also in $[\![f]\!]$. Therefore, all primitive irreducible factors of f and all non-zero constants of V, as well as all products of such elements, are in $[\![f]\!]$. Finally, by Lemma 1.4, we can multiply elements of $[\![f]\!]$ by any constant $a \in K$ with $v(a) < 0$, as long as the result is integer-valued on S. Therefore, $\mathcal{H} \cap \mathrm{Int}(S, V) \subseteq [\![f]\!]$. □

Theorem 5.3. *Let v be a normalized discrete valuation on K and V its valuation ring. Let $S \subseteq V$ and $f \in \mathrm{Int}(S, V)$, such that no root of f is an isolated point of S in v-adic topology. Let H be the set of different monic irreducible factors of f in $K[x]$ and $\mathcal{H}$ the multiplicative submonoid of $K[x]$ generated by H and the non-zero constants in K. By $[\![f]\!]$ denote the divisor-closed submonoid of* $\mathrm{Int}(S, V)$ *generated by f.*

There exists a finite polynomially dense subset T of S relative to $\mathcal{H}$ that does not contain any root of f; and for every such T

$$\varphi\colon [\![f]\!] \to \sum_{h \in H} (\mathbb{N}_0, +) \oplus \sum_{t \in T} (\mathbb{N}_0, +) \quad \varphi(g) = ((v_h(g) \mid h \in H), (v(g(t)) \mid t \in T)),$$

is a divisor homomorphism.

If $\mathrm{d_S}(f) \neq V$ and T is chosen minimal then φ is a divisor theory.

Proof. $[\![f]\!]$ is a submonoid of $\mathcal{H} \cap \mathrm{Int}(S, V)$. The monoid homomorphism φ in the theorem is the restriction of the divisor homomorphism of Theorem 4.2 to $[\![f]\!]$ and is therefore itself a divisor homomorphism. If $\mathrm{d_S}(f) \neq V$ then $[\![f]\!] = \mathcal{H} \cap \mathrm{Int}(S, V)$ by Theorem 5.2. In this case, φ is a divisor theory by Theorem 4.2, provided T is minimal. $\square$

Recall that a Krull domain D is a domain satisfying the following conditions with respect to $\mathrm{Spec}^1(D)$, the set of prime ideals of height 1:

(1) For every $P \in \mathrm{Spec}^1(D)$, the localization D_P is a DVR.
(2) $D = \bigcap_{P \in \mathrm{Spec}^1(D)} D_P$
(3) Each non-zero $r \in D$ lies in only finitely many $P \in \mathrm{Spec}^1(D)$.

If D is a Krull domain, we denote the normalized discrete valuation on the quotient field of D whose valuation ring is D_P, where $P \in \mathrm{Spec}^1(D)$, by $\mathrm{v_P}$. Such a valuation is called an essential valuation of the Krull domain D.

Theorem 5.4. *Let D be a Krull domain with quotient field K and $S \subseteq D$. Let $f \in \mathrm{Int}(S, D) \setminus \{0\}$, and $[\![f]\!]$ the divisor-closed multiplicative submonoid of $\mathrm{Int}(S, D)$ generated by f. Let H be the finite set of different monic irreducible factors of f in $K[x]$ and $\mathcal{H}$ the multiplicative submonoid of $K[x]$ generated by H and the non-zero constants. Let $\mathcal{P}$ be the finite set of primes P of height 1 of D such that either $f \notin D_P[x]$ or $f \in D_P[x]$ and $\mathrm{v_P}(f(S)) > 0$.*

If S doesn't contain any isolated points in $\mathrm{v_P}$-adic topology for any $P \in \mathcal{P}$, then for each $P \in \mathcal{P}$, there exists a finite subset T_P of S that is D_P-polynomially dense relative to $\mathcal{H}$ in S and contains no root of f. For any such choice of sets T_P, let

$$(M, +) = \sum_{h \in H} (\mathbb{N}_0, +) \oplus \sum_{P \in \mathcal{P}} \sum_{t \in T_P} (\mathbb{N}_0, +).$$

Then

$$\varphi \colon [\![f]\!] \to M, \qquad \varphi(g) = \left((v_h(g) \mid h \in H), ((\mathrm{v_P}(g(t)) \mid t \in T_P) \mid P \in \mathcal{P})\right),$$

is a divisor homomorphism.

Proof. The existence of the sets T_P is guaranteed by Proposition 3.3. Since no element of any T_P contains a root of any polynomial in $[\![f]\!]$, φ is a well-defined monoid homomorphism.

Now assume $a, b \in [\![f]\!]$ with $\varphi(a) \mid \varphi(b)$; we need to show $a \mid b$ in $[\![f]\!]$. By Remark 1.3, it suffices to show that a divides b in $K[x]$ and that the co-factor $c = b/a$ is in $\mathrm{Int}(S, D_P)$ for every $P \in \mathrm{Spec}^1(D)$.

Let $c = b/a$. That c is in $K[x]$ follows from $v_h(a) \leq v_h(b)$ for all irreducible factors h of a and b in $K[x]$.

Consider a prime P of height 1 of D that is not in $\mathcal{P}$. For such a prime, $f \in D_P[x]$ and f is image-primitive in $\mathrm{Int}(S, D_P)$. We may apply Lemma 5.1 (3) and deduce that $c \in \mathrm{Int}(S, D_P)$.

Now for $P \in \mathcal{P}$, let ψ_P be the projection of M onto $\sum_{h\in H}(\mathbb{N}_0,+)\oplus\sum_{t\in T_P}(\mathbb{N}_0,+)$, and call the latter monoid $M(P)$. From $\varphi(a) \mid \varphi(b)$ it follows that $\psi_P(\varphi(a))$ divides $\psi_P(\varphi(b))$. Let $[\![f]\!]_P$ be the divisor closed submonoid of $\mathrm{Int}(S, D_P)$ generated by f. Then $[\![f]\!]$ is a submonoid of $[\![f]\!]_P$, and $\psi_P \circ \varphi$ is the restriction to $[\![f]\!]$ of the divisor homomorphism in 4.2. Now the fact that $\psi_P(\varphi(a))$ divides $\psi_P(\varphi(b))$ implies $c \in \mathrm{Int}(S, D_P)$, by Theorem 4.2. □

Corollary 5.5. *Let D be a Krull domain and S a subset that doesn't have any isolated points in any of the topologies given by essential valuations of D. Let $f \in \mathrm{Int}(S, D)\setminus\{0\}$. Then $[\![f]\!]$, the divisor closed submonoid of* $\mathrm{Int}(S, D)$ *generated by f, is a Krull monoid.*

In particular, for every Krull domain D and every $f \in \mathrm{Int}(D)\setminus\{0\}$, the divisor closed submonoid $[\![f]\!]$ of $\mathrm{Int}(D)$ *generated by f is a Krull monoid.*

Proof. Indeed, the existence of a divisor homomorphism from $[\![f]\!]$ to a finite sum of copies of $(\mathbb{N}_0,+)$ in Theorem 5.4 ensures that $[\![f]\!]$ is a Krull monoid, see [5][Thm. 2.4.8]. □

Monoids with the property that the divisor closed submonoid generated by any single element is a Krull monoid have been called *monadically Krull* by A. Reinhart. Without using divisor homomorphisms, through an approach completely different from ours, Reinhart showed that $\mathrm{Int}(D)$ is monadically Krull whenever D is a principal ideal domain [9][Thm. 5.2].

Corollary 5.5 generalizes Reinhart's result to Krull domains, and also to integer-valued polynomials on (sufficiently nice) subsets. The explicit divisor homomorphisms of Theorem 4.2 and Theorems 5.3 and 5.4 give additional information on the arithmetic of submonoids of $\mathrm{Int}(D)$.

It remains an open problem to find the precise divisor theories (cf. Def. 4.1) of those monoids of integer-valued polynomials for which Theorems 5.3 and 5.4 provide divisor homomorphisms.

Acknowledgment. Enthusiastic thanks go out to the anonymous referee for his/her meticulous reading of the paper and the resulting corrections.

References

[1] P.-J. Cahen, *Polynomial closure*, J. Number Theory 61 (1996), 226–247.

[2] J.-L. Chabert, *On the polynomial closure in a valued field*, J. Number Theory 130 (2010), 458–468.

[3] S. Frisch, *Substitution and closure of sets under integer-valued polynomials*, J. Number Theory 56 (1996), 396–403.

[4] S. Frisch, *A construction of integer-valued polynomials with prescribed sets of lengths of factorizations*, Monatsh. Math. 171 (2013), 341–350.

[5] A. Geroldinger and F. Halter-Koch, *Non-unique factorizations*, vol. 278 of Pure and Applied Mathematics (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2006.

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

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

[8] M. H. Park and F. Tartarone, *Polynomial closure in essential domains*, Manuscr. Math. 117 (2005), 29–41.

[9] A. Reinhart, *On monoids and domains whose monadic submonoids are Krull*, in Commutative Algebra – Recent Advances in Commutative Rings, Integer-valued Polynomials, and Polynomial Functions, M. Fontana, S. Frisch, and S. Glaz, eds., Springer, 2014.

Institut für Mathematik A, Technische Universität Graz, Steyrergasse 30, 8010 Graz, Austria

E-mail address: frisch@math.tugraz.at