Nontriviality of rings of integral-valued polynomials

Giulio Peruginelli

Dipartimento di Matematica "Tullio Levi-Civita",
Università di Padova, Italy

gperugin@math.unipd.it

24 Luglio, 2024
Joint Meeting AMS-UMI, 23-26 Luglio 2024, Palermo.

Special Session: The Ideal Theory and Arithmetic of Rings, Monoids, and Semigroups.

joint work with N. J. Werner

Introduction

Let $\overline{\mathbb{Q}}$ be a fixed algebraic closure of the field of rational numbers and $\overline{\mathbb{Z}}$ be the absolute integral closure of $\mathbb{Z}$. Given a subset S of $\overline{\mathbb{Z}}$, we consider the ring of integral-valued polynomials on S:

$$\mathrm{Int}_{\mathbb{Q}}(S, \overline{\mathbb{Z}}) = \{f \in \mathbb{Q}[X] \mid f(S) \subseteq \overline{\mathbb{Z}}\}$$

If $S = \mathbb{Z}$ we get the classical ring of integer-valued polynomials $\mathrm{Int}(\mathbb{Z})$.

Introduction

Let $\overline{\mathbb{Q}}$ be a fixed algebraic closure of the field of rational numbers and $\overline{\mathbb{Z}}$ be the absolute integral closure of $\mathbb{Z}$. Given a subset S of $\overline{\mathbb{Z}}$, we consider the ring of integral-valued polynomials on S:

$$\text{Int}_{\mathbb{Q}}(S, \overline{\mathbb{Z}}) = \{f \in \mathbb{Q}[X] \mid f(S) \subseteq \overline{\mathbb{Z}}\}$$

If $S = \mathbb{Z}$ we get the classical ring of integer-valued polynomials $\text{Int}(\mathbb{Z})$.

Theorem (Loper-Werner, 2012)

Let $n \geq 1$ and let $\mathcal{A}_n$ be the subset of those elements of $\overline{\mathbb{Z}}$ whose degree over $\mathbb{Q}$ is bounded by n. Then $\text{Int}_{\mathbb{Q}}(\mathcal{A}_n, \overline{\mathbb{Z}}) = \text{Int}_{\mathbb{Q}}(\mathcal{A}_n)$ is a Prüfer domain, which is strictly contained in $\text{Int}(\mathbb{Z})$ if $n > 1$.

A chain of Prüfer domains

In particular,

$$\mathbb{Z}[X] \subset \ldots \subset \mathrm{Int}_{\mathbb{Q}}(\mathcal{A}_n) \subset \mathrm{Int}_{\mathbb{Q}}(\mathcal{A}_{n-1}) \subset \ldots \subset \mathrm{Int}_{\mathbb{Q}}(\mathcal{A}_1) = \mathrm{Int}(\mathbb{Z})$$

Moreover,

$$\bigcap_{n \in \mathbb{N}} \mathrm{Int}_{\mathbb{Q}}(\mathcal{A}_n) = \mathrm{Int}_{\mathbb{Q}}(\overline{\mathbb{Z}}, \overline{\mathbb{Z}}) = \{f \in \mathbb{Q}[X] \mid f(\overline{\mathbb{Z}}) \subseteq \overline{\mathbb{Z}}\} = \mathbb{Z}[X]$$

Definition

Given $S \subseteq \overline{\mathbb{Z}}$, we say that $\mathrm{Int}_{\mathbb{Q}}(S, \overline{\mathbb{Z}})$ is nontrivial if $\mathbb{Z}[X] \subsetneq \mathrm{Int}_{\mathbb{Q}}(S, \overline{\mathbb{Z}})$.

Objective

We characterize those subsets $S \subset \overline{\mathbb{Z}}$ for which $\mathrm{Int}_{\mathbb{Q}}(S, \overline{\mathbb{Z}})$ is nontrivial.

Example: If S has bounded degree (i.e., $S \subseteq \mathcal{A}_n$ for some $n \in \mathbb{N}$), then $\mathbb{Z}[X] \subsetneq \mathrm{Int}_{\mathbb{Q}}(\mathcal{A}_n) \subseteq \mathrm{Int}_{\mathbb{Q}}(S, \overline{\mathbb{Z}})$.

Examples of unbounded degree

Trivial example

Let $S = \{\zeta_n\}_{n\in\mathbb{N}} \subset \overline{\mathbb{Z}}$ be the set of all primitive n-th roots of unity. If $f \in \text{Int}_{\mathbb{Q}}(S, \overline{\mathbb{Z}})$ has degree d, say $f(X) = a_0 + a_1X + \ldots + a_dX^d$, choose $n \in \mathbb{N}$ such that $\varphi(n) > d$. Since $O_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$, we have

$$f(\zeta_n) = a_0 + a_1\zeta_n + \ldots + a_d\zeta_n^d \in \overline{\mathbb{Z}} \cap \mathbb{Q}(\zeta_n) = \mathbb{Z}[\zeta_n]$$

which forces $a_0, \ldots, a_d \in \mathbb{Z}$. Thus, $\text{Int}_{\mathbb{Q}}(S, \overline{\mathbb{Z}}) = \mathbb{Z}[X]$.

Examples of unbounded degree

Trivial example

Let $S = \{\zeta_n\}_{n\in\mathbb{N}} \subset \overline{\mathbb{Z}}$ be the set of all primitive n-th roots of unity. If $f \in \mathrm{Int}_{\mathbb{Q}}(S, \overline{\mathbb{Z}})$ has degree d, say $f(X) = a_0 + a_1X + \ldots + a_dX^d$, choose $n \in \mathbb{N}$ such that $\varphi(n) > d$. Since $O_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$, we have

$$f(\zeta_n) = a_0 + a_1\zeta_n + \ldots + a_d\zeta_n^d \in \overline{\mathbb{Z}} \cap \mathbb{Q}(\zeta_n) = \mathbb{Z}[\zeta_n]$$

which forces $a_0, \ldots, a_d \in \mathbb{Z}$. Thus, $\mathrm{Int}_{\mathbb{Q}}(S, \overline{\mathbb{Z}}) = \mathbb{Z}[X]$.

Nontrivial example

Fix a prime p. For each $k \in \mathbb{N}$ let $e_k = 1 - \frac{1}{2^k}$, and take $S = \{p^{e_k}\}_{k\in\mathbb{N}} = \{p^{1/2}, p^{3/4}, p^{7/8}, \ldots\}$. Then, S has unbounded degree, but $f(X) = X^2/p \in \mathrm{Int}_{\mathbb{Q}}(S, \overline{\mathbb{Z}})$ because $f(p^{e_k}) = p^{e_{k-1}}$ for all $k \geq 2$.

Over a valuation domain

Let V be a valuation domain with $K = QF(V)$, maximal ideal M, associated valuation v and value group Γ_v.

Definition (Chabert, 2010)

A sequence $E = \{s_i\}_{i \in \Lambda} \subset K$ is said to be

1. *pseudo-divergent* if $v(s_i - s_j) > v(s_j - s_k)$ for all $i < j < k \in \Lambda$;
2. *pseudo-stationary* if $v(s_i - s_j) = v(s_k - s_\ell)$ for all $i \neq j, k \neq \ell \in \Lambda$.

We define the *gauge* of E as the following sequence $\{\delta_i\}_{i \in \Lambda}$ of Γ_v:

1. if E is pseudo-divergent, for each $i \in \Lambda$ we set $\delta_i = v(s_i - s_j)$, $j < i$;
2. if E is pseudo-stationary, we let $\delta_i = v(s_i - s_j) = \delta$ for any $i, j \in \Lambda$, $i \neq j$.

The *breadth ideal* $\mathrm{Br}(E)$ is defined as:

1. If E is pseudo-divergent, then $\mathrm{Br}(E) = \{x \in K \mid v(x) > \delta_i \text{ for some } i \in \Lambda\}$;
2. If E is pseudo-stationary, then $\mathrm{Br}(E) = \{x \in K \mid v(x) \geq \delta\}$.

For a subset S of V, we consider:

$$\mathrm{Int}_K(S,V)=\{f\in K[X]\mid f(S)\subseteq V\}$$

Theorem

Let $S\subseteq V$. The following are equivalent:

1. $\mathrm{Int}_K(S,V)$ *is nontrivial (i.e., $V[X]\subsetneq \mathrm{Int}_K(S,V)$).*
2. *There exist a finite subset $T\subseteq S$ and $\delta\in\Gamma_v\cup\{\infty\}$, $\delta>0$ such that, for each $s\in S$, there exists $t\in T$ with $v(s-t)\geq\delta$.*
3. *There exists $b\in M$ such that S/bV is finite.*
4. *S contains neither a pseudo-divergent sequence E with $\mathrm{Br}(E)=M$, nor a pseudo-stationary sequence E with $\mathrm{Br}(E)=V$.*

Idea: Given $f\in\mathrm{Int}_K(S,V)\setminus V[X]$, we have

$$f(X)=\frac{g(X)}{c}$$

for some (monic) $g\in V[X]$ and $c\in M, c\neq 0$. The values $\{v(g(s)),s\in S\}$ cannot be too small ($\not\searrow 0$; no pdv) and there can be only finitely many elements in S/M (no pst).

From local to global

We let $\overline{\mathbb{Z}_p}$ be the absolute integral closure of the ring $\mathbb{Z}_p$ of p-adic integers.

Definition

Let $p \in \mathbb{P}$ and let $S \subseteq \overline{\mathbb{Z}_{(p)}}$. Let $\mathcal{P}(S) \subseteq \mathbb{Z}_{(p)}[X]$ be set of minimal polynomials over $\mathbb{Q}$ of all the elements of S. We define $\Sigma_p(S)$ to be the set of roots in $\overline{\mathbb{Z}_p}$ of the polynomials in $\mathcal{P}(S)$.

Theorem

Let $S \subseteq \overline{\mathbb{Z}}$. The following are equivalent.

1. $\mathrm{Int}_{\mathbb{Q}}(S, \overline{\mathbb{Z}})$ *is nontrivial.*
2. *There exists $p \in \mathbb{P}$ such that* $\mathrm{Int}_{\mathbb{Q}}(S, \overline{\mathbb{Z}_{(p)}})$ *is nontrivial.*
3. *There exists $p \in \mathbb{P}$ such that* $\mathrm{Int}_{\mathbb{Q}_p}(\Sigma_p(S), \overline{\mathbb{Z}_p})$ *is nontrivial.*
4. *There exists $p \in \mathbb{P}$ such that* $\mathrm{Int}_{\overline{\mathbb{Q}_p}}(\Sigma_p(S), \overline{\mathbb{Z}_p})$ *is nontrivial.*

Unbounded Sets with Trivial $\mathrm{Int}_{\mathbb{Q}}$-Ring

For each prime $p \in \mathbb{P}$, we fix an extension u_p of v_p to $\overline{\mathbb{Q}}$.

Example 1

Let $p \in \mathbb{P}$ and take $S = \{\zeta_{p^k}\}_{k \in \mathbb{N}}$. Then, $\mathrm{Int}_{\mathbb{Q}}(S, \overline{\mathbb{Z}})$ is trivial: S is a pseudo-divergent sequence with respect to u_p with $\mathrm{Br}(S) = M_{u_p}$ and it is pseudo-stationary with respect to u_q with $\mathrm{Br}(S) = U_q$ for every prime $q \neq p$.

Example 2

Let $S = \{\zeta_p\}_{p \in \mathbb{P}}$. Then $\mathrm{Int}_{\mathbb{Q}}(S, \overline{\mathbb{Z}})$ is trivial: S is pseudo-stationary with $\mathrm{Br}(S) = U_p$ with respect to every prime.

Example 3

Let $\mathbb{P} = \{p_1, p_2, \ldots\}$. Define $s_k = (p_1 \cdots p_k)^{1/k}$ for each $k \in \mathbb{N}$. For every p, $\{u_p(s_k)\}_{k \in \mathbb{N}}$ eventually strictly decreases to 0. Hence, S is eventually pseudo-divergent with respect to every prime p with $\mathrm{Br}(E) = M_{u_p}$.

Unbounded Sets with Nontrivial $\text{Int}_{\mathbb{Q}}$-Ring

Lemma

Let $S \subseteq \overline{\mathbb{Z}}$ and $p \in \mathbb{P}$. Assume there exist $e_0, f_0 \in \mathbb{N}$ such that for all $s \in S$ and every prime P_s of $O_{\mathbb{Q}(s)}$ above p, we have $e(P_s|p) \leq e_0$ and $f(P_s|p) \leq f_0$. Then, $\text{Int}_{\mathbb{Q}}(S, \overline{\mathbb{Z}_{(p)}})$ is nontrivial.

Remarks: The assumption does not imply that S has bounded degree! Moreover, neither one of the two conditions is necessary.

Example

Let $\mathbb{Q}^{(2)} = \mathbb{Q}(\mathcal{A}_2)$ be the compositum in $\overline{\mathbb{Q}}$ of all quadratic number fields. It is known that there exists $N \in \mathbb{N}$ such that if u_p is a valuation of $\mathbb{Q}^{(2)}$ extending some v_p, $p \in \mathbb{P}$, then $e(u_p|v_p) \leq N$ and $f(u_p|v_p) \leq N$. If $\mathbb{P} = \{p_k\}_{k \in \mathbb{N}}$, for each $k \in \mathbb{N}$, let $s_k = \sum_{i=1}^{k} \sqrt{p_i}$, and take $S = \{s_k\}_{k \in \mathbb{N}}$. Then for each k, $[\mathbb{Q}(s_k) : \mathbb{Q}] = 2^k$. By the Lemma, $\text{Int}_{\mathbb{Q}}(S, \overline{\mathbb{Z}})$ is nontrivial.

Fix $p \in \mathbb{P}$. Let K be an infinite algebraic extension of $\mathbb{Q}$ such that the integral closure D of $\mathbb{Z}_{(p)}$ in K is an almost Dedekind domain with finite residue fields satisfying either one of these 2 conditions:

i) $\{f(P \mid p) \mid p \in P \subset D\}$ is unbounded (Gilmer, 1990).

ii) $\{e(P \mid p) \mid p \in P \subset D\}$ is unbounded (Chabert, 1993).

Then $\text{Int}_{\mathbb{Q}}(D) = \mathbb{Z}_{(p)}[X]$. Note that there are neither pseudo-divergent sequences nor pseudo-stationary sequences in D with respect to any extension u_p of v_p.

However, if we consider all the embeddings in $\overline{\mathbb{Q}_p}$ of D at the same time:

$$\mathcal{D}_p = \bigcup_{p \in P \subset D} \tau_P(D_P) \subset \overline{\mathbb{Z}_p}$$

where τ_P is the $\mathbb{Q}$-embedding of K into $\overline{\mathbb{Q}_p}$, then

- $\text{Int}_{\mathbb{Q}}(D) = \text{Int}_{\mathbb{Q}}(\mathcal{D}_p, \overline{\mathbb{Z}_p})$
- $\mathcal{D}_p$ contains either a pseudo-stationary sequence E with $\text{Br}(E) = \overline{\mathbb{Z}_p}$ (i) or a pseudo-divergent sequence E with $\text{Br}(E) = \overline{M_p}$ (ii).

Case of rings (double boundedness is necessary)

Theorem

Let D be an integrally closed subring of $\overline{\mathbb{Z}_{(p)}}$ containing $\mathbb{Z}_{(p)}$. Then the following conditions are equivalent:

1. *the sets $F_p = \{f(P|p) \mid P \subset D\}$ and $E_p = \{e(P|p) \mid P \subset D\}$ are bounded.*
2. $\mathrm{Int}_{\mathbb{Q}}(D)$ *is nontrivial.*
3. $\mathrm{Int}_{\mathbb{Q}}(D)$ *is Prüfer.*

Corollary

Let $D \subseteq \overline{\mathbb{Z}}$ be an integrally closed subring. Then the following holds:

- $\mathrm{Int}_{\mathbb{Q}}(D)$ *is non-trivial if and only if there exists some $p \in \mathbb{P}$ such that E_p and F_p are bounded.*
- $\mathrm{Int}_{\mathbb{Q}}(D)$ *is Prüfer if and only if for each $p \in \mathbb{P}$ the sets E_p and F_p are bounded.*

Addendum 1: Another chain of Prüfer domains

For $n \in \mathbb{N}$, let $\mathbb{Q}^{(n)} = \mathbb{Q}(\mathcal{A}_n)$ be the compositum in $\overline{\mathbb{Q}}$ of all number fields of degree $\leq n$ and let $O_{\mathbb{Q}^{(n)}}$ be its ring of integers. It is known that $O_{\mathbb{Q}^{(n)}}$ is a non-Noetherian almost Dedekind domain with finite residue fields (that is, locally it is a DVR with finite residue fields).

Theorem

For each $n \in \mathbb{N}$, $\mathrm{Int}_{\mathbb{Q}}(O_{\mathbb{Q}^{(n)}})$ is a Prüfer domain.

Clearly, $\mathrm{Int}_{\mathbb{Q}}(O_{\mathbb{Q}^{(n)}}) \subseteq \mathrm{Int}_{\mathbb{Q}}(\mathcal{A}_n)$ and we don't know if the containment is strict. Moreover,

$$\ldots \subseteq \mathrm{Int}_{\mathbb{Q}}(O_{\mathbb{Q}^{(n+1)}}) \subseteq \mathrm{Int}_{\mathbb{Q}}(O_{\mathbb{Q}^{(n)}}) \subseteq \ldots \subseteq \mathrm{Int}_{\mathbb{Q}}(O_{\mathbb{Q}^{(1)}}) = \mathrm{Int}(\mathbb{Z}).$$

Addendum 2: Polynomial closure in $\overline{\mathbb{Z}}$

Definition

For $S \subseteq \overline{\mathbb{Z}}$, we consider the *polynomial closure* of S as the largest subset S' of $\overline{\mathbb{Z}}$ for which $\mathrm{Int}_{\mathbb{Q}}(S, \overline{\mathbb{Z}}) = \mathrm{Int}_{\mathbb{Q}}(S', \overline{\mathbb{Z}})$. We say that S is *polynomially closed in* $\overline{\mathbb{Z}}$ if $S' = S$.

Theorem

$\mathbb{Z}$ is polynomially closed in $\overline{\mathbb{Z}}$.

Namely, if $\alpha \in \overline{\mathbb{Z}}$ is such that $f(\alpha) \in \overline{\mathbb{Z}}$ for each $f \in \mathrm{Int}(\mathbb{Z})$, then $\alpha \in \mathbb{Z}$.

We conjecture that for each $n \in \mathbb{N}$, $\mathcal{A}_n = \{\alpha \in \overline{\mathbb{Z}} \mid [\mathbb{Q}(\alpha) : \mathbb{Q}] \leq n\}$ is polynomially closed in $\overline{\mathbb{Z}}$.

Thank you!

- J.-L. Chabert. *On the polynomial closure in a valued field*, J. Number Theory 130 (2010), no. 2, 458-468.
- A. K. Loper, N. J. Werner, *Generalized rings of integer-valued polynomials*. J. Number Theory 132 (2012), no. 11, 2481-2490.
- G. P., N. J. Werner, *Nontriviality of rings of integral-valued polynomials*, preprint, 2024, https://arxiv.org/abs/2407.09351.