

THE RING OF POLYNOMIALS INTEGRAL-VALUED OVER A FINITE SET OF INTEGRAL ELEMENTS

GIULIO PERUGINELLI

ABSTRACT. Let D be an integral domain with quotient field K and Ω a finite subset of D . McQuillan proved that the ring $\text{Int}(\Omega, D)$ of polynomials in $K[X]$ which are integer-valued over Ω , that is, $f \in K[X]$ such that $f(\Omega) \subset D$, is a Prüfer domain if and only if D is Prüfer. Under the further assumption that D is integrally closed, we generalize his result by considering a finite set S of a D -algebra A which is finitely generated and torsion-free as a D -module, and the ring $\text{Int}_K(S, A)$ of integer-valued polynomials over S , that is, polynomials over K whose image over S is contained in A . We show that the integral closure of $\text{Int}_K(S, A)$ is equal to the contraction to $K[X]$ of $\text{Int}(\Omega_S, D_F)$, for some finite subset Ω_S of integral elements over D contained in an algebraic closure \bar{K} of K , where D_F is the integral closure of D in $F = K(\Omega_S)$. Moreover, the integral closure of $\text{Int}_K(S, A)$ is Prüfer if and only if D is Prüfer. The result is obtained by means of the study of pullbacks of the form $D[X] + p(X)K[X]$, where $p(X)$ is a monic non-constant polynomial over D : we prove that the integral closure of such a pullback is equal to the ring of polynomials over K which are integral-valued over the set of roots Ω_p of $p(X)$ in \bar{K} .

1. Introduction. Rings of integer-valued polynomials are a prominent source for providing examples of non-Noetherian Prüfer domains (see the book [6, Chapter VI, page 123]). Throughout this paper, D is an integral domain which is not a field, and K is its quotient field. We denote by \bar{K} a fixed algebraic closure of K and by \bar{D} the integral closure of D in \bar{K} . We give the following definition, which generalizes

2010 AMS *Mathematics subject classification.* Primary 13B25, Secondary 13B22, 13F05, 13F20.

Keywords and phrases. Pullback, integral closure, integer-valued polynomial, divided differences, Prüfer ring.

This research was supported by the Austrian Science Foundation (FWF), Project Number P23245-N18, INDAM and also University of Roma 3.

Received by the editors on March 31, 2014, and in revised form on October 30, 2014.

the classical definition of the ring of integer-valued polynomials over a subset ([6, Chapter I.1, page 3]).

Definition 1.1. Let R be an integral domain containing D . Let F be the quotient field of R (so that $K \subseteq F$). For a subset Ω of F , we set

$$\text{Int}_K(\Omega, R) \doteq \{f \in K[X] \mid f(\Omega) \subset R\},$$

which is the ring of polynomials in $K[X]$ which map every element of Ω into R . If $F = K$ we omit the subscript K . Thus, $\text{Int}(\Omega, R)$ is a subring of $K[X]$ (the coefficients of the relevant polynomials are in the quotient field of R).

In the case of a finite subset Ω of D , McQuillan studied the algebraic structure of the corresponding ring of integer-valued polynomials $\text{Int}(\Omega, D)$, describing the spectrum of such a ring and also its additive structure ([13]). Using McQuillan's arguments, Boynton observed in [4] that $\text{Int}(\Omega, D)$ fits in a pullback diagram. Here we generalize this class of rings by first considering a finite set Ω of integral elements in \overline{D} and polynomials in $K[X]$ which preserve the integrality of the elements of Ω , that is, for each α in Ω , $f(\alpha)$ is integral over D ; according to the above definition, this ring is denoted by $\text{Int}_K(\Omega, \overline{D})$. For example, given a monic non-constant polynomial $p \in D[X]$, let Ω_p be the set of roots of $p(X)$ in a splitting field. Then the ring $\text{Int}_K(\Omega_p, \overline{D})$ is of the above kind, and it is not difficult to show that the ring $\text{Int}_K(\Omega, \overline{D})$, for a finite set Ω of \overline{D} , can be reduced to this case. More generally, we consider a finite set S of integral elements over D which do not necessarily lie in an algebraic extension of K , i.e., S is contained in a D -algebra A , which is finitely generated and torsion-free as a D -module (for example, a matrix algebra or a quaternion algebra). We then consider polynomials in $K[X]$ which map the elements of S into A : $\text{Int}_K(S, A) = \{f \in K[X] \mid f(S) \subset A\}$. Note that A is not necessarily commutative and may contain zero-divisors, and each of its elements satisfies a monic polynomial over D .

Given a monic polynomial $p(X)$ in $D[X]$, the study of the ring $\text{Int}_K(\Omega_p, \overline{D})$ goes through another kind of pullback ring. As for the rings $\text{Int}_K(\Omega, \overline{D})$, the ones we now introduce are the pullbacks of the canonical residue map $K[X] \rightarrow K[X]/p(X)K[X]$ with respect to some

subring of $K[X]/p(X)K[X]$; thus, they are subrings of $K[X]$ sharing with $K[X]$ the ideal $p(X)K[X]$.

Definition 1.2. Let $p(X)$ be a non-constant monic polynomial in $D[X]$. We consider the following subring of $K[X]$:

$$D(p) \doteq D[X] + p(X) \cdot K[X] = \{r(X) + p(X)q(X) \mid r \in D[X], q \in K[X]\}.$$

It is straightforward to verify that the elements of this set form a ring under the usual operation of sum and product induced by the polynomial ring $K[X]$. In Lemma 1.6, we will show that a polynomial $f(X)$ in $K[X]$ is in $D(p)$ if and only if the remainder in the division of $f(X)$ by $p(X)$ is in $D[X]$. Note that the principal ideal $p(X) \cdot K[X]$ of $K[X]$ is also an ideal of $D(p)$. We then have the following diagram:

$$\begin{array}{ccc} D(p) & \hookrightarrow & K[X] \\ \downarrow & & \downarrow \\ \frac{D(p)}{p(X)K[X]} & \hookrightarrow & \frac{K[X]}{p(X)K[X]} \end{array}$$

so that $D(p)$ is a pullback of $K[X]$ (for a general reference about pullbacks see [9]). Examples of such pullbacks appear in [4], and more widely in [16].

We see at once that $D(p)$ is contained in $\text{Int}_K(\Omega_p, \overline{D})$. Also, $\text{Int}_K(\Omega_p, \overline{D})$ has the ideal $p(X)K[X]$ in common with $K[X]$, so, like $D(p)$, also $\text{Int}_K(\Omega_p, \overline{D})$ is a pullback ring. This point of view is clearly a generalization of [4, Example 4.4 (1)], which we briefly recall below in subsection 1.2.

We give some motivations which led us to study the pullback rings $D(p) = D[X] + p(X) \cdot K[X]$. In [16], this kind of polynomial pullback arose as the ring of integer-valued polynomials over certain subsets of matrices. Let $M_n(D)$ be the D -algebra of $n \times n$ matrices with entries in D , and let $\text{Int}_K(M_n(D)) = \{f \in K[X] \mid f(M_n(D)) \subset M_n(D)\}$, the ring of integer-valued polynomials over $M_n(D)$. Given a monic polynomial $p \in D[X]$ of degree n , we denote by $M_n^p(D)$ the set of matrices M in $M_n(D)$ whose characteristic polynomial is equal to

$p(X)$. We consider the overring of $\text{Int}_K(M_n(D))$ made up by those polynomials which are integer-valued over $M_n^p(D)$, namely:

$$\text{Int}_K(M_n^p(D), M_n(D)) = \{f \in K[X] \mid f(M_n^p(D)) \subset M_n(D)\}.$$

This partition of $M_n(D)$ into subsets of matrices having a prescribed characteristic polynomial was used in [16] to give a characterization of the polynomials of $\text{Int}_K(M_n(D))$ in terms of their divided differences (see [16, Theorem 4.1]). By [16, Lemma 2.2 and Remark 2.1], we have

$$\text{Int}_K(M_n^p(D), M_n(D)) = D(p).$$

In particular, the ring $\text{Int}_K(M_n(D))$ is represented as an intersection of pullbacks $D(p)$, as $p(X)$ ranges through the set of all the monic polynomials in $D[X]$ of degree n ([16, Remarks 2.1 and 2.2]). In [17], the authors address the following question, which generalizes the previous case: for a D -algebra A as above, where D is integrally closed, we consider the ring $\text{Int}_K(A) = \{f \in K[X] \mid f(A) \subset A\}$ of integer-valued polynomials over A . Is $\text{Int}_K(A)$ equal to the intersection of pullbacks of the form $D(p)$? In general, we have

$$\bigcap_{a \in A} D(\mu_a) \subseteq \text{Int}_K(A),$$

where, for $a \in A$, $\mu_a(X)$ denotes the minimal polynomial of a over K (by assumption on A and D , $\mu_a \in D[X]$ and is monic). The conditions under which the previous containment is an equality are not known.

Throughout the paper, given a monic polynomial $p(X)$ in $D[X]$, we denote by Ω_p the multi-set of its roots in \overline{K} (we recall the notion of multi-set in Section 2).

This work is organized as follows. In Section 2, we recall a characterization for the polynomials in $D(p)$ in terms of their divided differences. We use this result to show that the ring $\text{Int}^{\{n\}}(\Omega, D)$ of polynomials whose divided differences of order less than or equal to n are integer-valued over a subset Ω of D can be represented as an intersection of such pullbacks. This ring has been introduced by Bhargava in [1]; we recall the definition in that section. In Section 3, we prove the following theorem:

Theorem 1.3. *Let $p(X)$ be a monic non-constant polynomial in $D[X]$. Then the integral closure of the ring $D(p) = D[X] + p(X)K[X]$ is the ring $\text{Int}_K(\Omega_p, \overline{D})$.*

As a corollary, we show that the integral closure of $\text{Int}^{\{n\}}(\Omega, D)$ is equal to the ring $\text{Int}(\Omega, D)$, in the case of a finite subset Ω of D . For a general subset Ω of D , in the case where D has finite residue rings, an argument from [17] gives the same conclusion. In Section 4, we prove the main theorem:

Theorem 1.4. *Assume D is integrally closed, and let Ω be a finite subset of \overline{D} . Then the ring $\text{Int}_K(\Omega, \overline{D})$ is Prüfer if and only if D is Prüfer.*

If $\Omega \subset D$, then this is precisely the main result obtained by McQuillan. The crucial remark is that, for a monic polynomial $p(X)$ in $D[X]$, $\text{Int}_K(\Omega_p, \overline{D}) \subseteq \text{Int}_F(\Omega_p, \overline{D})$ is an integral ring extension, where $F = K(\Omega_p)$ is the splitting field of $p(X)$. It is not difficult to see that $\text{Int}_F(\Omega, \overline{D})$ is equal to $\text{Int}_F(\Omega, D_F)$, where D_F is the integral closure of D in F , and this is precisely the kind of ring considered by McQuillan. We note that this is a partial answer to [17, Question 29], where we asked if $\text{Int}_K(\Omega, \overline{D})$ is Prüfer, when Ω is a subset of integral elements of degree over K bounded by some positive integer n . If D is integrally closed, we also give a criterion to establish when the pullback $D(p)$ is integrally closed, that is, equal to $\text{Int}_K(\Omega_p, \overline{D})$ (see Theorem 4.5). In particular, in the case of a Prüfer domain D , this condition is satisfied automatically if $D(p)$ is integrally closed.

Finally, in the last section, we apply the previous results in the more general setting of a finite set S of integral elements over D which do not necessarily lie in an algebraic extension of K .

Corollary 1.5. *Assume D is integrally closed, and let S be a finite set of a torsion-free D -algebra A , which is finitely generated as a D -module. Let Ω_S be the set of roots in \overline{D} of the minimal polynomials of s over D , as s ranges through S . Then the integral closure of $\text{Int}_K(S, A)$ is $\text{Int}_K(\Omega_S, \overline{D})$.*

1.1. Preliminary results. In the case of a monic polynomial, the following lemma determines the quotient of $D(p)$ by the ideal $p(X)K[X]$. We denote by $\pi : K[X] \twoheadrightarrow K[X]/p(X)K[X]$ the canonical residue map, which associates to a polynomial $f \in K[X]$ the residue class $f(X) + p(X)K[X]$.

Lemma 1.6. *Let $p \in D[X]$ be a monic non-constant polynomial. Then $D(p)$ is the pullback of $D[X]/p(X)D[X] \hookrightarrow K[X]/p(X)K[X]$ with respect to the canonical residue map $\pi : K[X] \twoheadrightarrow K[X]/p(X)K[X]$. In other words, the following is a pullback diagram (i.e., $D(p) = \pi^{-1}(D[X]/p(X)D[X])$):*

$$\begin{array}{ccc} D(p) & \hookrightarrow & K[X] \\ \downarrow & & \downarrow \\ \frac{D[X]}{p(X)D[X]} & \hookrightarrow & \frac{K[X]}{p(X)K[X]} \end{array}$$

In particular, a polynomial $f \in K[X]$ belongs to $D(p)$ if and only if the remainder in the division by $p(X)$ in $K[X]$ belongs to $D[X]$. Equivalently, we have

$$\frac{D(p)}{p(X) \cdot K[X]} \cong \frac{D[X]}{p(X) \cdot D[X]}.$$

Proof. Since $p(X)$ is monic, we have two consequences. Firstly, $D[t] \cong D[X]/p(X)D[X]$ is a free D -module of rank $n = \deg(p)$ with basis $\{1, t, \dots, t^{n-1}\}$, where t is the residue class of X modulo $p(X)D[X]$. In particular, every element $r \in D[t]$ can be uniquely represented as $r(t) = \sum_{i=0, \dots, n-1} c_i t^i$, with $c_i \in D$.

Secondly, $p(X) \cdot K[X] \cap D[X] = p(X) \cdot D[X]$, so the image of the restriction of π to $D[X]$ is isomorphic to $D[t]$. Therefore, $D[t] \cong D[X]/p(X)D[X]$ embeds naturally into $K[X]/p(X)K[X] \cong K[t]$ (the class $X \pmod{p(X)D[X]}$ is mapped to $X \pmod{p(X)K[X]}$), so without confusion we may denote them with the same letter t). Note that $K[t]$ is a free K -module of rank n with the same basis $\{1, t, \dots, t^{n-1}\}$.

We consider now the composition of mappings $D[X] \hookrightarrow D(p) \twoheadrightarrow D(p)/p(X)K[X]$. By the second consequence above, and by the second isomorphism theorem, we have the isomorphism of the claim. More

explicitly, given $f \in K[X]$, there exist (uniquely determined) a quotient $q \in K[X]$ and a remainder $r \in K[X]$ (with either $r = 0$ or $\deg(r) < \deg(p)$) such that $f(X) = r(X) + q(X)p(X)$. Hence, if $r(X) = \sum_i c_i X^i$, then $\pi(f) = \pi(r) = r(t) = \sum_i c_i t^i \in K[t]$. From the algebraic structure of $D[t]$ we deduce that $r(t)$ is in $D[t]$ if and only if the remainder $r(X)$ is in $D[X]$. This condition in turn is equivalent to $f \in D(p)$. \square

Lemma 1.7. *Let $p, q \in D[X]$ be monic polynomials. Then*

$$D(p) \text{ is contained in } D(q) \iff p(X) \text{ is divisible by } q(X).$$

In particular, $D(p) = D(q) \iff p(X) = q(X)$.

Proof. One direction is easy. Conversely, suppose $D(p) \subseteq D(q)$ so that $p(X) = r(X) + q(X)k(X)$, for some $r \in D[X]$, $r = 0$ or $\deg(r) < \deg(q)$, $k \in K[X]$. If $r \neq 0$, let $c \in K \setminus D$ be such that $c \cdot r(X)$ is not in $D[X]$. Then $c \cdot p$ is in $D(p)$, but it is not in $D(q)$, contradiction. Notice that $k(X)$ has to be in $D[X]$ (see also [12, Lemma]). \square

The following two cases, linear and irreducible polynomials, are given as an example and to further illustrate the connection between polynomial pullbacks and rings of integer-valued polynomials.

1.2. Linear case. In the linear case, the connection between the polynomial pullbacks and ring of integer-valued polynomials over finite sets becomes evident. Suppose $p(X) = X - a \in D[X]$. Then the remainder of the division of a polynomial $f \in K[X]$ by $X - a$ is the value of $f(X)$ at a . Hence,

$$D(p) = D + (X - a) \cdot K[X] = \text{Int}(\{a\}, D).$$

It is well known (see, for example [6, Proposition IV.4.1]) that $\text{Int}(\{a\}, D)$ is integrally closed if and only if D is. It is easy to see that the integral closure of $\text{Int}(\{a\}, D)$ is $\text{Int}(\{a\}, D')$, where D' is the integral closure of D in K (notice that $\text{Int}(\{a\}, D') = D' + (X - a)K[X]$ is a pullback). More generally, we recall the following result.

Lemma 1.8. *Let $E \subset K$ be a finite set. Then the integral closure of $\text{Int}(E, D)$ is $\text{Int}(E, D')$, where D' is the integral closure of D in K .*

Proof. By [6, Proposition IV.4.1], $\text{Int}(E, D')$ is integrally closed. Conversely, take $f \in \text{Int}(E, D')$. Then for each $a \in E$, there exists a monic polynomial $m_{f(a)} \in D[X]$ such that $m_{f(a)}(f(a)) = 0$. We consider the monic polynomial of $D[X]$ equal to the product of the $m_{f(a)}(X)$'s, as a ranges through E . Then $m(f(X))$ is in $\text{Int}(E, D)$, because, for each $a \in E$, we have $m(f(a)) = 0 \in D$. This gives a monic equation for $f(X)$ over $\text{Int}(E, D)$. \square

Remark 1.9. We now recall the following observation made in [4]. Under the assumptions of Lemma 1.8, $\text{Int}(E, D)$ is the pullback of $\prod_{i=1}^m D \subset \prod_{i=1}^m K$ with respect to the canonical mapping $\pi : K[X] \rightarrow K[X]/p(X)K[X] \cong \prod_{i=1}^m K$, where $p(X) = \prod_{a \in E} (X - a)$. The map π is given by $f(X) \mapsto (f(a))_{a \in E}$. Notice also that $p(X)K[X]$ is an ideal of $\text{Int}(E, D)$, because every polynomial of $K[X]$ which is divisible by $p(X)$ is zero on E . In particular, we have the following isomorphism of D -modules

$$\frac{\text{Int}(E, D)}{p(X)K[X]} \cong \prod_{i=1}^m D.$$

1.3. Irreducible polynomial case. We suppose now that D is integrally closed and $p(X)$ is a monic irreducible polynomial in $D[X]$ of degree $n > 0$. It is easy to see (for example, [12] or [2, Proposition 11, Chapter V]) that $p(X)$ is irreducible in $K[X]$, so that $p \in D[X]$ is also prime and $D[X]/(p(X)) \cong D[\alpha]$, where α is a root of $p(X)$ in \overline{K} . The next proposition follows by [15, Proposition 3.1] (which is proved in the case $D = \mathbb{Z}$). We sketch the proof for the sake of the reader, giving emphasis to the relevant points.

Proposition 1.10. *Let $p \in D[X]$ be a monic and irreducible polynomial, with a set of roots $\Omega_p \subset \overline{K}$. Let $F = K(\Omega_p)$ be the splitting field of $p(X)$ over K and D_F the integral closure of D in F . For each $\alpha \in \Omega_p$, we set*

$$S_\alpha \doteq \text{Int}_K(\{\alpha\}, D_\alpha),$$

where D_α is the integral closure of D in $K(\alpha) \subseteq F$.

Then, for each $\alpha \in \Omega_p$, $S_\alpha = \text{Int}_K(\Omega_p, D_F)$, and this ring is the integral closure of $D(p)$. Moreover, $D(p)$ is integrally closed if and only if $D_\alpha = D[\alpha]$, for some (hence all) $\alpha \in \Omega_p$.

Proof. Using a Galois-invariance argument it is easy to show that the ring S_α does not depend on the choice of the root α of $p(X)$ and is equal to $\text{Int}_K(\Omega_p, D_F)$. We observe that $S_\alpha = \{f \in K[X] \mid f(\alpha) \text{ is integral over } D\}$. Then, for a polynomial $f \in S_\alpha$, and for every conjugate α' of α over K , $f(\alpha')$ is integral over D as well. Since $D[\alpha]$, for $\alpha \in \Omega_p$, is a free D -module of rank n , we can show that

$$D(p) = \{f \in K[X] \mid f(\alpha) \in D[\alpha]\} = \text{Int}_K(\{\alpha\}, D[\alpha]).$$

Finally, using a pullback diagram argument, since D_α is the integral closure of $D[\alpha]$ in $K(\alpha)$, we deduce that $\text{Int}_K(\Omega_p, D_F)$ is the integral closure of $D(p)$ (see [15, Proposition 3.1] for details). \square

In particular, the proposition shows that all the subrings $\text{Int}(\{\alpha\}, D_F) \subset F[X]$, for $\alpha \in \Omega_p$, contract in $K[X]$ to the same ring S_α . Notice also that $\text{Int}_K(\Omega_p, \overline{D})$ is equal to $\text{Int}_K(\Omega_p, D_F)$, where D_F is the integral closure of D in the splitting field $F = K(\Omega_p)$ of $p(X)$ over K .

2. Pullbacks and divided differences. In this section we recall a result of [16] which characterizes a polynomial $f(X)$ in a pullback $D(p) = D[X] + p(X) \cdot K[X]$ in terms of a finite set of conditions on the evaluation of the divided differences of $f(X)$ at the roots of $p(X)$ in \overline{K} . We use this result to show that the ring of integer-valued polynomials whose divided differences are also integer-valued can be represented as an intersection of such pullbacks.

Given a polynomial $f \in K[X]$, the divided differences of $f(X)$ are defined recursively as follows:

$$\begin{aligned} \Phi^0(f)(X_0) &\doteq f(X_0) \\ \Phi^1(f)(X_0, X_1) &\doteq \frac{f(X_0) - f(X_1)}{X_0 - X_1} \\ &\dots \\ \Phi^k(f)(X_0, \dots, X_k) &\doteq \frac{\Phi^{k-1}(f)(X_0, \dots, X_{k-1}) - \Phi^{k-1}(f)(X_0, \dots, X_{k-2}, X_k)}{X_{k-1} - X_k}. \end{aligned}$$

For each $k \in \mathbb{N}$, $\Phi^k(f)$ is a symmetric polynomial over K in $k + 1$ variables (see [7, 16, 18, 19] for the main properties of the divided differences of a polynomial). We recall here that, given a finite sequence of elements a_0, \dots, a_n of a commutative ring R , and a polynomial $f \in R[X]$ of degree $\leq n$, we have the following expansion due to

Newton:

$$(2.1) \quad \begin{aligned} f(X) &= f(a_0) + \Phi^1(f)(a_0, a_1)(X - a_0) \\ &\quad + \Phi^2(f)(a_0, a_1, a_2)(X - a_0)(X - a_1) + \dots \\ &\quad + \Phi^n(f)(a_0, \dots, a_n)(X - a_0) \cdot \dots \cdot (X - a_{n-1}). \end{aligned}$$

Since in general a polynomial may not have distinct roots, we need to recall the following definition.

Definition 2.1. A *multi-set* is a collection of elements Ω in which elements may occur multiple times. The number of times an element occurs is called its *multiplicity* in the multi-set. The cardinality of a multi-set Ω is defined as the number of elements of Ω , each of them counted with multiplicity. The underlying set of Ω is the (proper) set containing the distinct elements in Ω .

A multi-set Ω_1 is a sub-multi-set of a multi-set Ω_2 if every element α of Ω_1 of multiplicity n_1 belongs to Ω_2 with multiplicity $n_2 \geq n_1$.

Remark 2.2. Let Ω be a multi-set of cardinality n , and let S be the underlying set of Ω . The choice of an ordering on the elements of Ω corresponds to an n -tuple in S^n (we have thus $n!$ choices). Conversely, given an n -tuple \underline{s} in S^n , where S is a set, if we do not consider the order of its components, we have a multi-set Ω of cardinality n .

Remark 2.3. A particular ring of integer-valued polynomials involving divided differences has been introduced by Bhargava in [1]. Given a subset S of D and $n \in \mathbb{N}$, we consider those polynomials $f(X)$ in $K[X]$ whose k th divided difference $\Phi^k(f)$ is integer-valued on S for all $k \in \{0, \dots, n\}$, namely:

$$\text{Int}^{\{n\}}(S, D) \doteq \{f \in K[X] \mid \text{for all } 0 \leq k \leq n, \Phi^k(f)(S^{k+1}) \subset D\}.$$

For $n = 0$, we recover the ring $\text{Int}(S, D)$, which contains $\text{Int}^{\{n\}}(S, D)$ for all $n \in \mathbb{N}$.

Given $f \in \text{Int}^{\{n\}}(S, D)$ and $k \in \{0, \dots, n\}$, we have:

$$(*) \quad \text{for all } (a_1, \dots, a_{k+1}) \in S^{k+1}, \Phi^k(f)(a_1, \dots, a_{k+1}) \in D.$$

Since $\Phi^k(f)$ is a symmetric polynomial in $k + 1$ variables, for all permutations $\sigma \in \mathcal{S}_{k+1}$, we have

$$\Phi^k(f)(a_1, \dots, a_{k+1}) = \Phi^k(f)(a_{\sigma(1)}, \dots, a_{\sigma(k+1)}).$$

Hence, we may disregard the order of the components of the chosen $(k + 1)$ -tuple. If we consider a multi-set Ω of cardinality $k + 1$ formed by the elements of S , we may define $\Phi^k(f)(\Omega)$ as the value of $\Phi^k(f)$ at one of the $(k + 1)$ -tuples associated to Ω . Thus, we choose an ordering of Ω and, by the above, the value $\Phi^k(f)(\Omega)$ does not depend on the chosen ordering. Notice that Ω is not necessarily a sub multi-set of S . We only require that the underlying set of Ω be contained in S . For example, if $S = \{1, 2, 3\}$ and $k = 1$, we have $\{1, 1\}$, $\{1, 3\}$ and $\{2, 2\}$ as possible choices for Ω .

We may rephrase the above property (*) by saying that, for all multi-sets Ω of cardinality $k + 1$ such that the underlying set Ω' is contained in S , we have $\Phi^k(f)(\Omega) \in D$.

2.1. Notation. We fix now the notation for the rest of this section.

- $p(X)$ is a monic non-constant polynomial in $D[X]$ of degree n .
- $\Omega_p = \{\alpha_1, \dots, \alpha_n\}$ is the multi-set of roots of $p(X)$ in \overline{K} (the α_i 's are integral over D).
- $F = K(\alpha_1, \dots, \alpha_n)$ the splitting field of $p(X)$.
- D_F the integral closure of D in F .

Given $f \in F[X]$, whenever we expand $f \in F[X]$ as in (2.1) in terms of the roots Ω_p of $p(X)$, we implicitly assume that an order of Ω_p has been fixed (so we choose one of the $n!$ associated n -tuples). Changing the order of Ω_p will give a different expansion.

We now need the following preliminary lemma: the divided differences of a polynomial $p(X)$ are zero when they are evaluated at the roots of the polynomial $p(X)$ itself.

Lemma 2.4. *For every sub-multi-set Ω of Ω_p of cardinality $k + 1$, $k < n - 1$, we have $\Phi^k(p)(\Omega) = 0$, and $\Phi^{n-1}(p)(\Omega_p) = 1$. Equivalently, we have:*

$$\Phi^k(p)(\alpha_1, \dots, \alpha_{k+1}) = \begin{cases} 0, & \text{if } 0 \leq k < n \\ 1, & \text{if } k = n \end{cases}$$

for any possible choice of an ordering for Ω_p .

Proof. We fix an ordering for Ω_p . We consider the Newton expansion of $p(X)$ over F with respect to Ω_p up to the order n ($p(X)$ is split over F). The coefficients of this expansion are exactly $\{\Phi^k(p)(\alpha_1, \dots, \alpha_{k+1})\}_{0 \leq k \leq n}$, where for $k = n$, we have the leading coefficient of $p(X)$ which is 1. Since $p(X)$ is divisible by itself, all the other coefficients in this expansion are zero. Obviously, the result does not depend on the chosen ordering for Ω_p . \square

Lemma 2.5. *Let $f \in K[X]$, and let $r \in K[X]$ be the unique remainder in the division of $f(X)$ by $p(X)$ in $K[X]$. If $r \neq 0$, let $m < n$ be the degree of $r(X)$. Then, over $F[X]$ we have*

$$(2.2) \quad r(X) = f(\alpha_1) + \Phi^1(f)(\alpha_1, \alpha_2) \cdot (X - \alpha_1) + \dots \\ + \Phi^m(f)(\alpha_1, \dots, \alpha_{m+1}) \prod_{i=1}^m (X - \alpha_i),$$

which is the Newton expansion of $r(X)$ with respect to $\Omega_p = \{\alpha_1, \dots, \alpha_n\}$.

Proof. If $f(X) = q(X)p(X) + r(X)$, by linearity of the divided difference operator, we have $\Phi^k(f) = \Phi^k(r) + \Phi^k(p \cdot q)$, for all $k \in \mathbb{N}$. Moreover, by the so-called Leibniz rule for divided differences (see, for example, [18]), we have $\Phi^k(p \cdot q) = \sum_{i=0, \dots, k} \Phi^i(p) \Phi^{k-i}(q)$ (we omit the variables). By Lemma 2.4, for $0 \leq k < n$, we get that

$$(2.3) \quad \Phi^k(f)(\alpha_1, \dots, \alpha_{k+1}) = \Phi^k(r)(\alpha_1, \dots, \alpha_{k+1}).$$

Notice that, for $k = m$, the above value is the leading coefficient of $r(X)$, and for $m < k < n$, it is zero. Because of the last formula, $r(X)$ has the desired expansion over $F[X]$. \square

By means of Lemma 2.4 and Lemma 2.5 we give a new proof of [16, Proposition 4.1], which says that a polynomial $f(X)$ of $K[X]$ is in $D(p)$ if and only if the divided differences of $f(X)$ up to the order $n - 1$ are integral on every sub-multi-set of the multi-set Ω_p of the roots of $p(X)$.

Proposition 2.6. *Let D be an integrally closed domain with quotient field K . Let $f \in K[X]$ and $p \in D[X]$ monic of degree n . Let*

$\Omega_p = \{\alpha_1, \dots, \alpha_n\}$ be the multi-set of roots of $p(X)$ in a splitting field F over K . Then the following are equivalent:

- (i) $f \in D(p)$.
- (ii) For all $0 \leq k < n$, $\Phi^k(f)(\alpha_1, \dots, \alpha_{k+1}) \in D[\alpha_1, \dots, \alpha_{k+1}]$.
- (iii) For all $0 \leq k < n$, $\Phi^k(f)(\alpha_1, \dots, \alpha_{k+1}) \in D_F$.

Proof. If (i) holds, let $f(X) = r(X) + p(X)q(X)$, for some $q \in K[X]$, $r \in D[X]$, $\deg(r) < n$ or $r = 0$. In particular, the divided differences of $r(X)$ are polynomials with coefficients in D . By (2.3), $\Phi^k(f)(\alpha_1, \dots, \alpha_{k+1}) = \Phi^k(r)(\alpha_1, \dots, \alpha_{k+1}) \in D[\alpha_1, \dots, \alpha_{k+1}]$, for all the relevant k 's. Hence, (i) \Rightarrow (ii).

Obviously (ii) \Rightarrow (iii), since the roots of $p(X)$ are integral over D , so that $D[\alpha_1, \dots, \alpha_{k+1}] \subseteq D_F$.

Suppose now that (iii) holds. We have to prove that the remainder $r(X)$ of the Euclidean division in $K[X]$ of $f(X)$ by $p(X)$ is in $D[X]$. Let $m < n$ be the degree of $r(X)$. Consider the Newton expansion of $r(X)$ with respect to Ω_p over $F[X]$ as in Lemma 2.5 (see (2.2)). By assumption, the coefficients $\{\Phi^k(f)(\alpha_1, \dots, \alpha_{k+1})\}_{k=0, \dots, m}$ of this expansion are in D_F . The leading coefficient of $r(X)$ is equal to $\Phi^m(f)(\alpha_1, \dots, \alpha_{m+1})$, so that it is in $D_F \cap K = D$ (we use here the assumption that D is integrally closed). The coefficient c_{m-1} of the term X^{m-1} of $r(X)$ is $\Phi^{m-1}(f)(\alpha_1, \dots, \alpha_m) \pm (\sum_{i=1, \dots, m} \alpha_i) \cdot \Phi^m(f)(\alpha_1, \dots, \alpha_{m+1})$ which is in D_F , so c_{m-1} is in $K \cap D_F = D$. If we continue in this way we prove that $r(X)$ is in $D[X]$, which gives (i). □

Remark 2.7. If we choose another ordering on the multi-set Ω_p of roots of $p(X)$ we have other conditions of integrality on the values of the divided differences of a polynomial $f \in D(p)$ at the vectors of elements in Ω_p . Since condition (i) of Proposition 2.6 does not depend on the order we choose on Ω_p , the above conditions are also equivalent to this one:

- (ii') for all $0 \leq k < n$, and for every sub-multi-set Ω of Ω_p
of cardinality $k + 1$, $\Phi^k(f)(\Omega) \in D[\Omega]$,

that is, $\Phi^k(f)$ is integral-valued on Ω : $\Phi^k(f)(\Omega) \in D_F$ (see also [16, Proposition 4.1 and Remark 4.1]).

Note that, if $p \in D[X]$ is a monic polynomial of degree n which is split over D , that is, $p(X) = \prod_{i=1}^n (X - a_i)$, $a_i \in D$, then conditions (i) and (ii) are equivalent without the assumption that D is integrally closed (this follows immediately from the formula (2.2)). In particular, condition (ii) becomes: for all $0 \leq k < n$, $\Phi^k(f)(a_1, \dots, a_{k+1}) \in D$. We have, thus, in this case found again the result of [7, Proposition 11] (see also [16, Lemma 2.2 and Remark 2.1]).

Now we give the link between the ring of integer-valued polynomials whose divided differences are also integer-valued introduced by Bhargava and the polynomial pullbacks $D(p)$ we are working with.

We observe first that, if $p \in D[X]$ is a monic polynomial of degree n which is split over D (i.e., the set of roots Ω_p is contained in D), then $\text{Int}^{\{n-1\}}(\Omega_p, D_F)$ is contained in $D(p)$, by Proposition 2.6. The next example shows that this containment can be strict.

Example 2.8. Let $n = 2$, $\Omega = \{1, 3\} \subset \mathbb{Z}$ and $p(X) = (X - 1)(X - 3)$. Let $f(X) = p(X)/3 \in \mathbb{Z}(p)$. We have that $\Phi^1(f)(1, 1) = -2/3$, so that $f \notin \text{Int}^{\{1\}}(\Omega, \mathbb{Z})$. Indeed, by Proposition 2.6, given any $f \in \mathbb{Z}(p)$, $\Phi^1(f)$ is integer-valued over $\{(1, 3), (3, 1)\} \subsetneq \Omega^2$.

We need to introduce more notation before the next theorem.

2.2. Notation. Let Ω be a subset of D , and let n be a positive integer. We denote by $\mathcal{P}_n(\Omega)$ the set of monic polynomials $q(X)$ over D of degree n whose set of roots is contained in Ω (so, in particular, they are split over D).

Theorem 2.9. *Let $\Omega \subseteq D$ and $n \in \mathbb{N}$. Then*

$$\text{Int}^{\{n-1\}}(\Omega, D) = \bigcap_{q \in \mathcal{P}_n(\Omega)} D(q).$$

Proof. (\subseteq). Let $f \in \text{Int}^{\{n-1\}}(\Omega, D)$, and let $q \in \mathcal{P}_n(\Omega)$. Since, for all $0 \leq k < n$, we have $\Phi^k(f)(\Omega^{k+1}) \subset D$, then for each sub-multi-set $\{a_1, \dots, a_{k+1}\}$ of Ω_q of cardinality $k+1$ we have $\Phi^k(f)(a_1, \dots, a_{k+1}) \in D$. Then, by Proposition 2.6 (see also Remark 2.7), we have that $f \in D(q)$.

(\supseteq). Let $f \in D(q)$, for all $q \in \mathcal{P}_n(\Omega)$. Let $k \in \{0, \dots, n-1\}$, and let $(a_1, \dots, a_{k+1}) \in \Omega^{k+1}$. We consider a polynomial $q \in \mathcal{P}_n(\Omega)$ such that the multi-set $\{a_1, \dots, a_{k+1}\}$ is a sub-multi-set of the multi-set of roots Ω_q (that is, $\prod_{i=1}^{k+1} (X - a_i)$ divides $q(X)$). Then by Proposition 2.6, condition (ii), $\Phi^k(f)(a_1, \dots, a_{k+1}) \in D$ (see also Remark 2.7, condition (ii')). Since (a_1, \dots, a_{k+1}) was chosen arbitrarily, $f(X)$ is in $\text{Int}^{\{n-1\}}(\Omega, D)$. \square

In Example 2.8 above, we have that $f(X) = q(X)/3 - 2/3(X - 1)$ is not in $\mathbb{Z}(q)$, where $q(X) = (X - 1)^2$ is a polynomial in $\mathcal{P}_2(\Omega) = \{(X - 1)(X - 3), (X - 1)^2, (X - 3)^2\}$.

Remark 2.10. By [16, Lemma 5.1], given a monic polynomial $p \in D[X]$ of degree n which is split over D , the pullback ring $D(p)$ is equal to $\text{Int}_K(T_n^p(D), M_n(D))$, where $T_n^p(D)$ is the set of $n \times n$ triangular matrices with characteristic polynomial equal to $p(X)$. In particular, we have this representation for the ring of integer-valued polynomials over the algebra of $n \times n$ triangular matrices over D :

$$(2.4) \quad \text{Int}_K(T_n(D)) = \bigcap_{p \in \mathcal{P}_n^s(D)} D(p),$$

where $\mathcal{P}_n^s(D)$ is the set of monic polynomials over D of degree n which are split over D ; as we mentioned in the introduction, a similar result holds for $\text{Int}_K(M_n(D))$, see [16]. We note that this gives a positive answer to [17, Question 31] for the algebra $T_n(D)$. Similarly, given any subset \mathcal{P} of $\mathcal{P}_n^s(D)$, the intersection of the pullbacks $D(p)$ as $p(X)$ ranges through \mathcal{P} is the ring of polynomials which are integer-valued over the set of triangular matrices whose characteristic polynomial belongs to \mathcal{P} . By Theorem 2.9, this ring is equal to $\text{Int}^{\{n-1\}}(\Omega, D)$, where $\Omega \subseteq D$ is the set of roots of the polynomials in \mathcal{P} .

In the case $\Omega = D$, [7, Theorem 16] proves that $\text{Int}^{\{n-1\}}(D) = \text{Int}_K(T_n(D))$, which by (2.4) is also equal to the intersection of the pullbacks $D(p)$, as $p(X)$ ranges through $\mathcal{P}_n^s(D)$. Therefore, Theorem 2.9 generalizes this result to any subset Ω of D .

3. Integral closure of polynomial pullbacks.

Remark 3.1. Let $\Omega \subset \overline{K}$ be a finite set. Let $F = K(\Omega)$, and let D_F be the integral closure of D in F . By [6, Proposition IV.4.1], $\text{Int}(\Omega, D_F)$ is integrally closed. Hence, $\text{Int}_K(\Omega, D_F) = \text{Int}(\Omega, D_F) \cap K[X]$ is integrally closed, too. The same remark was used in [17, Proposition 7].

Lemma 3.2. *Let D be an integrally closed domain. Let $p \in D[X]$ be a non-constant polynomial of degree n and $\Omega_p \subset \overline{K}$ the multi-set of its roots. Let $f \in K[X]$ be integral-valued over Ω_p , that is, $f \in \text{Int}_K(\Omega_p, \overline{D})$. Then the polynomial*

$$P(X) = P_{f,p}(X) \doteq \prod_{\alpha \in \Omega_p} (X - f(\alpha))$$

is in $D[X]$. Moreover, $P(f(X))$ is divisible by $p(X)$ in $K[X]$.

Proof. Notice that $P(X)$ has degree n , because the product is over the elements of the multi-set Ω_p . We set $g(X) \doteq p(X)/\text{lc}(p) = \prod_{\alpha \in \Omega_p} (X - \alpha)$, where $\text{lc}(p)$ is the leading coefficient of $p(X)$. The polynomial $g(X)$ is in $K[X]$ and is monic.

Let $M \in M_n(K)$ be a matrix with characteristic polynomial equal to $g(X)$ (e.g., the companion matrix of $g(X)$). The multi-set of eigenvalues of M over \overline{K} is exactly Ω_p . Notice that $f(M)$ is in $M_n(K)$, so its characteristic polynomial is in $K[X]$. By [3, Chapter VII, Proposition 10] (considering everything over \overline{K}) the characteristic polynomial of $f(M)$ is precisely $P(X)$. In particular, the set of eigenvalues of $f(M)$ is $f(\Omega_p) = \{f(\alpha) \mid \alpha \in \Omega_p\}$, which, by assumption on $f(X)$, is contained in \overline{D} . Hence, the coefficients of $P(X)$ are integral over D (being the elementary symmetric functions of the roots), and since D is integrally closed they are in D .

For the last statement, notice that, for each $\alpha \in \Omega_p$, $X - \alpha$ divides $f(X) - f(\alpha)$ over $F = K(\Omega_p)$. Hence, $p(X) = \prod_{\alpha \in \Omega_p} (X - \alpha)$ divides $P(f(X)) = \prod_{\alpha \in \Omega_p} (f(X) - f(\alpha))$ over F . Since both polynomials are in $K[X]$, one divides the other over K , as we wanted. \square

We now prove Theorem 1.3 of the introduction. For the sake of the reader we repeat the statement here.

Theorem 3.3. *Let $p \in D[X]$ be a monic non-constant polynomial, and let $\Omega_p \subset \overline{K}$ be the multi-set of its roots. Then the integral closure of $D(p)$ is $\text{Int}_K(\Omega_p, \overline{D})$.*

Notice that, by definition, $\text{Int}_K(\Omega_p, \overline{D}) = \text{Int}_K(\Omega'_p, \overline{D})$, where Ω'_p is the underlying set of Ω_p , the set of distinct roots of $p(X)$.

Proof. Remember that $\text{Int}_K(\Omega_p, \overline{D})$ is integrally closed by Remark 3.1. If D' is the integral closure of D in its quotient field K , then $D(p) \subseteq D'(p)$ is an integral ring extension, because $D[X] \subseteq D'[X]$ is. Since $D(p) \subseteq D'(p) \subseteq \text{Int}_K(\Omega_p, \overline{D})$ (because $p(X)$ is monic, so Ω_p is contained in \overline{D}), without loss of generality, we may assume that D is integrally closed (that is, $D = D'$). To prove the statement, it suffices to prove that $D(p) \subseteq \text{Int}_K(\Omega_p, \overline{D})$ is an integral ring extension.

Let $f \in \text{Int}_K(\Omega_p, \overline{D})$ and consider $P(X)$ as defined in Lemma 3.2. Then $P(X)$ is a monic polynomial in $D[X]$ such that $P(f(X))$ is divisible by $p(X)$ over K . Hence, $P(f(X))$ is in $D(p)$, and this gives a monic integral equation for $f(X)$ over the pullback ring $D(p)$. \square

We prove now that the ring of polynomials in $K[X]$ whose divided differences of order up to n are integer-valued over a finite subset Ω of D has integral closure equal to the ring of polynomials which are integer-valued over Ω .

Corollary 3.4. *Let D be an integrally closed domain. Let $\Omega \subset D$ be a finite set, and let $n \in \mathbb{N}$. Then the integral closure of $\text{Int}^{\{n\}}(\Omega, D)$ is $\text{Int}(\Omega, D)$.*

Proof. As in the proof of Theorem 3.3, it is sufficient to show that any $f \in \text{Int}(\Omega, D)$ satisfies a monic equation over the ring $\text{Int}^{\{n\}}(\Omega, D)$.

By Theorem 2.9, $\text{Int}^{\{n\}}(\Omega, D)$ is equal to the intersection of the pullbacks $D(p)$, as $p(X)$ ranges through the finite family $\mathcal{P}_{n+1}(\Omega)$ of monic polynomials over D of degree $n+1$ whose set of roots is contained in Ω . We consider the subset \mathcal{P} of $\mathcal{P}_{n+1}(\Omega)$ of those polynomials of the form $q(X) = (X - a)^{n+1}$, for $a \in \Omega$. For each of them, we consider the

polynomial $P_{f,q} \in D[X]$ as defined in Lemma 3.2. Therefore,

$$Q(X) \doteq \prod_{q \in \mathcal{P}} P_{f,q}(X)$$

is a monic polynomial in $D[X]$ such that $Q(f(X))$ is in $p(X)K[X]$ for each $p \in \mathcal{P}_{n+1}(\Omega)$. In fact, let $p \in \mathcal{P}_{n+1}(\Omega)$. If $a \in \Omega$ is a root of $p(X)$ of multiplicity $e \leq \deg(p) = n+1$, then $(X-a)^e$ divides $(f(X) - f(a))^{n+1}$ over K . Notice that the latter is a factor of $Q(f(X))$. Since this holds for every root of $p(X)$, then $p(X)$ divides $Q(f(X))$ over K , that is, $Q(f(X)) \in pK[X] \subset D(p)$. Since this holds for every $p \in \mathcal{P}_{n+1}(\Omega)$, this concludes the proof of Corollary 3.4. \square

Remark 3.5. If $\Omega \subseteq D$ is an infinite set and D has finite residue rings (that is, D/dD is a finite ring for every non-zero $d \in D$), reasoning as in [17] by means of the pullback representation of $\text{Int}^{\{n\}}(\Omega, D)$ given by Theorem 2.9, the same result of Corollary 3.4 holds. For $\Omega = D$, the result was given in [17, Corollary 17], where it is proved that the integral closure of $\text{Int}_K(T_{n+1}(D))$ is $\text{Int}(D)$. Note that, by [7, Theorem 16], the former ring is equal to $\text{Int}^{\{n\}}(D)$ (see Remark 2.10).

4. Prüfer rings of integral-valued polynomials. The next lemma, though easy, is a crucial step for establishing when $\text{Int}_K(\Omega, \overline{D})$ is a Prüfer domain, for a finite set Ω of integral elements over D .

Lemma 4.1. *Let $p \in D[X]$ be a monic non-constant polynomial and $K \subseteq F$ an algebraic extension. Let D_F be the integral closure of D in F . Then $D(p) \subseteq D_F(p)$ is an integral ring extension.*

Proof. We use the well-known fact that the integral closure of $D[X]$ in $F[X]$ is $D_F[X]$ ([2, Proposition 13, Chapter V]). Hence, given $f(X) = r(X) + p(X)q(X) \in D_F(p)$, for some $r \in D_F[X]$ ($r = 0$ or $\deg(r) < \deg(p)$) and $q \in F[X]$, the polynomial $r(X)$ is integral over $D[X]$, so in particular it is also integral over $D(p)$. We now show that $h(X) = p(X)q(X) \in p(X) \cdot F[X]$ is integral over $D(p)$.

It is easy to see that, if $\Psi_q(T, X)$ is the minimal polynomial of $q(X)$ over $K[X]$, then the minimal polynomial of $h(X)$ over $K[X]$ is given by $\Psi_h(T, X) = p^n \cdot \Psi_q(T/p, X)$, which is a monic polynomial in T over

D . Notice that the coefficients of $\Psi_h(T, X) - T^n$ are in $p(X) \cdot K[X]$, so that $\Psi_h(T, X) \in D(p)[T]$. This proves our assertion. \square

We prove now Theorem 1.4 of the introduction.

Theorem 4.2. *Assume that D is integrally closed, and let Ω be a finite subset of \overline{D} . Then $\text{Int}_K(\Omega, \overline{D})$ is Prüfer if and only if D is Prüfer.*

Proof. Given $f(X)$ in $\text{Int}_K(\Omega, \overline{D})$ and $\alpha \in \Omega$, $f(X)$ is integral-valued over all the conjugates of α over K (see Proposition 1.10). Hence, without loss of generality, we can assume that Ω is equal to the set of roots Ω_p of a monic polynomial $p(X)$ over D (more precisely, $p(X)$ is the product of all the minimal polynomials of the elements of Ω , without repetitions).

Let $F = K(\Omega_p)$ be the splitting field of $p(X)$ over D , and let D_F be the integral closure of D in F . By assumption, $\Omega_p \subset D_F$. Remember that $\text{Int}_K(\Omega_p, \overline{D}) = \text{Int}_K(\Omega_p, D_F)$ (see the remarks after Proposition 1.10). By the result of McQuillan ([13, Corollary 7]), $\text{Int}(\Omega_p, D_F)$ is a Prüfer domain if and only if D_F is a Prüfer domain. Since D is integrally closed, by [10, Theorem 22.3, 22.4] D is Prüfer if and only if D_F is Prüfer. We have the following diagram:

$$\begin{array}{ccccc}
 D_F(p) & \longrightarrow & \text{Int}(\Omega_p, D_F) & \longrightarrow & F[X] \\
 \uparrow & & \uparrow & & \uparrow \\
 D(p) & \longrightarrow & \text{Int}_K(\Omega_p, D_F) & \longrightarrow & K[X]
 \end{array}$$

By Theorem 3.3, $D(p) \subseteq \text{Int}_K(\Omega_p, D_F)$ and $D_F(p) \subseteq \text{Int}(\Omega_p, D_F)$ are integral ring extensions. Hence, by Lemma 4.1, $\text{Int}(\Omega_p, D_F)$ is integral over $\text{Int}_K(\Omega_p, D_F)$. Moreover, since the former ring is integrally closed, it is the integral closure of the latter ring in $F[X]$. Finally, we have these equivalences:

$$\begin{aligned}
 D \text{ Prüfer} & \iff D_F \text{ Prüfer} \iff \text{Int}(\Omega_p, D_F) \text{ Prüfer} \\
 & \iff \text{Int}_K(\Omega_p, D_F) \text{ Prüfer},
 \end{aligned}$$

where the last equivalence follows again by [10, Theorem 22.3, 22.4] ($\text{Int}_K(\Omega_p, D_F)$ is integrally closed by Remark 3.1). \square

As we recalled in the introduction, the intersection of the polynomial pullbacks $D(p)$ arises in many different contexts, especially those concerning rings of integer-valued polynomials over algebras. In Section 2, we saw that the ring of integer-valued polynomials whose divided differences are also integer-valued can be represented as an intersection of such pullbacks. We now investigate more deeply how these pullbacks intersect with each other. As a corollary, we obtain a criterion for a pullback $D(p)$ to be integrally closed.

At the beginning of Section 1.3 we recalled that a monic irreducible polynomial over an integrally closed domain D is still irreducible over the quotient field K . Moreover, a monic polynomial $p \in D[X]$ can be uniquely factored into monic irreducible polynomials over D (see [12]; this is a sort of Gauss's lemma for monic polynomials over an integrally closed domain). Therefore, given a monic polynomial $p(X)$ in $D[X]$, we have $p(X) = \prod_i q_i(X)$, where $q_i(X)$ are powers of monic irreducible polynomials in $D[X]$. In particular, the $q_i(X)$'s are pairwise coprime in $K[X]$ (but they may not be coprime over D , see below). A polynomial $p(X)$ is square-free exactly when each $q_i(X)$ is irreducible. Notice that $p(X)K[X]$ is an ideal of each pullback $D(q_i)$, for all i . In particular, it is an ideal of the intersection of the rings $D(q_i)$.

The next proposition is a generalization of Lemma 1.6. Recall that two ideals I, J of a commutative ring R are coprime if $I + J = R$ (see [2, Chapter 2, page 53]). For this statement, we do not require D to be integrally closed. Given $q_1, q_2 \in D[X]$, we simply say that $q_1(X)$ and $q_2(X)$ are coprime (over D) if the corresponding principal ideals $q_1(X)D[X]$ and $q_2(X)D[X]$ are coprime.

Proposition 4.3. *Let $p \in D[X]$ be a monic polynomial. Let $p(X) = \prod_i q_i(X)$ be a factorization into monic polynomials over D which are pairwise coprime when they are considered over K . Then*

$$\frac{\bigcap_i D(q_i)}{p(X)K[X]} \cong \prod_i \frac{D[X]}{q_i(X)D[X]}.$$

Moreover, $D(p) = \bigcap_i D(q_i)$ if and only if $\{q_i(X)\}_i$ are pairwise coprime over D .

Note that two polynomials $q_1, q_2 \in D[X]$ may be coprime over

K without being coprime over D : for example, $q_1(X) = X$ and $q_2(X) = X - 2$ over \mathbb{Z} . However, under this condition, it is easy to verify that $q_1(X)D[X] \cap q_2(X)D[X] = q_1(X)q_2(X)D[X]$.

Proof. It is sufficient to notice that $\bigcap_i D(q_i)$ is the pullback of

$$\prod_i \frac{D[X]}{q_i(X)D[X]} \subset \prod_i \frac{K[X]}{q_i(X)K[X]} \cong \frac{K[X]}{p(X)K[X]}$$

with respect to the canonical residue mapping

$$\pi : K[X] \twoheadrightarrow \frac{K[X]}{p(X)K[X]},$$

that is,

$$\pi^{-1}\left(\prod_i \frac{D[X]}{q_i(X)D[X]}\right) = \bigcap_i D(q_i).$$

Indeed, by definition, we have

$$\begin{aligned} \pi^{-1}\left(\prod_i \frac{D[X]}{q_i(X)D[X]}\right) &= \left\{ f \in K[X] \mid f \pmod{q_i(X)K[X]} \right. \\ &\quad \left. \in \frac{D[X]}{q_i(X)D[X]}, \text{ for all } i \right\}. \end{aligned}$$

Since each $q_i(X)$ is monic, by Lemma 1.6, this is equivalent to the fact that the remainder of the division of $f(X)$ by $q_i(X)$ is in $D[X]$, that is, $f(X)$ is in $D(q_i)$; hence, the statement regarding the isomorphism. We then have the following pullback diagram:

$$\begin{array}{ccc} D(p) \subset & \longrightarrow & \bigcap_i D(q_i) \\ \downarrow & & \downarrow \\ \frac{D[X]}{p(X)D[X]} \subset & \longrightarrow & \prod_i \frac{D[X]}{q_i(X)D[X]} \end{array}$$

where the vertical arrows are the quotient map modulo the common ideal $p(X)K[X]$. Note that the bottom horizontal arrow is injective by the remark above before the proof. Then $D(p) = \bigcap_i D(q_i)$ if and only if $D[X]/p(X)D[X]$ and $\prod_i D[X]/q_i(X)D[X]$ are isomorphic. By the converse of the Chinese remainder theorem (see [2, Chapter 2,

Section 1, Proposition 5]) this holds if and only if the principal ideals $q_i(X)D[X]$ are pairwise coprime. \square

Recall that, given two polynomials $p_1, p_2 \in D[X]$, the principal ideals $p_i(X)D[X]$, $i = 1, 2$, are coprime if and only if the resultant $\text{Res}(p_1, p_2)$ is a unit of D if and only if p_1, p_2 have no common root modulo any maximal ideal $M \subset D$. Notice that $p_1(X), p_2(X)$ are coprime in $K[X]$ if and only if $\text{Res}(p_1, p_2) \neq 0$.

The next proposition is a generalization of Remark 1.9: given a monic non constant square-free polynomial $p(X)$ in $D[X]$, we determine the quotient ring of $\text{Int}_K(\Omega_p, \overline{D})$ modulo the principal ideal $p(X)K[X]$. Note that, in the case $\Omega_p \subset D$, we have $\text{Int}_K(\Omega_p, \overline{D}) = \text{Int}(\Omega_p, D)$, and we are in the case already treated (essentially by McQuillan).

Proposition 4.4. *Let $p \in D[X]$ be a monic non-constant polynomial which is square-free, say $p(X) = \prod_{i=1}^k p_i(X)$, where $p_i(X)$, for $i = 1, \dots, k$, are monic, distinct and irreducible polynomials over D . Then*

$$\frac{\text{Int}_K(\Omega_p, \overline{D})}{p(X)K[X]} \cong \prod_{i=1}^k D_{K_i},$$

where D_{K_i} is the integral closure of D in the field $K_i \cong K[X]/p_i(X)K[X]$, for each $i = 1, \dots, k$.

Proof. For each $i = 1, \dots, k$, we set $K_i \doteq K[X]/(p_i(X)) \cong K[\alpha_i]$, which is a finite field extension of K , where α_i is a (fixed) root of $p_i(X)$. Also let D_{K_i} be the integral closure of D in K_i , for $i = 1, \dots, k$. By assumption on the $p_i(X)$'s, $D[X]/(p_i(X)D[X]) \cong D[\alpha_i] \subset K[\alpha_i]$. Note that $\text{Int}_K(\Omega_p, \overline{D}) = \text{Int}_K(\{\alpha_1, \dots, \alpha_k\}, \overline{D})$: if $f \in K[X]$ is integral-valued on α_i , then it is integral-valued on every conjugate root of α of α_i , that is on the set of roots Ω_{p_i} (see also Proposition 1.10).

As we remarked in the introduction, the rings $\text{Int}_K(\Omega_p, \overline{D}) \subset K[X]$ have the ideal $p(X)K[X]$ in common, so that $\text{Int}_K(\Omega_p, \overline{D})$ is a pullback with respect to the canonical residue map

$$\pi : K[X] \twoheadrightarrow \frac{K[X]}{p(X)K[X]}.$$

The polynomial ring $K[X]$ is mapped to

$$K[X]/(p(X)) \cong \prod_{i=1}^k K[\alpha_i]$$

by the map which sends X to $(\alpha_1, \dots, \alpha_k)$, so that a polynomial $f \in K[X]$ is mapped to $(f(\alpha_1), \dots, f(\alpha_k))$.

In the same way as in Proposition 4.3 we just have to prove that $\text{Int}_K(\Omega_p, \overline{D}) = \pi^{-1}(\prod_{i=1}^k D_{K_i})$. By definition,

$$\pi^{-1}\left(\prod_{i=1}^k D_{K_i}\right) = \{f \in K[X] \mid f(\alpha_i) \in D_{K_i}, \text{ for all } i = 1, \dots, k\},$$

so that a polynomial $f(X)$ is in this ring if and only if it is integral-valued on every α_i , that is, $f \in \text{Int}_K(\{\alpha_1, \dots, \alpha_k\}, \overline{D})$. \square

An equivalent statement of Proposition 4.4 is the following: let Ω be a finite subset of \overline{D} , and let $p \in D[X]$ be the product of the minimal polynomials $p_1(X), \dots, p_k(X)$ of the elements of Ω , without repetition. Then the quotient of $\text{Int}_K(\Omega, \overline{D})$ modulo $p(X)K[X]$ is isomorphic to $\prod_{i=1}^k D_{K_i}$, where D_{K_i} is as in the statement of Proposition 4.4. We notice that a proof of Theorem 4.2 also follows in another way by [4, Theorem 4.3], due to Proposition 4.4.

Theorem 4.5. *Let $p \in D[X]$ be a monic non-constant polynomial. Suppose that $p(X) = \prod_{k=1, \dots, k} p_i(X)^{e_i}$ is the unique factorization of $p(X)$ into powers of monic irreducible polynomials in $D[X]$, $e_i \geq 1$. Then $D(p)$ is integrally closed if and only if the following conditions are satisfied:*

- (i) $p(X)$ is squarefree (i.e., $e_i = 1$ for all i).
- (ii) For each $i = 1, \dots, k$, $D[X]/(p_i(X)) \cong D_{K_i}$, where the latter is the integral closure of D in the field $K_i \cong K[X]/(p_i(X))$.
- (iii) $\text{Res}(p_i, p_j) \in D^*$ for each $i \neq j$.

If D is a Prüfer domain, $D(p)$ is integrally closed if and only if $D(p)$ is a Prüfer domain, and in that case $D(p) = \text{Int}_K(\Omega_p, \overline{D})$.

Proof. Suppose that $D(p)$ is integrally closed. If $p(X)$ is not squarefree, then some exponent e_i is strictly greater than 1. Let

$q(X) = \prod_{i=1}^k p_i(X)$ be the square-free part of $p(X)$. By assumption, $q(X) \neq p(X)$ and $q(X)$ divides $p(X)$. So, by Lemma 1.7, $D(p) \subsetneq D(q)$. Since $q(X)$ has the same set of roots of $p(X)$, $D(q)$ is contained in $\text{Int}_K(\Omega_p, D_F)$. Hence, $D(p)$ cannot be equal to $\text{Int}_K(\Omega_p, D_F)$, which is in contradiction with Theorem 3.3. Then $p(X)$ is square-free.

By Propositions 4.3 and 4.4 (we retain the same notation of those Propositions) we have the following diagram of pullbacks (notice that $\Omega_p = \bigcup_{i=1}^k \Omega_{p_i}$ and $\bigcap_{i=1}^k \text{Int}_K(\Omega_{p_i}, \overline{D}) = \text{Int}_K(\Omega_p, \overline{D})$), where the vertical lines are the reduction map modulo $p(X)K[X]$:

$$(4.1) \quad \begin{array}{ccccccc} D(p) & \hookrightarrow & \bigcap_i D(p_i) & \hookrightarrow & \text{Int}_K(\Omega_p, \overline{D}) & \hookrightarrow & K[X] \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ \frac{D[X]}{p(X)D[X]} & \hookrightarrow & \prod_i D[\alpha_i] & \hookrightarrow & \prod_i D_{K_i} & \hookrightarrow & \prod_i K[\alpha_i] \end{array}$$

Obviously, $D(p)$ is integrally closed if and only if $D(p) = \bigcap_{i=1}^k D(p_i)$ and $\bigcap_{i=1}^k D(p_i) = \text{Int}_K(\Omega_p, \overline{D})$.

Since $D(p) = \bigcap_{i=1}^k D(p_i)$, by Proposition 4.3, this condition is equivalent to condition (iii). Looking at the above diagram, $\bigcap_{i=1}^k D(p_i) = \text{Int}_K(\Omega_p, \overline{D})$ if and only if $D[X]/p_i(X)D[X] = D_{K_i}$ for all $i = 1, \dots, k$, which is condition (ii).

Conversely, suppose conditions (i), (ii) and (iii) hold. Then looking at the above pullback diagram again, we have that $D(p)$ is equal to $\text{Int}_K(\Omega_p, \overline{D})$; hence, by Theorem 3.3, $D(p)$ is integrally closed.

Suppose now D is a Prüfer domain. If $D(p) = \text{Int}_K(\Omega_p, \overline{D})$, then $D(p)$ is a Prüfer domain by Theorem 4.2. Conversely, if $D(p)$ is Prüfer, then it is integrally closed. The very last assertion follows at once by Theorem 3.3. □

In the next examples, we show that the theorem does not hold if we remove one of the conditions.

Example 4.6. Let $p_1(X) = X^2 + 1, p_2(X) = X^2 - 2 \in \mathbb{Z}(X)$ and $p(X) = p_1(X)p_2(X)$. The resultant $\text{Res}(p_1, p_2)$ is equal to 9. Moreover, $K_1 = \mathbb{Q}(i) \supset O_{K_1} = \mathbb{Z}(X)/(p_1(X))$ and $K_2 = \mathbb{Q}(\sqrt{2}) \supset O_{K_2} = \mathbb{Z}(X)/(p_2(X))$. Then $\mathbb{Z}(p_1) \cap \mathbb{Z}(p_2) = \text{Int}_{\mathbb{Q}}(\Omega_p, \overline{\mathbb{Z}})$ (see the

proof of Theorem 4.5 and the diagram (4.1)) but $\mathbb{Z}(p_1 \cdot p_2) = \mathbb{Z}(p) \subsetneq \mathbb{Z}(p_1) \cap \mathbb{Z}(p_2)$ (Proposition 4.3). Notice that $\mathbb{Z}(p_1)$ and $\mathbb{Z}(p_2)$ are integrally closed: $\mathbb{Z}(p_i) = \text{Int}_{\mathbb{Q}}(\Omega_{p_i}, \overline{\mathbb{Z}})$ for $i = 1, 2$, but $\mathbb{Z}(p)$ is not integrally closed. Here, condition (iii) of Theorem 4.5 is not satisfied.

Example 4.7. $p_1(X) = X^2 - 5$, $p_2(X) = X^2 - 6$. The resultant of $p_1(X)$ and $p_2(X)$ is equal to 1. Then

$$K_1 = \mathbb{Q}(\sqrt{5}) \supset O_{K_1} = \mathbb{Z}\left[\frac{1 + \sqrt{5}}{2}\right] \supsetneq \mathbb{Z}[\sqrt{5}] \cong \mathbb{Z}[X]/(p_1(X))$$

and

$$K_2 = \mathbb{Q}(\sqrt{6}) \supset O_{K_2} = \mathbb{Z}[X]/(p_2(X)).$$

Then $\mathbb{Z}(p_1) \cap \mathbb{Z}(p_2) \subsetneq \text{Int}_{\mathbb{Q}}(\Omega_p, \overline{\mathbb{Z}})$, but $\mathbb{Z}(p) = \mathbb{Z}(p_1) \cap \mathbb{Z}(p_2)$. Hence, $\mathbb{Z}(p)$ is not integrally closed, because condition (ii) of Theorem 4.5 is not satisfied.

Corollary 4.8. *Let $p \in D[X]$ be a monic polynomial over D which is split in D . Then $D(p)$ is integrally closed if and only if the discriminant of $p(X)$ is a unit in D .*

Notice that, if the latter condition holds, in particular $p(X)$ is separable, it has no repeated roots. We denote by $\Delta(p)$ the discriminant of $p(X)$.

Proof. Let $\Omega_p = \{\alpha_1, \dots, \alpha_n\} \subset D$ be the multi-set of roots of $p(X)$. By Theorem 3.3, the integral closure of $D(p)$ is $\text{Int}(\Omega_p, D) = \bigcap_i D(X - \alpha_i)$.

It is enough to observe that $\Delta(p) = \prod_{i < j} (\alpha_i - \alpha_j)^2$ and that, if $p_i(X) = X - \alpha_i$, for $i = 1, \dots, n$, then $\text{Res}(p_i, p_j) = \pm(\alpha_j - \alpha_i)$. Then, by Theorem 4.5, Corollary 4.8 is proved. \square

Remark 4.9. The statement is false if we do not assume that $p(X)$ is split over D . For example, let $D = \mathbb{Z}$ and $p(X) = X^2 - 2$. Then $\mathbb{Z}(p)$ is integrally closed by Proposition 1.10 (see also Theorem 4.5), because $\mathbb{Z}[\sqrt{2}]$ is the ring of integers O_K of $K = \mathbb{Q}(\sqrt{2})$, so $\mathbb{Z}(p) = \text{Int}_{\mathbb{Q}}(\{\pm\sqrt{2}\}, O_K)$. However, $\Delta(p) = 8$. This implies that the pullback

$O_K(p) \subset K[X]$ is not integrally closed: the polynomial $f(X) = (X - \sqrt{2})/(2\sqrt{2})$ is in $\text{Int}(\{\pm\sqrt{2}\}, O_K)$ and not in $O_K(p)$, and by Theorem 3.3 $f(X)$ is integral over $O_K(p)$.

Remark 4.10. We can prove Theorem 3.3 by means of a pullback diagram argument. By Lemma 1.6 and Proposition 4.4, looking at the diagram (4.1), by [8, Lemma 1.1.4 (8)], $\text{Int}_K(\Omega_p, \overline{D})$ is the integral closure of $D(p)$, since $\prod_i D_{K_i}$ is the integral closure of $D[X]/p(X)D[X]$ in $K[X]/p(X)K[X]$. Indeed, it is known that $K[X]/p(X)K[X]$ is the total quotient ring of $D[X]/p(X)D[X]$ (see the proof of [14, Theorem 10.15]). Hence, by [10, Proposition 2.7], $K[X]/p(X)K[X]$ is the total quotient ring of every subring containing $D[X]/p(X)D[X]$, and, in particular, of $\prod_i D[\alpha_i]$. By [2, Proposition 9, Chapter V], $\prod_{i=1}^k D_{K_i}$ is the integral closure of D in $\prod_{i=1}^k K[\alpha_i]$. Since each α_i is integral over D , it follows that $\prod_{i=1}^k D_{K_i}$ is the integral closure of $\prod_{i=1}^k D[\alpha_i]$ in $\prod_{i=1}^k K[\alpha_i]$.

5. General case of a finite set of integral elements over D .

We show in this section how to apply the previous results to the more general setting mentioned in the introduction, namely, when the finite set of integral elements over D is not necessarily contained in an algebraic extension of K . We recall the assumptions we mentioned in the introduction.

For simplicity, we assume that D is integrally closed. Let A be a D -algebra, possibly non-commutative and with zero-divisors, which is finitely generated and torsion-free as a D -module. Note that every element a of A is integral over D . Let $\mu_a(X)$ be the minimal polynomial of a over D , which is not necessarily irreducible. To be precise, $\mu_a(X)$ is the monic generator of the ideal of $K[X]$ of those polynomials which are zero on a . Since D is supposed integrally closed and a is integral over D , $\mu_a \in D[X]$ (so that $\mu_a(X)$ is also the generator of the ideal of $D[X]$ of those polynomials which are zero at a). For short, we set $\Omega_a = \Omega_{\mu_a}$, the set of roots in \overline{D} of $\mu_a(X)$. We may evaluate polynomials of $K[X]$ at the elements of A in the extended K -algebra $B = A \otimes_D K$ (note that, by assumption, K and A embed into B). Given a subset S of A , we consider the ring of integer-valued polynomials over S :

$$\text{Int}_K(S, A) = \{f \in K[X] \mid f(S) \subset A\}.$$

For $S = A$, we have the ring $\text{Int}_K(A, A) = \text{Int}_K(A)$ of integer-valued polynomials over A . For more details about this setting we refer to [17]. As in [17], we consider polynomials over K whose evaluation at the elements of S are not necessarily in A but are still integral over D . For this reason, we call them *integral-valued* polynomials over S , since they preserve the integrality of the elements of S . We retain the notation introduced in [17].

Definition 5.1. Let $K[S]$ be the K -subalgebra of $B = A \otimes_D K$ generated by K and the elements of S . Also let S' be the subset of $K[S]$ of those elements which are integral over D . We set

$$\text{Int}_K(S, S') = \{f \in K[X] \mid f(S) \subset S'\},$$

which we call integral-valued polynomials over S .

Note that, in general, S' does not form a ring, if A is non-commutative (even if S is a ring; for example, consider the case $A = M_n(D)$). Nevertheless, $\text{Int}_K(S, S')$ does form a ring by the argument given in [17, Proposition 6]: in order to show that $\text{Int}_K(S, S')$ is closed under addition and multiplication, it is sufficient to consider what happens point-wise and use the fact that, for each $s \in S$, $K[s]$ is a commutative K -algebra. We note that the ring $\text{Int}_K(S, S')$ is equal to the ring of polynomials in $K[X]$ such that $f(s)$ (which a priori is in $K[s] \subseteq B$) is integral over D for each $s \in S$. Clearly, $\text{Int}_K(S, A) \subseteq \text{Int}_K(S, S')$, because every element of A is integral over D . The key result which links the ring of integral-valued polynomials $\text{Int}_K(S, S')$ to a previous ring of integral-valued polynomials over a subset Ω of \overline{D} is the following.

Theorem 5.2. [17, Theorem 9]. *Let S be a subset of A , and set $\Omega_S = \bigcup_{s \in S} \Omega_s \subset \overline{D}$. Then*

$$\text{Int}_K(S, S') = \text{Int}_K(\Omega_S, \overline{D}).$$

Proof. For the sake of the reader we give the proof. Since $1 \in D \subset B$, we may embed B into the endomorphism ring $\text{End}_K(B)$, via the map given by multiplication on the left by $b \in B$. In particular, A is a sub- D -algebra of $\text{End}_K(B)$, and for $s \in S$, Ω_s is the set of eigenvalues (in \overline{K}) of s considered as a K -endomorphism of B . Since A is finitely generated

as a D -module, by [3, Chapter VII, Section 5, Proposition 10], for any polynomial $f \in K[X]$, $f(\Omega_s) = \{f(\alpha) \mid \alpha \in \Omega_s\}$ is the set of eigenvalues of $f(s)$, so that in our notation $f(\Omega_s) = \Omega_{f(s)}$. Given $f \in K[X]$ and $s \in S$, $f(s)$ is integral over D if and only if the elements of $\Omega_{f(s)} = f(\Omega_s)$ are integral over D (because D is integrally closed). The claim is then proved. \square

We are ready to give the proof of the last main result of the paper, see Corollary 1.5 of the introduction.

Corollary 5.3. *Let S be a finite subset of A and $\Omega_S = \bigcup_{s \in S} \Omega_s \subset \overline{D}$. Then the integral closure of $\text{Int}_K(S, A)$ is $\text{Int}_K(\Omega_S, \overline{D})$.*

Proof. Let $p(X) = \prod_{s \in S} \mu_s(X) \in D[X]$. By the above, we have the following inclusions:

$$D(p) \subseteq \text{Int}_K(S, A) \subseteq \text{Int}_K(S, S') = \text{Int}_K(\Omega_S, \overline{D}),$$

and the claim follows by Theorem 3.3. \square

Note that, by Theorem 4.2, the ring $\text{Int}_K(S, A)$ has Prüfer integral closure if and only if D is Prüfer.

Acknowledgements. We wish to thank the referee for his/her valuable suggestions which improved the quality of the paper. The paper was prepared during a visit at the Department of Mathematics and Physics of the University of Roma 3. The author wishes to thank Francesca Tartarone for the hospitality.

REFERENCES

1. M. Bhargava, *On P -orderings, rings of integer-valued polynomials and ultrametric analysis*, J. Amer. Math. Soc. **22** (2009), 963–993.
2. N. Bourbaki, *Commutative algebra*, Addison-Wesley Publishing Co., Reading, MA, 1972.
3. ———, *Algebra*, P.M. Cohn and J. Howie, eds., in *Elements of mathematics*, Springer-Verlag, Berlin, 1990.
4. J.G. Boynton, *Pullbacks of arithmetical rings*, Comm. Alg. **35** (2007), 2671–2684.
5. J.G. Boynton and S. Sather-Wagstaff, *Regular pullbacks*, Progr. Comm. Alg. **2**, 145–169, Walter de Gruyter, Berlin, 2012.

6. J.-P. Cahen and J.-L. Chabert, *Integer-valued polynomials*, Amer. Math. Soc. Surv. Mono. **48**, Providence, 1997.
7. S. Evrard, Y. Fares and K. Johnson, *Integer valued polynomials on lower triangular integer matrices*, Monats. Math. **170** (2013), 147–160.
8. M. Fontana, J.A. Huckaba and I.J. Papick, *Prüfer domains*, Mono. Text. Pure Appl. Math. **203**, Marcel Dekker, Inc., New York, 1997.
9. S. Gabelli and E. Houston, *Ideal theory in pullbacks*, in *Non-Noetherian commutative ring theory*, Kluwer Academic Publishers, Dordrecht, 2000.
10. R. Gilmer, *Multiplicative ideal theory*, Corrected reprint of the 1972 edition, Queen's University, Kingston, Ontario, 1992.
11. M. Griffin, *Prüfer rings with zero divisors*, J. reine angew. Math. **239/240** (1969), 55–67.
12. S. McAdam, *Unique factorization of monic polynomials*, Comm. Alg. **29** (2001), 4341–4343.
13. D.L. McQuillan, *Rings of integer-valued polynomials determined by finite sets*, Proc. Roy. Irish Acad. **85** (1985), 177–184.
14. M. Nagata, *Local rings*, Intersci. Tracts Pure Appl. Math. **13**, John Wiley & Sons, New York, 1962.
15. G. Peruginelli, *Integral-valued polynomials over sets of algebraic integers of bounded degree*, J. Num. Theor. **137** (2014), 241–255.
16. ———, *Integer-valued polynomials over matrices and divided differences*, Monatsh. Math. **173** (2014), 559–571.
17. G. Peruginelli and N. Werner, *Integral closure of rings of integer-valued polynomials on algebras*, in *Commutative algebra: Recent advances in commutative rings, integer-valued polynomials, and polynomial functions*, M. Fontana, S. Frisch and S. Glaz, eds., Springer, 2014.
18. J.F. Steffensen, *Note on divided differences*, Danske Selsk. Math.-Fys. Medd. **17** (1939).
19. B.L. van der Waerden, *Algebra*, Volume I., Springer-Verlag, New York, 1991.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF PADOVA, VIA TRIESTE, 63 35121 PADOVA, ITALY

Email address: gperugin@math.unipd.it