Integer-Valued Polynomials on a Subset

Cătălin Bărbăciaru*

Department of Mathematics, University of Craiova,
A.I. Cuza 13, 1100 Craiova, Romania

Communicated by A. C. Woods

Received December 2, 1994; revised October 10, 1996

Let \( R \) be a Dedekind domain whose residue fields are finite, and let \( K \) be the field of fractions of \( R \). When \( S \) is a (non-empty) subset of \( K \) we write \( \text{Int}(S) \) for the subring of \( K[X] \) consisting of all polynomials \( f(X) \) in \( K[X] \) such that \( f(S) \subseteq R \).

We show that there exist fractional ideals \( J_0, J_1, \ldots, J_n \) and monic polynomials \( f_0, f_1, \ldots, f_n \) such that

\[
\text{Int}(S) \cap V_n = \sum_{i=0}^{n} J_i f_i, \quad n \geq 0,
\]

where \( V_n \) is the \( K \)-space of polynomials of degree at most \( n \) in \( K[X] \). This generalises classic results on \( \text{Int}(R) \).

Let \( R \) be a Dedekind domain with finite residue fields and field of fractions \( K \). Let \( E \) be a (non-empty) subset of \( K \). Write \( \text{Int}_R(E) \) or just \( \text{Int}(E) \) for the subring of polynomials \( f(X) \) in \( K[X] \) such that \( f(E) \subseteq R \). We are interested in the structure of the \( A \)-module of \( \text{Int}_R(E) \) (see [2, 6, 7]).

For a subset \( E \) of \( K \) we define the \( R \)-closure \( \text{cl}_R(E) \) or just \( \text{cl}(E) \) of \( E \) to be the set of all elements \( a \in K \) such that \( f(a) \in R \) for every polynomial \( f \in \text{Int}_R(E) \). Thus \( \text{cl}_R(E) \) is the largest subset of \( K \) such that \( \text{Int}_R(E) = \text{Int}_R(\text{cl}_R(E)) \).

We say that \( E \) is \( R \)-closed if \( E = \text{cl}_R(E) \) and \( E \) is \( R \)-fractional if there exists \( d \in R \), \( d \neq 0 \), such that \( dE \subseteq R \). It is easy to prove that \( cl(cl(E)) = cl(E) \) and so we may consider only the case when \( E \) is \( R \)-closed. In [5] McQuillan proved that for every not \( R \)-fractional subset \( E \) of \( K \), \( \text{Int}(E) = R \).

**Theorem 1.** Let \( R \) be a Dedekind domain with field of fractions \( K \) and let \( E \) be an infinite \( R \)-fractional set which is \( R \)-closed. Let \( V_n \) be the \( K \)-space
of polynomials of degree at most \( n \) in \( K[X] \). Then there exist monic polynomials \( f_0, f_1, ..., f_n \) and fractional ideals \( J_0, J_1, ..., J_n \) such that

\[
\text{Int}(S) \cap V_n = \sum_{i=0}^{n} J_i f_i, \quad n \geq 0.
\]

The proof needs some preliminary lemmas. First, following McQuillan [5], we say that an \( R \)-fractional set of the form \( \bigcup_{i=1}^{r} (a_i + I) \), where \( I \) is a non-zero ideal of \( R \) and \( a_i \in K \) for \( i = 1, ..., r \), is called a homogeneous set with ideal \( I \).

**Proposition 2** [4]. Let \( E \) be an infinite \( R \)-fractional set which is \( R \)-closed. Then the sets \( T_n = \{ x \in K \mid \text{for every } f \in \text{Int}(E) \cap V_n, f(x) \in R \} \) are homogeneous, \( \text{Int}(T_n) \cap V_n = \text{Int}(E) \cap V_n \), and \( \bigcap_{n \geq 1} T_n = E \).

So it remains to deal with the case when \( E \) is an infinite homogeneous \( R \)-closed subset of \( R \).

The first case we study is that of a discrete valuation domain with finite residue field. Let \( E = \bigcup_{i=1}^{r} (a_i + m^k) \) where \( m \) is the maximal ideal of \( R \) and \( a_i \) are non-congruent modulo \( m^k \). We denote by \( s \) the norm of residue ring \( R/m^k \). Let \( 0 = x_0, ..., x_{s-1} \) be a complete system of representatives modulo \( m^k \).

For every positive integer \( n \) let \( i_0 = n - r[n/r] \) and write \( [n/r] = \sum_{i=0}^{n} s_i\pi^i \) where \( [n/r] \) is the integer part of \( n/r \) and \( 0 \leq s_i < s \) for all \( i \geq 0 \). We define \( a_n = a_0 + \sum_{j=0}^{n} x_j\pi^{j+1} \) where \( \pi \) is a generator of \( m \). When \( E = R \) this is the sequence defined in [6, 7]. The first \( r \) terms of this sequence are \( a_0, a_1, ..., a_{r-1} \) (whose cosets define the set \( E \)).

**Lemma 3.** (i) For every positive integer \( n \) the set \( \{ a_0, a_1, ..., a_{r}, n - 1 \} \) is a complete system of representatives modulo \( (m^k)^n \).

(ii) If \( v \) is the discrete (rank-one) valuation of \( K \), then \( v(a_n - a_{n-1}) = kd \) where \( d \) is the greatest integer such that \( rs^{d-1} \) divides \( n_1 - n_2 \) if \( r \) divides \( n_1 - n_2 \), and \( v(a_n - a_{n-1}) = 0 \) otherwise.

Proof. Let \( n_1 \) and \( n_2 \) be two positive integers such that \( n_1, n_2 < rs^{n-1} \) and \( a_{n_1} \equiv a_{n_2} \mod(m^d)^n \). Let \( a_n = a_0 + \sum\{0 \leq k \leq n \} x_k(\pi^k)^{i+1} \) and \( a_n = a_0 + \sum\{0 \leq k \leq n \} x_k(\pi^k)^{i+1} \) be defined as above. Since \( a_{n_1} \equiv a_{n_2} \mod(m^d)^n \) then \( a_{n_1} \equiv a_{n_2} \mod m^d \). But this is possible if \( l_0 = j_0 \). Analogous, \( x_0 = \beta_0 \), \( x_1 = \beta_1 \), ..., and so \( n_1 = n_2 \). Thus, the elements \( a_0, a_1, ..., a_{n}, n - 1 \) are pairwise noncongruent \( \mod(m^d)^n \). So a complete system of representatives of \( E \mod(m^d)^n \) has \( rs^{n-1} \) elements then \( \{ a_0, a_1, ..., a_{n}, n - 1 \} \) is one of them.

(ii) Let \( a_n = a_0 + \sum\{j > 0 \} x_j(\pi^j)^{i+1} \) and \( a_n = a_0 + \sum\{j > 0 \} x_j(\pi^j)^{i+1} \) be defined as above. If \( r \) divides \( n_1 - n_2 \) and \( d \) is the greatest integer such that
\[ r^d - 1 \text{ divides } n_1 - n_2, \text{ then } i_0 = j_0, \alpha_0 = \beta_0, \alpha_1 = \beta_1, \ldots, \alpha_{d-1} = \beta_{d-1}, \text{ and } \alpha_d \neq \beta_d. \text{ This implies that } \nu(a_n - a_m) = kd. \]

Since \( \nu(a_n - a_m) \) depends only on \( n_1 - n_2 \) we shall denote this integer by \( \nu_r(i) \).

Let

\[ f_0 = 1, \ldots, f_n = (X - a_0) \cdots (X - a_{n-1}) \quad (1) \]

We denote by \( f_0(E) \) the ideal of \( R \) generated by the elements \( f_n(x) \) where \( x \in E \). Then \( f_0(E) \) is a power of \( m \) and we define \( S(n) \) to be the corresponding exponent of \( m \). We denote also by \( I_i \) the fractional ideal \( m^{S(i)} \).

**Theorem 4.** With the above hypothesis and notations, we have:

(i) \( \text{Int}(E) \cap V_n = I_0 f_0 + \cdots + I_n f_n; \)

(ii) \( S(n) = k \sum_{s \geq 0} [n/rs^*]. \quad (2) \)

**Proof.** (i) Since \( f_0, f_1, \ldots \) have increasing degrees, they form a base for the \( K \)-vector space \( K[X] \) and so every polynomial \( P \in K[X] \) can be written in a unique way as \( P = \lambda_0 f_0 + \cdots + \lambda_n f_n \) for \( n = \deg P \). Suppose now that \( \nu(\lambda_i) \geq -S(i) \) for every \( i = 0, \ldots, n \). Then \( \lambda_i f_i(E) \subseteq R \) since \( f_i(E) = m^{S(i)} \) and so \( P \in \text{Int}(E) \cap V_n. \)

Conversely, if \( P \) belongs to \( \text{Int}(E) \cap V_n \) then \( \lambda_i = P(a_i) \in I_i \). Inductively, if \( \lambda_i \in I_i \) for every \( i = 0, \ldots, m-1 \), then

\[ Q_m = P - \lambda_0 f_0 - \cdots - \lambda_{m-1} f_{m-1} \]

is a polynomial belonging to \( \text{Int}(E) \). But \( Q_m(a_m) = P(a_m) \) and so \( \nu(\lambda_m, f_m(a_m)) \geq 0 \) which implies that \( \nu(\lambda_m) \geq -\nu(f_m(a_m)) = -S(m) \).

(ii) Let \( x \) be an element of \( E \) and \( w = \nu(f_0(x)) \). If \( w \) is infinite then \( f_0(x) = 0 \) and so \( x = a_m \) for some \( 0 \leq m < n \). If \( w \) is finite and since \( \{a_0, \ldots, a_m, w\} \) is a complete system of representatives of \( E \) modulo \( (m^{k})^{n+1} \), then there exists \( a_m \) such that \( \nu(x - a_m) \geq w + 1 \) and so

\[ \nu(f_0(a_m)) = \nu(f_0(x) + f_0(a_m) - f_0(x)) = \nu(f_0(x)) = w. \]

Since \( w \) is finite then \( m \geq n \) and so

\[ w = \nu(f_0(a_m)) = \nu((a_m - a_0) \cdots (a_m - a_{n-1})) = \sum_{i=0}^{n-1} \nu(a_m - a_i) \]

\[ = \sum_{i=m-n+1}^{m} v_{r_0}(i) = \sum_{i=0}^{m} v_{r_0}(i) - \sum_{i=0}^{m-n} v_{r_0}(i). \]
It is easy to prove that
\[
\sum_{i=0}^{m} v_{r,i}(i) = k \sum_{s \geq 0} \left[ \frac{m}{rs^s} \right].
\]

For more details see [3, 6]. Then
\[
v(f_n(x)) = k \sum_{s \geq 0} \left[ \frac{m}{rs^s} \right] - k \sum_{s \geq 0} \left[ \frac{m - n}{rs^s} \right] = k \sum_{s \geq 0} \left( \left[ \frac{m}{rs^s} \right] - \left[ \frac{m - n}{rs^s} \right] \right)
\]
\[\geq k \sum_{s \geq 0} \left[ \frac{n}{rs^s} \right].
\]

Using the same formulas we may obtain that
\[
v(f_n(a_i)) = k \sum_{s \geq 0} \left[ \frac{n}{rs^s} \right].
\]

So, we have proved (2). \(\square\)

\textbf{Remark 1.} The fractional ideals \(I_i\) and the polynomials \(f_i\) do not depend on \(n\). We observe also that \(I_i\) are principal ideals and so \(\text{Int}(E)\) is a free module.

We return now to the case of Dedekind domains. Let \(R\) be a Dedekind domain with field of fractions \(K\), \(\nu\) be a discrete (rank-one) valuation of \(K\) corresponding to the maximal ideal \(m_\nu\) (or simply \(m\) when there is no confusion), \(R_\nu\) be the associate discrete valuation domain, \(N_\nu\) be the norm of the residue field \(R/m_\nu\), and \(E\) be an \(R\)-closed homogeneous subset of \(R\) with ideal \(I = \prod_{i=1}^r m_\nu^{e_i}\). If \(J\) is a fractional ideal of \(R\), let \(\nu(J)\) be the exponent of \(m_\nu\) which appears in the decomposition of \(J\). We recall that:

\textbf{Proposition 5 [2].} Let \(R\) be Noetherian, \(E \subseteq R\), and \(S\) be a multiplicative subset of \(R\), then
\[
S^{-1} \text{Int}_R(E) = \text{Int}_{S^{-1}R}(E).
\]

\textbf{Lemma 6.} Let \(R\) be a Dedekind domain, \(E = \bigcup_{i=0}^{r-1} (x_i + I)\) be a homogeneous subset of \(R\) with ideal \(I\), and \(\nu\) be as above. Then
\[
\cl_R(E) \supseteq \bigcup_{i=0}^{r-1} (x_i + m_\nu^{e_i}R_i).
\]

\textbf{Proof.} We know from [5] that \(\cl_R(E) = E_m \cap K\) where \(E_m\) is the closure of \(E\) in the \(m\)-adic completion of \(K\). Let \(x = x_i + y\) be an element of
the coset $x_i + m^{n/I}R_i$. We shall prove that for every $n \geq v(I)$ there exists $z = x_i + z_0 \in E$ such that $v(z - x) \geq n$ which is equivalent to $v(z_0 - y) \geq n$. Since $y \in m^{n/I}R_i$ then $y = y_1/y_2$ where $v(y_1) \geq v(I)$ and $v(y_2) = 0$. So we have the equivalence $v(z_0 - x) \geq n \iff v(y_2z_0 - y_1) \geq n$. The equation $y_2 \equiv y_1 \pmod{m^n}$ admits a solution $z_1$ in $R$ (see [1]) since the ideals $(y_2)$ and $m^n$ are coprime. So $v(y_2z_1 - y_1) \geq n$ and since $v(y_1) \geq v(I)$, $n \geq v(I)$, and $v(y_1, z_1) = v(z_1) \geq v(I)$.

Let $I = \prod_{i=1}^{r} m_i^{n_i}$ be the decomposition of $I$. If $m$ is one of the divisors of $I$, say $m = m_1$, then by the Chinese Remainder Theorem, the system

$$\begin{align*}
\epsilon &\equiv z_1 \pmod{m^n} \\
\epsilon &\equiv 0 \pmod{m_i^{n_i}} \\
&\vdots \\
\epsilon &\equiv 0 \pmod{m_i^{n_i}}
\end{align*}$$

admits a solution $z_0$ in $R$. Since $v(z_0 - z_1) \geq n \geq v(I)$ and $v(z_1) \geq v(I)$ then we have $v(z_0) \geq v(I)$ which means that $z_0 \in I$ and $v(z_0 - y) \geq n$. If $m$ is different from every divisor of $I$, then the system

$$\begin{align*}
\epsilon &\equiv z_1 \pmod{m^n} \\
\epsilon &\equiv 0 \pmod{m_i^{n_i}} \\
&\vdots \\
\epsilon &\equiv 0 \pmod{m_i^{n_i}}
\end{align*}$$

admits a solution $z_0$ in $R$. Then $z_0 \in I$ and $v(z_0 - y) \geq n$ and the proof is complete.

For every $R, v, E$ as above we have $E_v = \bigcup_{i=0}^{r-1} (x_i + m^{n/I}R_i)$.

**Corollary 7.** Let $R, v, E,$ and $E_v$ be as in the preceding lemma. Then

$$\text{Int}_{R_v}(E) = \text{Int}_{R}(E_v).$$

**Proof.** Since $E \subseteq E_v \subseteq \text{cl}_{R_v}(E)$ then

$$\text{Int}_{R_v}(E) \supseteq \text{Int}_{R_v}(E_v) \supseteq \text{Int}_{R_v}(\text{cl}_{R_v}(E)) = \text{Int}_{R}(E).$$

**Remark 2.** If $m$ is not a divisor of $I$ then $E_v = R_v$ and so $\text{Int}_{R_v}(E) = \text{Int}_{R_v}(R_v)$.
Lemma 8. Let \( P \in K[X] \) be a polynomial of degree \( n \). We denote by \( \nu(P) \) the least valuation of \( P \)'s coefficients and by \( P(E) \) the \( R \)-module generated by the values of \( P \) on \( E \). Then \( P(E) \) is a fractional ideal and

\[
\nu(P) \leq \nu(P(E)) \leq S(n) + \nu(P),
\]

where \( S \) is the function defined by (2) associated to the discrete valuation ring \( R \), and the homogeneous set \( E \), (this lemma is analogous to Proposition 2 of [3]).

Proof. Let \( d \in R \) such that \( dP \in R[X] \). Then \( dP(E) \subseteq R \) and so \( P(E) \) is a fractional ideal of \( K \). Since \( E \) is a subset of \( R \), then it is easy to see that

\[
\nu(P) \leq \nu(P(E))
\]

(in fact we have \( \nu(P) = \nu(P(R)) \)).

Let \( \pi_i \in R \) be an element such that \( \nu(\pi_i) = 1 \) and let \( Q = \pi^{-\nu(P(E))}P \).

Then \( Q(E) \subseteq R \) and so \( Q \in \text{Int}_{R}(E) \). From Corollary 7, we have that

\[
Q(E) \subseteq R.
\]

Let now \( f_0, \ldots, f_n, \ldots \) be defined as in (1) for the discrete valuation ring \( R \), and the homogeneous set \( E \) (in particular, \( f_n \in R[X] \)). Then there exist \( \lambda_0, \ldots, \lambda_n \in R \) such that

\[
Q = \lambda_0 f_0 + \cdots + \lambda_n f_n,
\]

and so \( \nu(P) \geq \nu[P(E)] - S(n) \) since \( f_i \) are monic polynomials. The proof is now complete.

Now we are able to prove Theorem 1.

Proof of Theorem 1. First we observe that, for every positive integer \( n \), there exists a finite number of valuations \( \nu \) on \( K \) such that \( N_{\nu} \leq n \) and so there exists a finite number of valuations \( \nu \) on \( K \) such that \( S_{\nu}(n) \neq 0 \). We define

\[
J_n = \prod_{\nu} m_{\nu}^{-S_{\nu}(n)}.
\]

Let \( a_0, \ldots, a_{n-1}, \ldots \) be the chain constructed above for the discrete valuation ring \( R \), and the homogeneous set \( E \). Let \( f_0, \ldots, f_n \) be the corresponding polynomials. For every \( i = 0, \ldots, n \), let \( b_i \) be an element of \( R \) such that \( \nu(b_i - a_i) > S_{\nu}(n) \) for every valuation \( \nu \) such that \( S_{\nu}(n) \neq 0 \). Let \( f_0 = 1 \) and \( f_n \) be the polynomial

\[
f_n = (X - b_{0,n}) \cdots (X - b_{n-1,n}).
\]
Then \( v(f_u - f_v) > S_v(n) \) for every valuation \( v \) such that \( S_v(n) \neq 0 \) and so, by Proposition 8, we have
\[
S_v(n) < v(f_u, \xi) - f_v, \xi) \quad \text{for all } \xi \in E \text{ (even for all } \xi \in R).
\]
Since \( E \) is a subset of \( E_v \), then
\[
v(f_u, \xi) \geq S_v(n) \text{ and } v(f_v, \xi) \geq S_v(n) \quad \text{for all } \xi \in E.
\]
We know that \( v(f_u, b_n) - f_v, b_n) > S_v(n) \) because \( b_n \in R \) and so \( v(f_u, b_n) - f_v, a_v) \geq S_v(n) \) which implies that \( v(f_u, b_n) = v(f_v, a_v) = S_v(n) \) and then \( v(f_u, b_n) = S_v(n) \).
So, we proved that \( v(f_u(E)) = v(f_v(b_n)) = S_v(n) \) for every valuation \( v \) such that \( S_v(n) \neq 0 \). If \( v \) is not such a valuation, then applying Proposition 8 we have \( 0 = v(f_u) \leq v(f_v(E)) \leq v(f_v) + S_v(n) = 0 \) and hence \( v(f_u(E)) = S_v(n) \) for every valuation \( v \) on \( K \); that is,
\[
f_u(E) = J_n^{-1},
\]
where \( J_n \) is defined in (3). Let \( P \in K[X] \) be a polynomial of degree \( n \). Then there exist \( \lambda_0, ..., \lambda_n \in K \) such that
\[
P = \lambda_0 f_0 + \cdots + \lambda_n f_n.
\]
If \( P \in \text{Int}_R(E) \), and since the leading coefficient of \( P \) is \( \lambda_n \), then
\[
-S_v(n) \leq v(P(E)) - S_v(n) \leq v(P) \leq v(\lambda_n)
\]
for every valuation \( v \). So \( \lambda_n \) is an element of \( J_n \). Then \( \lambda_n f_n \in \text{Int}_R(E) \). We may repeat the same argument for \( P - \lambda_n f_n \) to obtain that \( \lambda_{n-1} \in J_{n-1} \), and so on.
Conversely, if \( \lambda, f_n \in \text{Int}_R(E) \) from (5) and so the sum \( \lambda_0 f_0 + \cdots + \lambda_n f_n \) belongs to \( \text{Int}_R(E) \) and the theorem is proved.

**Remark 3.** If \( E \) is any infinite subset of \( R \) and \( n \) is a positive integer then \( \text{Int}_R(E) \cap V_n \) is the sum of ideals \( J_0, J_1, ..., J_n \) along the polynomials \( f_0, ..., f_n \) where the ideals \( J_0, ..., J_n \) and the polynomials \( f_0, ..., f_n \) are determined as in Theorem 1 relative to the homogeneous set \( T_n \) from Proposition 2, applied to the \( R \)-closure of \( E \).

**REFERENCES**