



ISSN: 2820-7114

Moroccan Journal of Algebra and Geometry with Applications

Supported by Sidi Mohamed Ben Abdellah University, Fez, Morocco

Volume 4 (2025), pp 1-291

Supported by:

Sidi Mohamed Ben Abdellah University, Fez, Morocco

جامعة سيدي محمد بن عبد الله بفاس
ⵜⴰⵎⴰⵎⴰⵔⵜ ⴰⵎⴰⵔⴰⵏ ⵏ ⵙⵉⴷⵉ ⵙⵉⴷⵉ ⵙⵉⴷⵉ ⵙⵉⴷⵉ ⵙⵉⴷⵉ
UNIVERSITÉ SIDI MOHAMED BEN ABDELLAH DE FES



Editor-in-Chief : Najib Mahdou
Managing Editors : Omar Ait Zemzami
Adam Anebri
Mohammed Tamekkante
Technical Editor : El Houssaine Oubouhou

Editorial Board :

Mohamed Tahar Kadaoui Abbassi (Morocco)	Mohammed Issoual (Morocco)
Toshiaki Adachi (Japan)	Ali Jaballah (United Arab Emirates)
Mohammad Ashraf (India)	El Amin Kaidi (Spain)
Abdelmalek Azizi (Morocco)	Hwankoo Kim (South Korea)
Ayman Badawi (United Arab Emirates)	Suat Koç (Turkey)
Mashhour Ibrahim Bani Ata (Kuwait)	Christian Lomp (Portugal)
Abdelmejid Bayad (France)	Marco Castrillon Lopez (Spain)
Samir Bouchiba (Morocco)	Najib Mahdou (Morocco)
Giovanni Calvaruso (Italy)	Abdenacer Makhoulouf (France)
Luisa Carini (Italy)	Lixin Mao (China)
Paula A. A. B. Carvalho (Portugal)	Hidetoshi Marubayashi (Japan)
Ece Yetkin Çelikel (Turkey)	Abdeslam Mimouni (Saudi Arabia)
Jean-Luc Chabert (France)	Dijana Mosić (Serbia)
M. P. Chaudhary (India)	Ali Mouhib (Morocco)
Mohamed Mahmoud Chems-Eddin (Morocco)	Moutu Abdou Salam Moutui (Qatar)
Marco D'Anna (Italy)	Abderrahmane Nitaj (France)
Ahmad Yousefian Darani (Iran)	Lahcen Oukhtite (Morocco)
Vincenzo DE Filippis (Italy)	Manoj Kumar Patel (India)
Nanqing Ding (China)	Kulumani M. Rangaswamy (USA)
David E. Dobbs (USA)	Masahisa Sato (Japan)
Maciej Dunajski (United Kingdom)	Mohammad Hasan Shahid (India)
Laiachi El Kaoutit (Spain)	Bouchaïb Sodaigui (France)
Abdelhaq El Khalfi (Morocco)	Ali Taherifar (Iran)
El Hassan El Kinani (Morocco)	Mohammed Tamekkante (Morocco)
Bayram Ali Ersoy (Turkey)	Ünsal Tekir (Turkey)
Anna Fino (Italy)	Rachid Tribak (Morocco)
Carmelo Antonio Finocchiaro (Italy)	Gabriel Eduard Țîlcu (Romania)
Marco Fontana (Italy)	Mirjana Vuković (Bosnia and Herzegovina)
Sophie Frisch (Austria)	Siamak Yassemi (Iran)
Ahmed Hamed (Tunisia)	Mohamed Yousif (USA)
Dolors Herbera (Spain)	Hassane Zguitti (Morocco)
Sana Hizem (Tunisia)	

The Moroccan Journal of Algebra and Geometry with Applications publishes two issues per year composed of high-quality original research papers with significant contributions in the fields of algebra, geometry and related fields. It publishes also invited survey articles on hot topics, from distinguished mathematicians from across the world. All published research articles are subject to rigorous peer review, based on initial screening by editors, refereeing by independent expert referees, and consequent revision by article authors when required. The published article constitutes the final and definitive version of the work. All manuscripts submitted to the journal must be original contributions, and must not be under consideration for publication with another journal, nor have been previously published, in part or whole.

Abstracting and Indexing

- Scopus
- MathSciNet / Mathematical Reviews
- Zentralblatt MATH
- Google Scholar
- CompuMath Citation Index
- Index Mathematical

Author Guidelines / Submissions

Manuscript Submission :

Submission of a manuscript implies that

- the work described has not been published before;
- it is not under consideration for publication anywhere else;
- its publication has been approved by all co-authors, if any, as well as by the responsible authorities – tacitly or explicitly – at the institute where the work has been carried out.

Articles must be written in English or, exceptionally, in French and prepared in Latex at MJAGA format. The format can be found here (<https://ced.fst-usmba.ac.ma/p/mjaga/author-guidelines-submissions>). Articles may be submitted directly via email as a PDF-file to any of the Journal Editors.

The manuscript should contain :

- A concise and informative title.
- The name(s) of the author(s), affiliation(s) of the author(s), a clear indication and an active e-mail address of the corresponding author, and the 16-digit ORCID of the author(s), if available.
- An abstract of 150 to 250 words.
- 4 to 6 keywords which can be used for indexing purposes.
- Appropriate numbers of MSC codes.

Peer review :

The submission will be initially assessed by the editor for suitability for the journal. Papers deemed suitable are then typically sent to a minimum of one independent expert reviewer to assess the scientific quality of the paper. The Editor is responsible for the final decision regarding acceptance or rejection of articles. The Editor's decision is final.

After acceptance :

After the paper is accepted for publication, the corresponding author will be required to submit the LaTeX file. Final formatting matters will follow, and publication will then be immediate.

Publication Charges :

There are no submission fees, publication fees or page charges for this journal.

Contents :

On graded almost-Bézout rings

Fatima-Zahra Guissi and Najib Mahdou

Pages: 1-10

Some New Fixed point theorems for asymptotically nonexpansive type mappings in CAT(k) space

R. Keshavarz and H. Azadi Kenary

Pages: 11-27

On superzeta functions of the first kind on function fields

Kajtaz H. Bllaca, Jawher Khmiri, Kamel Mazhouda, and Bouchaïb Sodaïgui

Pages: 28-37

Rings in which every S-prime ideal is prime

Chahrazade Bakkari and Rachid Hachache

Pages: 38-45

Finite direct projective Covers and Envelopes

Sonal Gupta, Manoj Kumar Patel and Ashok Ji Gupta

Pages: 46-53

Weakly S-2-prime ideals of commutative rings

Sanem Yavuz, Bayram Ali Ersoy, Ünsal Tekir, and Ece Yetkin Çelikel

Pages: 54-61

Squares of Fibonacci-like Numbers

Kunle Adegoke and Tokunbo Omiyinka

Pages: 62-73

On the finiteness of some noncommutative Gröbner bases over finite fields

Yatma Diop and Laila Mesmoudi

Pages: 74-80

On 2-nil-clean commutative rings

Chahrazade Bakkari, Mohamed Es-Saidi, and Moutu Abdou Salam Moutui

Pages: 81-89

A New Public Key Encryption Scheme Based on the Cubic Pell Curve Using Encoding Functions

Abderrahmane Nitaj and Michel Seck

Pages: 90-108

Survey on Side-Channel Attacks on Code-Based Key Encapsulation Mechanism

Pierre-Louis Cayrel, Mohamed Fall, Laila Mesmoudi, and Cheikh Tiecoumba Gueye

Pages: 109-137

Contents :

On nonnil-u-S-coherent rings

Najib Mahdou and El Houssaine Oubouhou

Pages: 138-151

On graded 1-absorbing primary ideals and graded weakly 1-absorbing primary ideals

Mohammed Issoual and Emel Aslankarayigit Ugurlu

Pages: 152-167

On $\sum$ -nil-good rings

Moutu Abdou Salam Moutui

Pages: 168-175

On ϕ -Gorenstein homological dimensions

Younes El Haddaoui, Hwankoo Kim, and Najib Mahdou

Pages: 176-197

New Eisenstein series identities for the Ramanujan-Göllnitz-Gordon continued fraction and combinatorial partition identities

Mahendra Mal Chaudhary and Ananda Rathna Kumara Vanitha

Pages: 198-206

Pairs of rings sharing their units

Gabriel Picavet and Martine Picavet-L'Hermitte

Pages: 207-238

On rings over which every flat module is finitely projective

Abdelhaq El Khalfi, Oussama Aymane Es-Safi, and Moutu Abdou Salam Moutui

Pages: 239-247

Weakly J -filters property in lattices

Shahabaddin Ebrahimi Atani

Pages: 248-258

On quasi $\$n\$$ -absorbing submodules

Malik Tusif Ahmed, Mohammed Issoual, and Mohammed Tamekkante

Pages: 259-267

On the lattice of basic z° -ideals

Ali Taherifar

Pages: 268-274

Evolution algebras satisfying a train identity of degree 2 and exponent $m > 3$

Savadogo Souleymane, Tenkodogo Joseph, and Conseibo André

Pages: 275-291



Celebrating the 80th birthday of Professor David E. Dobbs - A Pioneering Mathematician

By Salah-Eddine Kabbaj

Department of Mathematics

College of Computing and Mathematics

King Fahd University of Petroleum & Minerals

Dhahran 31261, Saudi Arabia

kabbaj@kfupm.edu.sa

We are honored to showcase Professor David E. Dobbs on the front page of Volume 4 of the Moroccan Journal of Algebra and Geometry with Applications (MJAGA), celebrating his outstanding contributions to the field of mathematics.

A Prolific Mathematician:

Professor Dobbs stands as one of the most prolific mathematicians in the United States, having left an indelible mark on the world of algebra. His dedication to advancing mathematical knowledge is evident in his remarkable portfolio, which includes 14 impactful papers published in MJAGA.

A Journey of Academic Excellence:

Born in Winnipeg, Professor Dobbs's academic journey began at St. John's (technical) High School. His pursuit of knowledge led him to the University of Manitoba, where he completed honors programs in mathematics, philosophy, and statistics for his B.A. He further earned his M.A. and Ph.D. at the University of Manitoba and Cornell University in 1969, respectively. Following a postdoctoral year at UCLA, he continued his illustrious career at Rutgers and the University of Tennessee, where he has held the distinguished position of full Professor since 1980, specializing in algebra.

A Legacy of Research:

Professor Dobbs's research legacy spans over five decades, with his earliest indexed publication dating back to 1969. His prolific output comprises a total of 351 publications and an impressive citation count over 2,000. His contributions cover various domains, including Commutative algebra, Field theory and polynomials, Real functions, Linear and multilinear algebra; matrix theory, and Group theory and generalizations.



**Moroccan Journal of Algebra
and Geometry with Applications**

Supported by Sidi Mohamed Ben Abdellah University, Fez, Morocco

ISSN: 2820-7114

Collaborative Endeavors:

Professor Dobbs has engaged in fruitful collaborations with esteemed coauthors, including Fontana, Marco; Shapiro, Jay Allen; Anderson, David F.; Picavet, Gabriel; Picavet-L'Hermitte, Martine; Mullins, Bernadette; Papick, Ira J.; Ayache, Ahmed; Anderson, Daniel D.; Barucci, Valentina; Lucas, Thomas G.; Kabbaj, Salah-Eddine; Coykendall, Jim; Houston, Evan G.; Jr., Zafrullah, Muhammad; Badawi, Ayman; Mahdou, Najib; Jarboui, Noômen; Hetzel, Andrew J.; Cahen, Paul-Jean; and many others.

Published Works and Achievements:

Highlighting his impactful contributions, Professor Dobbs coauthored two research volumes with Marcel Dekker, Inc., New York: 'Zero-dimensional commutative rings' with David F. Anderson in 1995 and 'Advances in commutative ring theory' with Marco Fontana and Salah Kabbaj in 1999. Professor Dobbs's work has found a home in numerous prestigious journals, including Communications in Algebra, Houston Journal of Mathematics, Palestine Journal of Mathematics, Canadian Mathematical Bulletin, Journal of Algebra and its Applications, Bulletin of the Australian Mathematical Society, Archiv der Mathematik, Proceedings of the American Mathematical Society, Canadian Journal of Mathematics, Journal of Pure and Applied Algebra, The Rocky Mountain Journal of Mathematics, Journal of Algebra, Pacific Journal of Mathematics, Tokyo Journal of Mathematics, and Semigroup Forum.

Continued Dedication:

Although Professor Dobbs has retired from teaching, he remains an active force in the realm of mathematics. As Professor Emeritus at the Department of Mathematics, University of Tennessee, he continues to conduct research in Commutative Algebra, with applications to Number Theory and Numerical Semigroups, Geometry, and Mathematical Education.

We extend our heartfelt gratitude to Professor David E. Dobbs for his enduring commitment to advancing mathematical knowledge and congratulate him on a distinguished career that has enriched our journal and the broader mathematical community.



**Moroccan Journal of Algebra
and Geometry with Applications**

Supported by Sidi Mohamed Ben Abdellah University, Fez, Morocco

ISSN: 2820-7114



ISSN: 2820-7114

Moroccan Journal of Algebra and Geometry with Applications

Supported by Sidi Mohamed Ben Abdellah University, Fez, Morocco

Volume 4, Issue 1 (2025), pp 1-10

Title :

On graded almost-Bézout rings

Author(s):

Fatima-Zahra Guissi and Najib Mahdou

On graded almost-Bézout rings

Fatima-Zahra Guissi¹ and Najib Mahdou²

¹ Department of Mathematics, Faculty of Science and Technology, Fez, Morocco.

e-mail: fatimazahra.guissi@usmba.ac.ma

² Department of Mathematics, Faculty of Science and Technology, Fez, Morocco.

e-mail: mahdou@hotmail.com

Communicated by Ünsal Tekir

(Received 14 May 2024, Revised 26 August 2024, Accepted 28 August 2024)

Abstract. Let $R = \bigoplus_{\alpha \in \Gamma} R_{\alpha}$ be a commutative ring graded by an arbitrary abelian group Γ . We say that R is graded almost-Bézout ring if for each $a, b \in h(R)$, there exists $n \geq 1$ and $x \in h(R)$ such that $(a^n, b^n) = (x)$. In this paper, we investigate the transfer of this property in different graded commutative ring extensions, namely, in graded trivial ring extensions $(A \ltimes E)$ and graded amalgamated algebras along an ideal $(A \bowtie^f J)$. Our aim is to provide examples of new classes of Γ -graded rings satisfying the above mentioned property.

Key Words: Graded almost Bézout ring, graded amalgamation of ring, gr-Bézout ring, graded trivial ring extension.

2020 MSC: 13A02, 13C13.

Dedicated to our Professor David E. Dobbs for his 80th Birthday.

1 Introduction

Throughout this paper, all rings are commutative with unity, Γ will denote an abelian group written additively with an identity element denoted by 0 and all the graded rings and modules are graded by Γ . The purpose of this paper is to study the possible transfer of the property of being a gr-AB ring to graded trivial ring extensions and graded amalgamated algebras along an ideal.

In [1], Anderson and Zaffrullah introduced and studied the notion almost Bézout domain (AB-domain for short). An integral domain R is an AB-domain if for $a, b \in R - \{0\}$ there is n such that (a^n, b^n) is principal. The notion of almost Bézout domains runs along lines somewhat similar to those of Bézout domains (i.e., every two generated, equivalently, every finitely generated, ideal is principal). In [3], Anderson, Knopp, and Lewin continued the study of almost Bézout domains, and after observing that each almost Bézout domain is nearly Bézout, they used the construction $K + XL[X]$ to disprove the converse. The same example shows that a Noetherian almost Bézout domain need not be an almost principal ideal domain (API-domain), even though each Noetherian Bézout domain is a principal ideal domain (PID). In [2], Anderson and Zaffrullah continued their study of almost Bézout domains and gave a new characterization of Cohen-Kaplansky domains. In [13], the generalization of the almost Bézout domains to arbitrary commutative rings (with zero-divisors) is considered as follows: R is called an almost Bézout ring (AB-ring for short) if, for any two elements a and b in R , there exists a positive integer n such that the ideal (a^n, b^n) is principal. In the setting of Γ -graded rings, Ahmed and Moh'D, in [5], introduced two graded types of Bézout modules. The first type is graded-Bézout modules (gr-Bézout modules for short) in which every finitely generated submodule with homogeneous generators is cyclic with a homogeneous generator. The second type is weakly graded-Bézout modules (weakly gr-Bézout modules for short) which satisfy the Bézout

property for the Bézout property for the graded submodules. They investigated the relationship among the three types of Bézout modules, the ordinary Bézout modules and the two graded types of Bézout modules. Notably, the graded Bézout ring is a gr-Bézout module over itself (see [5]).

Let A be a ring and E be an A -module. Then $A \rtimes E$, which is called the *trivial (ring) extension of A by E* , is the ring whose additive structure is that of the external direct sum $A \oplus E$ and whose multiplication is defined by $(a, e)(b, f) := (ab, af + be)$ for all $a, b \in A$ and all $e, f \in E$ (this construction is also known by other terms and by other forms of notation, such as the *idealization* $A(+E)$). Trivial ring extensions have been generalized and studied extensively in graded ring theory, often because of their usefulness in constructing new classes of graded rings satisfying various properties (see [4, 9, 12]). Let Γ be an abelian group, $A = \bigoplus_{\alpha \in \Gamma} A_\alpha$ be a Γ -graded ring and $E = \bigoplus_{\alpha \in \Gamma} E_\alpha$ be a Γ -graded A -module. Then $A \rtimes E$ is a Γ -graded ring with $(A \rtimes E)_\alpha = A_\alpha \oplus E_\alpha$ for every $\alpha \in \Gamma$ (cf. [4, Proposition 2]).

Let $A = \bigoplus_{\alpha \in \Gamma} A_\alpha$ and $B = \bigoplus_{\alpha \in \Gamma} B_\alpha$ be two commutative rings graded by an arbitrary commutative monoid Γ , J be a homogeneous ideal of B , and $f : A \rightarrow B$ be a graded ring homomorphism. Then $R := A \bowtie^f J$, which is called the *amalgamation of A with B along J with respect to f* (introduced and studied by D'Anna, Finocchiaro and Fontana in [6, 7]), is a graded ring $R = \bigoplus_{\alpha \in \Gamma} R_\alpha$ with $h(R) = \bigcup_{\alpha \in \Gamma} R_\alpha$, which is the set of all homogeneous elements of R , where for each $\alpha \in \Gamma$

$$R_\alpha = (A \bowtie^f J)_\alpha := \{(a_\alpha, f(a_\alpha) + j_\alpha) \mid a_\alpha \in A_\alpha, j_\alpha \in J_\alpha\}.$$

This construction, first introduced and studied in [10], allows us to meet the challenges posed by providing rich examples that enrich the current literature of graded ring theory. One of the key tools for studying $A \bowtie^f J$ is based on the fact that the graded amalgamation can be studied in the frame of the pullback constructions [11, Section 3]. Other classical constructions, such as the graded amalgamated duplication of a ring along an ideal denoted by $A \bowtie I$ and the graded trivial ring extension of A by E [4] ($A \rtimes E$), can be interpreted as a particular cases of the general graded amalgamation construction [10, Examples 3.3 & 3.4].

We can now specify the main purposes of this paper. More precisely, we start our investigation by studying the possible transfer of the gr-AB ring property to the graded trivial ring extension ($A \rtimes E$), combining the main transfert result (Theorem 2.1) and a well-known result on [13] we construct an example of a gr-AB ring which is not AB-ring (Example 2.4). Additionally, we present another special outcome through an example of gr-AB ring which is neither a gr-Bézout ring nor a gr-coherent ring (Examples 2.5 and 2.8). Subsequently, we turn our attention to explore how the graded amalgamation $A \bowtie^f J$ inherits the properties of being a gr-AB ring from the graded ring A for specific classes of homogeneous ideals J and graded homomorphisms f . Among other things, we show that if $J = 0$, then the graded amalgamation $A \bowtie^f J$ being a gr-AB ring is equivalent to A being a gr-AB ring, however the fact that J is nonzero necessitates additional conditions, such as A being a graded integral domain as per in Theorem 2.11, or a further requirements such as (A, M) being a gr-local ring with specific conditions on $f(M)J$ and $J \subseteq \text{gr-Nil}(B)$ (Proposition 2.15).

We pause to review some definitions and preliminary results on graded modules and rings, see for instance [14, 15]. Let Γ be a grading abelian group. By a *graded ring* R , we mean a ring graded by Γ , that is, a direct sum of subgroups R_α of R such that $R_\alpha R_\beta \subseteq R_{\alpha+\beta}$ for every $\alpha, \beta \in \Gamma$. The set $h(R) = \bigcup_{\alpha \in \Gamma} R_\alpha$ is called the set of homogeneous elements of R . An element $x \in R$ is called *homogeneous* if it belongs to one of the R_α , *homogeneous of degree α* if $x \in R_\alpha$. The element 0 is therefore homogeneous of all degrees; but if $x \neq 0$ is homogeneous, it belongs to only one of the R_α ; the index α such that $x \in R_\alpha$ is then called the *degree* of x and is sometimes denoted by $\deg(x)$. Every $y \in R$ may be written uniquely as a sum $\sum_\alpha y_\alpha$ of homogeneous elements with $y_\alpha \in R_\alpha$ and y_α is the *homogeneous component of degree α* of y . Clearly, R_0 is a subring of R (and in particular $1 \in R_0$).

By a *graded R -module* E , we mean an R -module graded by Γ , that is, a direct sum of subgroups E_α of E such that $R_\alpha E_\beta \subseteq E_{\alpha+\beta}$ for every $\alpha, \beta \in \Gamma$. Let R and R' be two graded rings. Then a ring

homomorphism $f : R \rightarrow R'$ is called graded if $f(R_\alpha) \subseteq R'_\alpha$ for all $\alpha \in \Gamma$. A graded ring isomorphism is a bijective graded ring homomorphism. Obviously $\text{Im}(f)$ is a graded subring of R' , $\text{Ker}(f)$ is a homogeneous ideal of R , and the bijection $R/\text{Ker}(f) \rightarrow \text{Im}(f)$ canonically associated with f is an isomorphism of graded rings.

Let I be an ideal of R . Then I is called a homogeneous ideal of R if one of the following equivalent conditions holds: (i) $I = \bigoplus_{\alpha \in \Gamma} I_\alpha$, where $I_\alpha = I \cap R_\alpha$ for all $\alpha \in \Gamma$ and (ii) $x = x_{\alpha_1} + x_{\alpha_2} + \cdots + x_{\alpha_n} \in I$ implies that $x_{\alpha_i} \in I$, where $x_{\alpha_i} \in R_{\alpha_i}$. Similarly, a submodule N of M is called a homogeneous submodule if and only if $N = \bigoplus_{\alpha \in \Gamma} N_\alpha$, where $N_\alpha = N \cap M_\alpha$ for all $\alpha \in \Gamma$ if and only if $m = m_{\alpha_1} + m_{\alpha_2} + \cdots + m_{\alpha_n} \in N$ implies that $m_{\alpha_i} \in N$, where $m_{\alpha_i} \in M_{\alpha_i}$. If I is a homogeneous ideal of a graded ring R , then R/I is a graded ring, where $(R/I)_\alpha := (R_\alpha + I)/I$. A homogeneous ideal P of R is called a prime homogeneous ideal (gr-prime) if P is a proper homogeneous ideal of R with the property that $a, b \in h(R)$ and $ab \in P$ implies either $a \in P$ or $b \in P$. A homogeneous ideal M of R is called a maximal homogeneous ideal (gr-maximal) if it is maximal among proper homogeneous ideals; equivalently, if every nonzero homogeneous element of R/M is invertible and it is not difficult to show that a maximal homogeneous ideal is prime homogeneous.

Let I be a proper homogeneous ideal of a graded ring R . Then the graded radical of I will be designated by $\text{Gr}(I) = \{x = \sum_{g \in \Gamma} x_g \in R : \text{for each } g \in \Gamma, \text{ there exists } n_g \in \mathbb{N} \text{ such that } x_g^{n_g} \in I\}$. Note that, if x is a homogeneous element, then $x \in \text{Gr}(I)$ if and only if $x^n \in I$ for some positive integer n (see [16]). It is shown in [16, Proposition 2.5] that $\text{Gr}(I)$ is the intersection of all prime homogeneous ideals of R containing I .

A graded ring is said to be graded-local (gr-local) if it has a unique maximal homogeneous (gr-maximal) ideal and a graded ring R is called a graded-field (gr-field) if every nonzero homogeneous element of R is invertible. Clearly every field is a graded field, however, the converse is not true in general, see [14, page 46]. Recall from [14] that a Γ -graded ring $R = \bigoplus_{g \in \Gamma} R_g$ is said to be a crossed product if R_g contain a unit for every $g \in \Gamma$ (i.e., $R_g \cap U(R) \neq \emptyset$ for each $g \in \Gamma$). Note that a Γ -crossed product $R = \bigoplus_{g \in \Gamma} R_g$ is a strongly graded ring, that is $R_{g+h} = R_g R_h$ for every $g, h \in \Gamma$.

We will be using the following definition (which agrees with the classical one if R is a graded integral domain). A graded R -module E is said to be a *torsion R -graded module* if, for each homogeneous $e \in E$, there exists $a \in R \setminus \{0\}$ such that $ae = 0$. We will also use the following standard definitions. A *regular homogeneous element* of a graded ring R is a non-zero-divisor homogeneous element; a graded R -module E is *gr-divisible* if, for each homogeneous $e \in E$ and each regular homogeneous element a of R there exists $f \in E$ such that $e = af$; a graded A -module E is a *torsion-free* (graded A -module) if whenever $a \in h(A)$ and $e \in E$ with $ae = 0$ implies that either $a = 0$ or $e = 0$. Denoted by H the multiplicative set of regular homogeneous elements of R . Then, by extending some definitions to the case where rings have zero-divisors, R_H , called the homogeneous total ring of quotients of R , is a Γ -graded ring, where $R_H = \bigoplus_{\alpha \in \Gamma} (R_H)_\alpha$ with

$$(R_H)_\alpha = \left\{ \frac{r}{s} \mid r \in R_\beta, s \text{ regular homogeneous in } R_\gamma \text{ and } \beta - \gamma = \alpha \right\}.$$

If R is a graded integral domain (an integral domain graded by Γ), then R_H is called the homogeneous quotient field of R . Obviously, every nonzero homogeneous element of R_H is invertible and $(R_H)_0$ is a field. For any Γ -graded ring R , we denote respectively by $h\text{-Z}(R)$, $h\text{-Reg}(R)$, $h\text{-Nil}(R)$, the set of all homogeneous zero-divisors of R , the set of regular homogeneous elements of R and the set of nilpotent homogeneous element of R .

The notion of gr-AB rings was recently introduced in [12] as follows:

Definition 1.1. Let $R = \bigoplus_{\alpha \in \Gamma} R_\alpha$ be a Γ -graded ring. Then R is said to be a graded almost Bézout ring (gr-AB ring) if for each $a, b \in h(R)$, there exist $n \geq 1$ and $x \in h(R)$ such that $(a^n, b^n) = (x)$.

2 Main results

Our first result studies the possible transfer of the gr-AB ring property between a graded ring A and a graded trivial ring extension $A \ltimes E$.

Theorem 2.1. Let A be a graded ring, E a graded A -module and $R := A \ltimes E$ be the graded trivial ring extension of A by E . Then, the following statements hold:

1. If R is a gr-AB ring, then so is A .
2. Suppose that A is a graded integral domain with $K := A_H$ its homogeneous quotient field, and E is a graded K -vector space. Then R is a gr-AB ring if and only if so is A .
3. Suppose that (A, M) is a gr-local ring and E is a graded A -module such that $ME = 0$. Then R is a gr-AB ring if and only if so is A .
4. Let $A \subseteq B$ be an extension of graded integral domains, and suppose that $\mathbb{Q} \subseteq B$. Further, assume that A is a crossed product. Then $R := A \ltimes B$ is a gr-AB ring if and only if A is a gr-AB ring and $A_H \subseteq B$.

The proof of this Theorem requires the following lemma, which can be viewed as a general indicator to check whether the graded trivial ring extension of graded integral domains is not gr-AB ring.

Lemma 2.2. Let $A \subseteq B$ be an extension of graded integral domains, and let $R := A \ltimes B$ be the graded trivial ring extension of A by B . If there exists a nonzero element $m \in A_0$ such that $n1_B \notin mB$ for each positive integer n , then R is not a gr-AB ring.

Proof. Deny, assume that R is a gr-AB ring. Let $0 \neq m \in A_0$ (along with the hypothesis that $n1_B \notin mB$ for each positive integer n), and consider the homogeneous elements $(m, 0)$ and $(m, 1)$ of R . Then, there exists a positive integer n and a homogeneous element $(a, b) \in R$ such that $R(m, 0)^n + R(m, 1)^n = R(a, b)$. Then there exists $(c_1, d_1), (c_2, d_2), (\alpha_1, \beta_1)$, and (α_2, β_2) in R such that

$$\left\{ \begin{array}{l} (m^n, 0) = (m, 0)^n = (c_1, d_1)(a, b) = (ac_1, bc_1 + ad_1) \\ (m^n, nm^{n-1}) = (m, 1)^n = (c_2, d_2)(a, b) = (ac_2, bc_2 + ad_2) \\ (a, b) = (m, 0)^n(\alpha_1, \beta_1) + (m, 1)^n(\alpha_2, \beta_2). \end{array} \right\}$$

Then we obtain the following equations:

- (1) $m^n = ac_1$;
- (2) $0 = bc_1 + ad_1$;
- (3) $m^n = ac_2$;
- (4) $nm^{n-1} = bc_2 + ad_2$;
- (5) $a = (\alpha_1 + \alpha_2)m^n$.

From the first and third equation, we obtain $ac_1 = ac_2$. Since $0 \neq m, a \neq 0$, and so $c_1 = c_2$. Set $c = c_1 = c_2$. Also from the fifth equation, we have $a = (\alpha_1 + \alpha_2)m^n = (\alpha_1 + \alpha_2)ac$. Then $(\alpha_1 + \alpha_2)c = 1$, and so c is a unit of A . Finally, from the second and fourth equation, we have $0 = bc + ad_1$ and $nm^{n-1} = bc + ad_2$. Thus $nm^{n-1} = a(d_2 - d_1) = c^{-1}m^n(d_2 - d_1)$. Hence $n = mc^{-1}(d_2 - d_1) \in mB$, a contradiction. It follows that $R = A \ltimes B$ is not a gr-AB ring. $\square$

Proof of Theorem 2.1

(1) This follows from [12, Theorem 4.28].

(2) Suppose that A is a graded integral domain with A_H its homogeneous quotient field, and E is a graded K -vector space. By (1), it is only required to prove that if A is a gr-AB ring, then R is a gr-AB

ring. Which means that if $\alpha := (a, e)$ and $\beta := (b, f)$ are homogeneous elements of R , then there exists a positive integer n and a homogeneous element $(x, y) \in R$ such that $R\alpha^n + R\beta^n = R(x, y)$. Then four cases are possible. The first case is when $a = 0$ and $b \neq 0$. Then $b^{-1}e \in E$. Thus

$$(a, e) = (0, e) = (b, f)(0, b^{-1}e) \subseteq R(b, f)$$

and so (b, f) divides (a, e) . Hence $R(a, e) + R(b, f) = R(b, f)$. Likewise, in the case where $a \neq 0$ and $b = 0$. We have $(b, f) = (0, f) = (a, e)(0, a^{-1}f)$. Thus (a, e) divides (b, f) ; and hence $R(a, e) + R(b, f) = R(a, e)$. In the case where $a = b = 0$, then

$$(a, e)^2 = (b, f)^2 = (0, 0) \text{ and so } R(a, e)^2 + R(b, f)^2 = R(0, 0).$$

In the remaining case, $a \neq 0$ and $b \neq 0$. Since A is a gr-AB ring, there exists a positive integer n and a homogeneous element x of A such that $(a^n, b^n)A = Aa^n + Ab^n = Ax = (x)$. So,

$$\begin{aligned} ((a, e)^n, (b, f)^n)R &= R(a, e)^n + R(b, f)^n \\ &= (A \ltimes E)(a^n, na^{n-1}e) + (A \ltimes E)(b^n, nb^{n-1}f) \\ &= Aa^n \ltimes E + Ab^n \ltimes E \\ &= (Aa^n + Ab^n) \ltimes E \\ &= Ax \ltimes E \\ &= Ax \ltimes xE = (x, 0)R. \end{aligned}$$

(3) Suppose that (A, M) is a gr-local ring and E is a graded A -module such that $ME = 0$. If R is a gr-AB ring, then by (1) A is a gr-AB ring. Conversely, suppose that A is a gr-AB ring, and let (a, b) and $(t, s) \in h(R)$. We may assume that (a, b) and (t, s) are nonunit elements of R and so $a, t \in M$. Since $ME = 0$, $(a, b)^2 = (a^2, 0)$ and $(t, s)^2 = (t^2, 0)$, and A is a gr-AB ring. Then there exists a positive integer n and a nonunit homogeneous element x of A such that $(a^{2n}, t^{2n})A = Aa^{2n} + At^{2n} = Ax = (x)$. Note that $x \in M$. Hence, we obtain

$$\begin{aligned} ((a, b)^{2n}, (t, s)^{2n})R &= R(a^2, 0)^n + R(t^2, 0)^n \\ &= Aa^{2n} \ltimes 0 + At^{2n} \ltimes 0 \\ &= (Aa^{2n} + At^{2n}) \ltimes 0 \\ &= Ax \ltimes xE = (x, 0)R. \end{aligned}$$

(4) Assume that $R = A \ltimes B$ is a gr-AB ring and $\mathbb{Q} \subseteq B$. Then A is a gr-AB ring by (1). Now, let a be a nonzero homogeneous element of A . Assume that $\deg(a) = h$. Since A is a crossed product ring, we can choose a unit homogeneous element $\alpha \in A_{-h}$. Note that αa is a homogeneous element of A with $\deg(\alpha a) = 0$. By Lemma 2.2, there is a positive integer n such that $n1_B \in \alpha aB$. Since $\mathbb{Q} \subseteq B$, $n^{-1} \in B$ and so $1 \in \alpha aB = aB$. Thus a is a unit of B and therefore $A_H \subseteq B$. The converse follows from (2). $\square$

Before stating the following corollary, we note that the graded trivial ring extension $R := A \ltimes E$ is a crossed product if and only if so is A . Define the support of A as $\text{sup}(A) = \{\gamma \in \Gamma \mid A_\gamma \neq 0\}$.

Corollary 2.3. *Let A be a graded integral domain containing the field of rational numbers. Then the following statements are equivalent:*

1. $A \ltimes A$ is a gr-AB ring and A is a crossed product ring.
2. A is a gr-field and $\text{sup}(A) = G$.

Proof. Assume that A is a crossed product ring and $A \ltimes A$ is a gr-AB ring. Then by Theorem 2.1(4) A is a gr-field. On the other hand, since A is a crossed product ring, for every $g \in G$, $A_g \cap U(A) \neq \emptyset$. Hence $A_g \neq \{0\}$ for each $g \in G$, and so $\sup(A) = G$. Conversely, if A is a gr-field and $\sup(A) = G$. Let $g \in G$, then there exist a nonzero element $x \in A_g$. Then x is unit and so for each $g \in G$, $A_g \cap U(A) \neq \emptyset$. This A is a crossed product. Consequently, by Theorem 2.1(4), $A \ltimes A$ is a gr-AB ring. $\square$

Combining Theorem 2.1 and [13] Corollary 3.3], we broaden our ability to construct straightforward examples of gr-AB ring which is not AB-ring.

Example 2.4. Let $A = \mathbb{Q}[X, X^{-1}]$ and $R := A \ltimes A$. Then R is gr-AB ring which is not AB-ring.

In the next example, first we show how to build a new family of non gr-coherent gr-AB rings that are not gr-Bézout rings. Recall from the introduction that a graded ring R is said to be a graded Bézout ring if every nonzero finitely generated graded ideal of R is gr-cyclic (i.e, with a homogeneous generator). While a Γ -graded ring R is said to be a weakly graded-Bézout (weakly gr-Bézout) if every finitely generated graded ideal is cyclic.

Example 2.5. Let A be a gr-Bézout domain which is not a gr-field, $K = A_H$, $E = K \oplus K$ and $R := A \ltimes E$ be the graded trivial ring extension of A by E . Then:

1. R is a gr-AB ring;
2. R is not a gr-Bézout ring;
3. R is not gr-coherent.

Proof. (1) By Theorem 2.1(2), R is a gr-AB ring since A is a gr-Bézout domain.

(2) Set the element $e = (1, 0)$ and $f = (0, 1)$ of E . Then the finitely generated homogeneous ideal of R , $R(0, e) + R(0, f)$ is not principal. Therefore R is not weakly gr-Bézout, and so not a gr-Bézout ring.

(3) Let e be a nonzero homogeneous element of E . Then it is easy to see that $(0 : (0, e)) = 0 \ltimes E$ is not finitely generated, since K is not finitely generated A -module, and therefore R is not gr-coherent. $\square$

Lemma 2.6. Let A be a graded ring, E a nonzero graded A -module, and $R := A \ltimes E$ is a gr-AB ring. Further, assume that A is a crossed product. Then for all $e \in h(E)$ and $a \in h\text{-Reg}(A)$, there exist $f \in E$ and a positive integer $n \geq 1$ such that $na^{n-1}e = a^n f$.

Proof. Now let a be a regular homogeneous element of A and $e \in h(E)$. Assume that $\deg(a) = h_1$ and $\deg(e) = h_2$. Since A is crossed product, we can choose a unit homogeneous element $x \in A_{h_2-h_1}$. Note that (xa, e) is a homogeneous element of R with $\deg(xa, e) = h_2$, and as R is a gr-AB ring, there is a positive integer n and a homogeneous element (c, d) of R such that $R(xa, 0)^n + R(xa, e)^n = R(c, d)$. Then there are $(\alpha_1, \beta_1), (\alpha_2, \beta_2), (c_1, d_1)$, and (c_2, d_2) in R such that:

$$\left\{ \begin{array}{l} (xa, 0)^n = (x^n a^n, 0) = (\alpha_1, \beta_1)(c, d) \\ (xa, e)^n = (x^n a^n, nx^{n-1} a^{n-1} e) = (\alpha_2, \beta_2)(c, d) \\ (c, d) = (c_1, d_1)(x^n a^n, 0) + (c_2, d_2)(x^n a^n, nx^{n-1} a^{n-1} e) \end{array} \right\}$$

Then we obtain the following equations:

- (1) $x^n a^n = \alpha_1 c$.
- (2) $x^n a^n = \alpha_2 c$.
- (3) $0 = \alpha_1 d + c\beta_1$.
- (4) $nx^{n-1} a^{n-1} e = \alpha_2 d + c\beta_2$.
- (5) $c = (c_1 + c_2)x^n a^n$.

As $x^n a^n = \alpha_1 c$, we get that c is a regular homogeneous element of A since a is regular. From the first and the second equation, we have $\alpha_1 = \alpha_2 = \alpha$. Finally, from the third, the fourth, and the fifth equation, we have $nx^{n-1}a^{n-1}e = c(\beta_2 - \beta_1) = x^n a^n (c_1 + c_2)(\beta_2 - \beta_1)$. Hence there exist $f \in E$ such that $na^{n-1}e = a^n f$ with $f = x(c_1 + c_2)(\beta_2 - \beta_1)$. $\square$

Proposition 2.7. *Let A be a graded integral domain and E a graded torsion-free A -module such that $\mathbb{Q} \cdot E \subseteq E$. Assume further that A is a crossed product. Then $R = A \ltimes E$ is a gr-AB ring if and only if A is a gr-AB domain and E is a graded divisible A -module.*

Proof. By Theorem [2.1](1) and [12] Theorem 4.28(2)], we need only to prove that if R is a gr-AB ring, then E is a graded divisible A -module; that is, if e is a nonzero homogeneous element of E and a is a nonzero homogeneous element of A , then $e \in aE$. Since R is a gr-AB ring and A is a crossed product, by Lemma [2.6], there is $f \in E$ and a positive integer $n \geq 1$ such that $na^{n-1}e = a^n f$. As E is a graded torsion-free A -module, we get $ne = af$. Therefore $e = an^{-1}f \in aE$ since $\mathbb{Q} \cdot E \subseteq E$. $\square$

Using Example [2.5] and [12] Theorem 4.28(2)], we are able to provide another example of non gr-Bézout gr-AB ring.

Example 2.8. Let A be a gr-Bézout domain, $K = A_H$ the homogeneous quotient field of A , and $F = K \oplus K$. Set $B = A \ltimes F$ and $E = K \ltimes F$. Then, $R = B \ltimes E$ is a gr-AB ring which is not a gr-Bézout ring.

Proof. By Example [2.5], B is a gr-AB ring which is not a gr-Bézout ring and so R is not gr-Bézout. We have $h - Z(B) = 0 \ltimes h(F) = h - \text{Nil}(B)$ and E is a graded divisible B -module. By [12] Theorem 4.28(2)], R is a gr-AB ring. $\square$

If (A, M) is a gr-local ring and E a graded A -module such that M is the only homogeneous prime ideal of A , then we obtain a new application in the following proposition.

Proposition 2.9. *Let (R, M) be a graded local ring, suppose that M is the only prime homogeneous ideal of R . Then R is a gr-AB ring.*

Proof. Let $a, b \in h(R)$, if a or b is unit, then $Ra + Rb = R$. In the case where a and b are nonunits in R , then both a and b are in M . Hence there exists a positive integer n such that $Ra^n + Rb^n = 0$. $\square$

Example 2.10. Let K be a gr-field and $E = K \oplus K$. Then $R := K \ltimes E$ is a gr-AB ring which is not gr-Bézout.

Now, we turn our attention to the transfer of the gr-AB ring property to graded amalgamation of rings $A \bowtie^f J$. It is easy to see that, if $J = 0$, then $A \bowtie^f J \cong A$, and so $A \bowtie^f J$ is a gr-AB ring if and only if so is A . Thus in the sequel, we assume that J is a nonzero proper homogeneous ideal of B .

Theorem 2.11. Let A and B be a pair of graded rings, where A is graded integral domain, $f : A \rightarrow B$ be a graded ring homomorphism and J be a regular homogeneous proper ideal of B . Then the following statements are equivalent:

1. $A \bowtie^f J$ is a gr-AB ring.
2. f is injective, $f(A) + J$ is a gr-AB ring and $f(A) \cap J = (0)$.
3. $f^{-1}(J) = 0$ and $f(A) + J$ is a gr-AB ring.

Before proving this theorem, we recall the following lemma which is a direct application of [10, Theorem 3.5(4)], using the fact that the gr-AB ring property is stable under factor graded ring and in view of the graded isomorphisms:

$$\frac{A \bowtie^f J}{\{0\} \times J} \cong A$$

and

$$\frac{A \bowtie^f J}{f^{-1}(J) \times \{0\}} \cong f(A) + J.$$

Lemma 2.12. *Let A and B be graded rings, $f : A \rightarrow B$ be a graded ring homomorphism, and J a homogeneous ideal of B . If $A \bowtie^f J$ is a gr-AB ring, then A and $f(A) + J$ are gr-AB rings.*

Proof of Theorem 2.11

(1) $\Rightarrow$ (2) Assume that $R := A \bowtie^f J$ is a gr-AB ring, and suppose that f is not injective. Let x be a homogeneous regular element of J and $0 \neq a = \sum_{i=0}^k a_{\alpha_i} \in \ker f$. Then there exists $i \in \{0, \dots, k\}$ such that $a_{\alpha_i} \neq 0$. Hence $(a_{\alpha_i}, 0) = (a_{\alpha_i}, f(a_{\alpha_i}))$ and $(0, x)$ are homogeneous element of $A \bowtie^f J$ for each $i, j \in \{0, \dots, k\}$ (zero is homogeneous of all degrees). Then there exists a positive integer n and $(r, f(r) + s) \in h(A \bowtie^f J)$ such that

$$(a_{\alpha_i}^n, 0)(A \bowtie^f J) + (0, x^n)(A \bowtie^f J) = (r, f(r) + s)(A \bowtie^f J).$$

Hence there exists $(u, f(u) + k), (v, f(v) + h), (\alpha, f(\alpha) + p)$ and $(\beta, f(\beta) + t)$ in R such that

$$\left\{ \begin{array}{l} (a_{\alpha_i}^n, 0) = (a_{\alpha_i}, 0)^n = (u, f(u) + k)(r, f(r) + s) \\ (0, x^n) = (0, x)^n = (v, f(v) + h)(r, f(r) + s) \\ (r, f(r) + s) = (a_{\alpha_j}^n, 0)(\alpha, f(\alpha) + p) + (0, x^n)(\beta, f(\beta) + t). \end{array} \right\}$$

Hence $vr = 0$ and $a_{\alpha_j}^n = ur$. Since A is a graded integral domain and $a_{\alpha_j} \neq 0, r \neq 0$. Thus $v = 0$ and so $f(v) = 0$. Therefore, $x^n = h(f(r) + s)$ and $f(r) + s = x^n(f(\beta) + t) = h(f(r) + s)(f(\beta) + t)$. As x is a regular element of B , then $f(r) + s$ is regular. Hence $1 = h(f(\beta) + t) \in J$, which is a contradiction. Therefore, it follows that f is injective. By Lemma 2.12, $f(A) + J$ is a gr-AB ring. It remains to prove that $f(A) \cap J = (0)$. Deny, let $0 \neq f(a) \in J$ for some $a = \sum_{i=0}^n a_{\alpha_i}$. Then there exists $i \in \{0, \dots, n\}$ such that $0 \neq f(a_{\alpha_i}) \in J$, then it is straightforward to see that $(a_{\alpha_i}, 0), (0, f(a_{\alpha_i})) \in h(A \bowtie^f J)$ for each $i \in \{0, \dots, n\}$. Since $A \bowtie^f J$ is a gr-AB ring, there exists a positive integer n and $(r, f(r) + s) \in h(A \bowtie^f J)$ such that

$$(a_{\alpha_i}, 0)^n (A \bowtie^f J) + (0, f(a_{\alpha_i}))^n (A \bowtie^f J) = (r, f(r) + s)(A \bowtie^f J).$$

By similar reasoning as above, we get that $J = B$, which is a contradiction since J is a proper homogeneous ideal of B . Hence $f(A) \cap J = (0)$, as desired.

(2) $\Rightarrow$ (3) if f is injective and $f(A) \cap J = (0)$, then $f^{-1}(J) = 0$.

(3) $\Rightarrow$ (1) If $f^{-1}(J) = 0$, then $A \bowtie^f J \simeq f(A) + J$ is a ring graded isomorphism and the conclusion is straightforward. $\square$

Recall from [10], that in the case where $B = A$, $I = \bigoplus_{\alpha \in \Gamma} I_\alpha$ is a homogeneous ideal of A and $f = id_A$ the identity map of A . Then $A \bowtie I$ the graded (amalgamated) duplication of A along I is a special graded amalgamation given by $A \bowtie I = \bigoplus_{\alpha \in G} (A \bowtie I)_\alpha$, where for each $\alpha \in G$:

$$(A \bowtie I)_\alpha := (A \bowtie^{id_A} I)_\alpha = \{(a_\alpha, a_\alpha + i_\alpha) \mid a_\alpha \in A_\alpha, i_\alpha \in I_\alpha\}.$$

The following corollary is an immediate result of Theorem 2.14, which examines the case of the graded amalgamated duplication.

Corollary 2.13. *Let A be a graded integral domain and I a nonzero proper homogeneous ideal of A . Then graded amalgamation duplication $A \bowtie I$ is never gr-AB ring.*

The following proposition provide a more general concept of transfer for the gr-AB ring property to graded amalgamation of rings.

Proposition 2.14. *Let A and B be a pair of graded rings, $f : A \longrightarrow B$ be a graded ring homomorphism, and J be a regular homogeneous proper ideal of B . If $R = A \bowtie^f J$ is a gr-AB ring, then $h(f^{-1}(J)) \subseteq h - Z(A)$.*

Proof. Deny, if we assume that $f^{-1}(J)$ contains a homogeneous regular element e and let j be a homogeneous regular element of J . Then, there is a positive integer n and $(r, f(r) + k) \in h(R)$ such that $R(e, 0)^n + R(0, j)^n = R(r, f(r) + k)$. Therefore, we have

$$\left\{ \begin{array}{l} (e, 0)^n = (e^n, 0) = (\alpha_1, f(\alpha_1) + k_1)(r, f(r) + k) \\ (0, j)^n = (0, j^n) = (\alpha_2, f(\alpha_2) + k_2)(r, f(r) + k) \\ (r, f(r) + k) = (c_1, f(c_1) + d_1)(e^n, 0) + (c_2, f(c_2) + d_2)(0, j^n) \end{array} \right\}$$

for some $(\alpha_1, f(\alpha_1) + k_1), (\alpha_2, f(\alpha_2) + k_2), (c_1, f(c_1) + d_1)$ and $(c_2, f(c_2) + d_2)$ in R . Then, we obtain the following equations:

- (1) $e^n = \alpha_1 r$.
- (2) $\alpha_2 r = 0$.
- (3) $j^n = (f(\alpha_2) + k_2)(f(r) + k)$.
- (4) $f(r) + k = (f(c_2) + d_2)j^n$.

From the first equation we get that r is a homogeneous regular element of A since e is regular and so $\alpha_2 = 0$ by the second equation. Also, $f(r) + k$ is a homogeneous regular element of B , since j is regular. Hence, from the third and the fourth equation, we obtain $f(r) + k = k_2(f(c_2) + d_2)(f(r) + k)$. Therefore, $1 = k_2(f(c_2) + d_2) \in J$, a contradiction. $\square$

Recall, from [16], that $\text{gr-Nil}(R) = \text{Gr}(0)$ is the set of all $x = \sum_{j=0}^k x_{\alpha_j} \in R$ such that x_{α_j} is a nilpotent element of R for each $i \in \{0, \dots, k\}$. We then highlight another context in which it is possible to determine if a graded amalgamated algebra along an ideal is a gr AB-ring.

Proposition 2.15. *Let A and B be a pair of graded rings and $f : A \longrightarrow B$ be a graded ring homomorphism. Suppose that A is a gr-local ring with maximal homogeneous ideal M , and J is a homogeneous proper ideal of B such that $f(M)J = 0$ and $J \subseteq \text{gr-Nil}(B)$. Set $R := A \bowtie^f J$. Then R is a gr-AB ring if and only if A is a gr-AB ring.*

Proof. Assume that R is a gr-AB ring. By Lemma 2.12, A is a gr-AB ring. Conversely, let $\alpha = (a, f(a) + i)$ and $\beta = (b, f(b) + j)$ be two homogeneous elements of R . Without loss of generality, we may assume that $a, b \in M$. Since $i, j \in J$, there are positives integers p and m such that $i^p = 0$ and $j^m = 0$. As A is a gr-AB ring, there exists a positive integer n and $c \in h(A)$ such that $Aa^{npm} + Ab^{npm} = Ac$. By using the fact that $f(M)J = 0$, we conclude easily that $Ra^{npm} + Rb^{npm} = R(a, f(a))^{npm} + R(b, f(b))^{npm} = R(c, f(c))$. Therefore R is a gr-AB ring. $\square$

Note that in the case where the A is a graded integral domain and I is a proper homogeneous ideal of A , then the graded amalgamation duplication is gr-AB ring if and only if so is A and $I = 0$ (Corollary 2.13). Besides the context of integral domains, the following example shows the faillure of this characterization.

Example 2.16. Let $R = \mathbb{Q}[X, X^{-1}] \bowtie \mathbb{Q}[X, X^{-1}]$. Then R is a gr-local ring with a homogeneous maximal ideal $M = 0 \bowtie \mathbb{Q}[X, X^{-1}] = \text{gr-Nil}(R)$. Using Proposition 2.15 and Example 2.4, we conclude that the graded duplication $R \bowtie M$ is a gr-AB ring, even if $M \neq 0$.

References

- [1] D. D. Anderson and M. Zafrullah, Almost Bezout domain, *J. Algebra*, 142(2) (1991), 285–309.
- [2] D. D. Anderson, K. R. Knopp and R. L. Lewin, *Almost Bezout domains II.*, *J. Algebra*, 167(3) (1994), 547–556.
- [3] D. D. Anderson and M. Zafrullah, *Almost Bezout domains III.*, *Bull. Math. Soc. Sci. Math. Roumanie (N.S.)*, 51(1) (2008), 3–9.
- [4] A. Assarrar, N. Mahdou, Ü. Tekir and S. Koç, *On graded coherent-like properties in trivial ring extensions*, *Boll. Unione Mat. Ital.*, (2022), 15 (2022), 437–449.
- [5] M. Ahmed and F. Moh'D, *Group graded types of Bezout modules*, *Commun. Korean Math. Soc.*, 32(3) (2017), 523–534.
- [6] M. D'Anna, C. A. Finocchiaro and M. Fontana, *Amalgamated algebras along an ideal*, *Comm. Algebra and Applications*, Walter de Gruyter, Berlin, (2009), 155–172.
- [7] M. D'Anna, C. A. Finocchiaro and M. Fontana, *Properties of chains of prime ideals in an amalgamated algebra along an ideal*, *J. Pure Appl. Algebra*, 214(9) (2010), 1633–1641.
- [8] A. El Khalfi and N. Mahdou, *Almost Bézout rings and almost GCD-rings*, *Asian-Eur. J. Math.*, 13(06) (2020), 2050107.
- [9] N. Guennach, N. Mahdou, Ü. Tekir and S. Koç, *On graded $(1, r)$ -ideals*, *Asian-Eur. J. Math.*, 16(12) (2023), 2350222.
- [10] F. Z. Guissi, H. Kim and N. Mahdou, *Graded amalgamated algebras along an ideal*, *J. Algebra Appl.*, 23(6) (2024), 2450116.
- [11] F. Z. Guissi, H. Kim and N. Mahdou, *The structure of prime homogeneous ideals in graded amalgamated algebra along an ideal*, *J. Algebra Appl.*, DOI: 10.1142/S0219498825501063.
- [12] F. Z. Guissi, N. Mahdou, Ü. Tekir and S. Koç, *Graded almost valuation ring*, *Rev. Union Mat. Argent.*, DOI: 10.33044/revuma.4036.
- [13] N. Mahdou, A. Mimouni and M. A. S. Moutui, *On almost valuation and almost Bezout rings*, *Comm. Algebra*, 43(1) (2015), 297–308.
- [14] C. Nastasescu, V. Oystaeyen and F. Van, *Methods of Graded Rings*, *Lecture Notes in Math*, 1836, Springer-Verlag, Berlin, 2004.
- [15] D. G. Northcott, *Lessons on Rings, Modules and Multiplicities*, Cambridge University press, Cambridge (1968).
- [16] M. Refai, M. Hailat and S. Obiedat, *Graded radicals on graded prime spectra*, *Far East J. of Math. Sci. (I)* (2000), 59–73.



ISSN: 2820-7114

Moroccan Journal of Algebra and Geometry with Applications

Supported by Sidi Mohamed Ben Abdellah University, Fez, Morocco

Volume 4, Issue 1 (2025), pp 11-27

Title :

**Some New Fixed point theorems for asymptotically nonexpansive
type mappings in $CAT(k)$ space**

Author(s):

R. Keshavarz and H. Azadi Kenary

Some New Fixed point theorems for asymptotically nonexpansive type mappings in $CAT(k)$ spaces

R. Keshavarz* and H. Azadi Kenary*

* Department of Mathematics, Yasouj University, Yasouj 75914-353, Iran.

e-mail: azadi@yu.ac.ir

Communicated by Ali Taherifar

(Received 25 April 2024, Revised 25 August 2024, Accepted 01 September 2024)

Abstract. In this paper we prove a convergence theorem of the Mann iteration scheme for a asymptotically nonexpansive type mappings in $CAT(k)$ spaces with $k > 0$. We also obtain a convergence theorem of the Ishikawa iteration scheme for asymptotically nonexpansive mappings.

Key Words: Mann and Ishikawa iteration; strong convergence; $CAT(k)$ space; common fixed point; R -convex space.

2020 MSC: 39B05; 39B22; 46B22; 20K30.

Dedicated to our Professor David E. Dobbs for his 80th Birthday.

1 Introduction and preliminaries

Roughly speaking, $CAT(k)$ spaces are geodesic spaces of bounded curvature and generalization of Riemannian manifold of sectional curvature bounded above. The letter C, A and T stand for Cartan, Alexandrov and Toponogov who have made important contributions to the understanding of curvature via inequalities for the distance function and k is a real number that we impose it as the curvature bound of the space. Fixed point theory in $CAT(k)$ spaces was first studied by Kirk [1]-[2]. Since any $CAT(k)$ space is a $CAT(k')$ space for $k' > k$, so, all results for $CAT(0)$ spaces immediately apply to any $CAT(k)$ spaces with $k \leq 0$. However, there are only a few articles that contain fixed point results in the setting of $CAT(k)$ spaces with $k > 0$, because in this case the proof seems to be more complicated. The interplay between the geometry of Banach spaces and fixed point theory has been very strong and fruitful. In particular, geometric properties play a Key role in metric fixed point problems.

Gromov [9], introduced the notation of $CAT(0)$ spaces as follows:

Definition 1.1. Let C be a nonempty subset of metric space (X, d) . A mapping $T : C \rightarrow C$ is said to be

- (i) Lipschitzian if $d(Tx, Ty) \leq kd(x, y)$ for all $x, y \in C, k \geq 0$,
- (ii) nonexpansive if $d(Tx, Ty) \leq d(x, y)$ for all $x, y \in C$
- (iii) asymptotically nonexpansive if there exists a sequence $\{k_n\} \in [0, 1)$ with $\lim_{n \rightarrow \infty} k_n = 1$ such that $d(T^n x, T^n y) \leq k_n d(x, y)$ for all $x, y \in C$. Class of asymptotically nonexpansive mappings includes a class of nonexpansive mapping as proper subclass and both the mappings are Lipschitzian.

In 1974, Kirk, substantially weaken the assumption of asymptotic nonexpansiveness of T by replacing it with assumption, which may hold even if none of the iterates of T is Lipschitzian. A

mapping $T : C \rightarrow C$ is said to be asymptotically nonexpansive type if for each $y \in C$ the following inequality holds:

$$\lim_{n \rightarrow \infty} \sup \{ \sup_{x \in C} \{ d(T^n x, T^n y) - d(x, y) \} \} \leq 0.$$

Every asymptotically nonexpansive mapping is asymptotically nonexpansive type but converse need not be true. The concept of asymptotically nonexpansive type mappings is more of asymptotically nonexpansive mappings. Iterative approximation of fixed points of asymptotically nonexpansive and asymptotically nonexpansive type mapping have been studied by various author in the setting of Hilbert spaces, Banach spaces and convex metric spaces (see [9] and reference therein).

Definition 1.2. Let (X, d) be a metric space. A geodesic path joining $x \in X$ to $y \in X$ is a map C from a closed interval $[0, l] \subset \mathbb{R}$ to X such that $C(0) = x, C(l) = y$ and $d(C(t), C(t')) = |t - t'|$ for all $t, t' \in [0, l]$. In particular, C is an isometry and $d(x, y) = l$. The image of C is called geodesic (or metric) segment joining x and y . When it is unique this geodesic segment is denoted by $[x, y]$.

Definition 1.3. The space (X, d) is said to be a geodesic space if every two points of X are joined by a geodesic, X is said to be uniquely geodesic if there is exactly one geodesic joining x and y for each $x, y \in X$. A subset $Y \subset X$ is said to be convex if Y includes every geodesic segment joining any two of its point.

Definition 1.4. A subset C of X is said to be bounded if $\text{diam}(C) = \sup \{ d(x, y) : x, y \in C \} < \infty$.

Definition 1.5. Given $k \in \mathbb{R}$, we denote by M_k^n the following metric spaces:

- (i) if $k = 0$ then M_k^n is the Euclidean space E^n ;
- (ii) if $k > 0$ then M_k^n is obtained from the spherical space S^n by multiplying the distance function by the constant $\frac{1}{\sqrt{k}}$;
- (iii) if $k < 0$ then M_k^n is obtained from the hyperbolic space H^n by multiplying the distance function by the constant $\frac{1}{\sqrt{-k}}$.

Definition 1.6. If x, y_1, y_2 are points in a $CAT(0)$ space and if y_0 is the midpoint of the segment $[y_1, y_2]$, then the $CAT(0)$ inequality implies

$$d^2(x, y_0) \leq \frac{1}{2} \left\{ d^2(x, y_1) + d^2(x, y_2) - \frac{1}{2} d^2(y_1, y_2) \right\},$$

the above inequality named as CN -inequality. In fact, a geodesic space is a $CAT(0)$ space if and only if it satisfies the CN -inequality. $CAT(0)$ spaces may be regarded as a metric version of Hilbert spaces. For example, in any Hilbert space H we have the following extended version of parallelogram law:

$$\|z - (\alpha x + (1 - \alpha)y)\|^2 = \alpha \|z - x\|^2 + (1 - \alpha) \|z - y\|^2 - \alpha(1 - \alpha) \|x - y\|^2$$

for any $\alpha \in [0, 1]$ and $x, y, z \in H$.

CN - inequality is extended by Dhom Pongsa and Panyanak [4] as CN^* -inequality such as :

$$d^2(z, \alpha x \oplus (1 - \alpha)y) \leq \alpha d^2(x, z) + (1 - \alpha) d^2(z, y) - \alpha(1 - \alpha) \alpha d^2(x, y)$$

for any $\alpha \in [0, 1]$ and $x, y, z \in X$. If $\alpha = \frac{1}{2}$, then the above inequality becomes the CN -inequality. Infact , If X is a geodesic space then the following statements are equivalent:

- (i) X is a $CAT(0)$ space
- (ii) X satisfies CN -inequality
- (iii) X satisfies CN^* -inequality.

Definition 1.7. Let $R \in (0, 2]$, a geodesic space (X, d) is said to be R -convex for R if for any three points $x, y, z \in X$ we have

$$d^2(z, \alpha x \oplus (1 - \alpha)y) \leq \alpha d^2(x, z) + (1 - \alpha)d^2(z, y) - \frac{R\alpha(1 - \alpha)d^2(x, y)}{2}.$$

It follows from CN^* -inequality that a geodesic space (X, d) is a $CAT(0)$ space if and only if (X, d) is R -convex for $R = 2$.

Lemma 1.8. Let k be an arbitrary positive real number and (X, d) be a $CAT(k)$ space with $\text{diam}(X) \leq \frac{\pi - 2\eta}{2\sqrt{k}}$ for some $\eta \in \left(0, \frac{\pi}{2}\right)$. Then (X, d) is R -convex for $R = (\pi - \eta)\tan\eta$.

Lemma 1.9. Let (X, d) be a $CAT(0)$ space, then

(i) for $x, y \in X$ and $t \in [0, 1]$ there exists a unique point $z \in [x, y]$ such that

$$d(z, x) = td(x, y) \text{ and } d(y, z) = (1 - t)d(x, y),$$

we use the notation $(1 - t)x \oplus ty$ for the unique point z satisfying the above equalities.

(ii) for $x, y, z \in X$ and $t \in [0, 1]$, we have

$$d((1 - t)x \oplus ty, z) \leq (1 - t)d(x, z) + td(y, z).$$

Definition 1.10. Let C be nonempty subset of a $CAT(k)$ space (X, d) and $T : C \rightarrow C$ be a mapping. We denote by $F(T)$ the set of all fixed points of T , i.e., $F(T) = \{x \in C : x = Tx\}$. Then T is said to

(i) be completely continuous if T is continuous and for any bounded sequence $\{x_n\}_{n=1}^{+\infty}$ in C , $\{Tx_n\}_{n=1}^{+\infty}$ has a convergent subsequence in C .

(ii) be uniformly L -Lipschitzian if there exists a constant $L > 0$ such that

$$d(T^n x, T^n y) \leq Ld(x, y) \text{ for all } x, y \in C \text{ and all } n \in \mathbb{N}.$$

(iii) be asymptotically demicontractive if $F(T) \neq \emptyset$ and there exists $k \in [0, 1)$ and a sequence $\{a_n\}$ with $\lim_{n \rightarrow \infty} a_n = 1$ such that

$$d^2(T^n x, p) \leq a_n^2 d^2(x, p) + kd^2(x, T^n x) \text{ for all } x \in C, p \in F(T) \text{ and all } n \in \mathbb{N}.$$

(iv) be asymptotically hemiccontractive if $F(T) \neq \emptyset$ and there exists a sequence $\{a_n\} \in [0, 1)$ with $\lim_{n \rightarrow \infty} a_n = 1$ such that

$$d^2(T^n x, p) \leq a_n d^2(x, p) + d^2(x, T^n x) \text{ for all } x \in C, p \in F(T) \text{ and all } n \in \mathbb{N}.$$

Remark 1.11. It follows from the definition that every asymptotically demicontractive mapping is asymptotically hemiccontractive.

Definition 1.12. A mapping $P : X \rightarrow C$ is said to be retraction if $C \subset X$ and P restricted to C is the identity, i.e., $Px = x$ for any $x \in C$. Clearly $P^2 = P$, the set C is called a retract of X .

Lemma 1.13. Let C be a convex subset of X which is complete in the induced metric. Then, for every $x \in X$, there exists a unique point $p(x) \in C$ such that $d(x, p(x)) = d(x, C) = \inf_{y \in C} d(x, y)$. Moreover, the map $x \rightarrow px$ is a nonexpansive retract from X onto C .

Lemma 1.14. Let $\{s_n\}_{n=1}^{+\infty}, \{t_n\}_{n=1}^{+\infty} \in \mathbb{R}^+$ be sequences satisfying $s_{n+1} \leq s_n + t_n$ for all $n \in \mathbb{N}$. If $\sum_{n=1}^{\infty} t_n < \infty$ and $\{s_n\}_{n=1}^{+\infty}$ has a subsequence converging to 0, then $\lim_{n \rightarrow \infty} s_n = 0$.

Definition 1.15. Let C be a nonempty convex subset of a $CAT(k)$ space (X, d) and $T : C \rightarrow C$ be a mapping. Given $x_1 \in C$ and the sequence $\{x_n\}_{n=1}^{+\infty}$ is defined by

$$\begin{cases} x_{n+1} = (1 - \alpha_n)x_n \oplus \alpha_n T^n y_n \\ y_n = (1 - \beta_n)x_n \oplus \beta_n T^n x_n. \end{cases}$$

is called an Ishikawa iterative sequence. If $\beta_n = 0$ for all $n \in \mathbb{N}$, then the above algorithm reduces to the following:

$$x_{n+1} = (1 - \alpha_n)x_n \oplus \alpha_n T^n x_n$$

is called a Mann iterative sequence.

Definition 1.16. Let C be a nonempty subset of a $CAT(0)$ space X . A map $T : C \rightarrow X$ is said to be asymptotically nonexpansive type, if for each $y \in C$

$$\lim_{n \rightarrow \infty} \sup \{ \sup_{x \in C} \{ d(T(PT)^{n-1}x, T(PT)^{n-1}y) - d(x, y) \} \} \leq 0.$$

where P is the nonexpansive retraction of X onto C .

Definition 1.17. Let $\{x_n\}_{n=1}^{+\infty}$ be bounded sequence in a $CAT(0)$ space X and C be a subset of X . In the rest of the present paper, we use the following notations:

- (i) $r(x, \{x_n\}_{n=1}^{+\infty}) = \lim_{n \rightarrow \infty} \sup d(x, x_n)$.
- (ii) $r(\{x_n\}_{n=1}^{+\infty}) = \inf_{x \in X} r(x, \{x_n\}_{n=1}^{+\infty})$.
- (iii) $r_C(\{x_n\}_{n=1}^{+\infty}) = \inf_{x \in C} r(x, \{x_n\}_{n=1}^{+\infty})$.
- (iv) $A(\{x_n\}_{n=1}^{+\infty}) = \{x \in X : r(x, \{x_n\}_{n=1}^{+\infty}) = r(\{x_n\}_{n=1}^{+\infty})\}$.
- (v) $A_C(\{x_n\}_{n=1}^{+\infty}) = \{x \in X : r(x, \{x_n\}_{n=1}^{+\infty}) = r_C(\{x_n\}_{n=1}^{+\infty})\}$.

Note that $x \in X$ is called an asymptotic center of $\{x_n\}$ if $x \in A(\{x_n\}_{n=1}^{+\infty})$.

Definition 1.18. Let (X, d) be a $CAT(0)$ space. A sequence $\{x_n\}_{n=1}^{+\infty}$ in X is said to be Δ -convergent to $x \in X$ if x is the unique asymptotic center of $\{u_n\}_{n=1}^{+\infty}$ for every subsequence $\{u_n\}_{n=1}^{+\infty}$ of $\{x_n\}_{n=1}^{+\infty}$, i.e., $A(\{u_n\}_{n=1}^{+\infty}) = \{x\}$ for every subsequence $\{u_n\}_{n=1}^{+\infty}$ of $\{x_n\}_{n=1}^{+\infty}$. In this case, we write $\Delta - \lim x_n = x$ and x is called Δ -limit of $\{x_n\}_{n=1}^{+\infty}$.

Definition 1.19. A map T from a subset K of a metric space (X, d) into itself is said to be semi-compact if every bounded sequence $\{x_n\}_{n=1}^{+\infty} \subset K$ satisfying $d(x_n, Tx_n) \rightarrow 0$ as $n \rightarrow \infty$ has a strongly convergent subsequence.

Definition 1.20. A nonself mapping $T : K \rightarrow X$ with $F(T) \neq \emptyset$ is said to satisfy the condition (I) if there exists a non-decreasing function $f : [0, \infty) \rightarrow [0, \infty)$ with $f(0) = 0$ and $f(r) > 0$ for all $r \in (0, \infty)$ such that $d(x, Tx) \geq f(d(x, F(T)))$ for all $x \in K$.

Lemma 1.21. Let $k > 0$ and (X, d) be a complete $CAT(k)$ space with $\text{diam}(X) \leq \frac{\pi - 2\eta}{2\sqrt{k}}$ for some $\eta \in \left(0, \frac{\pi}{2}\right)$.

Then the following statements hold:

- (i) Every sequence in X has a Δ -convergent subsequence;
- (ii) if $\{x_n\}_{n=1}^{+\infty} \subseteq X$ and $\Delta - \lim_{n \rightarrow \infty} x_n = x$ then $x \in \bigcap_{k=1}^{\infty} \overline{\text{conv}}\{x_k, x_{k+1}, \dots\}$, where $\overline{\text{conv}}(A) = \bigcap_{B \supseteq A} B$ where B is closed and convex.

Lemma 1.22. Let $k > 0$ and (X, d) be a complete $CAT(k)$ space with $\text{diam}(X) \leq \frac{\pi - 2\eta}{2\sqrt{k}}$ for some $\eta \in \left(0, \frac{\pi}{2}\right)$.

If $\{x_n\}_{n=1}^{+\infty}$ is a sequence in X with $A(\{x_n\}_{n=1}^{+\infty}) = \{x\}$, $\{u_n\}_{n=1}^{+\infty}$ is a subsequences of $\{x_n\}$ with $A(\{u_n\}_{n=1}^{+\infty}) = \{u\}$ and the sequence $\{d(x_n, u)\}_{n=1}^{+\infty}$ converges then $x = u$.

The concept of asymptotically nonexpansive type mappings is more general than that of asymptotically nonexpansive mappings. Iterative approximation of fixed points of asymptotically nonexpansive and asymptotically nonexpansive type mapping have been studied by various author in the setting of Hilbert spaces, Banach spaces and convex metric spaces (see [3]-[17] and reference therein).

2 Main Results

Theorem 2.1. Let $k > 0$ and (X, d) be a $CAT(k)$ space with $diam(X) \leq \frac{\pi-2\eta}{2\sqrt{k}}$ for some $\eta \in \left(0, \frac{\pi}{2}\right)$. Let C be a nonempty convex subset of X and $T : C \rightarrow C$ be asymptotically nonexpansive type and $\{\alpha_n\}_{n=1}^{+\infty}, \{\beta_n\}_{n=1}^{+\infty} \in [0, 1]$. Given $x_1 \in C$, define the iteration scheme $\{x_n\}_{n=1}^{+\infty}$ by

$$\begin{cases} x_{n+1} = (1 - \alpha_n)x_n \oplus \alpha_n T^n y_n \\ y_n = (1 - \beta_n)x_n \oplus \beta_n T^n x_n. \end{cases}$$

then

$$d(x_n, Tx_n) \leq d(x_n, T^n x_n) + 3d(x_{n-1}, T^{n-1} x_{n-1}) + \frac{2}{n^2}.$$

Proof. Let $C_n = d(x_n, T^n x_n)$, then we have

$$\begin{aligned} d(x_{n-1}, y_{n-1}) &= d(x_{n-1}, (1 - \beta_{n-1})x_{n-1} \oplus \beta_{n-1} T^{n-1} x_{n-1}) \\ &\leq \beta_{n-1} d(x_{n-1}, T^{n-1} x_{n-1}) \\ &= \beta_{n-1} C_{n-1}. \end{aligned} \tag{1}$$

Also

$$\begin{aligned} d(x_{n-1}, T^{n-1} y_{n-1}) &\leq d(x_{n-1}, T^{n-1} x_{n-1}) + d(T^{n-1} x_{n-1}, T^{n-1} y_{n-1}) \\ &\leq d(x_{n-1}, T^{n-1} x_{n-1}) + d(x_{n-1}, y_{n-1}) \\ &\quad + \{d(T^{n-1} x_{n-1}, T^{n-1} y_{n-1}) - d(x_{n-1}, y_{n-1})\} \\ &\leq d(x_{n-1}, T^{n-1} x_{n-1}) + d(x_{n-1}, y_{n-1}) \\ &\quad + \sup_{k \geq n} [\sup_{x_{n-1} \in C} \{d(T^{n-1} x_{n-1}, T^{n-1} y_{n-1}) - d(x_{n-1}, y_{n-1})\}]. \end{aligned} \tag{2}$$

Now, since T is asymptotically nonexpansive type we can choose n_0 such that $n \geq n_0$ implies that

$$\sup_{k \geq n} [\sup_{x_{n-1} \in C} \{d(T^{n-1} x_{n-1}, T^{n-1} y_{n-1}) - d(x_{n-1}, y_{n-1})\}] \leq \frac{1}{n^2},$$

therefore

$$d(x_{n-1}, T^{n-1} y_{n-1}) \leq C_{n-1} + \beta_{n-1} + \frac{1}{n^2}.$$

So, by the above inequalities we conclude that

$$\begin{aligned} d(x_n, Tx_n) &\leq d(x_n, T^n x_n) + d(T^n x_n, Tx_n) \\ &\leq C_n + d(T^n x_n, T^n x_{n-1}) + d(T^n x_{n-1}, Tx_n) \\ &\leq C_n + [d(T^n x_n, T^n x_{n-1}) - d(x_n, x_{n-1})] + d(x_n, x_{n-1}) + d(T^n x_{n-1}, Tx_n) \\ &\leq C_n + \sup_{k \geq n} [\sup_{x \in C} \{d(T^k x_n, T^k x_{n-1}) - d(x_n, x_{n-1})\}] \\ &\quad + d(x_n, x_{n-1}) + d(T^n x_{n-1}, Tx_n) \\ &\leq C_n + \frac{1}{n^2} + d(x_n, x_{n-1}) + d(T^n x_{n-1}, Tx_n), \end{aligned} \tag{3}$$

and then we have

$$\begin{aligned}
 d(x_n, Tx_n) &\leq C_n + \frac{1}{n^2} + d(x_n, x_{n-1}) + d(T^n x_{n-1}, Tx_n) \\
 &\leq C_n + \frac{1}{n^2} + d(x_n, x_{n-1}) + d(T^{n-1} x_{n-1}, x_n) \\
 &\quad + [d(T(T^{n-1} x_{n-1}), Tx_n) - d(T^{n-1} x_{n-1}, x_n)] \\
 &\leq C_n + d(x_n, x_{n-1}) + \frac{1}{n^2} \\
 &\quad + \sup_{k \geq n} [\sup_{x \in C} \{d(T(T^{k-1} x_{n-1}), Tx_n) - d(T^{k-1} x_{n-1}, x_n)\}] \\
 &\quad + d(T^{n-1} x_{n-1}, x_n).
 \end{aligned} \tag{4}$$

Thus

$$d(x_n, Tx_n) \leq C_n + C_{n-1} + \frac{2}{n^2} + 2d(x_n, x_{n-1}),$$

and finally we have

$$\begin{aligned}
 d(x_n, Tx_n) &\leq C_n + C_{n-1} + \frac{2}{n^2} + 2d((1 - \alpha_{n-1})x_{n-1} \oplus \alpha_{n-1} T^{n-1}(y_{n-1}), x_{n-1}) \\
 &\leq C_n + C_{n-1} + \frac{2}{n^2} + 2\alpha_{n-1} d(T^{n-1}(y_{n-1}), x_{n-1}) \\
 &\leq C_n + 3C_{n-1} + \frac{2}{n^2}
 \end{aligned} \tag{5}$$

□

Theorem 2.2. Let $k > 0$ and (X, d) be a $CAT(k)$ space with $diam(X) \leq \frac{\pi-2\eta}{2\sqrt{k}}$ for some $\eta \in (0, \frac{\pi}{2})$. Let C be a nonempty closed convex subset of X , $T : C \rightarrow C$ be a completely continuous asymptotically nonexpansive type and $\{\alpha_n\}_{n=1}^\infty \in [\varepsilon, \frac{R}{2} - k - \varepsilon]$ for some $\varepsilon > 0$ where $R = (\pi - 2\eta)\tan\eta$. Given $x_1 \in C$, let define the iteration scheme $\{x_n\}_{n=1}^\infty$ by $x_{n+1} = (1 - \alpha_n)x_n \oplus \alpha_n T^n x_n$, then the sequence $\{x_n\}_{n=1}^\infty$ convergence strongly to a fixed point of T .

Proof. Let $p \in F(T)$, since (X, d) is a R -convex for R , then we have

$$\begin{aligned}
 &d^2(x_{n+1}, p) \\
 &\leq (1 - \alpha_n)d^2(x_n, p) + \alpha_n d^2(T^n x_n, p) - \frac{R\alpha_n(1 - \alpha_n)d^2(x_n, T^n x_n)}{2} \\
 &\leq (1 - \alpha_n)d^2(x_n, p) + \alpha_n [d^2(T^n x_n, T^n p) - d^2(x_n, p)] \\
 &\quad + \alpha_n d^2(x_n, p) - \frac{R\alpha_n(1 - \alpha_n)d^2(x_n, T^n x_n)}{2} \\
 &\leq d^2(x_n, p) + \alpha_n \sup_{k \geq n} [\sup_{x_n \in C} \{d^2(T^k x_n, T^k p) - d^2(x_n, p)\}] \\
 &\quad + \alpha_n d^2(x_n, p) - \frac{R\alpha_n(1 - \alpha_n)d^2(x_n, T^n x_n)}{2} \\
 &\leq d^2(x_n, p) + \alpha_n \sup_{k \geq n} [\sup_{x_n \in C} \{d(T^k x_n, T^k p) - d(x_n, p)\} \times \{d(T^k x_n, T^k p) + d(x_n, p)\}] \\
 &\quad + \alpha_n d^2(x_n, p) - \frac{R\alpha_n(1 - \alpha_n)d^2(x_n, T^n x_n)}{2}.
 \end{aligned} \tag{6}$$

So we have

$$d^2(x_{n+1}, p) \leq d^2(x_n, p) + \frac{\alpha_n}{n^2} \frac{\pi^2}{2k} - \varepsilon^2 d^2(x_n, T^n x_n),$$

and therefore

$$\varepsilon^2 d^2(x_n, T^n x_n) \leq d^2(x_n, p) - d^2(x_{n+1}, p) + \frac{\alpha_n \pi^2}{n^2 2k},$$

and since $\sum_{n=1}^{\infty} \frac{\pi^2}{4kn^2} < \infty$ then $\sum_{n=1}^{\infty} d^2(x_n, T^n x_n) < \infty$ which implies that

$\lim_{n \rightarrow \infty} d(x_n, T^n x_n) = 0$. So, by theorem 2.1, we have $\lim_{n \rightarrow \infty} d(x_n, T x_n) = 0$. On the other hand, since T is completely continuous, so $\{T x_n\}_{n=1}^{\infty}$ has a convergent subsequence in C and therefore by the last equality, $\{x_n\}_{n=1}^{\infty}$ has a convergent subsequence, say $x_{n_k} \rightarrow q \in C$. Moreover

$$d(q, Tq) \leq d(q, x_{n_k}) + d(x_{n_k}, T x_{n_k}) + d(T x_{n_k}, Tq) \rightarrow 0 \text{ as } k \rightarrow \infty,$$

and it means that $q \in F(T)$. On the other hand $d^2(x_{n+1}, p) \leq d^2(x_n, p) + \frac{\alpha_n \pi^2}{n^2 2k}$ and since $\sum_{n=1}^{\infty} \frac{\pi^2}{4kn^2} < \infty$, so by lemma 1.14, we have $\{x_n\}_{n=1}^{\infty} \rightarrow q$. This completes the proof. $\square$

Corollary 2.3. Let $k > 0$ and (X, d) be a $CAT(k)$ space with $\text{diam}(X) \leq \frac{\pi-2\eta}{2\sqrt{k}}$ for some $\eta \in \left(0, \frac{\pi}{2}\right)$. Let C be a nonempty closed convex subset of X and $T : C \rightarrow C$ be a completely continuous asymptotically nonexpansive mapping. Also, $\{\alpha_n\}_{n=1}^{\infty}$ be a sequences in $\left[\varepsilon, \frac{R}{2} - k - \varepsilon\right]$ for some $\varepsilon > 0$ where $R = (\pi - 2\eta)\tan\eta$. Given $x_1 \in C$ and we define the iteration scheme $\{x_n\}_{n=1}^{\infty}$ by $x_{n+1} = (1 - \alpha_n)x_n \oplus \alpha_n T^n x_n$. Then the sequence $\{x_n\}_{n=1}^{\infty}$ convergence strongly to a fixed point of T .

Proof. We know that every asymptotically nonexpansive mapping is asymptotically nonexpansive mapping type and it is well known that every convex subset of a $CAT(0)$ space equipped with the induced metric is a $CAT(0)$ space. Then (C, d) is a $CAT(0)$ space and hence it is a $CAT(k)$ space for all $k > 0$. Notice, also that C is R -convex for $R = 2$. Since C is bounded, we can choose $\eta \in \left(0, \frac{\pi}{2}\right)$ and $k > 0$ so that $\text{diam}(X) \leq \frac{\pi-2\eta}{2\sqrt{k}}$ and then the conclusion follows from the previous theorem. $\square$

Now, we prove the strong convergence of Ishikawa iteration for asymptotically nonexpansive type mapping.

Theorem 2.4. Let $k > 0$ and (X, d) be a $CAT(k)$ space with $\text{diam}(X) \leq \frac{\pi-2\eta}{2\sqrt{k}}$ for some $\eta \in \left(0, \frac{\pi}{2}\right)$. Let $R = (\pi - 2\eta)\tan(\eta)$, C be a nonempty closed convex subset of X , $T : C \rightarrow C$ is asymptotically nonexpansive type mapping and $\{\alpha_n\}_{n=1}^{\infty}, \{\beta_n\}_{n=1}^{\infty} \in [0, 1]$. Also, let $x_1 \in C$ and define the iteration scheme $\{x_n\}_{n=1}^{\infty}$ by

$$\begin{cases} x_{n+1} = (1 - \alpha_n)x_n \oplus \alpha_n T^n y_n \\ y_n = (1 - \beta_n)x_n \oplus \beta_n T^n x_n. \end{cases}$$

Then the following inequality holds :

$$\begin{aligned} d^2(x_{n+1}, p) &= d^2((1 - \alpha_n)x_n \oplus \alpha_n T^n y_n, p) \\ &\leq d^2(x_n, p) + \alpha_n \pi \left(\frac{1 + \pi \beta_n}{4n^2 \sqrt{k}} \right) \\ &\quad - \frac{R \alpha_n \beta_n (1 - \beta_n) d^2(x_n, T^n x_n)}{2} - \frac{R \alpha_n (1 - \alpha_n) d^2(x_n, T^n y_n)}{2} \end{aligned} \quad (7)$$

Proof. Let $p \in F(T)$, since (X, d) is R -convex, so we have

$$d^2(x_{n+1}, p) \leq (1 - \alpha_n) d^2(x_n, p) + \alpha_n d^2(T^n y_n, p) - \frac{R \alpha_n (1 - \alpha_n) d^2(x_n, T^n y_n)}{2} \quad (8)$$

and

$$d^2(y_n, p) \leq (1 - \beta_n)d^2(x_n, p) + \beta_n d^2(T^n x_n, p) - \frac{R\beta_n(1 - \beta_n)d^2(x_n, T^n x_n)}{2}. \quad (9)$$

On the other hand, since T is asymptotically nonexpansive type mapping, so we obtain that

$$\begin{aligned} d^2(T^n y_n, p) &= [d^2(T^n y_n, T^n p) - d^2(y_n, p)] + d^2(y_n, p) \\ &= [d(T^n y_n, T^n p) - d(y_n, p)] \times [d(T^n y_n, T^n p) + d(y_n, p)] + d^2(y_n, p) \\ &\leq \sup_{k \geq n} [\sup_{x \in C} d(T^k y_n, T^k p) - d(y_n, p)] [d(T^n y_n, T^n p) + d(y_n, p)] + d^2(y_n, p) \\ &\leq \frac{\pi}{4n^2 \sqrt{k}} + d^2(y_n, p). \end{aligned} \quad (10)$$

In a similar way we have

$$d^2(T^n x_n, p) \leq \frac{\pi}{4n^2 \sqrt{k}} + d^2(x_n, p) \quad (11)$$

It follows from (9) and (11) that

$$\begin{aligned} d^2(y_n, p) &\leq (1 - \beta_n)d^2(x_n, p) + \beta_n \left(\frac{\pi}{4n^2 \sqrt{k}} + d^2(x_n, p) \right) \\ &\quad - \frac{R\beta_n(1 - \beta_n)d^2(x_n, T^n x_n)}{2} \\ &= d^2(x_n, p) + \beta_n \left(\frac{\pi}{4n^2 \sqrt{k}} \right) \\ &\quad - \frac{R\beta_n(1 - \beta_n)d^2(x_n, T^n x_n)}{2}, \end{aligned} \quad (12)$$

on the other hand, by substituting (12) in (10), we get

$$\begin{aligned} d^2(T^n y_n, p) &\leq \frac{\pi}{4n^2 \sqrt{k}} + d^2(x_n, p) + \beta_n \left(\frac{\pi}{4n^2 \sqrt{k}} \right) \\ &\quad - \frac{R\beta_n(1 - \beta_n)d^2(x_n, T^n x_n)}{2}. \end{aligned} \quad (13)$$

Substituting (13) in (8), we get

$$\begin{aligned} d^2(x_{n+1}, p) &\leq (1 - \alpha_n)d^2(x_n, p) + \alpha_n \left(\frac{\pi}{4n^2 \sqrt{k}} + d^2(x_n, p) + \beta_n \left(\frac{\pi}{4n^2 \sqrt{k}} \right) \right. \\ &\quad \left. - \frac{R\beta_n(1 - \beta_n)d^2(x_n, T^n x_n)}{2} \right) - \frac{R\alpha_n(1 - \alpha_n)d^2(x_n, T^n y_n)}{2}, \end{aligned}$$

so

$$\begin{aligned} d^2(x_{n+1}, p) &\leq d^2(x_n, p) + \alpha_n \pi \left(\frac{1 + \beta_n}{4n^2 \sqrt{k}} \right) \\ &\quad - \frac{R\alpha_n \beta_n (1 - \beta_n) d^2(x_n, T^n x_n)}{2} - \frac{R\alpha_n (1 - \alpha_n) d^2(x_n, T^n y_n)}{2}, \end{aligned}$$

and the proof is completed. $\square$

Theorem 2.5. Let $k > 0$ and (X, d) be a $CAT(k)$ space with $diam(X) \leq \frac{\pi-2\eta}{2\sqrt{k}}$ for some $\eta \in \left(0, \frac{\pi}{2}\right)$. Also, let $R = (\pi - 2\eta)\tan(\eta)$, C is a nonempty closed convex subset of X , $T : C \rightarrow C$ be asymptotically nonexpansive type mapping and $\{\alpha_n\}_{n=1}^{+\infty}, \{\beta_n\}_{n=1}^{+\infty} \in [\varepsilon, b]$ for some $\varepsilon > 0$ and $b \in (0, 1)$. Assume that $x_1 \in C$ and define the iteration scheme x_n by

$$\begin{cases} x_{n+1} = (1 - \alpha_n)x_n \oplus \alpha_n T^n y_n \\ y_n = (1 - \beta_n)x_n \oplus \beta_n T^n x_n. \end{cases}$$

then $\lim_{n \rightarrow \infty} d(x_n, T x_n) = 0$.

Proof. First of all, we prove that $\lim_{n \rightarrow \infty} d(x_n, T^n x_n) = 0$. By Theorem 2.4, we have

$$\begin{aligned} d^2(x_{n+1}, p) &\leq d^2(x_n, p) + \alpha_n \pi \left(\frac{1 + \beta_n}{4n^2 \sqrt{k}} \right) \\ &\quad - \frac{R \alpha_n \beta_n (1 - \beta_n) d^2(x_n, T^n x_n)}{2}, \end{aligned} \quad (14)$$

and so $D = R(1 - b)$ and this implies that

$$\frac{R(1 - \beta_n)}{2} > \frac{R(1 - b)}{2} > 0 \quad (15)$$

for all $n \in N$. Suppose that $\lim_{n \rightarrow \infty} d(x_n, T^n x_n) \neq 0$, then there exists $\varepsilon_0 > 0$ and a subsequence $\{x_{n_i}\}_{i=1}^{+\infty}$ of $\{x_n\}_{n=1}^{+\infty}$ such that

$$d^2(x_{n_i}, T^{n_i} x_{n_i}) \geq \varepsilon_0. \quad (16)$$

Without loss of generality, let $n_1 > N$ and then we have

$$\alpha_n \beta_n \left[\frac{R}{2} (1 - \beta_n) \right] d^2(x_n, T^n x_n) \leq d^2(x_n, p) - d^2(x_{n+1}, p) + \alpha_n \pi \left(\frac{1 + \beta_n}{4n^2 \sqrt{k}} \right),$$

then

$$\begin{aligned} \sum_{l=1}^i \alpha_{n_l} \beta_{n_l} \left[\frac{R}{2} (1 - \beta_{n_l}) \right] d^2(x_{n_l}, T^{n_l} x_{n_l}) &= \sum_{m=n_1}^{n_i} \alpha_m \beta_m \left[\frac{R}{2} (1 - \beta_m) \right] d^2(x_m, T^m x_m) \\ &\leq \sum_{m=n_1}^{n_i} d^2(x_m, p) - d^2(x_{m+1}, p) + \alpha_m \pi \left(\frac{1 + \beta_m}{4m^2 \sqrt{k}} \right) \end{aligned} \quad (17)$$

from this, together (15) and (16) and this fact that $\varepsilon \leq \alpha_n, \beta_n$ for every $n \in N$, we obtain that

$$i \cdot \varepsilon^2 \cdot \frac{D}{2} \cdot \varepsilon_0 \leq \sum_{m=n_1}^{n_i} d^2(x_m, p) - d^2(x_{m+1}, p) + \alpha_m \pi \left(\frac{1 + \beta_m}{4m^2 \sqrt{k}} \right).$$

If we take $i \rightarrow \infty$, then the right hand side of the above inequality is bounded while the left side is unbounded and this is contradiction. Therefore, $\lim_{n \rightarrow \infty} d(x_n, T^n x_n) = 0$ and hence $\lim_{n \rightarrow \infty} d(x_n, T x_n) = 0$ by theorem 2.1. $\square$

Theorem 2.6. Let $k > 0$ and (X, d) be a $CAT(k)$ space with $diam(X) \leq \frac{\pi-2\eta}{2\sqrt{k}}$ for some $\eta \in \left(0, \frac{\pi}{2}\right)$. Let $R = (\pi - 2\eta)\tan(\eta)$, C be a nonempty closed convex subset of X , $T : C \rightarrow C$ be a completely

continuous and asymptotically nonexpansive type mapping and $\{\alpha_n\}_{n=1}^\infty, \{\beta_n\}_{n=1}^\infty \in [\varepsilon, b]$ for some $\varepsilon > 0$ and $b \in (0, 1)$. Given $x_1 \in C$ and define the iteration scheme $\{x_n\}_{n=1}^\infty$ by

$$\begin{cases} x_{n+1} = (1 - \alpha_n)x_n \oplus \alpha_n T^n y_n \\ y_n = (1 - \beta_n)x_n \oplus \beta_n T^n x_n. \end{cases}$$

Then $\{x_n\}_{n=1}^\infty$ converges strongly to a fixed point of T .

Proof. Since T is completely continuous, $\{Tx_n\}_{n=1}^\infty$ has a convergent subsequence in C . By using previous theorem, we can show that $\{x_n\}_{n=1}^\infty$ has a convergence subsequence, say $\{x_{n_k}\}_{n=1}^\infty \rightarrow q \in C$. Hence $q \in F(T)$ and the continuity of T . It follows from the inequalities using in the proof of theorem 3.4 that,

$$d^2(x_{n+1}, p) \leq d^2(x_n, p) + \alpha_n \pi \left(\frac{1 + \beta_n}{4n^2 \sqrt{k}} \right).$$

On the other hand, since $\sum_{n=1}^\infty \alpha_n \pi \left(\frac{1 + \beta_n}{4n^2 \sqrt{k}} \right) < \infty$, by lemma 1.14 we have $\{x_n\}_{n=1}^\infty \rightarrow q$. This completes the proof. $\square$

Theorem 2.7. Let $k > 0$ and (X, d) be a complete $CAT(k)$ space with $diam(X) \leq \frac{\pi-2\eta}{2\sqrt{k}}$ for some $\eta \in (0, \frac{\pi}{2})$. Also, let K be a nonempty closed convex subset of X , P be non-expansive retraction of X on to K and $T : K \rightarrow X$ be a uniformly continuous and asymptotically nonexpansive type mapping with $F(T) \neq \emptyset$. If $\{x_n\}_{n=1}^{+\infty} \subseteq K$ such that $\lim_{n \rightarrow \infty} d(x_n, Tx_n) = 0$ and $\Delta - \lim_{n \rightarrow \infty} x_n = w$ then $w \in K$ and $Tw = w$.

Proof. By lemma 1.21, $w \in K$. Now, we define $\psi(u) = \limsup_{n \rightarrow \infty} d(x_n, u)$ for each $u \in K$. Since $\lim_{n \rightarrow \infty} d(x_n, Tx_n) = 0$, so by induction on m , we can prove

$$\lim_{n \rightarrow \infty} d(x_n, T(PT)^{m-1}x_n) = 0 \quad (18)$$

for all $m \in \mathbb{N}$. Because of uniform continuity of TP , we have

$$\lim_{n \rightarrow \infty} d(T(PT)^{m-1}x_n, T(PT)^m x_n) = 0$$

and then

$$d(x_n, T(PT)^m x_n) \leq d(x_n, T(PT)^{m-1}x_n) + d(T(PT)^{m-1}x_n, T(PT)^m x_n) \rightarrow 0,$$

as $n \rightarrow \infty$ and equation (18) is proved. This implies that

$$\psi(u) = \limsup_{n \rightarrow \infty} d(T(PT)^{m-1}x_n, u) \quad (19)$$

for each $u \in K$ and $m \in \mathbb{N}$. Now, taking $u = T(PT)^{m-1}w$ in (19), we have

$$\begin{aligned} \psi(T(PT)^{m-1}w) &= \limsup_{n \rightarrow \infty} d(T(PT)^{m-1}x_n, T(PT)^{m-1}w) \\ &= \limsup_{n \rightarrow \infty} \{d(T(PT)^{m-1}x_n, T(PT)^{m-1}w) - d(x_n, w)\} + d(x_n, w) \\ &\leq \limsup_{m \rightarrow \infty} \{Sup_{x_n \in K} \{d(T(PT)^{m-1}x_n, T(PT)^{m-1}w) - d(x_n, w)\}\} \\ &\quad + d(x_n, w). \end{aligned}$$

Now, since T is asymptotically nonexpansive type mapping we have

$$\limsup_{m \rightarrow \infty} \psi(T(PT)^{m-1}w) \leq d(x_n, w) \leq \psi(w). \quad (20)$$

Furthermore, for any $n, m \in N$ it follows from the CN^* -inequality with $\alpha = \frac{1}{2}$,

$$\begin{aligned} d^2\left(x_n, \frac{1}{2}w \oplus \frac{1}{2}T(PT)^{m-1}w\right) &\leq \frac{d^2(x_n, w)}{2} + \frac{d^2(x_n, T(PT)^{m-1}w)}{2} \\ &\quad - \frac{Rd^2(w, T(PT)^{m-1}w)}{8}, \end{aligned}$$

and since $\Delta - \lim_{n \rightarrow \infty} x_n = w$ so by letting $n \rightarrow \infty$ in the above inequality, we get

$$\begin{aligned} \psi^2(w) &\leq \psi^2\left(\frac{1}{2}w \oplus \frac{1}{2}T(PT)^{m-1}w\right) \\ &\leq \frac{\psi^2(w)}{2} + \frac{\psi^2(T(PT)^{m-1}w)}{2} - \frac{Rd^2(w, T(PT)^{m-1}w)}{8}, \end{aligned}$$

which yields that

$$d^2(w, T(PT)^{m-1}w) \leq \frac{4[\psi^2(T(PT)^{m-1}w) - \psi^2(w)]}{R}. \quad (21)$$

On the other hand, by (20) and (21) we have $\lim_{n \rightarrow \infty} d(w, T(PT)^{m-1}w) = 0$. So, in view of the continuity of TP we obtain that $w = \lim_{m \rightarrow \infty} T(PT)^m w = \lim_{m \rightarrow \infty} TP(T(PT)^{m-1}w) = TPw = Tw$. This completes the proof. $\square$

Corollary 2.8. Let K be a nonempty bounded closed convex subset of a complete $CAT(0)$ space (X, d) , P be a nonexpansive retraction of X onto K and $T : K \rightarrow X$ be a uniformly continuous and asymptotically nonexpansive type mapping. If $\{x_n\}_{n=1}^{+\infty} \subseteq K$ such that $\lim_{n \rightarrow \infty} d(x_n, Tx_n) = 0$ and $\Delta - \lim_{n \rightarrow \infty} x_n = w$ then $w \in K$ and $Tw = w$.

Proof. It is well known that every convex subset of a $CAT(0)$ space, equipped with the induced metric is a $CAT(0)$ space. Then (K, d) is a $CAT(0)$ space and hence it is a $CAT(k)$ space for all $k > 0$. Notice also that K is R -convex for $R = 2$ and since K is bounded, we can choose $\eta \in \left(0, \frac{\pi}{2}\right)$ and $k > 0$ so that $diam(K) \leq \frac{\pi-2\eta}{2\sqrt{k}}$. The conclusion follows from theorem 2.6. $\square$

Theorem 2.9. Let $k > 0$ and (X, d) be a complete $CAT(k)$ space with $diam(X) \leq \frac{\pi-2\eta}{2\sqrt{k}}$ for some $\eta \in \left(0, \frac{\pi}{2}\right)$, K be a nonempty closed convex subset of X , P be nonexpansive retraction of X onto K and $T : K \rightarrow X$ be a uniformly continuous and asymptotically nonexpansive type mapping. Also, let $\{x_n\}_{n=1}^{+\infty} \subseteq K$ defined by

$$\begin{cases} x_1 \in K \\ y_n = P((1 - \beta_n)x_n \oplus \beta_n T(PT)^{n-1}x_n) \\ x_{n+1} = P((1 - \alpha_n)T(PT)^{n-1}x_n \oplus \alpha_n T(PT)^{n-1}y_n) \end{cases}, \quad (22)$$

where $\{\alpha_n\}_{n=1}^{+\infty}, \{\beta_n\}_{n=1}^{+\infty} \subseteq (0, 1)$ such that

$$\begin{cases} \liminf_{n \rightarrow \infty} \alpha_n(1 - \alpha_n) > 0 \\ \liminf_{n \rightarrow \infty} \beta_n(1 - \beta_n) > 0 \end{cases}.$$

If $F(T) \neq \emptyset$ then $\{x_n\}_{n=1}^{+\infty}$ is Δ -convergent to a fixed point of T .

Proof. We divide our proof into three steps.

Step 1: First we prove that $\lim_{n \rightarrow \infty} d(x_n, q)$ exist for each $q \in F(T)$. For this, let $q \in F(T)$ and since T is a asymptotically nonexpansive type mapping, so by (22) we have

$$\begin{aligned}
 d(y_n, q) &= d(P((1 - \beta_n)x_n \oplus \beta_n T(PT)^{n-1}x_n), q) \\
 &= d(P((1 - \beta_n)x_n \oplus \beta_n T(PT)^{n-1}x_n), P(q)) \\
 &\leq d((1 - \beta_n)x_n \oplus \beta_n T(PT)^{n-1}x_n, q) \\
 &\leq (1 - \beta_n)d(x_n, q) + \beta_n d(T(PT)^{n-1}x_n, q) \\
 &= (1 - \beta_n)d(x_n, q) + \beta_n d(T(PT)^{n-1}x_n, T(PT)^{n-1}q) \\
 &\leq (1 - \beta_n)d(x_n, q) + \beta_n \{ \sup_{x_n \in K} d(T(PT)^{m-1}x_n, T(PT)^{m-1}q) \} \\
 &\leq (1 - \beta_n)d(x_n, q) + \beta_n \left(\frac{1}{n^2} + d(x_n, q) \right) = d(x_n, q) + \frac{\beta_n}{n^2}.
 \end{aligned} \tag{23}$$

and this implies that

$$\begin{aligned}
 d(x_{n+1}, q) &= d(P((1 - \alpha_n)T(PT)^{n-1}x_n \oplus \alpha_n T(PT)^{n-1}y_n), q) \\
 &= d(P((1 - \alpha_n)T(PT)^{n-1}x_n \oplus \alpha_n T(PT)^{n-1}y_n), P(q)) \\
 &\leq d((1 - \alpha_n)T(PT)^{n-1}x_n \oplus \alpha_n T(PT)^{n-1}y_n, q) \\
 &\leq (1 - \alpha_n)d(T(PT)^{n-1}x_n, q) + \alpha_n d(T(PT)^{n-1}y_n, q) \\
 &\leq (1 - \alpha_n) \left[\frac{1}{n^2} + d(x_n, q) \right] + \alpha_n \left[d(y_n, q) + \frac{1}{n^2} \right].
 \end{aligned} \tag{24}$$

Now, by the above inequality and (23) we obtain that

$$d(x_{n+1}, q) \leq d(x_n, q) + \frac{\beta_n \alpha_n + 1}{n^2} \tag{25}$$

Step 2: Now, we prove that $\lim_{n \rightarrow \infty} d(x_n, Tx_n) = 0$. Since $\{x_n\}_{n=1}^{+\infty}$ is bounded, so there exists $R' > 0$ such that $\{x_n\}_{n=1}^{+\infty}, \{y_n\}_{n=1}^{+\infty} \subset B(q, R')$ for all $n \in N$ with $R' < \frac{D_k}{2}$. Therefore we have

$$\begin{aligned}
 d^2(y_n, q) &= d^2(P((1 - \beta_n)x_n \oplus \beta_n T(PT)^{n-1}x_n), q) \\
 &= d^2(P((1 - \beta_n)x_n \oplus \beta_n T(PT)^{n-1}x_n), P(q)) \\
 &\leq d^2((1 - \beta_n)x_n \oplus \beta_n T(PT)^{n-1}x_n, q) \\
 &\leq (1 - \beta_n)d^2(x_n, q) + \beta_n d^2(T(PT)^{n-1}x_n, q) - \frac{R\beta_n(1 - \beta_n)}{2} d^2(T(PT)^{n-1}x_n, x_n) \\
 &\leq (1 - \beta_n)d^2(x_n, q) \\
 &+ \beta_n \{ \sup_{x_n \in K} \{ d^2(T(PT)^{m-1}x_n, T(PT)^{m-1}q) - d^2(x_n, q) \} \} + \beta_n d^2(x_n, q) \\
 &\leq (1 - \beta_n)d^2(x_n, q) + \beta_n \{ \sup_{x_n \in K} \{ [d(T(PT)^{m-1}x_n, T(PT)^{m-1}q) \\
 &- d(x_n, q)][d(T(PT)^{m-1}x_n, T(PT)^{m-1}q) + d(x_n, q)] \} \} + \beta_n d^2(x_n, q) \\
 &\leq (1 - \beta_n)d^2(x_n, q) + \beta_n \left(\frac{\pi - 2\eta}{n^2 \sqrt{k}} \right) + \beta_n d^2(x_n, q).
 \end{aligned}$$

Hence we obtain that

$$d^2(y_n, q) \leq d^2(x_n, q) + \beta_n \left(\frac{\pi - 2\eta}{n^2 \sqrt{k}} \right) \tag{26}$$

Now, from CN^* -inequality and using (26), we get

$$\begin{aligned}
 d^2(x_{n+1}, q) &= d^2(P((1 - \alpha_n)T(PT)^{n-1}x_n \oplus \alpha_n T(PT)^{n-1}y_n), q) \\
 &= d^2(P((1 - \alpha_n)T(PT)^{n-1}x_n \oplus \alpha_n T(PT)^{n-1}y_n), P(q)) \\
 &\leq d^2((1 - \alpha_n)T(PT)^{n-1}x_n \oplus \alpha_n T(PT)^{n-1}y_n, q) \\
 &\leq (1 - \alpha_n)d^2(T(PT)^{n-1}x_n, q) + \alpha_n d^2(T(PT)^{n-1}y_n, q) \\
 &\quad - \frac{R\alpha_n(1 - \alpha_n)}{2} d^2(T(PT)^{n-1}y_n, T(PT)^{n-1}x_n) \\
 &\leq (1 - \alpha_n) \left(\frac{\pi - 2\eta}{n^2 \sqrt{k}} + d^2(x_n, q) \right) + \alpha_n \left(\frac{\pi - 2\eta}{n^2 \sqrt{k}} + d^2(y_n, q) \right) \\
 &\quad - \frac{R\alpha_n(1 - \alpha_n)}{2} d^2(T(PT)^{n-1}y_n, T(PT)^{n-1}x_n)
 \end{aligned}$$

Therefore from the last inequality and (26) we have

$$\begin{aligned}
 d^2(x_{n+1}, q) &\leq \frac{2(1 + \alpha_n \beta_n)}{n^2} \frac{\pi}{2} - \eta + d^2(x_n, q) \\
 &\quad - \frac{R\alpha_n(1 - \alpha_n)}{2} d^2(T(PT)^{n-1}y_n, T(PT)^{n-1}x_n).
 \end{aligned} \tag{27}$$

Or

$$d^2(x_{n+1}, q) \leq \frac{2(1 + \alpha_n \beta_n)}{n^2} \frac{\pi}{2} - \eta + d^2(x_n, q). \tag{28}$$

Hence by (28) and lemma 1.14, we find that $\lim_{n \rightarrow \infty} d(x_n, q)$ exists for each $q \in F(T)$. Finally, we prove that $\lim_{n \rightarrow \infty} d(x_n, T x_n) = 0$. From (28) we have

$$\begin{aligned}
 \frac{R\alpha_n(1 - \alpha_n)d^2(T(PT)^{n-1}y_n, T(PT)^{n-1}x_n)}{2} &\leq \frac{(1 + \alpha_n \beta_n)(\pi - 2\eta)}{n^2 \sqrt{k}} \\
 &\quad + d^2(x_n, q) - d^2(x_{n+1}, q).
 \end{aligned} \tag{29}$$

Since $\sum_{n=1}^{\infty} \frac{2(1 + \alpha_n \beta_n)}{n^2} \frac{\pi}{2} - \eta < \infty$ and $d(x_n, q) < R'$, so we have

$$\sum_{n=1}^{\infty} \alpha_n(1 - \alpha_n)d^2(T(PT)^{n-1}y_n, T(PT)^{n-1}x_n) < \infty,$$

and by the fact that $\liminf_{n \rightarrow \infty} \alpha_n(1 - \alpha_n) > 0$ we get

$$\lim_{n \rightarrow \infty} d(T(PT)^{n-1}y_n, T(PT)^{n-1}x_n) = 0.$$

On the other hand

$$\begin{aligned}
 d^2(y_n, q) &= d^2(P((1 - \beta_n)x_n \oplus \beta_n T(PT)^{n-1}x_n), q) \\
 &= d^2(P((1 - \beta_n)x_n \oplus \beta_n T(PT)^{n-1}x_n), P(q)) \\
 &\leq d^2((1 - \beta_n)x_n \oplus \beta_n T(PT)^{n-1}x_n, q) \\
 &\leq (1 - \beta_n)d^2(x_n, q) + \beta_n d^2(T(PT)^{n-1}x_n, q) - \frac{R\beta_n(1 - \beta_n)d^2(T(PT)^{n-1}x_n, x_n)}{2}.
 \end{aligned}$$

Also, for the right hand side of the above inequality, we have

$$\frac{R\beta_n(1-\beta_n)d^2(T(PT)^{n-1}x_n, x_n)}{2} \leq (1-\beta_n)d^2(x_n, q) - d^2(y_n, q) + \beta_n \left(\frac{\frac{\pi}{2} - \eta}{n^2 \sqrt{k}} \right).$$

Now, since $\sum_{n=1}^{\infty} \frac{\beta_n \frac{\pi}{2} - \eta}{n^2 \sqrt{k}} < \infty$, $d(x_n, q) < R'$ and $d(y_n, q) < R'$, we obtain that

$$\sum_{n=1}^{\infty} \beta_n(1-\beta_n)d^2(x_n, T(PT)^{n-1}x_n) < \infty,$$

and by the fact that $\liminf_{n \rightarrow \infty} \beta_n(1-\beta_n) > 0$, we get

$$\lim_{n \rightarrow \infty} d(x_n, T(PT)^{n-1}x_n) = 0 \quad (30)$$

Now using (30) we get

$$\begin{aligned} d(y_n, x_n) &= d(P((1-\beta_n)x_n \oplus \beta_n T(PT)^{n-1}x_n), x_n) \\ &= d(P((1-\beta_n)x_n \oplus \beta_n T(PT)^{n-1}x_n), P(x_n)) \\ &\leq d((1-\beta_n)x_n \oplus \beta_n T(PT)^{n-1}x_n, x_n) \\ &\leq \beta_n d(T(PT)^{n-1}x_n, x_n) \rightarrow 0 \end{aligned}$$

Also we observe that

$$\begin{aligned} d(x_{n+1}, x_n) &= d(P((1-\alpha_n)T(PT)^{n-1}x_n \oplus \alpha_n T(PT)^{n-1}y_n), x_n) \\ &= d(P((1-\alpha_n)T(PT)^{n-1}x_n \oplus \alpha_n T(PT)^{n-1}y_n), P(x_n)) \\ &\leq d((1-\alpha_n)T(PT)^{n-1}x_n \oplus \alpha_n T(PT)^{n-1}y_n, x_n) \\ &\leq (1-\alpha_n)d(T(PT)^{n-1}x_n, x_n) + \alpha_n d(T(PT)^{n-1}y_n, x_n) \\ &\leq (1-\alpha_n)d(T(PT)^{n-1}x_n, x_n) + \alpha_n [d(T(PT)^{n-1}y_n, T(PT)^{n-1}x_n) \\ &\quad + d(T(PT)^{n-1}x_n, x_n)] \\ &= d((T(PT)^{n-1}x_n, x_n) + \alpha_n d(T(PT)^{n-1}y_n, T(PT)^{n-1}x_n) \rightarrow 0, \end{aligned}$$

as $n \rightarrow \infty$. Therefore, we obtain that $d(x_{n+1}, y_n) \leq d(x_{n+1}, x_n) + d(x_n, y_n) \rightarrow 0$ as $n \rightarrow \infty$. Furthermore

$$\begin{aligned} d(x_{n+1}, T(PT)^{n-1}y_n) &\leq d(x_{n+1}, x_n) + d(x_n, T(PT)^{n-1}x_n) \\ &\quad + d(T(PT)^{n-1}x_n, T(PT)^{n-1}y_n) \rightarrow 0 \end{aligned}$$

as $n \rightarrow \infty$. So we have

$$d(x_{n+1}, T(PT)^{n-1}y_n) \rightarrow 0. \quad (31)$$

Furthermore, we have

$$\begin{aligned} d(x_n, Tx_n) &\leq d(x_n, T(PT)^{n-1}x_n) + d(T(PT)^{n-1}x_n, T(PT)^{n-1}y_{n-1}) \\ &\quad + d(T(PT)^{n-1}y_{n-1}, Tx_n) \\ &\leq d(x_n, T(PT)^{n-1}x_n) + d(T(PT)^{n-1}x_n, T(PT)^{n-1}y_{n-1}) \\ &\quad + d(T(PT)^{n-1}y_{n-1}, Tx_n), \end{aligned} \quad (32)$$

and since $\lim_{n \rightarrow \infty} d(T(PT)^{n-2}y_{n-1}, x_n) = 0$ and TP is uniformly continuous, we have

$$\lim_{n \rightarrow \infty} d(TPT(PT)^{n-2}y_{n-1}, TPx_n) = \lim_{n \rightarrow \infty} d(T(PT)^{n-1}y_{n-1}, Tx_n) = 0.$$

Finally, from this, (30), (31) and (32), we have $d(x_n, Tx_n) \rightarrow 0$.

Step 3: Now, we prove that $\{x_n\}_{n=1}^{+\infty}$ is Δ -convergent to a fixed point of T .

Let $\omega_W = \bigcup A(\{u_n\})$, where the union is taken over all subsequences $\{u_n\}_{n=1}^{+\infty}$ of $\{x_n\}_{n=1}^{+\infty}$. First of all, we will show that $\omega_W(x_n) \subseteq F(T)$. For this, let $u \in \omega_W(x_n)$ and so, there exists a subsequence $\{u_n\}_{n=1}^{+\infty}$ of $\{x_n\}_{n=1}^{+\infty}$ such that $A(\{u_n\}) = \{u\}$.

On the other hand, by lemma 1.21 there exists a subsequence $\{v_n\}_{n=1}^{+\infty}$ of $\{u_n\}_{n=1}^{+\infty}$ such that $\Delta\text{-}\lim_{n \rightarrow \infty} v_n = v \in K$. Furthermore, by the fact that $d(x_n, Tx_n) \rightarrow 0$ we conclude that $d(v_n, Tv_n) \rightarrow 0$. Also, it follows from theorem 2.7 that $v \in F(T)$ and then by step1, we obtain that $\lim_{n \rightarrow \infty} d(x_n, v)$ exists. Thus, $u = v$ by lemma 1.22 and this implies that $\omega_W(x_n) \subseteq F(T)$. Next, we show that $\omega_W(x_n)$ consists of exactly one point. Let $\{u_n\}_{n=1}^{+\infty}$ be a subsequence of $\{x_n\}_{n=1}^{+\infty}$ with $A(\{u_n\}_{n=1}^{+\infty}) = \{u\}$ and $A(\{x_n\}_{n=1}^{+\infty}) = \{x\}$. Since $u \in \omega_W(x_n) \subseteq F(T)$, so from step1 we have $\lim_{n \rightarrow \infty} d(x_n, u)$ exists. Again, we obtain that $x = u$ and therefore $\omega_W(x_n) = \{x\}$. This means that $\{x_n\}_{n=1}^{+\infty}$ is Δ -convergent to a fixed point of T and the proof is completed. $\square$

Theorem 2.10. Let X, K, P, T and $\{x_n\}_{n=1}^{+\infty}$ be the same as in theorem 2.9. Then $\{x_n\}_{n=1}^{+\infty}$ converges strongly to a fixed point of T if and only if $\liminf_{n \rightarrow \infty} d(x_n, F(T)) = 0$ where $d(x, F(T)) = \inf\{d(x, q) : q \in F(T)\}$.

Proof. If $\{x_n\}_{n=1}^{+\infty}$ converges to $q \in F(T)$ then $\lim_{n \rightarrow \infty} d(x_n, q) = 0$ and since $0 \leq d(x_n, F(T)) \leq d(x_n, q)$, we have $\liminf_{n \rightarrow \infty} d(x_n, F(T)) = 0$.

Conversely, suppose that $\lim_{n \rightarrow \infty} d(x_n, F(T)) = 0$, then from step1 of the theorem 2.9, we have $\lim_{n \rightarrow \infty} d(x_n, F(T))$ exists. Thus by hypothesis $\lim_{n \rightarrow \infty} d(x_n, F(T)) = 0$. Next, we show that $\{x_n\}_{n=1}^{+\infty}$ is a Cauchy sequence. In fact, it follows from (25) that for any $q \in F(T)$

$$d(x_{n+1}, q) \leq d(x_n, q) + \frac{\beta_n \alpha_n + 1}{n^2} \leq d(x_n, q) + \frac{2}{n^2}.$$

Hence for any positive integers n, m , we have

$$\begin{aligned} d(x_{n+m}, x_n) &\leq d(x_{n+m}, q) + d(q, x_n) \\ &\leq d(x_{n+m-1}, q) + \frac{2}{(n+m-1)^2} + d(q, x_n) \\ &\leq d(x_{n+m-2}, q) + \frac{2}{(n+m-2)^2} + \frac{2}{(n+m-1)^2} + d(q, x_n) \\ &\dots \leq d(x_n, q) + \frac{2}{n^2} + \dots + \frac{2}{(n+m-2)^2} + \frac{2}{(n+m-1)^2} + d(q, x_n) \end{aligned}$$

So we get

$$d(x_{n+m}, x_n) \leq \sum_{i=n}^{n+m-1} \frac{2}{i^2} + 2d(x_n, q) \leq \sum_{i=n}^{n+m-1} \frac{2}{i^2} + 2d(x_n, F(T)) \rightarrow 0.$$

as $m, n \rightarrow \infty$ and this implies that $\{x_n\}_{n=1}^{+\infty}$ is a Cauchy sequence in K . Since, K is a closed subset in a complete $CAT(k)$ space X , it is complete. So, we can assume that $\{x_n\}_{n=1}^{+\infty}$ converges strongly to some point $q^* \in K$. Furthermore, as T is continuous, so $F(T)$ is closed subset in K and since $\lim_{n \rightarrow \infty} d(x_n, F(T)) = 0$ we obtain $q^* \in F(T)$. This completes the proof. $\square$

Theorem 2.11. Let X, K, P, T and $\{x_n\}_{n=1}^{+\infty}$ be the same as in theorem 2.9.

- (i) if T is semi-compact, then $\{x_n\}_{n=1}^{+\infty}$ converges strongly to a fixed point of T .
- (ii) if T satisfies condition (I) then $\{x_n\}_{n=1}^{+\infty}$ converges strongly to a fixed point of T .

Proof. It follows from step1 of theorem 2.9 that $\{x_n\}_{n=1}^{+\infty}$ is a bounded sequence in K . Also, since $\lim_{n \rightarrow \infty} d(x_n, Tx_n) = 0$ by the semi-compactness of T , there exists a subsequence $\{x_{n_k}\}_{k=1}^{+\infty} \subset \{x_n\}_{n=1}^{+\infty}$ such that $\{x_{n_k}\}_{k=1}^{+\infty}$ converges strongly to some point $q \in K$. Moreover, by the uniform continuity of T , we have $d(q, Tq) = \lim_{n \rightarrow \infty} d(x_n, Tx_n) = 0$ and this implies that $q \in F(T)$. Again by 24 $\lim_{n \rightarrow \infty} d(x_n, q)$ exists. Hence q is the strong limit of the sequence $\{x_n\}_{n=1}^{+\infty}$. As a result $\{x_n\}_{n=1}^{+\infty}$ converges strongly to a fixed point q of T .

For the proof of (ii), again from step1 of theorem 2.9 we know that $\lim_{n \rightarrow \infty} d(x_n, F(T))$ exists. Furthermore, by condition (I) and the fact that $\lim_{n \rightarrow \infty} d(x_n, Tx_n) = 0$, we have

$$\lim_{n \rightarrow \infty} f(d(x_n, F(T))) \leq \lim_{n \rightarrow \infty} d(x_n, Tx_n) = 0.$$

That is $\lim_{n \rightarrow \infty} f(d(x_n, F(T))) = 0$. since f is a non-decreasing function satisfying $f(0) = 0$ and $f(r) > 0$ for all $r \in (0, \infty)$, it follows that $\lim_{n \rightarrow \infty} d(x_n, F(T)) = 0$. Now theorem 2.8 implies that $\{x_n\}_{n=1}^{+\infty}$ converges strongly to a fixed point q in $F(T)$. $\square$

References

- [1] W.A. Kirk, *Geodesic geometry and fixed point theory*. In Seminar of mathematical analysis (Malaga/Seville, 2002/2003), 64 (2003), 195–225.
- [2] W. A. Kirk, *Geodesic geometry and fixed point theory II*, Fixed Point Theory and Applications, (2004).
- [3] Y.J. Cho,, L. Ciric and S. Wang, *Convergence theorems for nonexpansive semigroups in CAT(0) spaces*, Nonlinear Analysis: Theory, Methods and Applications, 74(17) (2011), 6050–6059.
- [4] S. Dhompongsa, A. Kaewkhao and B. Panyank, *Lim theorems for multivalued mappings in CAT(0) spaces*, Journal of Mathematical Analysis and Applications 312(2) (2005), 478–487.
- [5] W. R. Mann, *Mean value methods in iteration*, Proceedings of the American Mathematical Society 4(3) (1953), 506–510.
- [6] M. E. Gordji, E. Akbartabar, Y. J. Cho and M. Ramezani, *Coupled common fixed point theorems for mixed weakly monotone mappings in partially ordered metric spaces*, Fixed Point Theory and Applications, 2012 (2012), 1–12.
- [7] M. E. Gordji, H. Baghani and G. H. Kim *Common fixed point theorems for (ψ, ϕ) -weak nonlinear contraction in partially ordered sets*, Fixed point theory and applications, 2012 (2012), 1–12.
- [8] M. E. Gordji, S. Pirbavafa, M. Ramezani, C. Park and D. Y. Shin *Presic-Kannan-Rus fixed point theorem on partially order metric spaces*, Fixed Point Theory, 15 (2) (2014), 463–474.
- [9] M. Gromov *Metric structure for Riemannian and Non-Riemannian spaces*, Progress in Mathematics. Birkhäuser, 152 (1984).
- [10] T. M. Rassias, *On fixed point theory in non-linear analysis*, Tamkang Journal of Mathematics 8(2) (1977), 233–237.
- [11] T. M. Rassias, *Some theorems of fixed points in non-linear analysis*, Bulletin of the Institute of Mathematics, Academia Sinica. 13(1) (1985), 5–12.
- [12] A. Sahin and M. Basarır, *Some convergence results for nearly asymptotically nonexpansive nonself mappings in CAT(K) spaces*, Math Sci. 11(1) (2017), 79–86.

- [13] R. Saadati, SM. Vaezpour and P. vetro *Fixed point theorems in generalized partially orderd G -metric spaces*, Mathematical and Computer Modelling 52(5-6) (2010), 797–801.
- [14] R. Saadati, S. Sedghi and H. Zhou *A common fixed point theorem for ψ -weakly commuting maps in L -fuzzy metric spaces*, Iranian Journal of Fuzzy Systems, 5 (1) (2008), 47–53.
- [15] R. Saadati *Notes to the paper Fixed points in intuitionistic fuzzy metric spaces and its generalization to L -fuzzy metric spaces*, Chaos, Solutions and Fractals 35 (1) (2008), 176–180.
- [16] R. Saadati and S. Sedghi *A common fixed point theorem for R -weakly commuting maps in fuzzy metric spaces*, Iranian conference on fuzzy systems, (2006).
- [17] R. Saadati, SM. Vaezpour and LB. Circ *Generalized distance and some common fixed point theorems*, J. Comput. Anal. Appl. 48(1) (2010), 146–175.



ISSN: 2820-7114

Moroccan Journal of Algebra and Geometry with Applications

Supported by Sidi Mohamed Ben Abdellah University, Fez, Morocco

Volume 4, Issue 1 (2025), pp 28-37

Title :

On superzeta functions of the first kind on function fields

Author(s):

Kajtaz H. Bllaca, Jawher Khmiri, Kamel Mazhouda, and Bouchaïb Sodaïgui

On superzeta functions of the first kind on function fields

Kajtaž H. Bllaca¹, Jawher Khmiri², Kamel Mazhouda³ and Bouchaïb Sodaïgui⁴

¹ Department of Mathematics, University of Prishtina, Mother Theresa, no. 5, 10000 Prishtina, Kosovo
e-mail: kajtaž.bllaca@uni-pr.edu

² University of Monastir, Faculty of Science of Monastir, 5000 Monastir, Tunisia
e-mail: Jawherkhmiri11@gmail.com

³ University of Sousse, Higher Institute of Applied Sciences and Technology, 4003 Sousse, Tunisia
e-mail: kamel.mazhouda@fsm.rnu.tn

⁴ Univ. Polytechnique Hauts-De-France, INSA Hauts-De-France, FR CNRS 2037,
CERAMATHS, F-59313 Valenciennes, France

Communicated by Abdelmejid Bayad

(Received 12 June 2024, Revised 14 October 2024, Accepted 05 November 2024)

Abstract. In a recent article [2], we studied the superzeta functions on function fields. In this paper, we continue our investigation on the superzeta functions of the first kind. We prove results concerning their link with the Euler-Stieltjes constants and we give formulas for the r -depth regularized product of their zeros.

Key Words: Function fields, Superzeta functions, Riemann hypothesis, Li coefficients.

2020 MSC: Primary 11M41; Secondary 11M38.

Dedicated to our Professor David E. Dobbs for his 80th Birthday.

1 Introduction

1.1 Background

Functions defined by using the zeros of the Riemann zeta function as the building block of new Dirichlet series were studied firstly by Mellin in [6] (see an English translation in [12] Appendix D, p. 139). Voros in [12] gave the name *Superzeta functions* and introduced three types of such functions, and in [12] Chapter 10, p. 91] discussed possible extensions to other classes of zeta functions.

The purpose of the present paper is to continue our study on superzeta functions of the first kind on function fields started in [2].

For the convenience of the reader, let us recall the definition and some proprieties of the zeta function of a function field as stated in [2] §1.1] (for more details see [11] Chapter 5, Section 5.1 and Section 5.2, pp. 185–218] or [9]).

Let K denote an algebraic function field of genus g whose field of constants is the finite field $\mathbb{F}_q$. Let $Z_K(X)$ be the following power series

$$Z_K(X) = \sum_{n=0}^{+\infty} C_n X^n = \prod_{D \text{ prime}} (1 - X^{\deg(D)})^{-1},$$

where $C_n = \#\{D \in \text{Div}(K); D \geq 0, \deg(D) = n\}$; $Z_K(X)$ is actually a rational function

$$Z_K(X) = \frac{L(X)}{(1-X)(1-qX)}, \quad (1)$$

where $L(X)$ factors in $\mathbb{C}[X]$ as

$$L(X) = \prod_{j=1}^{2g} (1 - \alpha_j X) \in \mathbb{Z}[X]. \quad (2)$$

The special value $L(1) = \prod_{i=1}^{2g} (1 - \alpha_i)$ is the class number of K , denoted by h_K . The complex numbers $\alpha_1, \dots, \alpha_{2g}$ are algebraic integers and can be arranged so that $\alpha_j \alpha_{g+j} = q$ holds for $j = 1, \dots, g$. Since the Riemann hypothesis for function fields (abbreviated to RH) proved by A. Weil [13] states that α_i , $i = 1, \dots, 2g$ have absolute value $q^{1/2}$, we may order the indices $j \in \{1, \dots, g\}$ so that $\alpha_{g+j} = \overline{\alpha_j}$, and we then can write $\alpha_j = q^{1/2} \exp(i\theta_j)$ with $\theta_j \in [0, \pi]$.

Now, we define the (classical) zeta function ζ_K of K as follows: for $s \in \mathbb{C}$, we substitute X with q^{-s} in $Z_K(X)$ to get the function

$$\zeta_K(s) := Z_K(q^{-s}) = \sum_{n=0}^{+\infty} C_n q^{-ns}, \quad (3)$$

which converges for $\text{Re}(s) > 1$. We define the following completed zeta function

$$\xi_K(s) := q^s (1 - q^{-s}) (1 - q^{1-s}) q^{(g-1)s} \zeta_K(s) = q^{gs} L(q^{-s}), \quad (4)$$

which is an entire function of order one, whose zeros coincide with the zeros of ζ_K . Moreover, ξ_K satisfies the functional equation

$$\xi_K(s) = \xi_K(1-s). \quad (5)$$

Let us recall that all zeros of the zeta function ζ_K lie in the critical strip $0 \leq \text{Re}(s) \leq 1$, and they are symmetric with respect to the real axis and the line $\text{Re}(s) = 1/2$. Note that the RH in this context is equivalent to saying that the zeros of ζ_K lie on the line $\text{Re}(s) = 1/2$. Let $\mathbb{Z}(K)$ be the set of the zeros ρ of ζ_K . Using (1) and (2), we obtain

$$\mathbb{Z}(K) = \left\{ \frac{1}{2} \pm i \frac{\theta_j}{\log q} + i \frac{2k\pi}{\log q}, j \in \{1, \dots, g\}, k \in \mathbb{Z} \right\}.$$

For an integer $n \neq 0$, the n th Li coefficient for the function field K is defined as the sum

$$\lambda_K(n) = \sum_{\rho \in \mathbb{Z}(K)}^* \left(1 - \left(1 - \frac{1}{\rho} \right)^n \right) := \lim_{T \rightarrow +\infty} \sum_{\rho \in \mathbb{Z}(K); |\text{Im}(\rho)| \leq T} \left(1 - \left(1 - \frac{1}{\rho} \right)^n \right). \quad (6)$$

From the definition of $\mathbb{Z}(K)$, we deduce that $\mathbb{Z}(K) = 1 - \mathbb{Z}(K) = 1 - \overline{\mathbb{Z}(K)}$. Hence, the Li coefficients $\lambda_K(n)$ are real and $\lambda_K(-n) = \overline{\lambda_K(n)} = \lambda_K(n)$, for all $n \in \mathbb{N}$. The Li criterion for ζ_K states: the zeros of ζ_K lie on the line $\text{Re}(s) = 1/2$ if and only if the Li coefficients $\lambda_K(n)$ are nonnegative for all $n \geq 1$. Let us recall that

$$\frac{\xi'_K(z)}{\xi_K(z)} = \sum_{\rho \in \mathbb{Z}(K)}^* \frac{1}{z - \rho} \quad (7)$$

for all $z \in \mathbb{C} \setminus \mathbb{Z}(K)$ (here $\sum^*$ is defined as in (6)). One has the following Hadamard product

$$\xi_K(z) = \prod_{\rho \in \mathbb{Z}(K)}^* \left(1 - \frac{z}{\rho}\right) := \lim_{T \rightarrow +\infty} \prod_{\substack{\rho \in \mathbb{Z}(K) \\ |\operatorname{Im}(\rho)| \leq T}} \left(1 - \frac{z}{\rho}\right). \quad (8)$$

Using (6) and (8) we obtain

$$\frac{d}{dz} \log \left(\xi_K \left(\frac{1}{1-z} \right) \right) = \sum_{n=1}^{+\infty} \lambda_K(n) z^{n-1}. \quad (9)$$

The Li coefficients $\lambda_K(n)$ associated to the function field K can be expressed for any positive integer n as follows (see, [5] Proposition 3.1)

$$\lambda_K(n) = -\frac{1}{(n-1)!} \frac{d^n}{dz^n} \left((z-1)^{n-1} \log \xi_K(z) \right) \Big|_{z=0}.$$

1.2 Superzeta functions of the first kind on function fields

In this subsection, we recall definitions and previous results on superzeta functions of the first kind on function fields (we refer to [2] for more details).

Following the ideas of Voros in [12] Chapter 10, 10.2, p. 93], the authors in [2] define two types of superzeta functions on K . The superzeta functions of the first kind are

$$Z_K(s, z) = \sum_{\rho} \frac{1}{(z-\rho)^s}, \quad \operatorname{Re}(s) > 1, \quad (10)$$

where the sum is taken over the zeros ρ of the function ζ_K and $z \in X_K = \{z \in \mathbb{C}, \forall \rho \in \mathbb{Z}(K), z-\rho \notin \mathbb{R}_-\}$. Note that these functions are well-defined in the half-plane $\operatorname{Re}(s) > 1$, which can be seen if we put $(z-w)^{-s} := e^{-s \log(z-w)}$ for $w \in \mathbb{C} \setminus [z, +\infty[$, using the convention that $\log(z-w)$ is real-valued for real $w < z$. The authors in [2] Theorem 1.1] proved that for fixed $z \in X_K \setminus]-\infty, 1]$, the superzeta function $Z_K(s, z)$ of the first kind has a holomorphic continuation to all $s \in \mathbb{C}$. Furthermore, they expressed $Z_K(s, z)$ in terms of the Hurwitz zeta functions which provides a holomorphic continuation of it to the whole s -plane. An expression for the zeta regularized product associated to the superzeta functions of the first kind is also given.

1.3 Main results

In this subsection we give the main results of the paper.

In Section 2, we study special values of the derivative of the superzeta functions of the first kind using Seri's results (see Proposition 2.1 below from [10]).

Let us define $Z_{K,*}(n) := Z_K(n, 1)$. Let $\gamma_K(n)$ be the coefficients appearing in the Taylor series expansion of the function $\frac{\xi'_K(z)}{\xi_K(z)}$ around $z = 1$ so that

$$\frac{\xi'_K(z)}{\xi_K(z)} = g \log q + \sum_{n=0}^{+\infty} \gamma_K(n) (z-1)^n. \quad (11)$$

The coefficients $\gamma_K(n)$ are called the Euler-Stieltjes constants of the second kind on K .

In the following theorem, we consider some special values of $Z_K(s, z)$ and relate them to $\gamma_K(n)$.

Theorem 1.1. Let n be a positive integer. Then

$$Z_{K,*}(n) = \begin{cases} g \log q + \gamma_K(0) & \text{if } n = 1, \\ (-1)^{n-1} \gamma_K(n-1) & \text{if } n \geq 2. \end{cases} \quad (12)$$

In Section 3, we give in Theorem 3.1 and Proposition 3.3 two different expressions for the r -depth regularized product associated to the superzeta functions of the first kind which are generalizations of Proposition 3.1 in [2] for $r \geq 1$.

2 The superzeta functions of the first kind and the Euler-Stieltjes constants of the second kind

2.1 Special values of the derivative of the superzeta functions of the first kind

In this subsection, we only give an idea of how to obtain an expression for $Z_K^{(m)}(0, z)$ and $Z_K^{(m)}(-n, z)$, as the formulas used (16) and (14) below are complicated. However, these expressions can be evaluated numerically for the first m values, as Seri has done in [10].

The Hurwitz zeta function $\zeta_H(s, z)$ is defined for $\Re(s) > 1$ and $z \in \mathbb{C} \setminus \{-\mathbb{N}\}$ by the absolutely convergent series $\zeta_H(s, z) = \sum_{n=0}^{+\infty} \frac{1}{(n+z)^s}$. Let us recall the following formulas.

Proposition 2.1. For large $|a|$ and $|\arg(a)| < \pi$, we have (see [3] p. 3223] recalled in [10] Equation (2))

$$\zeta'_H(z+1, a) = -\left(\frac{1}{z} + \ln a\right) \zeta_H(z+1, a) + \frac{1}{2z} a^{-z-1} + \frac{1}{z} \sum_1 (z, a), \quad (13)$$

where

$$\sum_1 (z, a) := \sum_{k=2}^{\infty} B_k a^{-z-k} \sum_{j=0}^{k-1} \frac{(z)_k}{j!(k-j)}$$

and for $m \geq 2$, (see [10] Equation (4))

$$\begin{aligned} & \zeta_H^{(m)}(z+1, a) \\ = & \frac{(-1)^m \Gamma(m+1, z \log a)}{z^{m+1}} + \frac{(-1)^m}{2} \log^m(a) a^{-z-1} + \frac{1}{z} \sum_m (z, a) \\ & + \frac{1}{z} \sum_{i=0}^{m-1} \sum_i (z, a) \left\{ C_{m, m-i} + \sum_{l=1}^{m-i-1} \sum_{1 \leq k_0 < k_1 < \dots < k_{l-1} < m-i} \left[\prod_{j=0}^{l-1} C_{m-k_{j-1}, k_j - k_{j-1}} \right] C_{m-k_{l-1}, m-i-k_{l-1}} \right\}, \end{aligned} \quad (14)$$

where

$$\sum_m (z, a) = \sum_{j_0=2}^{+\infty} B_{j_0} a^{-z-j_0} \left\{ \sum_{j_1=0}^{j_0-1} \frac{1}{j_0-j_1} \sum_{j_2=0}^{j_1-1} \frac{1}{j_1-j_2} \dots \sum_{j_m=0}^{j_{m-1}-1} \frac{(z)_{j_m}}{j_m!(j_{m-1}-j_m)} \right\},$$

the B_k are the Bernoulli numbers and $(n)_k := n(n+1)\dots(n+k-1) = \frac{\Gamma(n+k)}{\Gamma(n)}$ and for $m \geq 1$ and $1 \leq j \leq m$, $C_{m,j} := C_{m,j}(z, a) := -\binom{m}{j} \left(\frac{j}{z} + \log a\right) \log^{j-1} a$.

Let denote

$$b_j^{\pm} = \frac{1}{2} \pm \frac{i\theta_j}{\log q} \text{ and } a_j^{\pm}(z) = \frac{(z - \frac{1}{2}) \log q}{2i\pi} \pm \frac{\theta_j}{2\pi}.$$

From [2, Proposition 2.1], for $z \in X'_K = \{z \in X_K \text{ and } \frac{(z-\frac{1}{2})\log q}{2i\pi} \pm \frac{\theta_j}{2\pi} \notin \mathbb{Z}\}$ one has

$$\begin{aligned} Z_K(s, z) = & - \sum_{j=1}^g \frac{1}{\left(z - \frac{1}{2} \pm \frac{i\theta_j}{\log q}\right)^s} + \left(\frac{2i\pi}{\log q}\right)^{-s} \sum_{j=1}^g \zeta_H\left(s, \frac{(z-\frac{1}{2})\log q}{2i\pi} \pm \frac{\theta_j}{2\pi}\right) \\ & + \left(-\frac{2i\pi}{\log q}\right)^{-s} \sum_{j=1}^g \zeta_H\left(s, \frac{-(z-\frac{1}{2})\log q}{2i\pi} \pm \frac{\theta_j}{2\pi}\right) \end{aligned} \quad (15)$$

for $\Re(s) > 1$ and by analytic continuation for all $s \in \mathbb{C}$. The m derivative of (15) with respect to the variable s gives

$$\begin{aligned} Z_K^{(m)}(s, z) = & \sum_{j=1}^g (-1)^{m+1} \frac{\log^m(z - b_j^\pm)}{(z - b_j^\pm)^s} \\ & + \sum_{j=1}^g \sum_{k=0}^m \left[(-1)^{m-k} \binom{m}{k} \left(\frac{2i\pi}{\log q}\right)^{-s} \log^{m-k} \left(\frac{2i\pi}{\log q}\right) \zeta_H^{(k)}(s, a_j^\pm(z)) \right] \\ & + \sum_{j=1}^g \sum_{k=0}^m \left[(-1)^{m-k} \binom{m}{k} \left(-\frac{2i\pi}{\log q}\right)^{-s} \log^{m-k} \left(-\frac{2i\pi}{\log q}\right) \zeta_H^{(k)}(s, -a_j^\pm(z)) \right]. \end{aligned} \quad (16)$$

Now, substituting s by 0 and $-n$ in (16), for large q and $|a_j^\pm(z)| < \pi$, we get an expression for $Z_K^{(m)}(0, z)$, where the terms $\zeta_H^{(k)}(0, a_j^\pm(z))$ (resp. $\zeta_H^{(k)}(-n, a_j^\pm(z))$) can be obtained from Proposition 2.1 by substituting z by -1 and a by $a_j^\pm(z)$ (rep. z by $-n-1$ and a by $a_j^\pm(z)$). Since they are very long formulas we will write them only for $m = 1$ and $s = 0$.

Example 2.2. For $m = 1$ and $s = 0$ one has

$$\begin{aligned} Z'_K(0, z) = & \sum_{j=1}^g \log(z - b_j^\pm) + \sum_{j=1}^g \left(\zeta'_H(0, a_j^\pm(z)) - \log\left(\frac{2i\pi}{\log q}\right) \zeta_H(0, a_j^\pm(z)) \right) \\ & + \sum_{j=1}^g \left(\zeta'_H(0, -a_j^\pm(z)) - \log\left(-\frac{2i\pi}{\log q}\right) \zeta_H(0, -a_j^\pm(z)) \right). \end{aligned} \quad (17)$$

Let us recall that

$$\zeta_H(-n, z) = -\frac{B_{n+1}(z)}{n+1},$$

where $n \in \mathbb{N}$ and B_n denotes the n -th Bernoulli polynomial. If $n = 0$, using $B_1(z) = z - 1/2$, we get $\zeta_H(0, z) = -B_1(z) = 1/2 - z$, then $\zeta_H(0, -z) = z + 1/2$. Furthermore, by (13), we have

$$\begin{aligned} \zeta'_H(0, a) = & (1 - \ln a) \zeta_H(0, a) - \frac{1}{2} - \sum_{k=2}^{\infty} B_k a^{1-k} \sum_{j=0}^{k-1} \frac{(-1)_k}{j!(k-j)} \\ = & (1 - \ln a) \left(\frac{1}{2} - a\right) - \frac{1}{2} - \sum_{k=2}^{\infty} B_k a^{1-k} \sum_{j=0}^{k-1} \frac{(-1)_k}{j!(k-j)}. \end{aligned}$$

Hence, we get

$$Z'_K(0, z) = \sum_{j=1}^g \left[\log \left(\frac{(z - b_j^\pm)(a_j^\pm(z))^{a_j^\pm(z)-1/2}}{(-a_j^\pm(z))^{a_j^\pm(z)+1/2}} \right) + \sum_{k=2}^{\infty} (1 + (-1)^{1+k}) B_k \times (a_j^\pm(z))^{1-k} \sum_{j=0}^{k-1} \frac{(-1)_k}{j!(k-j)} \right].$$

□

2.2 Superzeta functions of the first kind and the Euler-Stieltjes constants

In this subsection, we will consider special values of $Z_K(s, z)$ when s is a positive integer and relate them to the Euler-Stieltjes constants of the second kind $\gamma_K(n)$.

Proof of Theorem 1.1 By differentiating the logarithm of the Hadamard product formula (8), we obtain: for $z \in X_K$ and $n \geq 1$

$$Z_K(n, z) = \frac{(-1)^{n-1}}{(n-1)!} (\log \xi_K(z))^{(n)}.$$

Since the zeros are invariant by $\rho \mapsto 1 - \rho$, one has

$$Z_K(n, z) = (-1)^n Z_K(n, 1 - z).$$

Using $\xi_K(z) = \xi_K(1 - z)$, we get

$$Z_{K,*}(n) = \frac{(-1)^{n-1}}{(n-1)!} \left[(\log \xi_K(z))^{(n)} \right]_{z=1} = \frac{-1}{(n-1)!} \left[\left(\frac{\xi'_K(1-z)}{\xi_K(1-z)} \right)^{(n-1)} \right]_{z=0}. \quad (18)$$

From equations (18) and (11), we obtain the theorem. $\square$

Proposition 2.3. *Let n be a positive integer. We have*

$$Z_{K,*}(n) = \begin{cases} g \log q + \gamma_K(0) & \text{if } n = 1, \\ \sum_{j=1}^n \sum_{l=1}^j (-1)^{j+1} \binom{n}{j} \binom{j}{l} \gamma_K(l-1) & \text{if } n \geq 2. \end{cases}$$

Proof. From [2] p. 19, line 8], one has

$$\sum_{\rho \in \mathbb{Z}(K)} \frac{1}{\rho^n} = \sum_{j=1}^n (-1)^{j+1} \binom{n}{j} \lambda_K(j).$$

Since $\mathbb{Z}(K) = 1 - \mathbb{Z}(K)$, then

$$Z_{K,*}(n) = \sum_{j=1}^n (-1)^{j+1} \binom{n}{j} \lambda_K(j).$$

Hence, the proposition follows from the following formula (see [1] Theorem 2])

$$\lambda_K(j) = j g \log q + \sum_{l=1}^j \binom{j}{l} \gamma_K(l-1)$$

and

$$g \log q \sum_{j=1}^n (-1)^{j+1} j \binom{n}{j} = \begin{cases} g \log q & \text{if } n = 1, \\ 0 & \text{if } n \geq 2. \end{cases}$$

$\square$

3 Superzeta functions of the first kind and the r -depth regularized product

In this section, we derive an expression for the r -depth regularized product associated to the superzeta functions of the first kind.

The zeta regularized product of a complex sequence $(b_n)_{n \in I}$ is defined by

$$\prod_{n \in I} b_n := \exp \left(-\frac{d}{ds} \zeta_b(s) \Big|_{s=0} \right),$$

where $\zeta_b(s) := \sum_{n \in I} b_n^{-s}$ is the zeta function attached to $(b_n)_{n \in I}$, $b_n^{-s} := \exp(-s \log b_n)$, with $\log$ being the principal branch of the logarithm; we assume that ζ_b converges absolutely in some right half-plane, has a meromorphic continuation to a region containing the origin and is holomorphic at the origin.

Let r be a positive integer and consider the function

$$\phi_{K,r}(z) := \exp \left(-\frac{d}{ds} Z_K(s, z) \Big|_{s=1-r} \right). \quad (19)$$

For $r = 1$, the right-hand side of (19) is the zeta regularized product of the sequence $(z - \rho)_{\rho \in Z(K)}$. For $r > 1$, following [4] and [7] we call the function $\phi_{K,r}(z)$ an r -depth regularized product of the sequence $(z - \rho)_{\rho \in Z(K)}$.

Let us consider the Milnor gamma function of depth r defined by

$$\Gamma_r(z) := \exp \left(\frac{d}{ds} \zeta_H(s, z) \Big|_{s=1-r} \right).$$

For $r = 1$, the authors proved in [2] Proposition 3.1] that

$$\begin{aligned} \phi_{K,1}(z) &= \left(\frac{2i\pi}{\log q} \right)^{g \left(\frac{1}{2} - \frac{(z-1/2)\log q}{2i\pi} \right)} \left(-\frac{2i\pi}{\log q} \right)^{g \left(\frac{(z-1/2)\log q}{2i\pi} - \frac{1}{2} \right)} \\ &\quad \times \prod_{j=1}^g \left[(z - b_j^\pm) \left(\frac{\Gamma(a_j^\pm(z)) \Gamma(-a_j^\pm(z))}{2\pi} \right) \right]^{-1}. \end{aligned} \quad (20)$$

In the following theorem we generalize (20).

Theorem 3.1. Let r be a positive integer. We have

$$\begin{aligned} \phi_{K,r}(z) &= \prod_{j=1}^g \left[(z - b_j^\pm)^{-(z-b_j^\pm)^{r-1}} \left(\frac{2i\pi}{\log q} \right)^{-\frac{1}{r} \left(\frac{2i\pi}{\log q} \right)^{r-1} B_r(a_j^\pm(z))} \left(-\frac{2i\pi}{\log q} \right)^{\frac{1}{r} \left(\frac{2i\pi}{\log q} \right)^{r-1} \{B_r(a_j^\pm(z)) + r(a_j^\pm(z))^{r-1}\}} \right. \\ &\quad \left. \times \Gamma_r(a_j^\pm(z))^{-\left(\frac{2i\pi}{\log q} \right)^{r-1}} \Gamma_r(-a_j^\pm(z))^{-\left(-\frac{2i\pi}{\log q} \right)^{r-1}} \right]. \end{aligned} \quad (21)$$

Proof. The first derivative of (15) yields

$$\begin{aligned} -\frac{d}{ds} Z_K(s, z) &= -\sum_{j=1}^g \log(z - b_j^\pm) (z - b_j^\pm)^{-s} \\ &\quad + \log \left(\frac{2i\pi}{\log q} \right) \left(\frac{2i\pi}{\log q} \right)^{-s} \sum_{j=1}^g \zeta_H(s, a_j^\pm(z)) - \left(\frac{2i\pi}{\log q} \right)^{-s} \sum_{j=1}^g \zeta'_H(s, a_j^\pm(z)) \\ &\quad + \log \left(-\frac{2i\pi}{\log q} \right) \left(-\frac{2i\pi}{\log q} \right)^{-s} \sum_{j=1}^g \zeta_H(s, -a_j^\pm(z)) - \left(-\frac{2i\pi}{\log q} \right)^{-s} \sum_{j=1}^g \zeta'_H(s, -a_j^\pm(z)). \end{aligned}$$

Recall that $\zeta_H(1-r, w) = -\frac{B_r(w)}{r}$, then

$$\begin{aligned} -\frac{d}{ds}Z_K(s, z)\Big|_{1-r} &= -\sum_{j=1}^g \log(z - b_j^\pm)(z - b_j^\pm)^{r-1} \\ &\quad -\frac{1}{r} \log\left(\frac{2i\pi}{\log q}\right) \left(\frac{2i\pi}{\log q}\right)^{r-1} \sum_{j=1}^g B_r(a_j^\pm(z)) - \left(\frac{2i\pi}{\log q}\right)^{r-1} \sum_{j=1}^g \log(\Gamma_r(a_j^\pm(z))) \\ &\quad -\frac{1}{r} \log\left(-\frac{2i\pi}{\log q}\right) \left(-\frac{2i\pi}{\log q}\right)^{r-1} \sum_{j=1}^g B_r(-a_j^\pm(z)) - \left(-\frac{2i\pi}{\log q}\right)^{r-1} \sum_{j=1}^g \log(\Gamma_r(-a_j^\pm(z))). \end{aligned}$$

Using $B_r(-x) = (-1)^r B_r(x) + (-1)^r r x^{r-1}$, we obtain

$$\begin{aligned} -\frac{d}{ds}Z_K(s, z)\Big|_{s=1-r} &= -\sum_{j=1}^g \log(z - b_j^\pm)(z - b_j^\pm)^{r-1} \\ &\quad -\frac{1}{r} \log\left(\frac{2i\pi}{\log q}\right) \left(\frac{2i\pi}{\log q}\right)^{r-1} \sum_{j=1}^g B_r(a_j^\pm(z)) \\ &\quad -\frac{1}{r} \log\left(-\frac{2i\pi}{\log q}\right) \left(-\frac{2i\pi}{\log q}\right)^{r-1} \sum_{j=1}^g \{(-1)^r B_r(a_j^\pm(z)) + (-1)^r r (a_j^\pm(z))^{r-1}\} \\ &\quad -\left(\frac{2i\pi}{\log q}\right)^{r-1} \sum_{j=1}^g \log(\Gamma_r(a_j^\pm(z))) - \left(-\frac{2i\pi}{\log q}\right)^{r-1} \sum_{j=1}^g \log(\Gamma_r(-a_j^\pm(z))). \end{aligned}$$

Therefore (21) follows from $\phi_{K,r}(z) := \exp\left(-\frac{d}{ds}Z_K(s, z)\Big|_{s=1-r}\right)$. $\square$

Remark 3.2. The expression of $\phi_{K,r}(z)$ can be written differently using the following identity (see [8, Equation (14)]) in equation (21) :

$$\begin{aligned} \zeta'_H(1-r, w) &= -\frac{1}{r^2} \left(B_r(w) + \frac{r}{2} w^{r-1} \right) \\ &\quad + \frac{1}{r} B_r(w) \log w - \frac{1}{r} \sum_{k=2}^{+\infty} \frac{B_k}{k!} \left[\frac{d}{ds}(s)_k \right]_{s=-r} w^{r-k}, \end{aligned}$$

where $\frac{d}{ds}(s)_k = \sum_{l=0}^{k-1} \frac{(s)_k}{s+1}$ and $(-r)_k = (-1)^k r!/(r-k)!$. $\square$

Let r be a positive integer. Let us consider the polylogarithm function Li_r of degree r which is defined for $|z| < 1$ by $Li_r(z) := \sum_{m=1}^{+\infty} \frac{z^m}{m^r}$. Put $K_r(z) := \exp(-Li_r(z))$ and let $\zeta_K^{(r)}$ be the *poly-zeta-function* defined by

$$\zeta_K^{(r)}(s) = \prod_D K_r\left(\frac{1}{q^{s \deg(D)}}\right)^{-(\log D)^{1-r}}, \quad \Re(s) > 1. \quad (22)$$

Note that when $r = 1$, since $Li_1(z) = -\log(1-z)$ and $K_1(z) = (1-z)$, we have $\zeta_K^{(1)} = \zeta_K$.

In the following proposition, we give another expression for $\phi_{K,r}(z)$ using the poly-zeta-function $\zeta_K^{(r)}$ defined above (similar definition is given by Kurokawa et al. in [4, Section 4.2]).

Proposition 3.3. For $r \geq 1$ and $\Re(z) > 1$, we have

$$\begin{aligned} \phi_{K,r}(z) &= (z-1)^{(z-1)^{1-r}} z^{1-r} \left(\frac{2\pi i}{\log q} \right)^{-\frac{1}{r} \left(\frac{2\pi i}{\log q} \right)^{r-1}} \left[B_r \left(\frac{z \log q}{2\pi i} \right) + B_r \left(\frac{(z-1) \log q}{2\pi i} \right) \right] \\ &\times \left(-\frac{2\pi i}{\log q} \right)^{-\frac{(-1)^r}{r} \left(-\frac{2\pi i}{\log q} \right)^{r-1}} \left\{ B_r \left(\frac{z \log q}{2\pi i} \right) + B_r \left(\frac{(z-1) \log q}{2\pi i} \right) + r \left(-\frac{z \log q}{2\pi i} \right)^{r-1} + r \left(-\frac{(z-1) \log q}{2\pi i} \right)^{r-1} \right\} \\ &\times \left[\Gamma_r \left(\frac{z \log q}{2\pi i} \right) \Gamma_r \left(\frac{(z-1) \log q}{2\pi i} \right) \right]^{-\left(\frac{2\pi i}{\log q} \right)^{r-1}} \\ &\times \left[\Gamma_r \left(-\frac{z \log q}{2\pi i} \right) \Gamma_r \left(-\frac{(z-1) \log q}{2\pi i} \right) \right]^{-\left(-\frac{2\pi i}{\log q} \right)^{r-1}} \\ &\times \left(\zeta_K^{(r)}(z) \right)^{(-1)^r (r-1)!}. \end{aligned}$$

Proof. By [2] Proposition 4.1], we have

$$\begin{aligned} &(-1)^r (r-1)! \log \zeta_K^{(r)}(z) \\ &= \frac{\log(z-1)}{(z-1)^{1-r}} + \frac{\log z}{z^{1-r}} \\ &+ \frac{1}{r} \left(\frac{2\pi i}{\log q} \right)^{r-1} \log \left(\frac{2\pi i}{\log q} \right) \left[B_r \left(\frac{z \log q}{2\pi i} \right) + B_r \left(\frac{(z-1) \log q}{2\pi i} \right) \right] \\ &+ \frac{(-1)^r}{r} \left(-\frac{2\pi i}{\log q} \right)^{r-1} \log \left(-\frac{2\pi i}{\log q} \right) \left\{ B_r \left(\frac{z \log q}{2\pi i} \right) + B_r \left(\frac{(z-1) \log q}{2\pi i} \right) + r \left(-\frac{z \log q}{2\pi i} \right)^{r-1} + r \left(-\frac{(z-1) \log q}{2\pi i} \right)^{r-1} \right\} \\ &+ \left(\frac{2\pi i}{\log q} \right)^{r-1} \log \left(\Gamma_r \left(\frac{z \log q}{2\pi i} \right) \Gamma_r \left(\frac{(z-1) \log q}{2\pi i} \right) \right) \\ &+ \left(-\frac{2\pi i}{\log q} \right)^{r-1} \log \left(\Gamma_r \left(-\frac{z \log q}{2\pi i} \right) \Gamma_r \left(-\frac{(z-1) \log q}{2\pi i} \right) \right) \\ &- \frac{d}{ds} Z_K(s, z) \Big|_{s=1-r}. \end{aligned}$$

We finish the proof by using $\phi_{K,r}(z) = \exp \left(-\frac{d}{ds} Z_K(s, z) \Big|_{s=1-r} \right)$. □

Remark 3.4. Let us note that for $r = 1$ and $\Re(z) > 1$ we get (see [2] Corollary 4.4])

$$\phi_K(z) = z(z-1) \left(\frac{2\pi i}{\log q} \right)^{1 - \frac{(2z-1) \log q}{2\pi i}} \left(-\frac{2\pi i}{\log q} \right)^{1 + \frac{(2z-1) \log q}{2\pi i}} \left[\left(\frac{\Gamma \left(\frac{\pm z \log q}{2\pi i} \right)}{\sqrt{2\pi}} \right) \left(\frac{\Gamma \left(\frac{\pm(z-1) \log q}{2\pi i} \right)}{\sqrt{2\pi}} \right) \zeta_K(z) \right]^{-1}.$$

□

4 Concluding remarks

The zeros of the function ζ_K are denoted by

$$\rho_{k,j}^{\pm} = \frac{1}{2} + i\tau_{k,j}^{\pm}, \quad \text{where } \tau_{k,j}^{\pm} = \frac{\pm\theta_j + 2k\pi}{\log q}, \quad j = 1, \dots, g \text{ and } k \in \mathbb{Z}.$$

As in [2] and [12, Chapter 8 and 9], the superzeta functions of the second kind $\mathcal{Z}_K$ and the third kind $\mathfrak{Z}_K$ are defined by

$$\mathcal{Z}_K(s, t) = \sum_{k \in \mathbb{Z}} \sum_{j=1}^g \frac{1}{((\tau_{k,j}^{\pm})^2 + t^2)^s}, \quad \Re(s) > \frac{1}{2},$$

where $t \in \mathbb{C}$ such that $t^2 + (\tau_{k,j}^\pm)^2 \notin \mathbb{R}_-$ for all k , and

$$\mathfrak{Z}_K(s, \tau) = \sum_{k \in \mathbb{Z}} \sum_{j=1}^g \frac{1}{(\tau_{k,j}^\pm + \tau)^s}, \quad \operatorname{Re}(s) > 1,$$

where $\tau \in \mathbb{C}$ such that $\tau + \tau_{k,j}^\pm \notin \mathbb{R}_-$ for all $j = 1, \dots, g$.

As Voros did in [12] (9.3) and (9.4), pp. 87-88] for the classical zeta function, a perspective of this paper is to describe the family of $\mathfrak{Z}_K$ using that of Z_K and get similar results for superzeta functions of the third kind as for superzeta functions of the first kind and the second kind (see [2]).

References

- [1] K. H. Bllaca, K. Mazhouda, Explicit formula on function fields and application: Li coefficients, *Ann. Mat. Pura Appl.* (4) 200 (5) (2021) 1859–1869.
- [2] K. H. Bllaca, J. Khmiri, K. Mazhouda, B. Sodaïgui, Superzeta functions on function fields, *Finite Fields Appl.* (95) (2024), Paper No. 102367, 22 pp.
- [3] E. Elizalde, A simple recurrence for the higher derivatives of the Hurwitz zeta function, *J. Math. Phys.* (34) (7) (1993) 3222–3226.
- [4] N. Kurokawa, M. Wakayama, Y. Yamasaki, Milnor-Selberg zeta functions and zeta regularizations, *J. Geom. Phys.* (64) (2013) 120–145.
- [5] K. Mazhouda, L. Smajlović, Evaluation of the Li coefficients on function fields and applications, *Eur. J. Math.* (5) (2019) (2) 540–550.
- [6] Hj. Mellin, Über die nullstellen der Zetafunktion, *Ann. Acad. Sci. Fenn. A* 10 (11) (1917).
- [7] J. Milnor, On polylogarithms, Hurwitz zeta functions and the Kubert identities, *Enseign. Math.* (29) (1983) 281–322.
- [8] S. Rudaz, Note on asymptotic series expansions for the derivative of the Hurwitz zeta function and related functions, *J. Math. Phys.* (31) (1990) (12) 2832–2834.
- [9] G.D.V. Salvador, Topics in the theory of algebraic function fields, in: Nolan Wallach Ed., *Mathematics: Theory and Applications*, Birkhäuser (2006).
- [10] R. Seri, A non-recursive formula for the higher derivatives of the Hurwitz zeta function, *J. Math. Anal. Appl.* (424) (2015) (1) 826–834.
- [11] H. Stichtenoth, *Algebraic function fields and codes*, 2nd ed., GTM, vol. 254, Springer-Verlag, Berlin, 2009.
- [12] A. Voros, *Zeta functions over zeros of zeta functions*, Lecture Notes of UMI, vol. 8, Springer, 2010.
- [13] A. Weil, Sur les courbes algébriques et les variétés qui s’en déduisent, *Publ. Inst. Math. Univ. Strasbourg* (7) (1945). *Actualités Scientifiques et Industrielles* [Current Scientific and Industrial Topics], No. 1041 Hermann & Cie, Paris, 1948. iv+85 pp.



ISSN: 2820-7114

Moroccan Journal of Algebra and Geometry with Applications

Supported by Sidi Mohamed Ben Abdellah University, Fez, Morocco

Volume 4, Issue 1 (2025), pp 38-45

Title :

Rings in which every S -prime ideal is prime

Author(s):

Chahrazade Bakkari and Rachid Hachache

Rings in which every S -prime ideal is prime

Chahrazade Bakkari¹ and Rachid Hachache²

¹ Department of Mathematics, Faculty of Science, University Moulay Ismail Meknes, Morocco.
e-mail: cbakkari@hotmail.com

² Department of Mathematics, Faculty of Science, University Moulay Ismail Meknes, Morocco.
e-mail: rachid.hachache@hotmail.com

Communicated by Moutu Abdou Salam Moutui

(Received 09 May 2024, Revised 30 October 2024, Accepted 15 November 2024)

Abstract. In this paper, we study the S - α -ring property, that is a ring in which every S -prime ideal is prime. We investigate the possible transfer of this property to various context of commutative ring extensions including homomorphic image, localization, trivial ring extensions and amalgamation rings. Our results provide new classes of commutative rings satisfying the above property.

Key Words: S -prime ideal, prime ideal, S - α -ring, localization, trivial ring extension, amalgamation ring.

2020 MSC: 13F05, 13A15, 13E05, 13F20, 13C10, 13C11, 13F30, 13D05.

Dedicated to our Professor David E. Dobbs for his 80th Birthday.

1 Introduction

Throughout this paper, all rings are assumed to be commutative with nonzero identity and all modules are unital. The notion of prime ideal plays an important role in commutative ring theory. Several generalizations of the concept of a prime ideal are studied in the literature for example, almost prime, strongly prime, weakly prime and S -prime. In this paper, we are interested with the S -prime ideal property introduced by Ahmed Hamed and Achraf Malek [18]. Let A be a ring. Recall that a nonempty set S of A is said to be a multiplicative set if: $0 \notin S$, $1 \in S$ and $ab \in S$ for all $a, b \in S$. A proper ideal P of A disjoint with S is called S -prime if there exists $s \in S$ such that for all $a, b \in A$ with $ab \in P$, then $sa \in P$ or $sb \in P$. Equivalently, if there exists $s \in S$ such that for all ideals I, J of A , if $IJ \subset P$, then $sI \subset P$ or $sJ \subset P$ (see [18]). A proper ideal P of A disjoint with S is called S -weakly prime if there exists an $s \in S$ such that for all $a, b \in A$ if $0 \neq ab \in P$, then $sa \in P$ or $sb \in P$ (see [24]). Clearly, every prime ideal is S -prime, however the converse is not true in general. There is no investigation on the following natural question: when are every S -prime ideal is prime? To answer this question we will study a specific class of rings that satisfy this condition.

Let A be a ring and E an A -module. The trivial ring extension of A by E (also called the idealization of E over A) is a ring defined as follows:

$$R := A \ltimes E := \{(a, e) | a \in A \text{ and } e \in E\}$$

under the usual addition and the multiplication defined by $(a_1, e_1)(a_2, e_2) = (a_1a_2, a_1e_2 + a_2e_1)$ for all $(a_1, e_1), (a_2, e_2) \in A \ltimes E$. It is clear that $(1, 0)$ is the identity of $A \ltimes E$, and if S is a multiplicative

subset of A , then $S \propto E$, and $S \propto 0$ are multiplicative subsets of $A \propto E$. Trivial ring extensions play an important role in commutative ring theory due to their effectiveness of producing new classes of examples and counter examples of rings subject to various ring theoretic properties (see counter-examples [4, 5, 6, 8, 21, 22, 23]).

In [11], M. D'Anna considered a different type of construction, obtained involving a ring A and an ideal $I \subseteq A$, which is denoted by $A \bowtie I$ and defined as the following subring of $A \times A$.

$$A \bowtie I := \{(a, a + i) \mid a \in A, i \in I\}$$

This extension has been studied, in the general case, and from the different point of view of pull-backs, by D'anna and Fontana [10]. One main difference of this construction with respect to the idealization is that the ring $A \bowtie I$ is reduced whenever A is reduced.

Let A and B be two rings, let J be an ideal of B and let $f : A \longrightarrow B$ be a ring homomorphism. In this setting, we consider the following subring of $A \times B$:

$$A \bowtie^f J := \{(a, f(a) + j) \mid a \in A \text{ and } j \in J\}$$

called the amalgamation of A and B along J with respect to f . This construction is a generalization of the amalgamated duplication of a ring along an ideal denoted $A \bowtie^f J$ (introduced and studied by D'Anna and Fontana in [10]). Motivations and additional applications of the amalgamation are discussed in detail in [9, 10, 12, 13, 14, 15, 16].

In this paper, we introduce and study the class of rings in which every S -prime ideal is prime (S - α -ring). We next study the possible transfer of the property that every S -prime ideal is prime in direct product, homomorphic image, localization, trivial ring extensions, and the amalgamated algebra along an ideal, in order to give new examples.

2 Main Results

Let R be a ring and S be a multiplicative set of R . Recall from [18] that an ideal P of R disjoint with S is said to be an S -prime ideal of R if there exists an $s \in S$ such that for all $a, b \in R$ if $ab \in P$, then $sa \in P$ or $sb \in P$.

Definition 2.1. A ring R with multiplicative set S is called S - α -ring if every S -prime ideal of R disjoint with S is prime.

Example 2.2. Let $R = D$ be a integral domain and $S = D \setminus \{0\}$ be a multiplicative set of R , then R is S - α -ring.

Let R be a ring, $S \subseteq R$ be a multiplicative set and I an ideal of R . Assume that $I \cap S = \emptyset$. Notice that $\overline{S} = \{s + I \mid s \in S\}$ is a multiplicative subset of R/I .

Remark 2.3. Let R be a ring and $S \subseteq R$ be a multiplicative set.

1. If $S \subseteq U(R)$, then R is an S - α -ring.
2. Let P an ideal of R disjoint with S . If $Z(R/P) \cap \overline{S} = \emptyset$, then the S -prime ideals of R are exactly the prime ideals of R .

3. Let $S_1 \subseteq S_2$ be two multiplicative subsets of R , and P be an ideal of R disjoint with S_2 . If P is a S_1 -prime of R , then P is S_2 -prime. However, the converse is not true in general. Indeed, let $R = \mathbb{Z}[X]$, $S = \{2^n/n \in \mathbb{N}\}$ and $T = \{1\} \subseteq U(R)$. Then $T \subseteq S$ are two multiplicative subsets of R . Let $P = 4X\mathbb{Z}[X]$. By [18] Example 1], P is an S -prime ideal of R . Note that P is not a T -prime ideal of R because $4X \in P$ but neither $1.4 \in P$ nor $1.X \in P$.

Proof. 1. Trivial.

2. We can use the same proof as in [18] Example 2]. □

Proposition 2.4. *Let A be a ring and $S_1 \subseteq S_2$ be two multiplicatively closed subsets of A . If A is an S_2 - α -ring, then A is an S_1 - α -ring.*

Proof. Assume that A is an S_2 - α -ring. Let I be an S_1 -prime ideal of A . Then I is S_2 -prime ideal of A by Remark 2.3], and so I is a prime ideal of A . Hence, A is an S_1 - α -ring, as desired. □

Proposition 2.5. *Let R be a ring, $S \subseteq R$ be a multiplicative set and I an ideal of R disjoint with S . If R is an S - α -ring, then R/I is an $\bar{S}$ - α -ring.*

To prove the previous proposition, we need the following lemma.

Lemma 2.6. [18] Proposition 3]

Let R be a commutative ring with identity, $S \subset R$ be a multiplicative set and I be an ideal of R disjoint with S . Let P be a proper ideal of R containing I such that $P/I \cap \bar{S} = \emptyset$. Then P is an S -prime ideal of R if and only if P/I is an $\bar{S}$ -prime ideal of R/I .

Proof. Assume that R is an S - α -ring. Let P/I be an ideal of R/I is $\bar{S}$ -prime such that $P/I \cap \bar{S} = \emptyset$. By Lemma 2.6], P is an S -prime ideal of R . Since A is an S - α -ring, then P is a prime ideal and hence P/I is a prime ideal of R/I , as desired. □

Proposition 2.7. *Let $R = R_1 \times R_2$ be a ring, where R_1 and R_2 are two rings and $S = S_1 \times S_2$ be a multiplicative set of R , with S_1 and S_2 are multiplicative sets of R_1 and R_2 respectively. If R is an S - α -ring, then R_1 is S_1 - α -ring and R_2 is S_2 - α -ring.*

Proof. If $R = R_1 \times R_2$ is an S - α -ring, then by Proposition 2.5], R_1 is an S_1 - α -ring and R_2 is S_2 - α -ring, as $R_1 \simeq R/(0 \times R_2)$ and $R_2 \simeq R/(R_1 \times 0)$. □

The converse of Proposition 2.7] is not true in general, as shown in the following example.

Example 2.8. Let D be an integral domain, $R_1 = R_2 = D$ and $S_1 = S_2 = D \setminus \{0\}$, where S_i is a multiplicative set of A_i for $i = 1, 2$. Then R_1 is an S_1 - α -ring and R_2 is an S_2 - α -ring. However, $R = R_1 \times R_2$ is not an $(S_1 \times S_2)$ - α -ring.

Proof. By Example 2.2], R_1 is an S_1 - α -ring and R_2 is an S_2 - α -ring. Let P_1 be an S_1 -prime ideal of R_1 . Then P_1 is prime, since R_1 is an S_1 - α -ring and consider an S_2 -prime ideal P_2 of R_2 . Likewise. P_2 is prime. So, $P = P_1 \times P_2$ is an $(S_1 \times S_2)$ -prime ideal of $R = R_1 \times R_2$ by [28] Lemma 2.13]. However, P is not always a prime ideal, as desired. □

Recall that the prime ideals of a decomposable ring $R_1 \times R_2$ are $P_1 \times R_2$ and $R_1 \times P_2$ where P_1 (resp., P_2) is a prime ideal of R_1 (resp., R_2).

Theorem 2.9. Let $R = R_1 \times R_2$ be a ring, where R_1 and R_2 are two rings and $S = (S_1 \times S_2) \subseteq R$ be a multiplicative set. If R is an S - α -ring, then $S_1 \subseteq U(R_1)$ and $S_2 \subseteq U(R_2)$ (i.e, $S = S_1 \times S_2 \subseteq U(R_1 \times R_2)$).

Proof. Assume that $S_1 \not\subseteq U(R_1)$. Then there exists $a \in S_1 \setminus U(R_1)$, and let P_2 be a prime ideal of R_2 . Set $P = aR_1 \times P_2$, as $(P : (a, 1)) = R_1 \times P_2$ is a prime ideal of R , we get that P is an S -prime of R by [18, Proposition 1]. Thus P is a prime ideal of R since R is S - α -ring, a contradiction since $aR_1 \neq R_1$ and $P_2 \neq R_2$, as desired. $\square$

Let R be a ring and S be a multiplicative set of R . Recall from [24] that an ideal P of R disjoint with S is said to be an S -weakly prime ideal of R if there exists an $s \in S$ such that for all $a, b \in R$ if $0 \neq ab \in P$, then $sa \in P$ or $sb \in P$.

Remark 2.10. Let R be an integral domain, and S be a multiplicative subset of R . Then R is an S - α -ring if and only if every S -weakly prime ideal of R is prime.

Proof. Assume that R is an S - α -ring. Since R is a domain, then every S -weakly prime ideal of R is S -prime, and so every S -prime ideal is prime, as R is an S - α -ring. Consequently, every S -weakly prime ideal of R is prime. The converse is straightforward, as desired. $\square$

Proposition 2.11. Let (A, M) be a zero-dimensional local ring which is not a field, and S be a multiplicative subset of A . Then A is an S - α -ring if and only if M is the only S -prime ideal of A .

Proof. Assume that A is an S - α -ring. Let I be an S -prime ideal of A . Then I is a prime ideal of A . If $I \subseteq M$, then we get $\dim(A) \geq 1$, which is a contradiction. The converse is trivial. $\square$

Let S be a multiplicative subset of R , $S^* = \{r \in R \mid \frac{r}{1} \text{ is unit in } S^{-1}A\}$ denotes the saturation of S . Observe that S^* is a multiplicative subset containing S . A multiplicative subset S of A is called saturated if $S = S^*$. It is clear that S^* is always a saturated multiplicative subset of R .

Proposition 2.12. Let A be a ring, S be a multiplicative subset of R . Then A is an S - α -ring if and only if A is an S^* - α -ring.

To prove the previous proposition, we need the following lemmas.

Lemma 2.13. Let $S_1 \subseteq S_2$ be multiplicative subsets of A such that for any $s \in S_2$, there is an element $t \in S_1$ satisfying $st \in S_1$. If P is an S_2 -prime ideal of A , then P is an S_1 -prime ideal of A .

Proof. Let $a, b \in A$ such that $ab \in P$. So, there is $s \in S_2$ such that $sa \in P$ or $sb \in P$. From assumption, $s' = st \in S_1$ for some $t \in S_2$, and so $s'a \in P$ or $s'b \in P$. Consequently, P is an S_1 -prime ideal of A , as desired. $\square$

Lemma 2.14. [7, Proposition 5.1]

Let A be a ring, S be a multiplicative subset of A and P be an ideal of A disjoint with S . Then P is an S -prime ideal of A if and only if P is an S^* -prime ideal.

Proof. Assume that A is an S^* - α -ring. Then A is an S - α -ring by Proposition [2.4]. Conversely, assume that A is an S - α -ring. Let P be an S^* -prime ideal of A . Then P is an S -prime ideal of A by Lemma [2.14]. Therefore, P is a prime ideal of A . Hence, A is an S^* - α -ring, as desired. $\square$

Let $A \propto E$ be the trivial ring extension of a ring A by an A -module E . Note that if S is a multiplicative set of A , then $S \propto E$ and $S \propto 0$ are multiplicative subsets of $A \propto E$.

Theorem 2.15. Let A be a ring, E be an A -module, $R = A \propto E$ be the trivial ring extension of A by E and $S \subseteq A$ be a multiplicative set of A . Then the following statements hold:

- (1) If R is an $(S \propto E)$ - α -ring, then A is an S - α -ring.

(2) Assume that A is an integral domain, $K = qf(A)$, E be a K -vector space, and set $R = A \rtimes E$ be the trivial ring extension of A by E . Then the following assertions are equivalent:

- i) R is an $(S \rtimes 0)$ - α -ring.
- ii) A is an S - α -ring.
- iii) R is an $(S \rtimes E)$ - α -ring.

To prove this theorem, we need the following lemmas.

Lemma 2.16. [4 Corollary 3.4]

Let R be an integral domain and E be an R -module. Then the following conditions are equivalent:

- (1) Every ideal of $R \rtimes E$ is comparable to $0 \rtimes E$.
- (2) Every ideal of $R \rtimes E$ has the form $I \rtimes E$ or $0 \rtimes F$ for some ideal I of R or sub-module F of E .
- (3) Every ideal of $R \rtimes E$ is homogeneous.
- (4) E is divisible.

Lemma 2.17. Let A be an integral domain, $K = qf(A)$, E be a K -vector space, $R = A \rtimes E$ be the trivial ring extension of A by E and $S \subseteq A$ be a multiplicative set of A . Consider an ideal J of R . Then J is an $(S \rtimes E)$ -prime ideal of R if and only if $J = I \rtimes E$ where I is an S -prime ideal of A .

Proof. Assume that J is an $(S \rtimes E)$ -prime ideal of R . Then by Lemma 2.16, two cases are then possible:

Case 1: $J = I \rtimes E$ with I an ideal of A . Then we show that I is an S -prime ideal of A . Let $a, b \in A$ such that $ab \in I$. Hence, $(a, 0)(b, 0) = (ab, 0) \in I \rtimes E$ and so, there exists $(s, e) \in S \rtimes E$ such that $(s, e)(a, 0) \in I \rtimes E$ or $(s, e)(b, 0) \in I \rtimes E$, then either $sa \in I$ or $sb \in I$ and hence I is S -prime.

Case 2: $J = 0 \rtimes F$ with $F \neq E$ sub-module of E . In this case, we show that J is not $(S \rtimes E)$ -prime. Assume by the way of contradiction that J is $(S \rtimes E)$ -prime. Then there exists $(s, t) \in S \rtimes E$ for every $(a, e), (b, f) \in R$ such that $(a, e)(b, f) \in J$, then $(s, t)(a, e) \in J$ or $(s, t)(b, f) \in J$. Let $x \in E \setminus F$. Since $sE = E$, then $x = sy$ for some $y \in E$. On the other hand, $(0, y)(0, y) = (0, 0) \in J$, since J is $(S \rtimes E)$ -prime, so $(s, t)(0, y) = (0, sy) = (0, x) \in J$ thus $x \in F$, which is absurd.

Conversely, assume that $J = I \rtimes E$ where I is an S -prime ideal of A . Let $(a, e), (b, f) \in A \rtimes E$ such that $(a, e)(b, f) = (ab, af + be) \in J$. Thus, $ab \in I$ and so either $sa \in I$ or $sb \in I$ for some $s \in S$. Consequently, $(s, 0)(a, e) \in I \rtimes E$ or $(s, 0)(b, f) \in I \rtimes E$, making J , an $(S \rtimes E)$ -prime ideal of R , as desired. $\square$

Proof of Theorem 2.15

- (1) Assume that R is an $(S \rtimes E)$ - α -ring. Let I be an S -prime ideal of A and $(a, e), (b, f) \in A \rtimes E$ such that $(a, e)(b, f) = (ab, af + be) \in I \rtimes E$. Then $ab \in I$ and so either $sa \in I$ or $sb \in I$ for some $s \in S$. Consequently, $(s, 0)(a, e) \in I \rtimes E$ or $(s, 0)(b, f) \in I \rtimes E$. Therefore, $I \rtimes E$ is an $(S \rtimes E)$ -prime ideal of $A \rtimes E$, and so $I \rtimes E$ is a prime ideal of R . Now, let $a, b \in A$ with $ab \in I$. Then $(a, 0)(b, 0) \in I \rtimes E$, and so $(a, 0) \in I \rtimes E$ or $(b, 0) \in I \rtimes E$. Consequently, $a \in I$ or $b \in I$, making I , a prime ideal of A . Hence, A is an S - α -ring.

- (2) (i) $\Rightarrow$ (ii). Trivial.

(ii) $\Rightarrow$ (iii). Assume that A is an S - α -ring. By Lemma 2.16, every ideal of $A \rtimes E$ has the form $I \rtimes E$ or $0 \rtimes F$ for some ideal I of A or sub-module F of E .

Let J be an $(S \rtimes E)$ -prime ideal of R . Then by Lemma 2.17, $J = I \rtimes E$ for some ideal I of A . Let $a, b \in A$ such that $ab \in I$. Hence $(a, 0)(b, 0) = (ab, 0) \in I \rtimes E$, and so there exists $s \in S$ such

that $(s, 0)(a, 0) \in I \propto E$ or $(s, 0)(b, 0) \in I \propto E$. Therefore, either $sa \in I$ or $sb \in I$ and hence I is an S -prime ideal of A . So, I is a prime ideal of A , as A is an S - α -ring. Let $(a, e), (b, f) \in A \propto E$ with $(a, e)(b, f) = (ab, af + be) \in I \propto E$. Then $ab \in I$, and so $a \in I$ or $b \in I$. Consequently, $(a, e) \in I \propto E$ or $(b, f) \in I \propto E$, making J , a prime ideal of R .

(iii) $\Rightarrow$ (i). This follows from Proposition 2.4 as $S \propto 0 \subseteq S \propto E$. $\square$

Example 2.18. Let $A = D$ be an integral domain, $S = D \setminus \{0\}$ be a multiplicative set of A and E be an A -module. Since A is an S - α -ring, then $R = D \propto E$ is an $(S \propto E)$ - α -ring by assertion (2) of Theorem 2.15.

Theorem 2.19. Let (D, M) be a local domain with a prime element a of D , $S \subseteq D$ be a multiplicative set of D with $S \not\subseteq U(D)$, E be an D -module such that $ME = 0$, and let $R = D \propto E$ be the trivial ring extension of D by E . Then $J = (a, 1)R$ is an $(S \propto E)$ -prime ideal of R which is not prime. In particular, R is not an $(S \propto E)$ - α -ring.

Proof. We first claim that J is an $(S \propto E)$ -prime ideal of R . Indeed, consider a non-unit element $(s, t) \in S \propto E$. Let $(x, e), (y, f) \in R$ such that $(x, e)(y, f) \in J$. If $x \notin M$, then (x, e) is a unit and so $(y, f) \in J$ and therefore, $(s, t)(y, f) \in J$. Similarly, if $y \notin M$, then $(s, t)(x, e) \in J$. On the other hand, $(x, e)(y, f) = (xy, 0) = (a, 1)(b, d)$ hence $xy = ab \in aD$, so $x \in aD$ or $y \in aD$. Without loss of generality, we may assume that $x \in aD$. Thus $x = ad$ hence $(s, t)(x, e) = (sx, 0) = (sad, 0) = (sd, 0)(a, 1) \in J$. Hence, $J = (a, 1)R$ is $(S \propto E)$ -prime. Next, we claim that J is not a prime ideal of R . Indeed, from [23, Example 2.5], it follows that $J = (a, 1)R$ is not homogeneous, and so $\text{Nil}(R) \not\subseteq J = (a, 1)R$. Thus J is not prime ideal of R . In particular, R is not an $(S \propto E)$ - α -ring, as desired. $\square$

The next example illustrates Theorem 2.19.

Example 2.20. Let $(D, M) = (\mathbb{Z}_2, 2\mathbb{Z}_2)$ be a local domain, $S \subseteq D$ be a multiplicative set, with $S \not\subseteq U(D)$, and $E = D/M$ a D -module. Then $R = D \propto E$ is not an $(S \propto E)$ - α -ring by Theorem 2.19.

Let S be a multiplicative set of a ring A . Notice that $S' = \{(s, f(s)) \mid s \in S\}$. Observe that S' is a multiplicative set of $A \bowtie^f J$. Also, if $0 \notin f(S)$ then $f(S)$ is a multiplicative set of B . Set $T = \{I \bowtie^f J \mid I \text{ ideal of } A\}$. Our next result establishes the transfer of the S - α -ring property to amalgamation rings.

Theorem 2.21. Let (A, B) be a pair of rings, J be an ideal of B , $f : A \rightarrow B$ be a ring homomorphism, and S be a multiplicative set of A . Then the following statements hold :

- (1) If $A \bowtie^f J$ is an S' - α -ring, then A is an S - α -ring.
- (2) Assume that $f^{-1}(J) = \{0\}$. Then $A \bowtie^f J$ is an S' - α -ring if and only if $f(A) + J$ is an $f(S)$ - α -ring.
- (3) A is an S - α -ring if and only if every S' -prime ideal of $A \bowtie^f J$ in T is prime.

Proof. (1) Assume that $A \bowtie^f J$ is an S' - α -ring. Let I be an S -prime ideal of A . We first show that $I \bowtie^f J$ is an S' -prime ideal of $A \bowtie^f J$. Let $(a, f(a) + i), (b, f(b) + j) \in A \bowtie^f J$ with $(a, f(a) + i)(b, f(b) + j) \in I \bowtie^f J$. Then $ab \in I$ which is S -prime and so there exists $s \in S$ such that $sa \in I$ or $sb \in I$. One can easily check that $(s, f(s))(a, f(a) + i) \in I \bowtie^f J$ or $(s, f(s))(b, f(b) + j) \in I \bowtie^f J$. Consequently, $I \bowtie^f J$ is an S' -prime ideal of $A \bowtie^f J$ which is prime, as $A \bowtie^f J$ is an S' - α -ring. Let $a, b \in A$ such that $ab \in I$. Then $(a, f(a))(b, f(b)) \in I \bowtie^f J$, and so $(a, f(a)) \in I \bowtie^f J$ or $(b, f(b)) \in I \bowtie^f J$. It follows that $a \in I$ or $b \in I$. Finally, I is a prime ideal of A , making A , an S - α -ring.

- (2) This due to the fact that $A \bowtie^f J \simeq f(A) + J$, as $f^{-1}(J) = 0$.

- (3) Assume that A is an S - α -ring. Let $I \bowtie^f J$ be an S' -prime ideal of $A \bowtie^f J$ in T . We claim that $I \bowtie^f J$ is a prime ideal of $A \bowtie^f J$. Let $a, b \in A$ with $ab \in I$. Then $(a, f(a))(b, f(b)) \in I \bowtie^f J$. So, there exists $(s, f(s)) \in S'$ such that $(s, f(s))(a, f(a)) \in I \bowtie^f J$ or $(s, f(s))(b, f(b)) \in I \bowtie^f J$. It follows that $sa \in I$ or $sb \in I$. Therefore, I is a prime ideal of A since A is an S - α -ring. Let $(a, f(a) + i), (b, f(b) + j) \in A \bowtie^f J$ with $(a, f(a) + i)(b, f(b) + j) = (ab, f(a)j + f(b)i + ij) \in I \bowtie^f J$. Then $ab \in I$ and so $a \in I$ or $b \in I$. Consequently, it follows that $(a, f(a) + i) \in I \bowtie^f J$ or $(b, f(b) + j) \in I \bowtie^f J$, making $I \bowtie^f J$, a prime ideal of $A \bowtie^f J$. The converse is straightforward. $\square$

Next, let I be a proper ideal of A . The (amalgamated) duplication of A along I is a special amalgamation given by

$$A \bowtie I := \{(a, a + i) \mid a \in A, i \in I\}$$

Note that if S is a multiplicative set of A , then $S' = \{(s, s) \mid s \in S\}$ is a multiplicative set of $A \bowtie I$. Set $T' = \{K \bowtie I \mid K \text{ ideal of } A\}$. The next corollary is an immediate consequence of assertion (3) of Theorem 2.21

Corollary 2.22. *Let A be a ring, I an ideal of A and S be a multiplicative set of A . Then A is an S - α -ring if and only if every S' -prime ideal of $A \bowtie I$ in T' is prime.*

References

- [1] F. A. Almahdi, E. M. Bouba and M. Tamekkante, On weakly S -prime ideals of commutative rings, An. Ştiinţ. Univ. "Ovidius" Constanţa Ser. Mat. 29 (2021), no. 2, 173-186.
- [2] D. D. Anderson and T. Dumitrescu, S -Noetherian rings, Comm. Algebra 30 (2002), no. 9, 4407-4416.
- [3] D. D. Anderson and E. Smith, Weakly prime ideals, Houston J. Math. 29 (2003), no. 4, 831-840.
- [4] D. D. Anderson and M. Winders, Idealization of a module, J. Commut. Algebra 1 (2009), no. 1, 3-56.
- [5] M. M. Ali, Idealization and Theorems of D. D. Anderson, Comm. Algebra 34 (2006), no. 12, 4479-4501.
- [6] M. M. Ali, Idealization and Theorems of D. D. Anderson II, Comm. Algebra 35 (2007), no. 9, 2767-2792.
- [7] M. Aqalmoun, S -prime ideals in principal domain, J. Indones. Math. Soc. 29 (2023), no. 1, 93-98.
- [8] C. Bakkari, S. Kabbaj and N. Mahdou, Trivial extension defined by Prüfer conditions, J. Pure Appl. Algebra 214 (2010), no. 1, 53-60.
- [9] M. D'Anna, C.A. Finocchiaro and M. Fontana, Amalgamated algebras along an ideal, in: Commutative Algebra and Applications, Proceedings of the Fifth International Fez Conference on Commutative Algebra and Applications, Fez, Morocco, 2008, W. de Gruyter Publisher, Berlin, 2009, pp. 155-172.
- [10] M. D'Anna and M. Fontana, An amalgamated duplication of a ring along an ideal: the basic properties, J. Algebra Appl. 6 (2007), no. 3, 443-459.
- [11] M. D'Anna, A construction of Gorenstein rings, J. Algebra 306 (2006), no. 2, 507-519.

- [12] M. D'Anna and M. Fontana, The amalgamated duplication of a ring along a multiplicative-canonical ideal, *Ark. Mat.* 45 (2007), no. 2, 241-252.
- [13] M. D'Anna, C. A. Finacchiaro, and M. Fontana, Amalgamated algebras along an ideal, *Commutative Algebra and Applications*, Walter De Gruyter, (2009), 241-252.
- [14] M. El Ouarrachi, N. Mahdou, and A. Mimouni, On Armendariz-like properties in Amalgamated algebras along ideals, *Turkish J. Math.* 41 (2017), no. 6, 1673-1686.
- [15] A. El Khalfi, H. Kim and N. Mahdou, Amalgamation extension in commutative ring theory, a survey, *Moroccan J. Algebra Geom. Appl.* 1(1) (2022), 139-182.
- [16] A. El Khalfi, H. Kim, and N. Mahdou, Amalgamated Algebras Issued from ϕ -Chained Rings and ϕ -Pseudo-Valuation Rings, *Bull. Iranian Math. Soc.* 47 (2021), no. 5, 1599-1609.
- [17] J. A. Huckaba, *Commutative Coherent Rings with Zero Divisors*, Marcel Dekker, New York Basel, (1988).
- [18] A. Hamed and A. Malek, S -prime ideals of a commutative ring, *Beitr. Algebra Geom.* 61 (2020), no. 3, 533-542.
- [19] A. Hamed, S -strong Mori domain of $A + XB[X]$, *Moroccan J. Algebra Geom. Appl.* 1(2) (2022), 183-188.
- [20] A. Hamed, Generalized S -prime ideals of commutative rings, *Moroccan J. Algebra Geom. Appl.*, 1(1) (2024), 1-9.
- [21] S. Kabbaj and N. Mahdou, Trivial Extensions Defined by Coherent-like Conditions, *Comm. Algebra* 32 (2004), no. 10, 3937-3953.
- [22] S. Kabbaj, Matlis' semi-regularity and semi-coherence in trivial ring extensions: a survey, *Moroccan J. Algebra Geom. Appl.*, 1(1) (2021), 1-17.
- [23] S. Kabbaj and N. Mahdou, Trivial extensions defined by coherent-like conditions, *Comm. Algebra* 32 (2004), no. 10, 3937-3953.
- [24] N. Mahdou, M. A. S. Moutui and Y. Zahir, On S -Weakly prime ideals of commutative rings, *Georgian Math. J.* 29 (2022), no. 3, 397-405.
- [25] N. Mahdou, M. A. S. Moutui and Y. Zahir, Weakly prime ideals issued from an amalgamated algebra, *Hacet. J. Math. Stat.* 49 (2020), no. 3, 1159-1167.
- [26] N. Mahdou, A. E. Khalfi and Y. Zahir, Rings in which every nonzero weakly prime ideal is prime, *São Paulo J. Math. Sci.* 14 (2020), no. 2, 689-697.
- [27] N. Mahdou, A. Mimouni and Y. Zahir, On weakly prime ideals and weak Krull dimension, *Moroccan J. Algebra Geom. Appl.* 2(2) (2023), 307-314.
- [28] E. S. Sevim, T. Arabaci and U. Tekir, S. Koc, On S -prime submodules, *Turkish J. Math.* 43 (2019), no. 2, 1036-1046.



ISSN: 2820-7114

Moroccan Journal of Algebra and Geometry with Applications

Supported by Sidi Mohamed Ben Abdellah University, Fez, Morocco

Volume 4, Issue 1 (2025), pp 46-53

Title :

Finite direct projective Covers and Envelopes

Author(s):

Sonal Gupta, Manoj Kumar Patel and Ashok Ji Gupta

Finite direct projective Covers and Envelopes

Sonal Gupta¹, Manoj Kumar Patel² and Ashok Ji Gupta³

¹ Department of Mathematical Sciences, IIT(BHU), Varanasi, 221005, India.

e-mail: sonalgupta.rs.mat17@itbhu.ac.in

² Department of Mathematics, National Institute of Technology Nagaland, Dimapur, 797103, India.

e-mail: manoj@nitnagaland.ac.in

³ Department of Mathematical Sciences, IIT(BHU), Varanasi, 221005, India.

e-mail: agupta.apm@itbhu.ac.in

Communicated by Najib Mahdou

(Received 02 June 2024, Revised 08 November 2024, Accepted 17 November 2024)

Abstract. In this paper, we explore the concept of finite direct projective covers and envelopes. We identify the conditions under which a projective cover of a module is finite direct projective cover. Additionally, we provide descriptions of modules with finite direct projective covers in the context of semi-perfect and semi-regular rings. We also discuss the properties of finite direct projective envelopes.

Key Words: Finite direct projective module, semi-perfect ring, semi-regular ring.

2020 MSC: Primary 16D10, 16E50, 16E60, 16S50.

Dedicated to our Professor David E. Dobbs for his 80th Birthday.

1 Introduction

Unless otherwise stated, this work takes into account rings that are associative with unity and modules that are unital-right modules. Direct injective and direct projective modules were first presented in 1976 by Nicholson [10]. The concept of direct projective modules is dual to that of direct injective modules. Direct injective refers to a module if any submodule isomorphic direct summand is also a direct summand. And a module M is said to be direct projective if for any submodule T of M and a direct summand K of M , such that $M/T \cong K \leq \bigoplus M$, then T is a direct summand of M . Finite direct injective modules were first introduced by Maurya and Gupta in 2018 [7], and defined as, if a finitely generated submodule K of a module M is isomorphic to a direct summand T of a module M , then K is a direct summand of M . In [4] the idea of finite direct injective modules is dualized to finite direct projective modules. Let M be a finite direct projective module and K and T submodules of M such that $M/T \cong K \leq \bigoplus M$ and K is finitely generated, then T is a direct summand of M . A projective module P is called a projective cover of a module M , if epimorphism $f : P \rightarrow M$ exists and $\text{Ker}(f)$ is a small submodule of P .

In section 2, we introduce the concept of a finite direct projective cover of a module. A finite direct projective module S is called a finite direct projective cover of a module M , if epimorphism $f : S \rightarrow M$

exists and $\text{Ker}(f)$ is a small submodule of S . The paper contains several results related to finite direct projective covers. We show if the direct sum of a projective module and a finitely generated module has a finite direct projective cover, then the finitely generated module has a projective cover (Proposition 2.7). We characterized that if every finitely generated submodule of an R -module M has a finite direct projective cover, then R is a semi-perfect ring (Proposition 2.11). We also show that every finite direct projective cover is a projective cover, if a module is finitely generated (Proposition 2.8). Finally, we characterized the semi-regular ring with finite direct projective cover. If every finitely presented R -module M has a finite direct projective cover, then R is a semi-regular ring (Proposition 2.13). The section concludes with an example that illustrates not all modules possess a finite direct projective cover.

In section 3, we explore the extension of the projective envelope as the finite direct projective envelope. In particular, we investigate the condition under which a 2-generated R -module M has a finite direct projective envelope and our study shows that this condition is satisfied if and only if R is a semi-simple Artinian ring (Proposition 3.4). Furthermore, we provide an example illustrating that every module need not have a finite direct projective envelope (Example 3.5). Additionally, we show that the ring is a S -ring if and only if every 2-generated flat module has a finite direct projective envelope (Proposition 3.8).

2 Finite Direct Projective Cover

This section discusses the finite direct projective covers and some of their related properties. We begin by defining the finite direct projective cover of a module.

Definition 2.1. A finite direct projective module S is a finite direct projective cover of module M if there is an epimorphism $f : S \rightarrow M$ such that the kernel of f , denoted $\text{Ker}(f)$, is a small submodule of S .

Note 2.2. This paper will only focus on R -module M that is not finite direct projective. This means that we will consider non-trivial coverings of M by other modules. It is worth noting that any finite direct projective module is a cover for itself, as the identity R -homomorphism has a kernel zero, which is always minimal.

Proposition 2.3. Let $M = M_1 \oplus M_2$ for some direct summands M_1 and M_2 with M_2 finitely generated. If M is finite direct projective and $f : M_1 \rightarrow M_2$ is a homomorphism and $\text{Img}(f) \leq \oplus M_2$, then $\text{Ker}(f) \leq \oplus M_1$.

Proof. Follows from proof of Proposition 2.3 [4].

Corollary 2.4. Let $M = M_1 \oplus M_2$ for some direct summands M_1 and M_2 with M_2 finitely generated. If M is finite direct projective and $f : M_1 \rightarrow M_2$ is an epimorphism, then $\text{Ker}(f) \leq \oplus M_1$.

Proof. Follows from above Proposition.

Proposition 2.5. Let P be any projective module, and $P \oplus M$ is a finite direct projective module and M is a finitely generated module. If an epimorphism exists from P to M , then M is a projective module.

Proof. Since $P \oplus M$ is a finite direct projective module and f is an R -epimorphism from P to M . Therefore from above Corollary, $\text{Ker}(f) \leq \oplus P$. Hence, f splits and M is a projective module.

Corollary 2.6. Let module $R \oplus M$ be a finite direct projective module, where M is finitely generated. If an epimorphism exists from R to M , then R is a semi-simple ring.

Proof. Follows from the Proposition [2.5](#).

Proposition 2.7. Let P be a projective module and M be a finitely generated module. If $P \oplus M$ has a finite direct projective cover. Then projective cover exists for M if there exists an epimorphism $f : P \rightarrow M$.

Proof. Suppose we have an epimorphism $f : P \rightarrow M$. Let $g : S \rightarrow P \oplus M$ be a finite direct projective cover of $P \oplus M$. We define an exact sequence $0 \rightarrow g^{-1}(M) \rightarrow S \rightarrow P \rightarrow 0$. This sequence splits as inclusion $g^{-1}(M)$ to S has splitting which is $\pi \circ g$, where $\pi : P \oplus M \rightarrow M$ is a projection map. Hence, by the property of exact sequences, we know that $S \cong P \oplus g^{-1}(M)$. We can define $g' = g|_{g^{-1}(M)}$ and construct another exact sequence $0 \rightarrow \text{Ker}(g) \rightarrow g^{-1}(M) \rightarrow M \rightarrow 0$. Since $\text{Ker}(g)$ is small in S , we can conclude that $\text{Ker}(g) = \text{Ker}(g')$ is small in $g^{-1}(M)$, and $g' : g^{-1}(M) \rightarrow M$ is an epimorphism. We only need to prove that $g^{-1}(M)$ is a projective module. Also, we know that $S = P \oplus g^{-1}(M)$ is a finite direct projective module where P is projective. By setting $f = g' \circ h$, where $\text{Ker}(g)$ is small in $g^{-1}(M)$, we can conclude that h is an epimorphism such that $h : P \rightarrow g^{-1}(M)$, from Corollary 5.15 [\[1\]](#). By using Proposition [2.5](#), we conclude $g^{-1}(M)$, is a projective module. Therefore, M has a projective cover.

Proposition 2.8. Every finitely generated R -module M has a finite direct projective cover if and only if it has a projective cover.

Proof. For a given finitely generated module M , we can always find a free module F of finite rank such that there is an epimorphism $f : F \rightarrow M$. Since $F \oplus M$ is finitely generated, it has a finite direct projective cover. By Proposition [2.7](#), we can conclude that M has a projective cover. The converse is straightforward to verify.

Corollary 2.9. Every finitely generated R -module M has a finite direct projective cover if R is a local ring.

Proof. From the fact, if R is a local ring, every finitely generated module possesses a projective cover [\[2\]](#) Example 2].

Corollary 2.10. Let M be a Noetherian module. Then every submodule of M has finite direct projective cover if and only if it has a projective cover.

Proof. Follows from Proposition [2.8](#).

Proposition 2.11. The following statements are equivalent for a ring R :

1. R is a semi-perfect ring;
2. Every 2-generated R -module M has a finite direct projective cover;
3. Every finitely generated submodule of an R -module M has a finite direct projective cover.

Proof. (1) $\Rightarrow$ (2) and (1) $\Rightarrow$ (3) are clear. Since R is a semi-perfect ring, every finitely generated submodule of an R -module M has a projective cover, equivalent to M has a finite direct projective cover.

(2) $\Rightarrow$ (1) To demonstrate that R is semi-perfect, we must show that each finitely generated module M has a projective cover. Since M has a finite number of generators, there exists an epimorphism $g : F \rightarrow M$, where F is a free R -module of finite rank. Because $F \oplus M$ is finitely generated, it has a finite

direct projective cover. By applying Proposition 2.7, we can then conclude that M has a projective cover.

(3) $\Rightarrow$ (1) Follows from Proposition 2.8

Corollary 2.12. *Every module over the perfect ring has a finite direct projective cover.*

Proof. Follows from Proposition 2.11 since every perfect ring is semi-perfect.

Let us revisit the definition of finitely presented modules. An R -module M is said to be finitely presented or finitely related if there exists an exact sequence $0 \rightarrow T \rightarrow F \rightarrow M \rightarrow 0$ of R -modules, where F is free with finite rank and T is finitely generated. A ring is called semi-regular if every finitely presented module has a projective cover.

Proposition 2.13. *The following statements are equivalent for a ring R :*

1. R is a semi-regular ring;
2. Every finitely presented R -module M has a finite direct projective cover.

Proof. (1) $\Rightarrow$ (2) Since R is semi-regular, every finitely presented module has a projective cover.

(2) $\Rightarrow$ (1) Let R module M is finitely presented, and there exists an exact sequence of R -modules $0 \rightarrow T \rightarrow F \rightarrow M \rightarrow 0$, where T is a finitely generated R -module and F is a free module of finite rank. Since module $F \oplus M$ is finitely presented and has a finite direct projective cover. This implies that there exists a finite direct projective module covering $F \oplus M$. Since every finitely presented module is finitely generated, it follows from Proposition 2.7 that M has a projective cover.

Next, we recall that a module M is finitely generated and coherent if it is a finitely presented module. We now seek to establish a condition for a coherent module over a semi-regular ring with respect to a finite direct projective cover.

Corollary 2.14. *Let M be a finitely generated and coherent module over a semi-regular ring. Then it has a finite direct projective cover.*

Proof. Follows from the definition of the coherent module and the Proposition 2.13.

In the following example, we show that every R -module M need not have a finite direct projective cover.

Example 2.15. Consider the $\mathbb{Z}$ -module $M = \mathbb{Z} \oplus \mathbb{Z}_2$. We assert that M does not have a finite direct projective cover. If M has a finite direct projective cover, then $\mathbb{Z}_2$ has a projective cover follows from Proposition 2.7. Since we know that $\mathbb{Z}_2$ do not have a projective cover because of the epimorphism $f : \mathbb{Z} \rightarrow \mathbb{Z}_2$ and $\text{Ker}(f) = 2\mathbb{Z}$, which is not small since $2\mathbb{Z} + 3\mathbb{Z} = \mathbb{Z}$. As a result, we get our assertion that M does not have a finite direct projective cover.

Remark 2.16. Based on the above example, we conclude that the direct sum of two finite direct projective modules need not have a finite direct projective cover.

Proposition 2.17. *Let M_1 and M_2 be two finitely generated modules with finite direct projective covers. Then $M_1 \oplus M_2$ has a finite direct projective cover.*

Proof. Since M_1 and M_2 are finitely generated modules with finite direct projective covers. Therefore, from Proposition 2.8, M_1 and M_2 have projective covers. The proof follows from Theorem 7.23, [2].

Note 2.18. The above Proposition follows for the sum of a finite family of finitely generated modules M_k 's.

3 Finite Direct Projective Envelope

In this section, we will study finite direct projective envelopes.

Definition 3.1. If F is a finite direct projective module, as shown in the diagrams below, then a R -homomorphism $f : M \rightarrow F$ is said to have a finite direct projective envelope of M .

$$\begin{array}{ccc} M & \xrightarrow{f} & F \\ & \searrow f' & \downarrow \exists \Phi' \\ & & F' \end{array}$$

where F' is a finite direct projective module, the diagram below

$$\begin{array}{ccc} M & \xrightarrow{f} & F \\ & \searrow f & \downarrow \exists \Phi \\ & & F \end{array}$$

can be commuted only by an automorphism Φ .

Example 3.2. Every right R -module has a finite direct projective envelope if R is right perfect and left coherent ring. This follows from Proposition 3.5, [8] as the projective envelope also acts as a finite direct projective envelope.

Lemma 3.3. [4 2.1] *The direct summand of a finite direct projective module is a finite direct projective module.*

The following claim uses the fact that if all cyclic modules over the ring are projective, then the ring is a semi-simple Artinian ring [3].

Proposition 3.4. *The following statements are equivalent for a ring R :*

1. R is a semi-simple Artinian ring;
2. Every 2-generated R -module has a finite direct projective envelope.

Proof. (1) $\Rightarrow$ (2) If E is a 2-generated R -module over a semi-simple Artinian ring, then E is a semi-simple module. Therefore, E is a finite direct projective module, and its envelope is trivial.

(2) $\Rightarrow$ (1) To show that every cyclic module N of M is projective, consider a two-generated R -module $E = N \oplus R$. By assumption, E has a finite direct projective envelope.

$$\begin{array}{ccc} E & \xrightarrow{f} & F \\ & \searrow p_R & \downarrow \exists \Phi \\ & & R \end{array}$$

$$\begin{array}{ccc}
 E & \xrightarrow{f} & F \\
 & \searrow p_N & \downarrow \exists \alpha \\
 & & N
 \end{array}$$

with canonical projections p_N and p_R , respectively. Let $f : E \rightarrow F$ be a finite direct-projective envelope. Since R and N are both finite direct-projective modules, there exist R -homomorphisms $\phi : F \rightarrow R$ and $\alpha : F \rightarrow N$ such that $\phi \circ f = p_R$ and $\alpha \circ f = p_N$. Define an R -homomorphism $g : F \rightarrow N \oplus R$ as $g = \alpha + \phi$ for each $x \in F$. It can be easily verified that g is a well-defined function, and also $g \circ f(x) = (\alpha + \phi) \circ f(x) = p_N(x) + p_R(x) = x$. This implies that g is a split R -epimorphism, so we have $E \cong K \leq^\oplus F$. Every direct summand of a finite direct-projective module is also a finite direct-projective module, according to Lemma 3.3. As a result, E is a finite direct-projective module. Every onto homomorphism $h : R \rightarrow N$ splits, therefore we can use Proposition 2.5 to determine that N is projective since R is projective.

Proposition 3.5. *Let R be a ring and I be an ideal of R such that R/I is a finitely generated finite direct projective module and I is not the direct summand of R . Then R module $M = R \oplus R/I$ has no finite direct projective envelope.*

Proof. We will prove our claim using contradiction. Let R -homomorphism f be a finite direct projective envelope of M . Then the following diagrams must commute,

$$\begin{array}{ccc}
 M & \xrightarrow{f} & F \\
 & \searrow p_R & \downarrow \exists \phi \\
 & & R
 \end{array}$$

$$\begin{array}{ccc}
 M & \xrightarrow{f} & F \\
 & \searrow p_{R/I} & \downarrow \exists \alpha \\
 & & R/I
 \end{array}$$

Let p_R and $p_{R/I}$ be the canonical projections of M . Since both R and R/I are finite direct projective modules and $f : M \rightarrow F$ is a finite direct projective envelope of M , we can find R -homomorphisms $\phi : F \rightarrow R$ and $\alpha : F \rightarrow R/I$ such that $\phi \circ f = p_R$ and $\alpha \circ f = p_{R/I}$. We define a function $g : F \rightarrow M$ by $g = \alpha + \phi$ for each $x \in F$. We can easily check that g is well-defined and that $g \circ f = i_M$, which implies that g is a split R epimorphism and M is isomorphic to a direct summand K of F , denoted $M \cong K \leq^\oplus F$. However, every direct summand of a finite direct projective module is finite direct projective. Every epimorphism $f' : R \rightarrow R/I$ splits. Hence I is a direct summand of R , which is false. Therefore, there exists no finite direct projective envelope for M .

Example 3.6. For $\mathbb{Z}$ -module $M = \mathbb{Z} \oplus \mathbb{Z}_n$, $n \in \mathbb{N}$ where $\mathbb{Z}_n$ is finitely generated finite direct projective module over $\mathbb{Z}$. So module M has no finite direct projective envelope (Follows from above Proposition).

Remark 3.7. Similarly, as Remark 2.16, we assert that the direct sum of two finite direct projective modules may not have a finite direct projective envelope.

The following proposition shows an equivalence between S -rings and a 2-generated flat module, which possesses a finite direct projective envelope. From [12], a ring R is called a right S -ring if every

finitely generated flat right R -module is projective.

Proposition 3.8. *The following statements are equivalent:-*

1. R is S -ring;
2. Every 2-generated flat R -module has finite direct projective envelope.

Proof. (1) $\Rightarrow$ (2) Let R be a S -ring. Then every finitely generated flat R -module is a projective module. Hence has identity homomorphism as a projective envelope which is also a finite direct projective envelope.

(2) $\Rightarrow$ (1) In particular, we prove this result for cyclic flat R -module and that can be easily extended for finitely generated flat R -modules. We must prove that every cyclic flat R -module M is projective. Let us consider $T = M \oplus R$, where T is a 2-generated flat R -module with a finite direct projective envelope. Therefore the following diagram must commute,

$$\begin{array}{ccc} T & \xrightarrow{f} & F \\ & \searrow p_R & \downarrow \exists \phi \\ & & R \end{array}$$

$$\begin{array}{ccc} T & \xrightarrow{f} & F \\ & \searrow p_M & \downarrow \exists \alpha \\ & & M \end{array}$$

with p_R and p_M be the canonical projections of T , and R and M are both finite direct-projective modules. Moreover, let $f : T \rightarrow F$ be a finite direct projective envelope. Then, there exist homomorphisms $\phi : F \rightarrow R$ and $\alpha : F \rightarrow M$ such that $\phi \circ f = p_R$ and $\alpha \circ f = p_M$. Now, we define a homomorphism $g : F \rightarrow M \oplus R$ such that $g(x) = \alpha(x) + \phi(x)$ for each $x \in F$. Since g is well-defined and satisfies $g \circ f(x) = (\alpha + \phi) \circ f(x) = p_M(x) + p_R(x) = x$. Thus, g is a split R -epimorphism, and we have $T \cong K \leq^{\oplus} F$. Using Lemma 3.3, we know that every direct summand of a finite direct-projective module is also finite direct-projective. Therefore, T is a finite direct-projective module. Additionally, since M is a cyclic module, an epimorphism $h : R \rightarrow M$ exists. Using Proposition 2.5, epimorphism h splits therefore M is a projective module.

Acknowledgements: The authors would like to extend their heartfelt thanks to the anonymous referee for their meticulous review of the paper and for providing insightful feedback and suggestions that helped to enhance the overall quality of the manuscript.

References

- [1] F. W. Anderson, and K. R. Fuller, Rings and categories of modules, Springer Science and Business Media, Vol. 13, 1992.
- [2] P. E. Bland, Rings and their modules, Walter De Gruyter, 2011.
- [3] S. C. Geol, S. K. Jain, and S. Singh, Rings whose cyclic modules are injective or projective. Proc. Amer. Math. Soc., 53(1) (1975), 16–18.

- [4] S. Gupta, and A. J. Gupta, Finite direct projective modules, Asian Euro. J. of Math., 16(12) (2023), 2350218.
- [5] D. V. Huynh, and P. F. Smith, Some rings characterised by their modules. Comm. in Algebra, 18(6) (1990), 1971–1988.
- [6] Y. Ibrahim, M. T. Kosan, T. C. Quynh, and M. Yousif, Simple-direct-projective modules, Comm. in Algebra, 44(12) (2016), 5163–5178.
- [7] S. K. Maurya, and A. J. Gupta, Finite-direct-injective modules. Int. Electr. J. of Algebra, 23(23) (2018), 143–152.
- [8] J. A. Mayor, and J. M. Hernandez, On flat and projective envelopes, J. of algebra, 160(2) (1993), 434–440.
- [9] S. H. Mohamed, and B. J. Müller, Continuous and discrete modules, Cambridge University Press, Vol. 147, 1990.
- [10] W. K. Nicholson, Semiregular modules and rings, Can. J. of Math., 28(5) (1976), 1105–1120.
- [11] B. M. Pandeya, and A. J. Gupta, Characterizations of Rings using Direct Projective modules, Int. J. of Math. Sci., 3(1) (2004), 53–60.
- [12] G. Puninski, and P. Rothmaler, When every finitely generated flat module is projective. J. of Algebra, 277(2) (2004), 542–558.
- [13] R. Wisbauer, Foundations of module and ring theory, Gordon and Breach Science Publishers, 1991.
- [14] W. Xue, Characterization of rings using direct projective modules and direct injective modules, J. of pure and app. algebra, 87(1) (1993), 99–104.
- [15] M. Yousif, I. Amin, and Y. Ibrahim, D3-Modules. Comm. in Algebra, 42(2) (2014), 578–592.



ISSN: 2820-7114

Moroccan Journal of Algebra and Geometry with Applications

Supported by Sidi Mohamed Ben Abdellah University, Fez, Morocco

Volume 4, Issue 1 (2025), pp 54-61

Title :

Weakly S-2-prime ideals of commutative rings

Author(s):

Sanem Yavuz, Bayram Ali Ersoy, Ünsal Tekir, and Ece Yetkin Çelikel

Weakly S -2-prime ideals of commutative rings

Sanem Yavuz¹, Bayram Ali Ersoy², Ünsal Tekir³ and Ece Yetkin Çelikel⁴

^{1,2} Department of Mathematics, Yildiz Technical University, Istanbul, Türkiye.

e-mail: ssanemy@gmail.com, ersoya@gmail.com

³ Department of Mathematics, Marmara University, Istanbul, Türkiye.

e-mail: utekir@marmara.edu.tr

⁴ Department of Software Engineering, Hasan Kalyoncu University, Gaziantep, Türkiye.

e-mail: yetkinece@gmail.com, ece.celikel@hku.edu.tr

Communicated by Suat Koç

(Received 26 May 2024, Revised 18 November 2024, Accepted 21 November 2024)

Abstract. The objective of this paper is to introduce and investigate the concept of weakly S -2-prime ideals which are extensions of weakly 2-prime ideals in commutative rings. Let R be a commutative ring with identity and S be a multiplicative subset of R with $1 \in S$. A proper ideal Q of R with $Q \cap S = \emptyset$ is called a weakly S -2-prime ideal of R if there exists an $s \in S$ such that for all $\alpha, \beta \in R$ with $0 \neq \alpha\beta \in Q$, we have $s\alpha^2 \in Q$ or $s\beta^2 \in Q$. Various characterizations of weakly S -2-prime ideals are given and the relationship between weakly S -2-prime ideals and other classical ideals are illustrated by a diagram. For this relationship, a myriad of supporting examples and counter examples are presented. Moreover, this class of ideals is analyzed in idealization rings and amalgamated duplication along an ideal. Besides, the rings over which every weakly S -2-prime ideal is S -2-prime ideal is examined.

Key Words: 2-prime ideals, S -2-prime ideals, weakly 2-prime ideals, weakly S -2-prime ideals.

2020 MSC: Primary 13A15, 13C05; Secondary 13A99.

Dedicated to our Professor David E. Dobbs for his 80th Birthday.

1 Introduction

In this article, we only take into consideration on commutative rings with identity and unitary modules. Unless otherwise stated, R will always describe such a ring and M will be such an R -module. The concept of prime ideals and its generalizations have a crucial role in commutative algebra as they have many applications in different research areas. For instance, prime ideals and their generalizations were used to characterize specific rings such as fields, Von-Neumann regular rings, and Dedekind domains. As it is well-known a proper ideal Q of R is called a prime ideal if $\alpha, \beta \in R$ such that $\alpha\beta \in Q$ refers that $\alpha \in Q$ or $\beta \in Q$. In 2003, Anderson and Smith [2] introduced the notion of weakly prime ideals which is a generalization of prime ideals in order to examine factorization in commutative rings with zero divisors. A proper ideal Q of R is called weakly prime if $0 \neq \alpha\beta \in Q$ for some $\alpha, \beta \in R$ implies that $\alpha \in Q$ or $\beta \in Q$. Afterwards, many studies generalizing prime ideals

have been done. One of them was the work entitled S -prime ideals by Hamed and Malek [7]. Recall that a subset S of R is called multiplicatively closed subset (in briefly m.c.s) if S is closed under multiplication and $1 \in S$. Let S be a m.c.s of R and Q be an ideal with $Q \cap S = \emptyset$. According to their paper [7], Q is called an S -prime ideal of R if there exists an $s \in S$ such that for all $\alpha, \beta \in R$ with $\alpha\beta \in Q$, we have $s\alpha \in Q$ or $s\beta \in Q$. Moreover, Almahdi et. al. [1] described weakly S -prime ideals so as to characterize S -Noetherian rings and S -principal ideal rings. An ideal Q disjoint with S is said to be a weakly S -prime ideal if there exists an element $s \in S$ such that for all $\alpha, \beta \in R$ whenever $0 \neq \alpha\beta \in Q$ implies $s\alpha \in Q$ or $s\beta \in Q$. On the other hand, Beddani and Messirdi [4] introduced and studied 2-prime ideals which is a different generalization of prime ideals and they used this notion to present specific characterizations of valuation rings. A proper ideal Q of R is called a 2-prime ideal if $\alpha, \beta \in R$ such that $\alpha\beta \in Q$, then either $\alpha^2 \in Q$ or $\beta^2 \in Q$. This class of ideals is examined by Nikandish et.al. as well [12]. Furthermore, Koç [10] defined weakly 2-prime ideals and examined compactly packedness and coprimely packedness on trivial extention. Moreover, Issoual et.al. [8] further investigated properties of this concept of ideals. Q is called a weakly 2-prime ideal of R if whenever $0 \neq \alpha\beta \in Q$ for some $\alpha, \beta \in R$, then either $\alpha^2 \in Q$ or $\beta^2 \in Q$. As a recent research, in [14] the concept of S -2-prime ideals is defined. A proper ideal Q of R with $Q \cap S = \emptyset$ is called an S -2-prime ideal of R if there exists an $s \in S$ such that for all $\alpha, \beta \in R$ with $\alpha\beta \in Q$, we have $s\alpha^2 \in Q$ or $s\beta^2 \in Q$. As usual, for any proper ideal Q of R , the radical of Q is defined by the intersection of all prime ideals containing Q , denoted by $\sqrt{Q}$ which is equivalent to the set $\{r \in R : r^n \in Q \text{ for some } n \in \mathbb{N}\}$ in commutative rings. In particular, $\sqrt{0_R} = Nil(R)$.

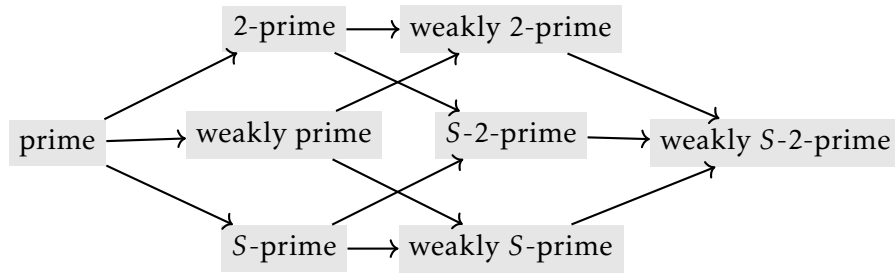
Our aim of this study is to introduce weakly S -2-prime ideals which are generalization of S -2-prime ideals. A proper ideal Q of R disjoint with S is called a weakly S -2-prime ideal if there exists an $s \in S$ such that for all $\alpha, \beta \in R$ with $0 \neq \alpha\beta \in Q$, we have $s\alpha^2 \in Q$ or $s\beta^2 \in Q$. We give a chart which demonstrate the relationship among weakly S -2-prime ideals and other classical ideals such as 2-prime ideal, S -prime ideal, weakly S -prime ideal etc. with several supporting examples. Besides, we investigate the behavior of weakly S -2-prime ideals under homomorphism, in the direct product of rings and in localization rings (Theorems 2.9-2.12, Proposition 2.13). Furthermore, we discuss weakly S -2-prime ideals in trivial extention rings and amalgamated duplication along an ideal which is defined by [3, 6, 11] (Theorems 2.14-2.15). Finally, with the help of [5, 9, 13], we give the rings over which every weakly S -2-prime ideal is S -2-prime ideal (Propositions 2.16, 2.17).

2 Properties of Weakly S -2-Prime Ideals

Definition 2.1. Let S be a m.c.s of a ring R and Q be a proper ideal of R with $Q \cap S = \emptyset$. Then, Q is called a weakly S -2-prime ideal of R if there exists an $s \in S$ such that for all $\alpha, \beta \in R$ with $0 \neq \alpha\beta \in Q$, we have $s\alpha^2 \in Q$ or $s\beta^2 \in Q$. In this case, Q is called associated to s .

The diagram below shows the relationship among weakly S -2-prime ideals with other classical ideals.

Every weakly 2-prime ideal of R disjoint with S is weakly S -2-prime ideal of R , where S is a m.c.s of R . If S consists of units of R , then weakly 2-prime ideals and weakly S -2-prime ideals are coincide. Otherwise, these are distinct notions. The following examples are given to verify that the rows above are not reversible. (see also [1, Examples 2-3], [2, Example 20], [7, Example 1], [10, Examples 1-2], [12, Example of the ideal $9\mathbb{Z}$ of the ring $\mathbb{Z}$] and [14, Example 3]).



Example 2.2. (Weakly S -2-prime ideal which is not weakly 2-prime) Let $R = \mathbb{Z}[X]$ and $S = \{5^n \mid n \in \mathbb{N}\}$. Consider $Q = 5X\mathbb{Z}[X]$. It is clear that $Q \cap S = \emptyset$ and Q is a weakly S -2-prime ideal of R . Indeed, if $0 \neq fg \in Q = 5X\mathbb{Z}[X]$ for all $f, g \in R$, then since $Q \subset X\mathbb{Z}[X]$ and $X\mathbb{Z}[X]$ is a prime ideal of R , we have $X|f$ or $X|g$. Hence, $5f^2 \in Q$ or $5g^2 \in Q$ for $s := 5$. However, Q is not a weakly 2-prime ideal since $0 \neq 5 \cdot X \in Q$ but $5^2 \notin Q$ and $X^2 \notin Q$.

Example 2.3. (S -2-prime ideal which is not 2-prime) Consider $R = \mathbb{Z}$, $Q = 24\mathbb{Z}$ and $S = \{3^n \mid n \in \mathbb{N}\}$. Then, Q is not a 2-prime ideal of R since $6 \cdot 4 \in Q$ but $6^2, 4^2 \notin Q$. However, Q is an S -2-prime ideal of R . Indeed, it is clear that $Q \cap S = \emptyset$. Let $\alpha, \beta \in \mathbb{Z}$ such that $\alpha\beta \in Q$. Since $\alpha\beta \in 8\mathbb{Z}$ and $8\mathbb{Z}$ is a primary ideal of R , we have either $\alpha \in 8\mathbb{Z}$ or $\beta \in \sqrt{8\mathbb{Z}} = 2\mathbb{Z}$. Put $s := 3$. In the former case, we conclude that $s\alpha^2 \in Q$. Suppose that the latter case holds. If $\beta \in 2\mathbb{Z} \setminus 4\mathbb{Z}$, then it is clear that $\alpha \in 4\mathbb{Z}$, and we have $s\alpha^2 \in Q$. If $\beta \in 4\mathbb{Z}$, then $s\beta^2 \in Q$, so we are done.

Example 2.4. (Weakly S -2-prime ideal which is not S -2-prime) Suppose that p, q are distinct prime numbers and $R = \mathbb{Z}_{pq^2}$, $S = \{\bar{s}^n \mid n \in \mathbb{N} \text{ and } s \text{ is a prime number with } s \neq p, q\}$ and consider $Q = (\bar{0})$. Then, Q is a weakly S -2-prime ideal of R . However, Q is not an S -2-prime ideal of R since $\bar{p} \cdot \bar{q}^2 \in Q$ but $s \cdot \bar{p}^2 \notin Q$ and $s \cdot \bar{q}^4 \notin Q$ for all $s \in S$.

Note that if R is a Von-Neumann regular ring, then every weakly S -2-prime ideal is weakly S -prime ideal. However, these are different concepts.

Example 2.5. (Weakly S -2-prime ideal which is not weakly S -prime) Suppose that K is a field and $R = K[X, Y]$, where X and Y are indeterminates. Let $Q = (XY, Y^2)$ and S be the set of constant polynomials from K . Suppose that $0 \neq g(X, Y)h(X, Y) \in Q \subseteq \sqrt{Q} = (Y)$. This implies that either $Y|g(X, Y)$ or $Y|h(X, Y)$. Thus, $sg^2(X, Y) \in Q$ or $sh^2(X, Y) \in Q$ for all $s \in S$, and so Q is a weakly S -2-prime ideal. However, Q is not a weakly S -prime ideal of R as $0 \neq Y \cdot Y \in Q$ but $s \cdot Y \notin Q$ for all $s \in S$.

Theorem 2.6. Let S be a m.c.s of R and Q be a weakly S -2-prime ideal of R . If Q is not an S -2-prime ideal of R , then $Q^2 = (0)$. In this case, $\sqrt{Q} = \sqrt{0_R}$.

Proof. Assume that $Q^2 \neq (0)$. We claim that Q is an S -2-prime ideal of R . Let $x, y \in R$ such that $xy \in Q$. If $0 \neq xy \in Q$, then there exists an $s \in S$ such that $sx^2 \in Q$ or $sy^2 \in Q$, as desired. If $0 = xy \in Q$, we have three cases. Firstly, if $xQ \neq 0$, then there exists an $m \in Q$ such that $0 \neq xm$, and so $0 \neq xm = x(m+y) \in Q$. Therefore, there exists an $s \in S$ such that $sx^2 \in Q$ or $s(m+y)^2 \in Q$. Thus, we have $sx^2 \in Q$ or $sy^2 \in Q$. Secondly, if $yQ \neq 0$, we achieve a similar result. Finally, let $xQ = 0$ and $yQ = 0$. Because of $Q^2 \neq 0$, then there exist $m, n \in Q$ such that $mn \neq 0$. Therefore, $0 \neq mn = (x+m)(y+n) \in Q$. Then, there exists an $s \in S$ such that $s(x+m)^2 \in Q$ or $s(y+n)^2 \in Q$. Thus, we have $sx^2 \in Q$ or $sy^2 \in Q$. From all of cases, we conclude that Q is an S -2-prime ideal of R . $\square$

Consequently, one can observe that any weakly S -2-prime ideal Q of R with $\text{Nil}(R) \not\supseteq Q$ is an S -2-prime ideal of R . In particular, if R is a reduced ring, then a proper ideal Q disjoint with S is a weakly S -2-prime ideal of R if and only if $Q = (0)$ or Q is an S -2-prime ideal of R . The next example is given to show that the situation $Q^2 = (0)$ in the Theorem 2.6 does not guarantee that Q is a weakly S -2-prime ideal of R .

Example 2.7. Let p, q be distinct prime numbers and $R = \mathbb{Z}_{p^2q^2}$, $S = \{\bar{1}, \bar{s} : s \text{ is a prime number with } s \neq p, q\}$ and $Q = (\overline{pq})$. Then, $Q^2 = (0)$. Nevertheless, Q is not a weakly S -2-prime ideal of R since $0 \neq \bar{p} \cdot \bar{q} \in Q$ but $s \cdot \bar{p}^2 \notin Q$ and $s \cdot \bar{q}^2 \notin Q$ for all $s \in S$.

Let S be a m.c.s of R and Q be an ideal of R with $Q \cap S = \emptyset$. As it is shown in [14] that if Q is an S -2-prime ideal of R , then $\sqrt{Q}$ is an S -prime ideal of R . A similar statement does not hold for weakly S -2-prime ideals.

Example 2.8. Let p, q be distinct prime numbers and $R = \mathbb{Z}_{p^2q^2}$, $S = \{\bar{1}, \bar{s} : s \text{ is a prime number with } s \neq p, q\}$. Then $Q = (\bar{0})$ is a weakly S -2-prime ideal of R , but $\sqrt{Q} = (\overline{pq})$ is not a weakly S -prime ideal of R as $0 \neq \bar{p} \cdot \bar{q} \in \sqrt{Q}$ but $s \cdot \bar{p} \notin \sqrt{Q}$ and $s \cdot \bar{q} \notin \sqrt{Q}$ for all $s \in S$.

Theorem 2.9. Suppose that $f : R \rightarrow R'$ is a ring homomorphism and S is a m.c.s of R . Then, the following statements are provided:

1. If f is an epimorphism and Q is a weakly S -2-prime ideal of R containing $\ker(f)$, then $f(Q)$ is a weakly $f(S)$ -2-prime ideal of R' .
2. If f is a monomorphism and Q' is a weakly $f(S)$ -2-prime ideal of R' , then $f^{-1}(Q')$ is a weakly S -2-prime ideal of R .

Proof. (1) Let $r \in f(S) \cap f(Q)$. Then, $r = f(q) = f(s)$ for some $q \in Q$ and $s \in S$. We have $s - q \in \ker(f) \subseteq Q$, that is $s \in Q$ which contradicts with $Q \cap S = \emptyset$. Hence, $f(S) \cap f(Q) = \emptyset$. Now, let $0 \neq \alpha'\beta' \in f(Q)$. Then, there is $\alpha, \beta \in R$ such that $f(\alpha) = \alpha'$ and $f(\beta) = \beta'$ with $0 \neq f(\alpha\beta) = \alpha'\beta' \in f(Q)$. Since $\ker(f) \subseteq Q$, we get $0 \neq \alpha\beta \in Q$. From our assumption, there exists an $s \in S$ such that $s\alpha^2 \in Q$ or $s\beta^2 \in Q$. This implies that $f(s\alpha^2) = f(s)(\alpha')^2 \in f(Q)$ or $f(s\beta^2) = f(s)(\beta')^2 \in f(Q)$. Hence, $f(Q)$ is a weakly $f(S)$ -2-prime ideal of R' .

(2) Suppose that Q' is a weakly $f(S)$ -2-prime ideal of R' . Clearly, $f^{-1}(Q') \cap S = \emptyset$. Let $\alpha, \beta \in R$ with $0 \neq \alpha\beta \in f^{-1}(Q')$. Because of $\ker(f) = \{0\}$, we have $0 \neq f(\alpha\beta) = f(\alpha)f(\beta) \in Q'$. Then, there exists $f(s) \in f(S)$ such that $f(s)(f(\alpha))^2 \in Q'$ or $f(s)(f(\beta))^2 \in Q'$. Thus, $f(s\alpha^2) \in Q'$ or $f(s\beta^2) \in Q'$, that is $s\alpha^2 \in f^{-1}(Q')$ or $s\beta^2 \in f^{-1}(Q')$. Hence, $f^{-1}(Q')$ is a weakly S -2-prime ideal of R . $\square$

Let S be a m.c.s of R and Q be an ideal of R such that $Q \cap S = \emptyset$. Let $s \in S$. By $\bar{s}$, we denote the class of s in R/Q and set $\bar{S} = \{\bar{s} : s \in S\}$. It is clear that $\bar{S}$ is a m.c.s of R/Q .

Corollary 2.10. Let S be a m.c.s of R . Then

1. Let $J \subseteq K$ are two ideals of R . If K is a weakly S -2-prime ideal of R , then K/J is a weakly $\bar{S}$ -2-prime ideal of R/J .
2. If R is a subring of R' and K' is a weakly S -2-prime of R' with $R \not\subseteq K'$, then $K' \cap R$ is a weakly S -2-prime ideal of R .

Proof. (1) Consider the epimorphism $f : R \rightarrow R/J$, described by $f(r) = r + J$ for each $r \in R$. Moreover, $\ker(f) = J \subseteq K$ and by Theorem 2.9 (1.), we have $f(K) = K/J$ is a weakly $\bar{S}$ -2-prime ideal of R/J .

(2) It is clear that $(K' \cap R) \cap S = \emptyset$. Consider the monomorphism $h : R \rightarrow R'$, described by $h(r) = r$ for each $r \in R$. Since K' is a weakly S -2-prime of R' by Theorem 2.9 (2.), $h^{-1}(K') = K' \cap R$ is a weakly S -2-prime ideal of R . $\square$

Theorem 2.11. Let $R = R_1 \times R_2$ and $S = S_1 \times S_2$, where S_1 is a m.c.s of R_1 and S_2 is a m.c.s of R_2 . Suppose that Q_1 and Q_2 are non-zero proper ideals of R_1 and R_2 , respectively. The following statements are equivalent:

1. $Q = Q_1 \times Q_2$ is a weakly S -2-prime ideal of R .
2. Either Q_1 is an S_1 -2-prime ideal of R_1 with $S_2 \cap Q_2 \neq \emptyset$ or Q_2 is an S_2 -2-prime ideal of R_2 with $S_1 \cap Q_1 \neq \emptyset$.
3. $Q = Q_1 \times Q_2$ is an S -2-prime ideal of R .

Proof. (1) $\Rightarrow$ (2) Let $0 \neq (g, h) \in Q$ for all $g \in R_1$ and $h \in R_2$. Then, $0 \neq (g, h) = (g, 1)(1, h) \in Q$. From our assumption, there exists an $s = (s_1, s_2) \in S$ such that $(s_1, s_2)(g, 1)^2 = (s_1 g^2, s_2) \in Q$ or $(s_1, s_2)(1, h)^2 = (s_1, s_2 h^2) \in Q$. Therefore, we have $S_1 \cap Q_1 \neq \emptyset$ or $S_2 \cap Q_2 \neq \emptyset$. Let $S_2 \cap Q_2 \neq \emptyset$. Since $Q \cap S = \emptyset$, we have $S_1 \cap Q_1 = \emptyset$. We will indicate that Q_1 is an S_1 -2-prime ideal of R_1 . Now, let $gg_1 \in Q_1$ for all $g, g_1 \in R_1$. Because of $S_2 \cap Q_2 \neq \emptyset$, then there is $0 \neq m \in S_2 \cap Q_2$ such that $0 \neq (g, m)(g_1, 1) \in Q$. From assumption, there exists an $s = (s_1, s_2) \in S = S_1 \times S_2$ such that $(s_1, s_2)(g, m)^2 = (s_1 g^2, s_2 m^2) \in Q$ or $(s_1, s_2)(g_1, 1)^2 = (s_1 g_1^2, s_2) \in Q$. Hence, $s_1 g^2 \in Q_1$ or $s_1 g_1^2 \in Q_1$, and so Q_1 is an S_1 -2-prime ideal of R_1 . Similarly, if $S_1 \cap Q_1 \neq \emptyset$, then we could prove that Q_2 is an S_2 -2-prime ideal of R_2 .

(2) $\Rightarrow$ (3) Follows from [14], Lemma 1].

(3) $\Rightarrow$ (1) The proof is straightforward. $\square$

Theorem 2.12. Let $n \geq 2$, $R = R_1 \times R_2 \times \cdots \times R_n$ and $S = S_1 \times S_2 \times \cdots \times S_n$ where S_i is a m.c.s of R_i and Q_i is a non-zero proper ideal of R_i for $i = 1, 2, \dots, n$, respectively. The following statements are equivalent:

1. $Q = Q_1 \times Q_2 \times \cdots \times Q_n$ is a weakly S -2-prime ideal of R .
2. Q_m is an S_m -2-prime ideal of R_m for some $m \in \{1, 2, \dots, n\}$ and $Q_i \cap S_i \neq \emptyset$ for each $i \in \{1, 2, \dots, n\} - \{m\}$.
3. $Q = Q_1 \times Q_2 \times \cdots \times Q_n$ is an S -2-prime ideal of R .

Proof. (1) $\Rightarrow$ (2) In order to prove the claim, we will use induction on n . If $n = 2$, then the result follows from the Theorem 2.11. Suppose that the claim is true for all $k < n$. Let $R' = R_1 \times R_2 \times \cdots \times R_{n-1}$, $S' = S_1 \times S_2 \times \cdots \times S_{n-1}$ and $Q' = Q_1 \times Q_2 \times \cdots \times Q_{n-1}$. Since $0 \neq Q = Q' \times Q_n$ is a weakly $S = S' \times S_n$ -2-prime ideal of $R = R' \times R_n$, by Theorem 2.11, we have Q_n is an S_n -2-prime of R_n and $Q' \cap S' \neq \emptyset$ or Q' is an S' -2-prime ideal of R' and $Q_n \cap S_n \neq \emptyset$. If $Q' \cap S' \neq \emptyset$ and Q_n is an S_n -2-prime of R_n , then proof is complete. So, suppose that $Q_n \cap S_n \neq \emptyset$ and Q' is an S' -2-prime ideal of R' . In this case, using the induction hypothesis for $k = n - 1$, we have Q_j is an S_j -2-prime ideal of R_j for some $j \in \{1, 2, \dots, n - 1\}$ and $Q_i \cap S_i \neq \emptyset$ for each $i \in \{1, 2, \dots, n - 1\} - \{j\}$, which completes the proof.

(2) $\Rightarrow$ (3) Follows from [14], Theorem 3].

(3) $\Rightarrow$ (1) The proof is straightforward. $\square$

Let Q be an ideal of R . By $Z_Q(R)$, we mean $Z_Q(R) = \{\alpha \in R : \alpha\beta \in Q \text{ for some } \beta \notin Q\}$. Besides, if $Q = (0)$, then $Z_Q(R)$ is the set of all zero divisors of R . In this case, we can use $zd(R)$ in the place of $Z_Q(R)$. Moreover, we will describe the set of all regular elements of R , that is they are non-zero divisors, with $reg(R) = R - zd(R)$. [10]

Proposition 2.13. Suppose that $S, S' \subseteq R$ are m.c.s.s of R and Q is an ideal of R . If Q is a weakly S' -2-prime ideal of R with $Q \cap S = \emptyset$, then $S^{-1}Q$ is a weakly $S^{-1}S'$ -2-prime ideal of $S^{-1}R$. The converse of this implication also holds provided that $Z_Q(R) \cap S = \emptyset$ and $S \subseteq reg(R)$.

Proof. It is clear that $S^{-1}S'$ is a m.c.s of $S^{-1}R$ as S' is a m.c.s of R . Also, $S^{-1}Q \cap S^{-1}S' = \emptyset$ because of $Q \cap S = \emptyset$. Let $m, n \in R$ and $s, t \in S$ such that $0 \neq \frac{m}{s} \frac{n}{t} = \frac{mn}{st} \in S^{-1}Q$. Then, $0 \neq \widetilde{s}(mn) = (\widetilde{s}m)n \in Q$ for some $\widetilde{s} \in S$. By assumption, there exists an $s' \in S'$ such that $s'(\widetilde{s}m)^2 \in Q$ or $s'n^2 \in Q$. This yields that $\frac{s'}{1}(\frac{m}{s})^2 = \frac{s'}{1}(\frac{\widetilde{s}m}{\widetilde{s}s})^2 \in S^{-1}Q$ or $\frac{s'}{1}(\frac{n}{t})^2 \in S^{-1}Q$. Hence, $S^{-1}Q$ is a weakly $S^{-1}S'$ -2-prime ideal of $S^{-1}R$. Conversely, it is clear that $Q \cap S' = \emptyset$. Suppose that $0 \neq mn \in Q$ for all $m, n \in R$. Then, we have $0 \neq \frac{m}{1} \frac{n}{1} \in S^{-1}Q$ because of $S \subseteq reg(R)$. From assumption, there exists an $\frac{s'}{s} \in S^{-1}S'$ such that $\frac{s'}{s}(\frac{m}{1})^2 \in S^{-1}Q$ or $\frac{s'}{s}(\frac{n}{1})^2 \in S^{-1}Q$. Then, there exists $\widetilde{s} \in S$ such that $\widetilde{s}s'm^2 \in Q$ or $\widetilde{s}s'n^2 \in Q$. Since $Z_Q(R) \cap S = \emptyset$, we have $s'm^2 \in Q$ or $s'n^2 \in Q$ for $s' \in S'$. Thus, Q is a weakly S' -2-prime ideal of R . $\square$

Let R be a commutative ring with identity and M be a unitary R -module. The trivial extention of R in M denoted by $R(+M) = \{(\widetilde{r}, m) : \widetilde{r} \in R, m \in M\}$ is a commutative ring with usual addition and the multiplication $(\widetilde{r}_1, m_1)(\widetilde{r}_2, m_2) = (\widetilde{r}_1\widetilde{r}_2, \widetilde{r}_1m_2 + \widetilde{r}_2m_1)$ for all $(\widetilde{r}_1, m_1), (\widetilde{r}_2, m_2) \in R(+M)$ [3, 11]. Clearly, if S is a m.c.s of R , then $S(+0)$ and $S(+M)$ are m.c.s.s of $R(+M)$.

Theorem 2.14. Let R and M be the above statement and S be a m.c.s of R . For a proper ideal Q disjoint with S , the following statements are equivalent:

1. $Q(+M)$ is a weakly $(S(+M))$ -2-prime ideal of $R(+M)$.
2. $Q(+M)$ is a weakly $(S(+0))$ -2-prime ideal of $R(+M)$.
3. Q is a weakly S -2-prime ideal of R associated to $s \in S$, and if there exist $\alpha, \beta \in R$ with $\alpha\beta = 0$, but $s\alpha^2 \notin Q$ and $s\beta^2 \notin Q$, then $\alpha \in ann_R(M)$ and $\beta \in ann_R(M)$.

Proof. (1) $\Rightarrow$ (3) Let $\alpha, \beta \in R$ with $0 \neq \alpha\beta \in Q$. Then, $(0, 0) \neq (\alpha, 0)(\beta, 0) \in Q(+M)$. From assumption, there exists $(s, m) \in S(+M)$ such that $(s, m)(\alpha, 0)^2 = (s\alpha^2, m\alpha^2) \in Q(+M)$ or $(s, m)(\beta, 0)^2 = (s\beta^2, m\beta^2) \in Q(+M)$. Therefore, $s\alpha^2 \in Q$ or $s\beta^2 \in Q$, and so Q is a weakly S -2-prime ideal of R associated to that $s \in S$. Now, let $\alpha\beta = 0$ but $s\alpha^2 \notin Q$ and $s\beta^2 \notin Q$. Suppose $\alpha \notin ann_R(M)$. Then, there is $m' \in M$ with $\alpha m' \neq 0$. So, we have $(0, 0) \neq (\alpha, 0)(\beta, m') \in Q(+M)$. From assumption, there exists $(s, m) \in S(+M)$ such that $(s, m)(\alpha, 0)^2 = (s\alpha^2, m\alpha^2) \in Q(+M)$ or $(s, m)(\beta, m')^2 = (s\beta^2, 2s\beta m' + m\beta^2) \in Q(+M)$. Thus, $s\alpha^2 \in Q$ or $s\beta^2 \in Q$, a contradiction. So, $\alpha \in ann_R(M)$, and similarly we can obtain $\beta \in ann_R(M)$.

(3) $\Rightarrow$ (2) Let $(\alpha, m), (\beta, m') \in R(+M)$ with $(0, 0) \neq (\alpha, m)(\beta, m') \in Q(+M)$. If $\alpha\beta \neq 0$, then $s\alpha^2 \in Q$ or $s\beta^2 \in Q$. So, $(s, 0)(\alpha, m)^2 \in Q(+M)$ or $(s, 0)(\beta, m')^2 \in Q(+M)$. If $\alpha\beta = 0$ but $s\alpha^2 \notin Q$ and $s\beta^2 \notin Q$, then $\alpha, \beta \in ann_R(M)$. Hence, we have $(\alpha, m)(\beta, m') = (0, 0)$ and it is a contradiction because of our assumption. We conclude that $Q(+M)$ is a weakly $(S(+0))$ -2-prime ideal of $R(+M)$.

(2) $\Rightarrow$ (1) The proof is clear. $\square$

Recall from [6] that the amalgamated duplication of R along an ideal I of R is defined as follow:

$$R \bowtie I = \{(\widetilde{r}, \widetilde{r} + i) : \widetilde{r} \in R, i \in I\}$$

$R \bowtie I$ is the subring of $R \times R$.

Theorem 2.15. Suppose that I is an R -module, S is a m.c.s of R and Q is a proper ideal of R with $Q \cap S = \emptyset$. Then, the following statements are equivalent:

1. $Q \bowtie I$ is a weakly $(S \bowtie I)$ -2-prime ideal of $R \bowtie I$.
2. $Q \bowtie I$ is a weakly $(S \bowtie 0)$ -2-prime ideal of $R \bowtie I$.
3. Q is a weakly S -2-prime ideal of R associated to $s \in S$, and if there exist $\alpha, \beta \in R$ with $\alpha\beta = 0$, but $s\alpha^2 \notin Q$ and $s\beta^2 \notin Q$, then $\alpha, \beta \in \text{ann}_R(I)$ and $I^2 = (0)$.

Proof. (1) $\Rightarrow$ (3) Let $Q \bowtie I$ be a weakly $(S \bowtie I)$ -2-prime ideal of $R \bowtie I$ associated to $(s, s+i)$ and $0 \neq \alpha\beta \in Q$ for all $\alpha, \beta \in R$. Then, $(0, 0) \neq (\alpha, \alpha)(\beta, \beta) \in Q \bowtie I$. Hence, $(s, s+i)(\alpha, \alpha)^2 \in Q \bowtie I$ or $(s, s+i)(\beta, \beta)^2 \in Q \bowtie I$. So, $s\alpha^2 \in Q$ or $s\beta^2 \in Q$ and Q is a weakly S -2-prime ideal of R associated to $s \in S$. Now, suppose $\alpha\beta = 0$, but $s\alpha^2 \notin Q$ and $s\beta^2 \notin Q$. Let $\alpha \notin \text{ann}_R(I)$. Then, there is $i' \in I$ such that $\alpha i' \neq 0$. Therefore, we have $(0, 0) \neq (\alpha, \alpha)(\beta, \beta + i') \in Q \bowtie I$. Thus, $(s, s+i)(\alpha, \alpha)^2 \in Q \bowtie I$ or $(s, s+i)(\beta, \beta + i')^2 \in Q \bowtie I$ which contradicts with our assumption. Hence, $\alpha \in \text{ann}_R(I)$ and similarly $\beta \in \text{ann}_R(I)$. Let $m, n \in I$. Then, $(\alpha, \alpha+m)(\beta, \beta+n) = (0, mn) \in Q \bowtie I$. If $mn \neq 0$, then $(\alpha, \alpha+m)(\beta, \beta+n) \neq (0, 0)$. Hence, $(s, s+i)(\alpha, \alpha+m)^2 \in Q \bowtie I$ or $(s, s+i)(\beta, \beta+n)^2 \in Q \bowtie I$, again a contradiction. Thus, $I^2 = (0)$.

(3) $\Rightarrow$ (2) Let $(0, 0) \neq (\alpha, \alpha+m)(\beta, \beta+n) \in Q \bowtie I$ for all $(\alpha, \alpha+m), (\beta, \beta+n) \in R \bowtie I$. If $\alpha\beta \neq 0$, then $s\alpha^2 \in Q$ or $s\beta^2 \in Q$. So, we have $(s, s)(\alpha, \alpha+m)^2 \in Q \bowtie I$ or $(s, s)(\beta, \beta+n)^2 \in Q \bowtie I$. If $\alpha\beta = 0$ but $s\alpha^2 \notin Q$ and $s\beta^2 \notin Q$, then $\alpha, \beta \in \text{ann}_R(I)$ and $I^2 = (0)$. So, $(\alpha, \alpha+m)(\beta, \beta+n) = (0, 0)$ and it is a contradiction from assumption. Hence, $Q \bowtie I$ is a weakly $(S \bowtie 0)$ -2-prime ideal of $R \bowtie I$.

(2) $\Rightarrow$ (1) The proof is clear. □

Finally, we will examine the rings over which every weakly S -2-prime ideal is S -2-prime ideal. Note that every weakly S -2-prime ideal is an S -2-prime ideal of R if and only if (0) is an S -2-prime ideal of R . Recall from [5], Definition 1.4.3] a commutative ring with identity R is called an S -integral domain if there exists an $s \in S$ such that for all $\alpha, \beta \in R$ with $\alpha\beta = 0$, we have $s\alpha = 0$ or $s\beta = 0$ where S is a m.c.s of R .

Proposition 2.16. Let R be an S -integral domain and M be an R -module where S is a m.c.s of R . Then, an ideal Q of $R(+)M$ is a weakly $(S(+)0)$ -2-prime ideal of $R(+)M$ if and only if Q is an $(S(+)0)$ -2-prime ideal of $R(+)M$.

Proof. To verify that weakly $(S(+)0)$ -2-prime ideals and $(S(+)0)$ -2-prime ideals coincide in $R(+)M$, it is enough to show that the zero ideal of $R(+)M$ is an $(S(+)0)$ -2-prime ideal of $R(+)M$. Since $0 \notin S$, it is clear that $((0, 0)) \cap (S(+)0) = \emptyset$. Let $(\alpha, \sigma), (\beta, \gamma) \in R(+)M$ such that $(\alpha, \sigma)(\beta, \gamma) = (\alpha\beta, \alpha\gamma + \beta\sigma) = (0, 0)$. Then, $\alpha\beta = 0$, and since R is an S -integral domain, there exists an $s \in S$ such that $s\alpha = 0$ or $s\beta = 0$. Hence, $(s, 0)(\alpha, \sigma)^2 = (s\alpha^2, 2s\alpha\sigma) = (0, 0)$ or $(s, 0)(\beta, \gamma)^2 = (s\beta^2, 2s\beta\gamma) = (0, 0)$ for $s' := (s, 0) \in S(+)0$. Thus, the zero ideal is an $(S(+)0)$ -2-prime ideal of $R(+)M$ associated to s' , as required. □

A ring R is called a Von-Neumann regular ring if for every $\alpha \in R$, there exists $r \in R$ such that $\alpha = \alpha^2 r$ [13]. Moreover, it is shown that in a Von-Neumann regular ring every ideal Q of R is a semiprime ideal or $Q = \sqrt{Q}$ [9], Theorem 1].

Proposition 2.17. If R is an S -integral domain, then every weakly S -2-prime ideal is S -2-prime ideal of R , where S is a m.c.s of R . The converse also holds if R is a Von-Neumann regular ring.

Proof. Let R be an S -integral domain. Suppose that Q is a weakly S -2-prime ideal of R and $\alpha\beta \in Q$ for all $\alpha, \beta \in R$. If $\alpha\beta \neq 0$, then there exists an $s \in S$ such that $s\alpha^2 \in Q$ or $s\beta^2 \in Q$, as desired. If $\alpha\beta = 0$, then we have $s\alpha = 0$ or $s\beta = 0$ as R is an S -integral domain. Hence, $s\alpha^2 = 0 \in Q$ or $s\beta^2 = 0 \in Q$ and Q is an S -2-prime ideal of R . Conversely, assume that R is a Von-Neumann regular ring and every weakly S -2-prime ideal is S -2-prime ideal of R . Then, (0) is an S -2-prime ideal of R . Let $\alpha, \beta \in R$ with $\alpha\beta = 0$. From assumption, there exists an $s \in S$ such that $s\alpha^2 = 0$ or $s\beta^2 = 0$. Then, $\alpha \in \sqrt{(0:s)}$ or $\beta \in \sqrt{(0:s)}$. Since R is a Von-Neumann regular ring, we have $s\alpha = 0$ or $s\beta = 0$, and so R is an S -integral domain. $\square$

References

- [1] F. A. A. Almahdi, E. M. Bouba, M. Tamekkante, On weakly S -prime ideals of commutative rings, *An. Stiint. Univ. Ovidius Constanta, Ser. Mat.* 29 (2021), 173–186.
- [2] D. D. Anderson, E. Smith, Weakly prime ideals, *Houston J. Math.* 29 (2003), 831–840.
- [3] D. D. Anderson, M. Winders, Idealization of a module, *J. Commutative Algebra* 1 (2009), 3–56.
- [4] C. Beddani, W. Messirdi, 2-prime ideals and their applications, *J. Algebra Appl.* 15 (2016):1650051, DOI:10.1142/S0219498816500511.
- [5] B. Düzgün, S -semiprime ideals of commutative rings, *Yök Open Science* (2020), <https://acikbilim.yok.gov.tr/handle/20.500.12812/222763>.
- [6] M. D’Anna, M. Fontana, An amalgamated duplication of a ring along an ideal: the basic properties, *J. Algebra Appl.* 6 (2007), 443–459.
- [7] A. Hamed, A. Malek, S -prime ideals of a commutative ring, *Beitr. Algebra Geom.* 61 (2020), 533–542.
- [8] M. Issoual, N. Mahdou, Ü. Tekir, S. Koç, More on the weakly 2-prime ideals of commutative rings, *Filomat* 38 (2024), 6099–6108.
- [9] C. Jayaram, Ü. Tekir, Von Neumann regular modules, *Commun. Algebra* 46 (2017), 2205–2217.
- [10] S. Koç, On weakly 2-prime ideals in commutative rings, *Commun. Algebra* 49 (2021), 3387–3397.
- [11] M. Nagata, *Local Rings*, Interscience Publishers, New York, 1962.
- [12] R. Nikandish, M. J. Nikmehr, A. Yassine, More on the 2-prime ideals of commutative rings, *Bull. Korean Math. Soc.* 57 (2020), 117–126.
- [13] J. Von Neumann, On regular rings, *Proceedings of the National Academy of Sciences* 22 (1936), 707–713.
- [14] S. Yavuz, B. A. Ersoy, Ü. Tekir, E. Yetkin Çelikel, On S -2-prime ideals of commutative rings, *Mathematics* 12 (2024), 1–12, <https://doi.org/10.3390/math12111636>.



ISSN: 2820-7114

Moroccan Journal of Algebra and Geometry with Applications

Supported by Sidi Mohamed Ben Abdellah University, Fez, Morocco

Volume 4, Issue 1 (2025), pp 62-73

Title :

Squares of Fibonacci-like Numbers

Author(s):

Kunle Adegoke and Tokunbo Omiyinka

Squares of Fibonacci-like Numbers

Kunle Adegoke¹ and Tokunbo Omiyinka²

¹ Department of Physics and Engineering Physics, Obafemi Awolowo University, Ile-Ife, Nigeria
e-mail: adegoke00@gmail.com

² Department of Mathematical and Physical Sciences, Concordia University of Edmonton
and
Faculty of Education, University of Alberta, Edmonton, Alberta
e-mail: omiyinka@ualberta.ca

Communicated by Abdelmejid Bayad

(Received 10 June 2023, Revised 24 November 2024, Accepted 27 November 2024)

Abstract. Given arbitrary integers G_0 and G_1 , not both zero, Fibonacci-like numbers, G_j , are defined for all non-negative integers j by the recurrence relation $G_j = G_{j-1} + G_{j-2}$ ($j \geq 2$). In this paper, we derive a general identity involving the squares of Fibonacci-like numbers. Closed formulas exist for $\sum_{j=0}^n x^j G_j^2$ and $\sum_{j=0}^n G_{j+k} G_{j-k}$. We extend these results by providing evaluations for $\sum_{j=0}^n x^j G_{j+k}^2$ and $\sum_{j=0}^n x^j G_{j+k} G_{j+s}$ for integers n, s and k and a real or complex variable x . Various other properties are developed, including double binomial summation identities. As a bonus unexpected result we derive a generalization of the alternating sum of the products of three consecutive Fibonacci-like numbers.

Key Words: Fibonacci number, Lucas number, Fibonacci-like number, generating function.

2020 MSC: Primary 11B39; Secondary 11B37.

Dedicated to our Professor David E. Dobbs for his 80th Birthday.

1 Introduction

The Fibonacci numbers, F_j , and the Lucas numbers, L_j , $j \in \mathbb{Z}$, are defined by:

$$F_0 = 0, F_1 = 1, F_j = F_{j-1} + F_{j-2} \ (j \geq 2), \quad F_{-j} = (-1)^{j-1} F_j \quad (1.1)$$

and

$$L_0 = 2, L_1 = 1, L_j = L_{j-1} + L_{j-2} \ (j \geq 2), \quad L_{-j} = (-1)^j L_j. \quad (1.2)$$

Both $(F_j)_{j \in \mathbb{Z}}$ and $(L_j)_{j \in \mathbb{Z}}$ are examples of a Fibonacci-like sequence. We define a Fibonacci-like sequence (also called a gibbonacci sequence), $(G_j)_{j \in \mathbb{Z}}$, as one having the same recurrence relation as the Fibonacci sequence, but with arbitrary initial terms. Thus, given arbitrary integers G_0 and G_1 , not both zero, we define

$$G_j = G_{j-1} + G_{j-2} \ (j \geq 2); \quad (1.3)$$

and also extend the definition to negative subscripts by writing the recurrence relation as

$$G_{-j} = G_{-j+2} - G_{-j+1}. \quad (1.4)$$

We have [2] equation (1.5)]

$$G_{-j} = (-1)^j (G_0 L_j - G_j). \quad (1.5)$$

The identity (see Brousseau [4] equation (2))

$$F_{j-1}^2 + F_{j+2}^2 = 2F_j^2 + 2F_{j+1}^2, \quad (1.6)$$

or, more generally,

$$G_{j-1}^2 + G_{j+2}^2 = 2G_j^2 + 2G_{j+1}^2, \quad (1.7)$$

is well known.

Less familiar are identities such as

$$G_{j+2}^2 + 2G_{j-2}^2 = 3G_{j-1}^2 + 6G_j^2, \quad (1.8)$$

$$3G_{j+3}^2 + G_{j-3}^2 = 16G_{j+1}^2 + 12G_j^2 \quad (1.9)$$

and

$$F_k F_{k+1} G_{j+1}^2 - F_k F_{k-1} G_{j-1}^2 = G_{j+k}^2 - F_{k+1} F_{k-1} G_j^2. \quad (1.10)$$

Our aim in writing this paper is to derive the identity

$$\begin{aligned} F_s F_m F_{m-s} G_{j+k}^2 &= F_{m-s} F_{m-k} F_{s-k} G_j^2 + (-1)^{s+k} F_k F_m F_{m-k} G_{j+s}^2 \\ &\quad - (-1)^{s+k} F_k F_s F_{s-k} G_{j+m}^2, \end{aligned}$$

of which (1.7), (1.8), (1.9) and (1.10) are particular cases, being evaluations at certain m, k, j and s choices.

Closed formulas are known for $\sum_{j=0}^n x^j G_j^2$ and $\sum_{j=0}^n G_{j+k} G_{j-k}$. We will extend these results by providing evaluations for $\sum_{j=0}^n x^j G_{j+k}^2$ and $\sum_{j=0}^n x^j G_{j+k} G_{j+s}$ for integers n, s and k and arbitrary x .

As a bonus surprise result we will discover a generalization (Theorem 4.3) of the following alternating sum of products of three consecutive Fibonacci-like numbers:

$$\begin{aligned} 2 \sum_{j=0}^n (-1)^j G_{j+k+1} G_{j+k} G_{j+k-1} &= (-1)^n G_{n+k+1}^3 + (-1)^{n+1} G_{n+k+2} G_{n+k}^2 \\ &\quad + G_k^3 - G_{k+1} G_{k-1}^2. \end{aligned}$$

Finally, we will derive double binomial identities involving the squares of Fibonacci-like numbers.

2 Main identity

The main identity with which we are concerned, proved in Theorem 2.2, utilizes the result stated in Lemma 2.1

Lemma 2.1. *The following identity holds for arbitrary integers s, k, m and j :*

$$F_{s-k}G_{j+m} = F_{m-k}G_{j+s} + (-1)^{s+k+1}F_{m-s}G_{j+k}.$$

Proof. Let h, n and r be arbitrary integers. Let $(G_j)_{j \in \mathbb{Z}}$ and $(H_j)_{j \in \mathbb{Z}}$ be two Fibonacci-like sequences. It is known [5, Formula (18)] that:

$$H_n G_{n+h+r} = H_{n+h} G_{n+r} + (-1)^{n+1} (H_h G_r - H_0 G_{h+k}).$$

Choosing $(H_j)_{j \in \mathbb{Z}}$ as the Fibonacci sequence gives

$$F_n G_{n+h+r} = F_{n+h} G_{n+r} + (-1)^{n+1} F_h G_r. \quad (2.1)$$

Setting $h = m - s$, $n = s - k$ and $r = j + k$ in (2.1) gives the identity stated in Lemma 2.1. $\square$

Theorem 2.2. If j, k, m and s are integers, then

$$\begin{aligned} F_s F_m F_{m-s} G_{j+k}^2 &= F_{m-s} F_{m-k} F_{s-k} G_j^2 + (-1)^{s+k} F_k F_m F_{m-k} G_{j+s}^2 \\ &\quad - (-1)^{s+k} F_k F_s F_{s-k} G_{j+m}^2. \end{aligned}$$

Proof. Setting $m = 0$ in the identity stated in Lemma 2.1 gives

$$(-1)^k F_{s-k} G_j = F_s G_{j+k} - F_k G_{j+s}, \quad (2.2)$$

from which, by squaring and re-arranging, we get

$$2F_s F_k G_{j+k} G_{j+s} = F_s^2 G_{j+k}^2 + F_k^2 G_{j+s}^2 - F_{s-k}^2 G_j^2. \quad (2.3)$$

The statement of the theorem now follows by squaring the identity stated in Lemma 2.1 and using (2.3) to eliminate the cross-term $G_{j+k} G_{j+s}$ from the right hand side, while making use also of the multiplication formula

$$5F_m F_n = L_{m+n} - (-1)^n L_{m-n}. \quad (2.4)$$

$\square$

3 Partial sums and generating function

Theorem 3.1. The following identity holds for arbitrary x and integers k and n :

$$\begin{aligned} \sum_{j=0}^n x^j G_{j+k}^2 &= \frac{x G_{k+1}^2 - (2x-1) G_k^2 - x^2 G_{k-1}^2}{x^3 - 2x^2 - 2x + 1} \\ &\quad - \frac{x^{n+1} (x G_{n+k+2}^2 - (2x-1) G_{n+k+1}^2 - x^2 G_{n+k}^2)}{x^3 - 2x^2 - 2x + 1}. \end{aligned} \quad (3.1)$$

Proof. Write $j + k$ for j in (1.7), multiply through by x^j and sum to obtain

$$\sum_{j=0}^n x^j G_{j+k-1}^2 + \sum_{j=0}^n x^j G_{j+k+2}^2 = 2 \sum_{j=0}^n x^j G_{j+k}^2 + 2 \sum_{j=0}^n x^j G_{j+k+1}^2. \quad (3.2)$$

Shifting the summation index in each case gives

$$\sum_{j=0}^n x^j G_{j+k-1}^2 = G_{k-1}^2 - x^{n+1} G_{n+k}^2 + xS(x; n, k), \quad (3.3)$$

$$\sum_{j=0}^n x^j G_{j+k+1}^2 = -\frac{1}{x} G_k^2 + x^n G_{n+k+1}^2 + \frac{1}{x} S(x; n, k), \quad (3.4)$$

and

$$\sum_{j=0}^n x^j G_{j+k+2}^2 = -\frac{1}{x^2} G_k^2 - \frac{1}{x} G_{k+1}^2 + x^{n-1} G_{n+k+1}^2 + x^n G_{n+k+2}^2 + \frac{1}{x^2} S(x; n, k); \quad (3.5)$$

where

$$S(x; n, k) = \sum_{j=0}^n x^j G_{j+k}^2.$$

Substituting (3.3), (3.4) and (3.5) into (3.2) and solving for $S(x; n, k)$ gives the identity of Theorem 3.1. $\square$

In particular,

$$\begin{aligned} \sum_{j=0}^n x^j G_j^2 &= \frac{xG_1^2 - (2x-1)G_0^2 - x^2(G_1 - G_0)^2}{x^3 - 2x^2 - 2x + 1} \\ &\quad - \frac{x^{n+1}(xG_{n+2}^2 - (2x-1)G_{n+1}^2 - x^2G_n^2)}{x^3 - 2x^2 - 2x + 1}; \end{aligned} \quad (3.6)$$

so that

$$\begin{aligned} \sum_{j=0}^n x^j F_j^2 &= \frac{x - x^2}{x^3 - 2x^2 - 2x + 1} \\ &\quad - \frac{x^{n+1}(xF_{n+2}^2 - (2x-1)F_{n+1}^2 - x^2F_n^2)}{x^3 - 2x^2 - 2x + 1} \end{aligned} \quad (3.7)$$

and

$$\begin{aligned} \sum_{j=0}^n x^j L_j^2 &= \frac{4 - 7x - x^2}{x^3 - 2x^2 - 2x + 1} \\ &\quad - \frac{x^{n+1}(xL_{n+2}^2 - (2x-1)L_{n+1}^2 - x^2L_n^2)}{x^3 - 2x^2 - 2x + 1}. \end{aligned} \quad (3.8)$$

We also have

$$\sum_{j=0}^n G_{j+k}^2 = G_{n+k} G_{n+k+1} - G_{k-1} G_k, \quad (3.9)$$

with the special value

$$\sum_{j=0}^n G_j^2 = G_n G_{n+1} - (G_1 - G_0) G_0, \quad (3.10)$$

giving the classical results

$$\sum_{j=0}^n F_j^2 = F_n F_{n+1}, \quad \sum_{j=0}^n L_j^2 = L_n L_{n+1} + 2. \quad (3.11)$$

Observe that setting $x = -1$ in the identity of Theorem 3.1 makes the right hand side to be an indeterminate form. Application of L'Hospital's rule however provides

$$\begin{aligned} \sum_{j=0}^n (-1)^j G_{j+k}^2 &= (-1)^n \left(\frac{n+2}{5} G_{n+k+2}^2 - \frac{3n+5}{5} G_{n+k+1}^2 + \frac{n+3}{5} G_{n+k}^2 \right) \\ &\quad + \frac{1}{5} G_{k+1}^2 - \frac{2}{5} G_{k+1} G_{k-2}. \end{aligned} \quad (3.12)$$

Theorem 3.2 (Generating function of F_j^2).

$$\sum_{j=0}^{\infty} x^j F_j^2 = \frac{x(1-x)}{1-2x-2x^2+x^3}, \quad |x| < \frac{3-\sqrt{5}}{2}. \quad (3.13)$$

Proof. Identity (3.7) as n approaches infinity; with $x^n F_n^2 \rightarrow 0$ as n approaches infinity. $\square$

Next, we provide an alternative evaluation of $\sum_{j=0}^n x^j G_{j+k}^2$ in terms of $\sum_{j=0}^n x^j F_j^2$.

Theorem 3.3. The following identity holds for arbitrary $x \neq -1$ and integers k and n :

$$\begin{aligned} \sum_{j=0}^n x^j G_{j+k}^2 &= \left(G_{k+1}^2 + x G_k^2 + 2(1-x) G_k G_{k+1} \right) \sum_{j=0}^n x^j F_j^2 \\ &\quad + \left(1 - x^{n+1} F_n^2 \right) \left(G_k^2 - 2 G_k G_{k+1} \right) \\ &\quad + \left(\frac{1 + (-1)^n x^{n+1}}{1+x} \right) 2 G_k G_{k+1}. \end{aligned}$$

Proof. Squaring the addition formula $G_{j+k} = F_{j-1} G_k + F_j G_{k+1}$ gives

$$G_{j+k}^2 = G_k^2 F_{j-1}^2 + G_{k+1}^2 F_j^2 + 2 G_k G_{k+1} F_j F_{j-1}. \quad (3.14)$$

But,

$$\begin{aligned} F_j F_{j-1} &= F_{j-1} (F_{j+1} - F_{j-1}) = F_{j-1} F_{j+1} - F_{j-1}^2 \\ &= F_j^2 - F_{j-1}^2 + (-1)^j, \end{aligned} \quad (3.15)$$

by Cassini's identity. Using (3.15) in (3.14), multiplying through by x^j and summing over j yields the identity of the theorem. $\square$

Setting $x = 1$ in the identity of Theorem 3.3 produces

$$\begin{aligned} \sum_{j=0}^n G_{j+k}^2 &= F_n F_{n+1} (G_{k+1}^2 + G_k^2) + (F_n^2 - 1)(G_{k+1}^2 - G_{k-1}^2) \\ &\quad + (1 + (-1)^n) G_{k+1} G_k; \end{aligned} \quad (3.16)$$

so that

$$\sum_{j=0}^{2n-1} G_{j+k}^2 = F_{2n-1} F_{2n} (G_{k+1}^2 + G_k^2) + (F_{2n-1}^2 - 1)(G_{k+1}^2 - G_{k-1}^2) \quad (3.17)$$

and

$$\begin{aligned} \sum_{j=0}^{2n} G_{j+k}^2 &= F_{2n} F_{2n+1} (G_{k+1}^2 + G_k^2) + (F_{2n}^2 - 1)(G_{k+1}^2 - G_{k-1}^2) \\ &\quad + 2G_{k+1} G_k. \end{aligned} \quad (3.18)$$

In particular,

$$\sum_{j=0}^n F_{j+k}^2 = F_n F_{n+1} F_{2k+1} + (F_n^2 - 1) F_{2k} + (1 + (-1)^n) F_k F_{k+1}; \quad (3.19)$$

so that

$$\sum_{j=0}^{2n-1} F_{j+k}^2 = F_{2n} F_{2n-1} F_{2k+1} + (F_{2n-1}^2 - 1) F_{2k} \quad (3.20)$$

and

$$\sum_{j=0}^{2n} F_{j+k}^2 = F_{2n} F_{2n+1} F_{2k+1} + (F_{2n}^2 - 1) F_{2k} + 2F_k F_{k+1}. \quad (3.21)$$

4 Sums of products

Theorem 4.1. The following identity holds for integers n, s, k and arbitrary x :

$$\begin{aligned}
 & 2F_s F_k \sum_{j=0}^n x^j G_{j+k} G_{j+s} \\
 &= \frac{x(F_s^2 G_{k+1}^2 + F_k^2 G_{s+1}^2) - (2x-1)(F_s^2 G_k^2 + F_k^2 G_s^2) - x^2(F_s^2 G_{k-1}^2 + F_k^2 G_{s-1}^2)}{x^3 - 2x^2 - 2x + 1} \\
 &\quad - \frac{x^{n+1}(x(F_s^2 G_{n+k+2}^2 + F_k^2 G_{n+s+2}^2) - (2x-1)(F_s^2 G_{n+k+1}^2 + F_k^2 G_{n+s+1}^2))}{x^3 - 2x^2 - 2x + 1} \\
 &\quad - \frac{F_{s-k}^2(xG_1^2 - (2x-1)G_0^2 - x^2(G_1 - G_0)^2)}{x^3 - 2x^2 - 2x + 1} \\
 &\quad + \frac{x^{n+1}F_{s-k}^2(xG_{n+2}^2 - (2x-1)G_{n+1}^2 - x^2G_n^2)}{x^3 - 2x^2 - 2x + 1} \\
 &\quad + \frac{x^{n+3}(F_s^2 G_{n+k}^2 + F_k^2 G_{n+s}^2)}{x^3 - 2x^2 - 2x + 1}.
 \end{aligned} \tag{4.1}$$

Proof. Multiply through (2.3) by x^j and sum over j , obtaining

$$2F_s F_k \sum_{j=0}^n x^j G_{j+k} G_{j+s} = F_s^2 \sum_{j=0}^n x^j G_{j+k}^2 + F_k^2 \sum_{j=0}^n x^j G_{j+s}^2 - F_{s-k}^2 \sum_{j=0}^n x^j G_j^2,$$

from which (4.1) follows upon using (3.1) and (3.6). $\square$

In particular, setting $x = 1$ in (4.1) produces

$$\begin{aligned}
 2F_s F_k \sum_{j=0}^n G_{j+k} G_{j+s} &= F_k^2 (G_{n+s} G_{n+s+1} - G_{s-1} G_s) + F_s^2 (G_{n+k} G_{n+k+1} - G_{k-1} G_k) \\
 &\quad - F_{s-k}^2 (G_n G_{n+1} + G_0^2 - G_0 G_1),
 \end{aligned} \tag{4.2}$$

which, by shifting the summation index and writing $k+1$ for k and $s+1$ for s , can also be written as

$$\begin{aligned}
 & 2F_{s+1} F_{k+1} \sum_{j=0}^n G_{j+k} G_{j+s} \\
 &= F_{k+1}^2 (G_{n+s+1} G_{n+s+2} - G_s G_{s+1}) + F_{s+1}^2 (G_{n+k+1} G_{n+k+2} - G_k G_{k+1}) \\
 &\quad - F_{s-k}^2 (G_n G_{n+1} + G_0^2 - G_0 G_1) - 2F_{s+1} F_{k+1} (G_{n+k+1} G_{n+s+1} - G_k G_s);
 \end{aligned} \tag{4.3}$$

giving, in particular,

$$\sum_{j=0}^n G_{j+1} G_{j-2} = (G_n - G_1 + G_0)(G_n + G_1 - G_0). \tag{4.4}$$

Identity (4.3) subsumes Berzsenyi's results [3].

The next result provides an evaluation of the partial sum of the products of two consecutive Fibonacci-like numbers.

Theorem 4.2. The following identity holds for arbitrary integers n and k and arbitrary non-zero number x :

$$2 \sum_{j=0}^n x^j G_{j+k} G_{j+k-1} = \frac{(1-x-x^2)(xG_{k+1}^2 - (2x-1)G_k^2 - x^2G_{k-1}^2)}{x(x^3 - 2x^2 - 2x + 1)} - \frac{x^{n+1}(1-x-x^2)(xG_{n+k+2}^2 - (2x-1)G_{n+k+1}^2 - x^2G_{n+k}^2)}{x(x^3 - 2x^2 - 2x + 1)} + x^2G_{n+k+1}^2 + x^{n+1}G_{n+k}^2 - \frac{1}{x}G_k^2 - G_{k-1}^2. \quad (4.5)$$

In particular,

$$2 \sum_{j=0}^n x^j G_j G_{j-1} = \frac{(1-x-x^2)(xG_1^2 - (2x-1)G_0^2 - x^2(G_1 - G_0)^2)}{x(x^3 - 2x^2 - 2x + 1)} - \frac{x^{n+1}(1-x-x^2)(xG_{n+2}^2 - (2x-1)G_{n+1}^2 - x^2G_n^2)}{x(x^3 - 2x^2 - 2x + 1)} + x^n G_{n+1}^2 + x^{n+1}G_n^2 - \frac{1}{x}G_0^2 - (G_1 - G_0)^2, \quad (4.6)$$

with the special value

$$2 \sum_{j=0}^n G_j G_{j-1} = G_{n+1}G_{n-1} + (G_n - G_0)(G_n + G_0) + (G_1 - G_0)(2G_0 - G_1). \quad (4.7)$$

Proof. Squaring and re-arranging the recurrence relation

$$G_{j+k+1} = G_{j+k} + G_{j+k-1},$$

and multiplying through by x^j and summing, gives

$$2 \sum_{j=0}^n x^j G_{j+k} G_{j+k-1} = \sum_{j=0}^n x^j G_{j+k+1}^2 - \sum_{j=0}^n x^j G_{j+k}^2 - \sum_{j=0}^n x^j G_{j+k-1}^2. \quad (4.8)$$

Shifting the summation index in each case provides

$$\sum_{j=0}^n x^j G_{j+k-1}^2 = x \sum_{j=0}^n x^j G_{j+k}^2 + G_{k-1}^2 - x^{n+1}G_{n+k}^2$$

and

$$\sum_{j=0}^n x^j G_{j+k+1}^2 = \frac{1}{x} \sum_{j=0}^n x^j G_{j+k}^2 - \frac{1}{x}G_k^2 + x^n G_{n+k+1}^2;$$

which when substituted in (4.8) gives (4.5) in view of (3.1). $\square$

Theorem 4.3. If $(G_j)_{j \in \mathbb{Z}}$ and $(H_j)_{j \in \mathbb{Z}}$ are two Fibonacci-like sequences, then

$$2 \sum_{j=0}^n (-1)^j H_{j+r} G_{j+k} G_{j+k-1} = (-1)^n H_{n+r} G_{n+k+1}^2 + (-1)^{n+1} H_{n+r+1} G_{n+k}^2 + H_{r-1} G_k^2 - H_r G_{k-1}^2. \quad (4.9)$$

In particular, we have the alternating sum of the products of three consecutive Fibonacci-like numbers, namely

$$2 \sum_{j=0}^n (-1)^j G_{j+k+1} G_{j+k} G_{j+k-1} = (-1)^n G_{n+k+1}^3 + (-1)^{n+1} G_{n+k+2} G_{n+k}^2 + G_k^3 - G_{k+1} G_{k-1}^2. \quad (4.10)$$

Proof. Set $x = -(1 + \sqrt{5})/2 = -\alpha$ in (4.5) and multiply through by α^r , where r is an arbitrary integer, to obtain

$$2 \sum_{j=0}^n (-1)^j \alpha^{j+r} G_{j+k} G_{j+k-1} = (-1)^n \alpha^{n+r} G_{n+k+1}^2 + (-1)^{n+1} \alpha^{n+r+1} G_{n+k}^2 + \alpha^{r-1} G_k^2 - \alpha^r G_{k-1}^2. \quad (4.11)$$

Similarly, $x = -(1 - \sqrt{5})/2 = -\beta$ in (4.5) gives

$$2 \sum_{j=0}^n (-1)^j \beta^{j+r} G_{j+k} G_{j+k-1} = (-1)^n \beta^{n+r} G_{n+k+1}^2 + (-1)^{n+1} \beta^{n+r+1} G_{n+k}^2 + \beta^{r-1} G_k^2 - \beta^r G_{k-1}^2. \quad (4.12)$$

The identity of the theorem now follows by combining (4.11) and (4.12), since

$$H_j = \frac{C\alpha^j - D\beta^j}{\alpha - \beta},$$

where

$$C = H_1 - H_0\beta, \quad D = H_1 - H_0\alpha.$$

□

The next lemma facilitates deriving an alternative version of Theorem 4.1 and the evaluation of the product $\sum_{j=0}^n x^j G_{j-k} G_{j+k}$.

Lemma 4.4. If j, k and s are integers, then

$$G_{j+k} G_{j+s} = F_{s-1} F_{k-1} G_j^2 + (F_{s-1} F_k + F_s F_{k-1}) G_j G_{j+1} + F_s F_k G_{j+1}^2 \quad (4.13)$$

and

$$G_{j-k} G_{j+k} = (-1)^k F_{k-1} F_{k+1} G_j^2 + (-1)^k F_k^2 G_j G_{j+1} + (-1)^{k-1} F_k^2 G_{j+1}^2. \quad (4.14)$$

Proof. Since, for integers j and m ,

$$G_{j+m} = F_{m-1} G_j + F_m G_{j+1},$$

we have

$$G_{j+k} = F_{k-1}G_j + F_kG_{j+1}, \quad (4.15)$$

$$G_{j+s} = F_{s-1}G_j + F_sG_{j+1}, \quad (4.16)$$

and

$$G_{j-k} = (-1)^k F_{k+1}G_j + (-1)^{k-1} F_kG_{j+1}. \quad (4.17)$$

Multiplication of (4.15) and (4.16) gives (4.13) while multiplication of (4.15) and (4.17) produces (4.14). $\square$

In view of (4.13) we now state an alternative version of Theorem 4.1.

Theorem 4.5. The following identity holds for integers j, s, k and arbitrary x :

$$\begin{aligned} (1-x) \sum_{j=0}^n x^j G_{j+k} G_{j+s} \\ = \left((1-x) F_{s-1} F_{k-1} + F_{s-1} F_k + F_s F_{k-1} + \frac{(1-x)}{x} F_s F_k \right) \sum_{j=0}^n x^j G_j^2 \\ + (F_{s-1} F_k + F_s F_{k-1}) \left(-x^{n+1} G_{n+1} G_n + G_0 G_{-1} \right) \\ + F_s F_k \left(-\frac{1-x}{x} G_0^2 + x^n (1-x) G_{n+1}^2 \right). \end{aligned} \quad (4.18)$$

Proof. Multiply through (4.13) by x^j and sum over j . $\square$

Theorem 4.6. If k and n are integers and x is a variable, then

$$\begin{aligned} \sum_{j=0}^n x^j G_{j-k} G_{j+k} &= (-1)^k \left(F_{k-1} F_{k+1} - \frac{F_k^2}{x} \right) \sum_{j=0}^n x^j G_j^2 + (-1)^k \frac{F_k^2}{x} \sum_{j=0}^n x^j G_{j-1} G_j \\ &+ (-1)^{k-1} F_k^2 \left(-\frac{1}{x} G_0^2 + x^n G_{n+1}^2 \right) \\ &+ (-1)^k \frac{F_k^2}{x} \left(-G_{-1} G_0 + x^{n+1} G_n G_{n+1} \right), \end{aligned} \quad (4.19)$$

where $\sum_{j=0}^n x^j G_j^2$ and $\sum_{j=0}^n x^j G_{j-1} G_j$ are as given in (3.6) and (4.6).

Proof. Multiply (4.14) by x^j and sum. $\square$

In particular,

$$\begin{aligned} \sum_{j=0}^n G_{j-k} G_{j+k} &= (-1)^k \frac{F_k^2}{2} \left(G_n^2 - G_{n+1} G_{n-1} + G_0 G_2 - G_1^2 \right) \\ &+ G_n G_{n+1} - G_{-1} G_0; \end{aligned} \quad (4.20)$$

on account of (3.10) and (4.7).

Corollary 4.7 (Generating function of $G_{j+k}G_{j-k}$).

$$\begin{aligned} \sum_{j=0}^{\infty} x^j G_{j-k} G_{j+k} &= (-1)^k \left(F_{k-1} F_{k+1} - \frac{F_k^2}{x} \right) \frac{x G_1^2 - (2x-1) G_0^2 - x^2 (G_1 - G_0)^2}{x^3 - 2x^2 - 2x + 1} \\ &\quad + (-1)^k F_k^2 \frac{(1-x-x^2)}{2x^2} \frac{(x G_1^2 - (2x-1) G_0^2 - x^2 (G_1 - G_0)^2)}{(x^3 - 2x^2 - 2x + 1)} \\ &\quad - \frac{G_0^2}{x} \left((-1)^{k-1} F_k^2 + \frac{1}{2} \right) - \frac{1}{2} (G_1 - G_0)^2 \\ &\quad - (-1)^k \frac{F_k^2}{x} G_{-1} G_0; \end{aligned} \quad (4.21)$$

valid for $|x| < (3 - \sqrt{5})/2$.

5 Double binomial sums

Lemma 5.1 ([1 Lemma 5]). Let (X_r) be any arbitrary sequence, X_r satisfying a four-term recurrence relation $hX_r = f_1 X_{r-a} + f_2 X_{r-b} + f_3 X_{r-c}$, where h, f_1, f_2 and f_3 are arbitrary non-vanishing functions and a, b and c are integers. Then, the following identities hold:

$$\sum_{j=0}^n \sum_{i=0}^j \binom{n}{j} \binom{j}{i} f_3^{n-j} f_2^{n+j-i} f_1^i X_{r-cn+(c-b)j+(b-a)i} = h^n f_2^n X_r, \quad (5.1)$$

$$\sum_{j=0}^n \sum_{i=0}^j \binom{n}{j} \binom{j}{i} f_2^{n-j} f_3^{n+j-i} f_1^i X_{r-bn+(b-c)j+(c-a)i} = h^n f_3^n X_r, \quad (5.2)$$

$$\sum_{j=0}^n \sum_{i=0}^j \binom{n}{j} \binom{j}{i} f_1^{n-j} f_3^{n+j-i} f_2^i X_{r-an+(a-c)j+(c-b)i} = h^n f_3^n X_r, \quad (5.3)$$

$$\sum_{j=0}^n \sum_{i=0}^j (-1)^i \binom{n}{j} \binom{j}{i} h^i f_3^{n-j} f_2^{j-i} X_{r-(c-a)n+(c-b)j+bi} = (-f_1)^n X_r, \quad (5.4)$$

$$\sum_{j=0}^n \sum_{i=0}^j (-1)^i \binom{n}{j} \binom{j}{i} h^i f_3^{n-j} f_1^{j-i} X_{r-(c-b)n+(c-a)j+ai} = (-f_2)^n X_r \quad (5.5)$$

and

$$\sum_{j=0}^n \sum_{i=0}^j (-1)^i \binom{n}{j} \binom{j}{i} h^i f_2^{n-j} f_1^{j-i} X_{r-(b-c)n+(b-a)j+ai} = (-f_3)^n X_r. \quad (5.6)$$

Theorem 5.2. The following identities hold for non-negative integer n and integers s, k, m, r :

$$\begin{aligned} \sum_{j=0}^n \sum_{i=0}^j (-1)^{i+(s+k+1)j} \binom{n}{j} \binom{j}{i} F_s^{n-j+i} F_k^{n+j} F_m^{2n-i} F_{m-s}^{n-j} F_{m-k}^{n+j-i} F_{s-k}^i G_{r+kn+(s-k)j+(m-s)i}^2 \\ = (F_m F_k F_{m-k}^2 F_{m-s} F_{s-k})^n G_r^2, \end{aligned} \quad (5.7)$$

$$\sum_{j=0}^n \sum_{i=0}^j (-1)^{j+(s+k)(i+j)} \binom{n}{j} \binom{j}{i} F_s^{n+j} F_k^{n-j+i} F_m^{2n-i} F_{m-s}^{n+j-i} F_{m-k}^{n-j} F_{s-k}^i G_{r+sn+(k-s)j+(m-k)i}^2$$

$$= (-1)^{(s+k-1)n} (F_m F_s F_{m-s}^2 F_{m-k} F_{s-k})^n G_r^2, \quad (5.8)$$

$$\sum_{j=0}^n \sum_{i=0}^j (-1)^{(s+k)(i+j)+i} \binom{n}{j} \binom{j}{i} F_s^{n+j-i} F_k^i F_m^{n+j} F_{m-s}^{n+j-i} F_{m-k}^i G_{r+mn+(k-m)j+(s-k)i}^2$$

$$= (-1)^{(s+k)n} (F_m F_s F_{m-k} F_{s-k} F_{m-s}^2)^n G_r^2. \quad (5.9)$$

Proof. Change j to r and re-arrange the identity of Theorem 2.2 as

$$F_{m-s} F_{m-k} F_{s-k} G_r^2 = (-1)^{s+k} F_k F_s F_{s-k} G_{r+m}^2$$

$$+ (-1)^{s+k+1} F_k F_m F_{m-k} G_{r+s}^2$$

$$+ F_s F_m F_{m-s} G_{r+k}^2.$$

In Lemma 5.1 with $X_r = G_r^2$, set $h = F_{m-s} F_{m-k} F_{s-k}$, $f_1 = (-1)^{s+k} F_k F_s F_{s-k}$, $f_2 = (-1)^{s+k+1} F_k F_m F_{m-k}$, $f_3 = F_s F_m F_{m-s} G_{r+k}^2$, $a = -m$, $b = -s$ and $c = -k$ in identities (5.1) – (5.6). $\square$

Acknowledgement

We thank a referee whose comments and suggestions helped to improve the presentation.

References

- [1] K. Adegoke, *Weighted tribonacci sums*. *Konuralp Journal of Mathematics* **8**:2 (2020), 355–360.
- [2] K. Adegoke, *A new Fibonacci identity and its associated summation identities*. Preprint, available at <https://arxiv.org/abs/1809.06850> (2018).
- [3] G. Berzsenyi, *Sums of products of generalized Fibonacci numbers*. *The Fibonacci Quarterly* **13** (1975), 343–344.
- [4] B.A. Brousseau, *A sequence of power formulas*. *The Fibonacci Quarterly* **6** (1968), 81–83.
- [5] S. Vajda, *Fibonacci and Lucas Numbers, and the Golden Section: Theory and applications*, Dover Press, (2008).
- [6] D. Zeitlin, *On the sums $\sum_{k=0}^n k^p$ and $\sum_{k=0}^n (-1)^k k^p$* . *Proceedings of the American Mathematical Society* **2** (1964), 105–107.



ISSN: 2820-7114

Moroccan Journal of Algebra and Geometry with Applications

Supported by Sidi Mohamed Ben Abdellah University, Fez, Morocco

Volume 4, Issue 1 (2025), pp 74-80

Title :

On finiteness of some noncommutative Gröbner bases over finite fields

Author(s):

Yatma Diop and Laila Mesmoudi

On finiteness of some noncommutative Gröbner bases over finite fields

Yatma Diop¹ and Laila Mesmoudi²

^{1,2} Department of Mathematics and Computer Sciences, Cheikh Anta Diop University, Dakar, Senegal.

¹e-mail: yatma.diop@ucad.edu.sn

²e-mail: laila.mesmoudi@ucad.edu.sn

Communicated by Najib Mahdou

(Received 26 July 2024, Revised 28 November 2024, Accepted 03 December 2024)

Abstract. Eisenbud and al. proved that if $\mathbb{K}$ is a field of characteristic 0 and $\gamma : \mathbb{K}\langle X_1, \dots, X_n \rangle \longrightarrow \mathbb{K}[x_1, \dots, x_n]$, the map from the noncommutative polynomial ring to the commutative one which sends X_i to x_i then any noncommutative ideal $\mathcal{J} = \gamma^{-1}(\mathcal{I})$ has a finite Gröbner basis even after a linear change of variables. By an example they prove that if $\mathbb{K}$ is of characteristic $p \neq 0$ then this result does not always hold. In this work, we consider a coefficient finite field $\mathbb{K}$. Then we first give a necessary and sufficient condition for any ideal of the form $\gamma^{-1}(\mathcal{I})$ to have finite Gröbner basis. We secondly prove that this condition is satisfied for any 0-dimensionnal $\mathcal{I}$. We finish by investigating the particular case where $\mathcal{I}$ is a principal ideal.

Key Words: Finite field, Finiteness, Initial ideal, Linear change of variables, Noncommutative Gröbner bases.

2020 MSC: 16Z05, 08A62, 13B25, 13B02.

Dedicated to our Professor David E. Dobbs for his 80th Birthday.

1 Introduction

The concept of Gröbner basis was introduced by Bruno Buchberger in the context of commutative polynomial ring $\mathbb{K}[x_1, \dots, x_n]$ with coefficients in a field $\mathbb{K}$ during his PhD thesis. See [2]. Naively, a Gröbner basis of an ideal $\mathcal{I} \subset \mathbb{K}[x_1, \dots, x_n]$ can be defined as a set of generators of $\mathcal{I}$ which solves efficiently the ideal membership problem by using the generalization of the euclidean algorithm to the multivariate polynomials. Furthermore, Buchberger's algorithm guarantees the existence of a finite Gröbner basis for any ideal of $\mathbb{K}[x_1, \dots, x_n]$.

Except the ideal membership problem solving, Gröbner bases have several other interesting applications: polynomial system solving, determination of a basis of an intersection, a product or a quotient of two ideals, etc. See [3] and [7].

Gröbner bases were then extended to many other algebras. One of the first generalizations was their adaptation to the noncommutative polynomial ring $\mathbb{K}\langle X_1, \dots, X_n \rangle$ presented in [1] and [8]. An immediate consequence of this extension is the lost of the finiteness. Most of the ideals of $\mathbb{K}\langle X_1, \dots, X_n \rangle$ do not have a finite Gröbner basis. The classical example is the principal ideal $\mathcal{J} = \langle X_1 X_2 X_1 - X_2 X_1 \rangle$. Any generator set of $\mathcal{J}$ which solves the ideal membership problem contains polynomials $f_k = X_1 X_2^k X_1 - X_2^k X_1$ for any $k \in \mathbb{N}^*$. So $\mathcal{J}$ does not admit a finite Gröbner basis. Thus characterizing

noncommutative ideals that have a finite Gröbner basis became an interesting challenge. In this direction, D. Eisenbud, I. Peeva and B. Sturmfels proved in [6] that if $\mathbb{K}$ is a field of characteristic 0 and if $\gamma : \mathbb{K}\langle X_1, \dots, X_n \rangle \longrightarrow \mathbb{K}[x_1, \dots, x_n]$ is the map from the noncommutative polynomial ring to the commutative one which sends X_i to x_i then any noncommutative ideal $\mathcal{J} = \gamma^{-1}(\mathcal{I})$ has a finite Gröbner basis even after a linear change of variables. In [5], Y. Diop and D. Sow treated the opposite problem. They showed that if a noncommutative ideal $\mathcal{J}$ has a finite Gröbner basis and contains all commutators then there exists an ideal $\mathcal{I}$ of $\mathbb{K}[x_1, \dots, x_n]$ such that $\mathcal{J} = \gamma^{-1}(\mathcal{I})$. They also described how to find a generator set of the ideal $\mathcal{I}$.

The combination of these two results yields a characterization of noncommutative ideals that have a finite Gröbner basis and contain commutators in the case of a field of characteristic 0.

Recently, L. Mesmoudi and Y. Diop proved in [4] that the map γ can be replaced by any surjective homomorphism $\lambda : \mathbb{K}\langle X_1, \dots, X_n \rangle \longrightarrow \mathbb{K}[x_1, \dots, x_n]$.

When the coefficient field $\mathbb{K}$ is finite then we can have an ideal $\mathcal{I}$ of $\mathbb{K}[x_1, \dots, x_n]$ such that $\gamma^{-1}(\mathcal{I})$ has no finite Gröbner basis. See *Example 3*. Hence we are interested into finding conditions for which a noncommutative ideal of the form $\mathcal{J} = \gamma^{-1}(\mathcal{I})$ has a finite Gröbner basis when $\mathbb{K}$ is a finite field.

In all the paper:

1. $\mathbb{K}$ is a field;
2. (a) $\mathbb{K}[x_1, \dots, x_n]$ is the n -variate commutative polynomial ring over $\mathbb{K}$;
 (b) $\mathbb{M} = \{x_1^{\alpha_1} \dots x_n^{\alpha_n}\}$ is the set of monomials of $\mathbb{K}[x_1, \dots, x_n]$;
 (c) $<$ is a monomial order on $\mathbb{M}$;
 (d) For a non nil polynomial g , $\text{in}_{<}(g)$ is the leading monomial g w.r.t $<$;
 (e) $\mathcal{I} \subset \mathbb{K}[x_1, \dots, x_n]$ is an ideal given by a minimal Gröbner basis G w.r.t $<$ and $\text{in}_{<}(\mathcal{I}) = \langle \text{in}_{<}(g), g \in \mathcal{I} \rangle$ is the initial ideal of $\mathcal{I}$;
3. (a) $\mathbb{K}\langle X_1, \dots, X_n \rangle$ is the n -variate noncommutative polynomial ring over $\mathbb{K}$;
 (b) $\mathbb{M}'$ is the set of monomials of $\mathbb{K}\langle X_1, \dots, X_n \rangle$;
 (c) $<<$ is the lexicographic extension of $<$ on $\mathbb{M}'$ (see *Proposition 2.3.* for the definition);
 (d) $\text{in}_{<<}(g)$ is the leading monomial of $0 \neq g \in \mathbb{K}\langle X \rangle$ w.r.t $<<$;
 (a) $\gamma : \mathbb{K}\langle X_1, \dots, X_n \rangle \longrightarrow \mathbb{K}[x_1, \dots, x_n]$ replaces X_i by x_i ;
 (b) $\delta : \mathbb{K}[x_1, \dots, x_n] \longrightarrow \mathbb{K}\langle X_1, \dots, X_n \rangle$ replaces x_i by X_i by putting variables in the increasing order

2 Preliminaries

In this section, we recall the Gröbner bases computation of an ideal of type $\mathcal{J} = \gamma^{-1}(\mathcal{I})$ designed in [6]. The two elements in the next definition play a fundamental role.

Definition 2.1. Let $\mathcal{L}$ be a monomial ideal of $\mathbb{K}[x_1, \dots, x_n]$.

1. A monomial $m \in \mathcal{L}$ is called a minimal generator of $\mathcal{L}$ if $\frac{m}{u} \notin \mathcal{L}$ for any monomial $u \neq 1$ which divides m .

The set of minimal generators of $\mathcal{L}$ will be denoted $\mathcal{M}(\mathcal{L})$.

2. Let $m = x_p^{\alpha_p} \cdots x_q^{\alpha_q}$, $p < \cdots < q$ be a minimal generator of $\mathcal{L}$. We define the set

$$U_{\mathcal{L}}(m) = \{u \in \mathbb{M} \cap \mathbb{K}[x_{p+1}, \dots, x_{q-1}] \mid u \frac{m}{x_p} \notin \mathcal{L}, u \frac{m}{x_q} \notin \mathcal{L}\}.$$

Example 2.2. Let $\mathcal{L} = \langle x_1 x_2 x_3, x_1^2 x_3, x_2 x_3^2 \rangle$ be an ideal of $\mathbb{K}[x_1, x_2, x_3]$. Then $x_1 x_2 x_3$ and $x_2 x_3^2$ are minimal generators of $\mathcal{L}$.

$$U_{\mathcal{L}}(x_1 x_2 x_3) = \{u \in \mathbb{K}[x_2] \mid u x_2 x_3 \notin \mathcal{L}, u x_1 x_2 \notin \mathcal{L}\} = \{x_2^d, d \in \mathbb{N}\} \text{ and } U_{\mathcal{L}}(x_2 x_3^2) = \{1\}$$

Remark that the second point of the definition can be extended to the case $p = q$. If $m = x_p^{\alpha_p}$ then $U_{\mathcal{L}}(m) = \{1\}$.

More generally, $1 \in U_{\mathcal{L}}(m)$ for any minimal generator m of a monomial ideal $\mathcal{L}$.

The following theorem is the main result of [6]. It described a computation of a Gröbner basis of $\gamma^{-1}(\mathcal{I})$ from one of $\mathcal{I}$.

Proposition 2.3. (See [6]) Let $<$ be a monomial order on $\mathbb{M}$. Then the ordering $\ll$ on $k\langle X \rangle$ defined by

$$u \ll v \Leftrightarrow \begin{cases} \gamma(u) < \gamma(v) \\ \text{or} \\ \gamma(u) = \gamma(v) \text{ and } u <_{\text{lex}} v \end{cases}$$

is a monomial order on $\mathbb{M}'$. It is called the lexicographic extension of $<$.

Theorem 2.4 (Eisenbud, Peeva, Sturmfels). If $\mathcal{J} = \gamma^{-1}(\mathcal{I})$ and G , a minimal Gröbner basis of $\mathcal{I}$ w.r.t. $<$ then the set

$$\{X_i X_j - X_j X_i \mid i > j, x_i, x_j \notin \text{in}_{<}(\mathcal{I})\} \cup \{\delta(uf) \mid f \in G, u \in U_{\text{in}_{<}(\mathcal{I})}(\text{in}_{<}(f))\}$$

is a minimal Gröbner basis of $\mathcal{J}$ w.r.t. lexicographic extension $\ll$ of $<$.

This theorem appeared first in [6] (page 2.) and was then revisited and improved in [5] (pages 3. and 4.).

In the rest, when talking about Gröbner bases of $\gamma^{-1}(\mathcal{I})$, it is always w.r.t. lexicographic extension $\ll$ of the considered monomial $<$ on $\mathbb{M}$.

It is clear that the Gröbner basis in Theorem 2.4. is finite if and only if $U_{\text{in}_{<}(\mathcal{I})}(\text{in}_{<}(f))$ is a finite set for any $f \in G$. Some conditions of finiteness are given in the two following results.

Definition 2.5. Let $\mathcal{L}$ be a monomial ideal of $\mathbb{K}[x_1, \dots, x_n]$.

1. $\mathcal{L}$ is said 0-Borel fixed if for any generator m of $\mathcal{L}$ and x_i a divisor of m then $x_j \frac{m}{x_i} \in \mathcal{L} \forall x_j < x_i$.
2. $\mathcal{L}$ is said p -Borel fixed if the following condition is satisfied: for any generator m of $\mathcal{L}$, if x_i^t divides m and x_i^{t+1} does not divide m then $(\frac{x_j}{x_i})^s m \in \mathcal{L} \forall x_j < x_i$ and $s \leq p \cdot t$.

Proposition 2.6. (Refer to [6] page 3. for the proof)

If $\text{in}_{<}(\mathcal{I})$ is 0-Borel fixed or p -Borel fixed for some prime integer p then $U_{\text{in}_{<}(\mathcal{I})}(m)$ is finite for any minimal generator m of $\text{in}_{<}(\mathcal{I})$.

The following theorem is enonciated and used in the Proof of Corollary 1.1. in [6]. Moreover a reference for it is given in the same document.

Theorem 2.7 (Bayer-Galligo-Stilman). If $\mathbb{K}$ is infinite then after a linear change of variables $in_{\prec}(\mathcal{I})$ is 0-Borel fixed or p -Borel fixed for some prime integer p .

Proposition 2.6. and *Theorem 2.7.* imply that if $\mathbb{K}$ is of characteristic 0 then Gröbner bases computed in *Theorem 2.4.* are finite even after a linear change of variables. In other words, for some well chosen linear change of variables and $\mathcal{I}'$, the ideal corresponding to $\mathcal{I}$, $\gamma^{-1}(\mathcal{I}')$ has a finite Gröbner basis.

Example 2.8. Let $\mathcal{I} = \langle x_1 x_2 x_3 + x_1 x_2 + x_1 x_3 + x_2 x_3 \rangle \subset \mathbb{R}[x_1, x_2, x_3]$ be the ideal generated by $x_1 x_2 x_3 + x_1 x_2 + x_1 x_3 + x_2 x_3$.

For any fixed monomial order $\prec$, $in_{\prec}(\mathcal{I}) = \langle x_1 x_2 x_3 \rangle$.

Then a first computation yields $U_{in_{\prec}(\mathcal{I})}(x_1 x_2 x_3) = \{x_2^d, d \in \mathbb{N}\}$.

But after the change of variables $\begin{cases} x_1 \mapsto y_1 + y_3 \\ x_2 \mapsto y_2 + y_3 \\ x_3 \mapsto y_3 \end{cases}$ the ideal becomes:

$$\begin{aligned} \mathcal{I}' &= \langle (y_1 + y_3)(y_2 + y_3)y_3 + (y_1 + y_3)(y_2 + y_3) + (y_1 + y_3)y_3 + (y_2 + y_3)y_3 \rangle \\ &= \langle y_1 y_2 y_3 + y_1 y_3^2 + y_2 y_3^2 + y_3^3 + y_1 y_2 + 2y_1 y_3 + 2y_2 y_3 + 3y_3^2 \rangle \end{aligned}$$

Then by the lexicographic order with $y_1 < y_2 < y_3$ its initial ideal is $\langle y_3^3 \rangle$ and then $U_{in_{\prec}(\mathcal{I}')}(\mathcal{I}') = \{1\}$. So by *Theorem 2.4.* the set:

$$\{Y_1 Y_2 Y_3 + Y_1 Y_3^2 + Y_2 Y_3^2 + Y_3^3 + Y_1 Y_2 + 2Y_1 Y_3 + 2Y_2 Y_3 + 3Y_3^2, Y_2 Y_1 - Y_1 Y_2, Y_3 Y_1 - Y_1 Y_3, Y_3 Y_2 - Y_2 Y_1\}$$

is a Gröbner basis of $\gamma^{-1}(\mathcal{I}')$.

In the case of finite fields there are examples of ideals $\mathcal{I}$ for which there is any finite Gröbner basis for the ideal $\gamma^{-1}(\mathcal{I})$. The following example is discussed in a more general case in [6].

Example 2.9. Let $\mathcal{I} = \langle x_1^4 x_2^2 x_3 + x_1^4 x_2 x_3^2 + x_1^2 x_2^4 x_3 + x_1^2 x_2 x_3^4 + x_1 x_2^4 x_3^2 + x_1 x_2^2 x_3^4 \rangle$ be an ideal of $\mathbb{F}_2[x_1, x_2, x_3]$. $\mathcal{I}$ is invariant under any linear change of variables. Then its initial ideal with respect to any monomial order is of the form $in_{\prec}(\mathcal{I}) = \langle x_i x_j^2 x_k^4 \rangle$ and $U_{in_{\prec}(\mathcal{I})}(x_i x_j^2 x_k^4) = \{x_j^d, d \in \mathbb{N}\}$.

This implies that $U_{in_{\prec}(\mathcal{I})}(in_{\prec}(f))$ is an infinite set and then $\gamma^{-1}(\mathcal{I})$ has no finite Gröbner basis.

By *Theorem 2.7.*, we know that if $\mathbb{K}$ is of characteristic 0 then there exists a change of variables that yields a finite Gröbner basis of $\gamma^{-1}(\mathcal{I})$ for any ideal $\mathcal{I}$. Thus in what follows we will work exclusively with finite fields. More precisely, in all the rest $\mathbb{K} = \mathbb{F}_q$ is the finite field of q elements. Under some conditions we can decide whether $\gamma^{-1}(\mathcal{I})$ has a finite Gröbner basis. We discuss them in the next section.

3 On finiteness of Gröbner bases of $\gamma^{-1}(\mathcal{I})$ with a finite coefficient field

For a monomial ideal $\mathcal{L} \subset \mathbb{F}_q[x_1, \dots, x_n]$ and a minimal generator m of $\mathcal{L}$, the following result yields a sufficient and necessary condition for $U_{\mathcal{L}}(m)$ to be finite.

Proposition 3.1. Let $\mathcal{L} \subset \mathbb{F}_q[x_1, \dots, x_n]$ be a monomial ideal and $m = x_p^{\alpha_p} \dots x_q^{\alpha_q}$ a minimal generator of $\mathcal{L}$. The two following statements are equivalent.

1. For any integer i in $[p+1, q-1]$ there exists $d_i \in \mathbb{N}$ such that $x_i^{d_i} \notin U_{\mathcal{L}}(m)$.
2. $U_{\mathcal{L}}(m)$ is a finite set.

Proof. Let $\mathcal{L}$ be a monomial ideal, $m = x_p^{\alpha_p} \dots x_q^{\alpha_q}$, a minimal generator of $\mathcal{L}$ and $u \in U_{\mathcal{L}}(m)$. Then we can write $u = x_{p+1}^{\beta_{p+1}} \dots x_{q-1}^{\beta_{q-1}}$, $\beta_{p+1}, \dots, \beta_{q-1} \in \mathbb{N}$.

1) $\implies$ 2)

Suppose that for any integer i in $[p+1, q-1]$ there is $d_i \in \mathbb{N}$ such that $x_i^{d_i} \notin U_{\mathcal{L}}(m)$.

$$\begin{aligned} x_i^{d_i} \notin U_{\mathcal{L}}(m) &\implies x_i^d \notin U_{\mathcal{L}}(m) \forall d > d_i \\ &\implies U_{\mathcal{L}}(m) \subseteq \{x_{p+1}^{\beta_{p+1}} \dots x_{q-1}^{\beta_{q-1}}, \beta_i \leq d_{i_0}\} \text{ where } d_{i_0} = \max\{d_i : x_i^{d_i} \in U_{\mathcal{L}}(m)\} \\ &\implies \text{Card}(U_{\mathcal{L}}(m)) \leq \prod_{p+1}^{q-1} d_{i_0} \end{aligned}$$

2) $\implies$ 1)

Conversely if there exists i such that $x_i^{d_i} \in U_{\mathcal{L}}(m) \forall d_i$ then $U_{\mathcal{L}}(m)$ is an infinite set. So if $U_{\mathcal{L}}(m)$ is a finite set then for any i there exists $d_i \in \mathbb{N}$ such that $x_i^{d_i} \notin U_{\mathcal{L}}(m)$. $\square$

Corollary 3.2. Let $\mathcal{I} \subset \mathbb{F}_q[x_1, \dots, x_n]$ be an ideal. Then $\gamma^{-1}(\mathcal{I})$ has a finite Gröbner basis if and only if the first condition of Proposition 3.1. is satisfied for any minimal generator of the initial ideal of $\mathcal{I}$.

For so well-called 0-dimensionnal ideals, we prove that this condition is always satisfied. Those ideals have interesting properties and applications.

Definition 3.3. Let $\mathbb{K}$ be a field. An ideal $\mathcal{I} \subset \mathbb{K}[x_1, \dots, x_n]$ is called a 0-dimensionnal ideal if the quotient ring $\mathbb{K}[x_1, \dots, x_n]/\mathcal{I}$ has a finite dimension as a vector space.

Theorem 3.4. Let $\mathbb{K}$ be a field, $\mathcal{I} \subset \mathbb{K}[x_1, \dots, x_n]$, an ideal and G , a Gröbner basis of $\mathcal{I}$ w.r.t. $<$. Then $\mathcal{I}$ is 0-dimensionnal if and only if for any x_i , there exists $d_i \in \mathbb{N}^*$ and $g \in G$ such that $\text{in}_{<}(g) = x_i^{d_i}$.

From Theorem 3.4. and Corollary 3.2. we have the following result.

Corollary 3.5. Let $\mathcal{I} \subset \mathbb{F}_q[x_1, \dots, x_n]$ be a 0-dimensionnal ideal. Then $\gamma^{-1}(\mathcal{I})$ has a finite Gröbner basis.

Proof. Let $\mathcal{I}$ be a 0-dimensionnal and G , a minimal Gröbner basis of $\mathcal{I}$. Then for any $i \in [1, n]$ there exists $g \in G$ s.t. $\text{in}_{<}(g) = x_i^{d_i}$ for some $d_i \in \mathbb{N}^*$.

Thus for any $f \in G$, $x_i^{d_i} \notin U_{\mathcal{L}}(\text{in}_{<}(f))$. $\square$

Because of Corollary 3.5., the ideals we consider in the rest of the paper are non 0-dimensionnal. Then for any ideal $\mathcal{I} \subset \mathbb{F}_q[x_1, \dots, x_n]$ in the following there exists $i \in [1, n]$ such that $x_i^{d_i} \neq \text{in}_{<}(g)$ for any $d_i \in \mathbb{N}^*$ and any $g \in G$. It is equivalent to say $x_i^{d_i} \notin \text{in}_{<}(\mathcal{I})$ for $d_i \in \mathbb{N}^*$. So the set $A = \{i \in [1, n] \mid x_i^{d_i} \notin \text{in}_{<}(\mathcal{I}) \forall d_i \in \mathbb{N}^*\}$ is non empty.

In the following, we improve the result of Proposition 3.1..

For a monomial $m = x_1^{\beta_1} \dots x_n^{\beta_n}$, we set $\deg_{(m)}(x_i) = \beta_i$.

Proposition 3.6. Let $\mathcal{I} \subset \mathbb{F}_q[x_1, \dots, x_n]$ be a non 0-dimensionnal ideal and A defined as before. Let $i \in A$, $d = \max\{\deg_{m'}(x_i), m' \in \mathcal{M}(\text{in}_{<}(\mathcal{I}))\}$ and $m = x_p^{\alpha_p} \dots x_i^{\alpha_i} \dots x_q^{\alpha_q}$ a minimal generator of $\text{in}_{<}(\mathcal{I})$ such that $\alpha_i \neq d$.

If $x_i^{d-\alpha_i} \in U_{\text{in}_{<}(\mathcal{I})}(m)$ then $x_i^{d_i} \in U_{\text{in}_{<}(\mathcal{I})}(m) \forall d_i \in \mathbb{N}$.

Proof. Let m and d choosen as declared and suppose that $x_i^{d-\alpha_i} \in U_{in_{<}(\mathcal{I})}(m)$. Then $u \in U_{in_{<}(\mathcal{I})}(m)$ for any monomial u which divides $x_i^{d-\alpha_i}$. It follows that $x_i^{d_i} \in U_{in_{<}(\mathcal{I})}(m)$ for any $d_i < d - \alpha_i$ (1*).

In the other side, from $x_i^{d-\alpha_i} \in U_{in_{<}(\mathcal{I})}(m)$ we obtain $m_p = x_i^{d-\alpha_i} \frac{m}{x_p} \notin in_{<}(\mathcal{I})$ and $m_q = x_i^{d-\alpha_i} \frac{m}{x_q} \notin in_{<}(\mathcal{I})$.

We can remark that $\deg_{m_p}(x_i) = \deg_{m_q}(x_i) = d$.

Let m' be a minimal generator.

$$\begin{aligned} m_p, m_q \notin in_{<}(\mathcal{I}) &\implies m' \nmid m_p \wedge m' \nmid m_q \\ &\implies \forall \beta_i \in \mathbb{N}^*, m' \nmid x_i^{\beta_i} m_p \wedge m' \nmid x_i^{\beta_i} m_q \\ &\implies x_i^{d-\alpha_i} x_i^{\beta_i} \in U_{in_{<}(\mathcal{I})}(m) \\ &\implies x_i^{d_i} \in U_{in_{<}(\mathcal{I})}(m) \forall d_i > d - \alpha_i \text{ (2*)} \end{aligned}$$

From (1*) and (2*) we have the result. $\square$

The *Proposition 3.6.* yields a tool to check whether the noncommutative ideal $\gamma^{-1}(\mathcal{I})$, for a commutative ideal $\mathcal{I}$ given by a minimal Gröbner basis, has a finite Gröbner basis. It requires less computation than *Proposition 3.1.*

Now we investigate the special case of principal ideals. For any principal ideal $\mathcal{I} = \langle g \rangle \subset \mathbb{F}_q[x_1, \dots, x_n]$ and its initial ideal $\mathcal{L} = \langle in_{<}(g) \rangle$, we have $U_{\mathcal{L}}(in_{<}(g)) = \{1\}$ or $U_{\mathcal{L}}(in_{<}(g))$ is an infinite set. A necessary and sufficient condition to obtain $U_{\mathcal{L}}(in_{<}(g)) = \{1\}$ is given in the following result.

Proposition 3.7. *Let $\mathcal{I} = \langle g \rangle \subset \mathbb{F}_q[x_1, \dots, x_n]$ be a principal ideal. Then $\gamma^{-1}(\mathcal{I})$ has a finite Gröbner basis if and only if $in_{<}(g)$ is a product of powers of two consecutive variables even after a linear change of variables.*

Proof. After a linear change of variables, if $in_{<}(g) = y_i^{\alpha_i} y_{i+1}^{\alpha_{i+1}}$ for some $1 \leq i \leq n-1$ and $\alpha_i, \alpha_{i+1} \in \mathbb{N}$ then $U_{\mathcal{L}}(in_{<}(g)) = \{1\}$.

If $in_{<}(g) \neq y_i^{\alpha_i} y_{i+1}^{\alpha_{i+1}}$ for any $1 \leq i \leq n-1$ and $\alpha_i, \alpha_{i+1} \in \mathbb{N}$ then $in_{<}(g) = y_p^{\alpha_p} \dots y_q^{\alpha_q}$ with $p+1 < q$ and $\alpha_p \neq 0, \alpha_q \neq 0$. Thus $y_t^{\alpha_t} \in U_{\mathcal{L}}(in_{<}(g)) \forall (t, \alpha_t) \in [p, q] \times \mathbb{N}$. And then $U_{\mathcal{L}}(in_{<}(g))$ is an infinite set. $\square$

The previous result means that in the case of a principal ideal $\mathcal{I} = \langle g \rangle$, to decide whether $\gamma^{-1}(\mathcal{I})$ has a finite Gröbner basis or not, one has only to look for the existence of a linear change variables for which $in_{<}(g) \in \mathbb{F}_q[y_i, y_{i+1}]$.

Example 3.8. Let $\mathcal{I} = \langle x_1^4 x_2^2 x_3 \rangle \subset \mathbb{F}_2[x_1, x_2, x_3]$. By the change of variables in *Example 2.8.*, $\{Y_1^4 Y_2^2 Y_3 + Y_1^4 Y_3^3 + Y_2^2 Y_3^5 + Y_3^7, Y_2 Y_1 - Y_1 Y_2, Y_3 Y_1 - Y_1 Y_3, Y_3 Y_2 - Y_2 Y_3\}$ is a Gröbner basis of $\gamma^{-1}(\mathcal{I})$.

More generally, for a principal monomial ideal, such a change of variables always works.

Corollary 3.9. *$\gamma^{-1}(\mathcal{I})$ has a finite Gröbner basis for any monomial principal ideal $\mathcal{I} \subset \mathbb{F}_q[x_1, \dots, x_n]$.*

Proof. Let m be a monomial and $\mathcal{I} = \langle m \rangle$. We order variables such that those of m are the last q ones.

Namely $m = x_{n-q+1}^{\alpha_{n-q+1}} \dots x_n^{\alpha_n}$ where $\alpha_i \neq 0 \forall 1 \leq i \leq q$. Consider the change of variables $\begin{cases} x_n \mapsto y_n \\ x_i \mapsto y_n + y_i \forall i < n \end{cases}$

Then m becomes $m' = y_n^{\beta_n} + \sum_j \lambda_j m_j$, where m_j is a monomial $\forall j$ and

$\deg_{m_j}(y_n) < \beta_n$. So by the lexicographic order with $y_1 < \dots < y_n$ we have $in_{<}(\mathcal{I}') = \langle y_n^{\beta_n} \rangle$ and then $U_{in_{<}(\mathcal{I}')} (y_n^{\beta_n}) = \{1\}$. $\square$

Acknowledgment

We are grateful of the "Ecole Doctorale de Mathématiques et Informatique" of the Cheikh Anta Diop University of Dakar which partially funded this investigation.

References

- [1] G. M. Bergmann, *The diamond lemma for ring theory*, *Adv. Math.* 29 (1978), 178-218.
- [2] B. Buchberger, *PhD thesis 1965: An algorithm for finding the basis elements of the residue class of a zero dimensional ideal*, *Journal of Symbolic Computation* 41(2006) 475-511.
- [3] D. Cox, J. Little and D. O'Shea, *Ideals, Varieties and Algorithms An Introduction to Computational Algebraic Geometry and Commuative Algebra*, Second edition Springer, Unergraduate Texts in Mathematics 1997.
- [4] Y. Diop and L. Mesmoudi, *A contribution to the study of a class of noncommutative ideals admitting finite Gröbner bases* (to appear soon in Springer).
- [5] Y. Diop and D. Sow, *On finite noncommutative Gröbner bases*, *Algebra Colloq.* 27(3) (2020), 381-388.
- [6] D. Eisenbud, I. Peeva and B. Sturmfels, *Noncommutative Gröbner bases for commutative algebras*, *Proc. Amer. Math. Soc.* 126 (1998), 687-691
- [7] J. C. Faugère, *Calcul efficace des bases de Gröbner et applications*, Février 2007.
- [8] T. Mora, *An introduction to commutative and non-commutative Gröbner Bases*, *Journal of Theoretical Computer Science*, 13 (1994), 131-173.
- [9] I. Peeva, *0-Borel fixed ideals*, *J. Algebra* 184 (1996), 945-984.
- [10] I. Peeva, M. Stillman, *The minimal free resolution of a Borel ideal*, *Expo. Math.* 26(3) (2008), 237-247.



ISSN: 2820-7114

Moroccan Journal of Algebra and Geometry with Applications

Supported by Sidi Mohamed Ben Abdellah University, Fez, Morocco

Volume 4, Issue 1 (2025), pp 81-89

Title :

On 2-nil-clean commutative rings

Author(s):

Chahrazade Bakkari, Mohamed Es-Saidi, and Moutu Abdou Salam Moutui

On 2-nil-clean commutative rings

Chahrazade Bakkari¹, Mohamed Es-Saidi² and Moutu Abdou Salam Moutui³

¹ Department of Mathematics, Faculty of Science, University Moulay Ismail Meknes, Morocco.

e-mail: cbakkari@hotmail.com

² Department of Mathematics, Faculty of Science, University Moulay Ismail Meknes, Morocco.

e-mail: saidi1972@gmail.com

³ STEM Division, American University of Afghanistan, Doha Campus, Qatar.

e-mail: mmoutui@auaf.edu.af

Communicated by Najib Mahdou

(Received 14 July 2024, Revised 09 December 2024, Accepted 16 December 2024)

Abstract. A ring R is said to be 2-nil-clean if any element in R can be written as the sum of two idempotents and a nilpotent [\[7\]](#). In this paper, we exhibit the connections between this ring and other related classes of rings. Our specific aim is to illustrate how the 2-nil clean condition behaves with respect to several types of ring extensions such as polynomial ring, power series ring, amalgamated algebra and pullback. Our results produce new and original classes of 2-nil-clean rings subject to various ring theoretic properties.

Key Words: Amalgamated algebra, trivial ring extension, nil-clean ring, 2-nil-clean ring, weakly-nil-clean ring, pullback.

2020 MSC: 13F05, 13A15, 13E05, 13F20, 13C10, 13C11, 13F30, 13D05.

Dedicated to our Professor David E. Dobbs for his 80th Birthday.

1 Introduction

Throughout this paper all rings are assumed to be commutative with unity. We denote respectively by $U(R)$, $\text{Idem}(R)$ and $\text{Nilp}(R)$ the multiplicative group of units of R , the set of all idempotent elements of R , and the set of all nilpotent elements of the ring R . The determinant of a square matrix B is denoted by $\det(B)$. Let A be a ring and M be an A -module. The trivial ring extension of A by M (also called the idealization of M over A) is the ring $R = A \ltimes M$ whose underlying group is $A \times M$ with multiplication given by $(a, m)(b, n) = (ab, an + bm)$ for each $a, b \in A$ and $m, n \in M$. This notion has been the subject of several works in the area, and it is a fertile field of research in the theory of rings (see [\[16, 18\]](#) and the reference therein). Trivial ring extensions have been studied extensively; and considerable work, part of is summarized in Glaz's book [\[16\]](#) and Huckaba's book [\[18\]](#), has been concerned with these extensions. Mainly, Trivial ring extensions have been useful for solving many open problems and conjectures in both commutative and non-commutative ring theory.

In 2006, M. D'Anna and M. Fontana [\[13\]](#) introduced a new construction, called amalgamated duplication of a ring A along an A -submodule E of $Q(A)$ (the total ring of fractions of A) such that $E^2 \subseteq E$. When $E^2 = \{0\}$, this construction coincides with the trivial ring extension of A by E . Motivations and more applications of the amalgamated duplication $A \bowtie E$ of A along an A -submodule E of $Q(A)$ are discussed in more details, especially in the case E is an ideal of A , see for instance [\[13, 11\]](#). In 2010, D'Anna, Finocchiaro and Fontana [\[11\]](#) extended the notion of amalgamated duplication

construction $A \bowtie I$ of a ring A along an ideal I of A to the general context of ring homomorphism extensions as follows:

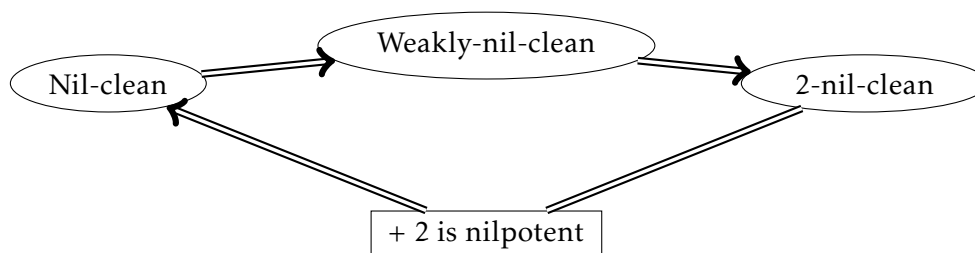
Let A and B be two rings with identity elements, J be an ideal of B and let $f : A \rightarrow B$ be a ring homomorphism. In this setting, we consider the following subring of $A \times B$; $A \bowtie^f J := \{(a, f(a) + j) \mid a \in A, j \in J\}$ called the amalgamation of A and B along J with respect to f . This construction is a generalization of the amalgamated duplication of a ring along an ideal (introduced and studied by D'Anna and Fontana in [13, 11]). The usefulness of amalgamation, as mentioned in [11], comes from the fact that many of the classical constructions (such as $A + XB[X]$, $A + XB[[X]]$, and the $D + M$ constructions) can be studied as a special case of amalgamation, and amalgamation itself can be studied using pullbacks.

In [10], A. J. Diesl introduced a new class of rings and called it nil-clean ring. Recall that a ring R is called nil-clean if each of its elements can be written as the sum of an idempotent and a nilpotent. It was proved in [10] that every nil-clean ring is clean. Various authors have studied nil-clean rings and related notions in [9, 10, 19]. Examples of nil clean elements include all idempotents, nilpotents and unipotents (that is an element which can be written in the form $1 + n$ for some nilpotent n), also, any Boolean ring is a nil-clean ring. It is worthwhile noting that any homomorphic image of a nil-clean ring is also nil-clean.

In [9], P. V. Danchev and W. Wm. McGovern introduced a generalization of the nil-clean rings, and they called it the weakly-nil-clean rings, recall that a ring is said to be weakly-nil-clean if each of its elements can be written as a sum or difference of a nilpotent and an idempotent. They proved that the class of weakly-nil-clean rings is closed under homomorphic images. They proved, again, that if R is a ring and I is an ideal of R then if R is weakly-nil-clean then R/I so is, the converse holds when I is nil ideal of R , ie., there is a positive integer $n \geq 2$ such that $I^n = 0$.

In [7], H. Chen and M. Sheibani introduced a new generalization of the nil-clean rings, and called it 2-nil-clean ring. Recall that a ring R is called 2-nil-clean if each of its elements can be written as the sum of two idempotents and a nilpotent. It is clear that any homomorphic image of a 2-nil-clean ring is, again, 2-nil-clean. It was proved that a ring R is strongly 2-nil-clean if and only if for all $a \in R$, $a - a^3 \in R$ is nilpotent, if and only if for all $a \in R$, $a^2 \in R$ is nil-clean, if and only if every element in R is the sum of a tripotent and a nilpotent, recall that an element $e \in R$ is tripotent if $e^3 = e$. It is proved, again, that a ring R is nil-clean if and only if $2 \in R$ is nilpotent and R is 2-nil-clean.

The following diagram of implications summarizes the relations between the main three notions involved in this paper:



In this paper, we exhibit the connections between this ring and other related classes of rings. We examine how the 2-nil-clean property behave with respect to several ring-theoretic constructions such as polynomial ring, power series ring, amalgamated algebra and pullback. Our results produce new and original classes of 2-nil-clean rings subject to various ring theoretic properties.

2 Main Results

Our first proposition of this section establishes the relationship between the three notions of nil-clean, weakly-nil-clean and 2-nil-clean.

Proposition 2.1. 1. Every nil-clean ring is weakly-nil-clean.

2. Every weakly-nil-clean ring is 2-nil-clean.

Proof.

(1) Trivial.

(2) This follows from [7] Corollary 4.6]. □

Remark 2.2. Note that a 2-nil-clean need not be weakly-nil-clean. For instance, take $A := \mathbb{Z}_3$, the ring of integers modulo 3. One can easily check that $A \times A$ is 2-nil-clean which is not weakly-nil-clean.

In the next proposition, we show that a 2-nil-clean ring R with unit stable range 1 is a 4-good ring. Recall that a ring R is 4-good if each of its element can be written as a sum of 4 units.

Proposition 2.3. Let R be a ring with unit stable range 1. If R is 2-nil-clean, then R is a 4-good ring.

Proof. Assume that R is 2-nil-clean with unit stable range 1. Let $x \in R$. Then $x = e_1 + e_2 + w$ for some idempotent elements e_1, e_2 and a nilpotent element w of R . Using the fact that R has unit stable range 1, there exists $u \in U(R)$ such that $e_1 - 1.u \in U(R)$. Likewise, $e_2 - 1.u' \in U(R)$ for some $u' \in U(R)$. Therefore, $e_1 = u + v$ and $e_2 = u' + v'$ for some $v, v' \in U(R)$. Hence, $x = u + v + u' + v' + w$, making x , a 4-good element. Thus, R is a 4-good ring. □

It is well known that if $f(X) = \sum_{i=0}^{\infty} a_i X^i$ is nilpotent then for all i , a_i is nilpotent. The next proposition shows that the polynomial and power series rings are never 2-nil-clean.

Proposition 2.4. Let A be a commutative ring A . Then:

1. The ring of formal power series $A[[X]]$ is never 2-nil-clean.
2. The polynomial ring $A[X]$ is never 2-nil-clean.

Proof. Assume by the way of contradiction that the element of $A[[X]]$ (resp., $A[X]$) X is 2-nil-clean. Then $X = e + f + b$ (resp., $X = e' + f' + b'$) where $e, f \in \text{Idem}(A[[X]])$ (resp., $e', f' \in \text{Idem}(A[X])$) and $b \in \text{Nilp}(A[[X]])$ (resp., $b' \in \text{Nilp}(A[X])$). Note that $\text{Idem}(A[[X]]) = \text{Idem}(A[X]) = \text{Idem}(A)$ since A is commutative ring, so $-e - f + X \in \text{Nilp}(A[[X]])$ (resp., $-e' - f' + X \in \text{Nilp}(A[X])$), which is a contradiction. Hence, $A[[X]]$ (resp., $A[X]$) is never 2-nil-clean. □

The next proposition exhibits the relationship between the 2-nil-clean and 2-nil-good properties. Recall that a ring R is said to be 2-nil-good if each of its element is sum of two units and a nilpotent element of R .

Proposition 2.5. Let R be a ring in which 2 is invertible. If R is 2-nil-clean, then R is 2-nil-good. The converse holds if R is UU(every unit is unipotent).

Proof. Assume that R is 2-nil-clean. Let $a \in R$. Then $\frac{a+2}{2} = e_1 + e_2 + w$ for some $e_1, e_2 \in \text{Idem}(R)$ and $w \in \text{Nilp}(R)$. So, $a + 2 = 2e_1 + 2e_2 + 2w$ and therefore, $a = (2e_1 - 1) + (2e_2 - 1) + 2w$, with $(2e_1 - 1)^2 = 1$ and $(2e_2 - 1)^2 = 1$, making a , a 2-nil-good element. Hence, R is 2-nil-good. Conversely, assume that R is a UU 2-nil-good ring. Let $x \in R$. Then $x = u_1 + u_2 + w$ for some $u_1, u_2 \in U(R)$ and $w \in \text{Nilp}(R)$. Using the fact that R is UU, it follows that $x = 1 + b_1 + 1 + b_2 + w = 1 + 1 + W$, where $W = b_1 + b_2 + w \in \text{Nilp}(R)$. Hence, x is a 2-nil-good element, making R , a 2-nil-good ring. □

Recall that a ring A is tripotent if for any element a of A , $a^3 = a$. Also, in view of [7] Theorem 3.6] we have a ring A is 2-nil-clean if and only if $A/Nilp(A)$ is tripotent. Next, we examine the 2-nil-clean property in reduced ring.

Proposition 2.6. *For a commutative ring A , the following assertions are equivalent:*

1. A is tripotent.
2. A is 2-nil-clean and reduced ring.

Proof.

(1) $\Rightarrow$ (2) It is clear that any tripotent ring is 2-nil-clean (for all $x \in A$, we have $x^3 = x$ and we can write $x = x + 0$). Furthermore, every tripotent ring (that is, a ring R is tripotent if for any $r \in R$, there exist an integer $n > 1$ such that $r^n = r$) is reduced (see [15] Lemma 2.19 and Proposition 3.1]). In particular, for $n = 3$, any tripotent ring is reduced.

(2) $\Rightarrow$ (1) It is known by [7] Theorem 3.6] that a ring A is 2-nil-clean if and only if $A/Nilp(A)$ is tripotent. Since A is reduced, A is tripotent. □

3 2-nil-clean property in amalgamated algebra

The following result is to study the transfer of tripotent property to amalgamated algebras, recall that a ring R is tripotent if for every element $r \in R$, $r^3 = r$.

Proposition 3.1. *Let (A, B) be a pair of commutative rings, J be an ideal of B and $f : A \rightarrow B$ be a ring homomorphism. Then the following are equivalent.*

- (1) $A \bowtie^f J$ is tripotent.
- (2) A and $f(A) + J$ are tripotent.

Proof.

(1) $\Rightarrow$ (2) In virtue of [11] Proposition 5.1], A and $f(A) + J$ are homomorphic images of $A \bowtie^f J$, the result follows, since any homomorphic image of a tripotent element is, again, tripotent.

(2) $\Rightarrow$ (1) Assume that A and $f(A) + J$ are tripotent. Let $(x, f(x) + j) \in A \bowtie^f J$ such that $x \in A$, $j \in J$. Then x and $f(x) + j$ are tripotent. Then $x^3 = x$ and $(f(x) + j)^3 = f(x) + j$. Thus $(x, f(x) + j) = (x, f(x) + j)^3$ is tripotent. □

In particular, we have the following result:

Corollary 3.2. *Let A be a ring and I be an ideal of A . Then:*

$A \bowtie I$ is tripotent if and only if so is A .

Proof. In this case we have $f = id_A$ and $f(A) + I = A$. In view of Proposition 3.1, we have the desired result. □

Now we investigate the transfer of the 2-nil-clean property to the amalgamated algebras.

Theorem 3.3. *Let (A, B) be a pair of rings, J be an ideal of B and $f : A \rightarrow B$ be a ring homomorphism. Then the following assertions hold:*

- (a) $A \bowtie^f J$ is 2-nil-clean if and only if A and $f(A) + J$ are 2-nil-clean.
- (b) Assume that $J \subseteq Nilp(B)$. Then $A \bowtie^f J$ is 2-nil-clean if and only if so is A .
- (c) If $J \cap Idem(B) = 0$, then the following assertions are equivalent:

1. $A \bowtie^f J$ is 2-nil-clean.

2. A is 2-nil-clean and $J \subseteq \text{Nilp}(B)$.

Proof.

(a) $\Rightarrow$ By [11, Proposition 5.1], A and $f(A) + J$ are homomorphic images of $A \bowtie^f J$.

$\Leftarrow$ Assume that A and $f(A) + J$ are 2-nil-clean. Let $(x, f(x) + j) \in A \bowtie^f J$ such that $x \in A, j \in J$. Then x and $f(x) + j$ are 2-nil-clean. From [7, Theorem 2.3], $x - x^3 \in \text{Nilp}(A)$ and $(f(x) + j) - (f(x) + j)^3 \in \text{Nilp}(B)$. Thus $(x, f(x) + j) - (x, f(x) + j)^3 = (x - x^3, f(x) + j - (f(x) + j)^3) \in A \bowtie^f J$ is nilpotent. Hence, $(x, f(x) + j)$ is 2-nil-clean by [7, Theorem 2.3].

(b) Assume that $J \subseteq \text{Nilp}(B)$. If $A \bowtie^f J$ is 2-nil-clean, then by assertion (a) above, so is A . Conversely, assume that A is 2-nil-clean. Let $(a, f(a) + j) \in A \bowtie^f J$ with $a \in A$ and $j \in J$. Then, there exist two idempotents $e_1, e_2 \in A$ and a nilpotent $w \in A$ such that $a = e_1 + e_2 + w$. So,

$$(a, f(a) + j) = (e_1, f(e_1)) + (e_2, f(e_2)) + (w, f(w) + j)$$

It is clear that $(e_1, f(e_1))$ and $(e_2, f(e_2))$ are idempotents in $A \bowtie^f J$. Furthermore, since $J \subseteq \text{Nilp}(B)$, one can easily check that $(w, f(w) + j)$ is a nilpotent element of $A \bowtie^f J$. Hence, $(a, f(a) + j)$ is 2-nil-clean.

(c) In virtue of Theorem 3.3(b), we have (2) implies (1). Furthermore, if $A \bowtie^f J$ is 2-nil-clean then so is A , as homomorphic image of $A \bowtie^f J$. It remains to show, only, $J \subseteq \text{Nilp}(B)$. Let $j \in J$. By [8, Lemma 2.10], we obtain:

$$(0, j) = (e_1, f(e_1)) + (e_2, f(e_2)) + (w, f(w) + k).$$

with $e_1, e_2 \in \text{Idem}(A)$, $w \in \text{Nilp}(A)$ and $k \in \text{Nilp}(B)$. It follows that $j \in \text{Nilp}(B)$. $\square$

The following corollary is an immediate consequence of Theorem 3.3 on the transfer of the 2-nil-clean property to duplications.

Corollary 3.4. *Let A be a ring and I be an ideal of A . Then $A \bowtie I$ is 2-nil-clean if and only if so is A .*

Proof. In this case, we have $f = \text{id}_A$ and $f(A) + I = A$. In view of Theorem 3.3(a), the result follows. $\square$

Example 3.5.

Let T be a ring, I be an ideal of T and let D be a subring of T such that $I \cap D = (0)$. Then the ring $D + I$ is 2-nil-clean if and only if D so is.

Proof.

By [11, Example 2.6], $D + I$ is isomorphic to $D \bowtie^i I$ where $i : D \hookrightarrow T$ is the natural embedding. Thus, by Theorem 3.3(a), $D + I$ is 2-nil-clean if and only if D is 2-nil-clean. $\square$

The next result is to study the transfer of 2-nil-clean property to the trivial extension.

Corollary 3.6. *Let A be a ring, E be an A -module and $R := A \ltimes E$ be the trivial ring extension of A by E . Then R is 2-nil-clean if and only if A is 2-nil-clean.*

Proof.

In this case $J = 0 \ltimes E \subseteq \text{Nilp}(R)$. Thus, in view of Theorem 3.3(b), we obtain the desired result. $\square$

The following example shows the failure of assertion (b) of Theorem 3.3, beyond the context " $J \subseteq \text{Nilp}(B)$ ".

Example 3.7. Let A be a 2-nil-clean ring (for instance, $A := \mathbb{Z}_6$, the ring of integers modulo 6), $B = A[X]$, $J := XA[X]$ and $f : A \hookrightarrow B$ the natural injection. Then:

- (1) $J \not\subseteq \text{Nilp}(B)$.
- (2) A is 2-nil-clean.
- (3) $A \bowtie^f J$ is not 2-nil-clean.

Proof.

(1) This follows from assumption.

(2) Trivial.

(3) Indeed, $f(A) + J = A + XA[X] = A[X]$ is not 2-nil-clean since $f(1) + X = 1 + X \in f(A) + J$ is not 2-nil-clean. Therefore, in virtue of Theorem 3.3(1), $A \bowtie^f J$ is not 2-nil-clean. $\square$

Theorem 3.3 allows us to construct new original class of 2-nil-clean which is not nil-clean.

Example 3.8. Let B be a 2-nil-clean ring (for instance take $B := \mathbb{Z}_3[X] / \langle X^m(X-1)^m(X-2)^m \rangle$), $A := B \ltimes E$ be the trivial ring extension of B by a B -module E , $f : A \rightarrow B$ be a surjective ring homomorphism and $J := \langle \bar{X} \rangle$ be an ideal of B . Then:

1. $A \bowtie^f J$ is 2-nil-clean.
2. $A \bowtie^f J$ is not nil-clean.

Proof. (1) From [20, Remark 2], it follows that B is 2-nil-clean. By Corollary 3.6, A is 2-nil-clean. Using assertion (a) of Theorem 3.3, $A \bowtie^f J$ is 2-nil-clean.

(2) One can easily check that $((\bar{X}, 0), \bar{X})^2 - ((\bar{X}, 0), \bar{X}) = ((\bar{X}^2 - \bar{X}, 0), \bar{X}^2 - \bar{X}) \notin \text{Nilp}(A \bowtie^f J)$ since $(\bar{X}^2 - \bar{X}, 0) \notin \text{Nilp}(A)$. Therefore, $A \bowtie^f J$ is not nil-clean. $\square$

Theorem 3.3 enriches the current literature with a new original class of 2-nil-clean rings which are not weakly nil-clean.

Example 3.9. Consider the homomorphism $h : \mathbb{Z}_6 \rightarrow \mathbb{Z}_3$ by $h(0) = h(3) = 0$, $h(1) = h(4) = 1$ and $h(2) = h(5) = 2$. Now, let $A := \mathbb{Z}_6 \times \mathbb{Z}_3$ be 2-nil-clean ring, $B := \mathbb{Z}_3 \times \mathbb{Z}_3$ be a ring and $f : A \rightarrow B$ be a ring homomorphism defined by $f(a, b) = (h(a), b)$ and $J := 0 \times \mathbb{Z}_3$ be an ideal of B . Then:

- (1) $A \bowtie^f J$ is 2-nil-clean.
- (2) $A \bowtie^f J$ is not weakly nil clean.

Proof. (1) Since A and $f(A) + J = B$ are 2-nil-clean, then by assertion (a) of Theorem 3.3, it follows that $A \bowtie^f J$ is 2-nil-clean.

(2) We claim that $A \bowtie^f J$ is not weakly nil-clean. Indeed, observe that $f(A) + J = \mathbb{Z}_3 \times \mathbb{Z}_3$ is not weakly nil clean. Since $f(A) + J$ is a homomorphic image of $A \bowtie^f J$ which is not weakly nil clean, it follows that $A \bowtie^f J$ is not weakly nil clean, as the class of weakly nil clean rings is closed under homomorphic images [9, Proposition 1.9]. $\square$

4 Pullbacks

In this section, we examine the 2-nil-clean (resp. nil-clean) property into pullback constructions. It is worth to mention that many of our proofs of this section are straightforward. We are very grateful to [7] for their results. Recall that a pullback can be defined as follows:

Let T be a ring, I be a nonzero ideal of T , $\phi : T \rightarrow T/I$ be the natural surjection and D be a subring of T/I . Let R be the pullback of the following diagram:

$$\begin{array}{ccc} R = \phi^{-1}(D) & \xrightarrow{\phi/R} & D = R/I \\ i \downarrow & & \downarrow j \\ T & \xrightarrow{\phi} & T/I \end{array} \quad (\Delta)$$

where i and j are the natural injections. We assume that $R \subset T$ and refer to this diagram as a diagram of type (Δ) . If $I = M$ is a maximal ideal of T , we refer to this diagram as diagram of type $(\square)$.

Proposition 4.1. *For the diagram of type (Δ) :*

- (1) *If R is 2-nil-clean (resp., nil-clean), then so is D .*
- (2) *If T is 2-nil-clean (resp., nil-clean), then so is R .*
- (3) *Assume that I is nil. Then R is 2-nil-clean (resp., nil-clean) if and only if so is D .*

Proof.

- (1) Assume that R is 2-nil-clean. Then D is 2-nil-clean as a homomorphic image of R .
- (2) If T is 2-nil-clean then so is R by [7 Corollary 2.4].
- (3) Assume that I is nil. Then, in virtue of [7 Lemma 3.1], R is 2-nil-clean if and only if so is D .

The proof for nil-clean rings is similar. $\square$

Remark 4.2. It is worthwhile noting that the converse of the assertion (1) of Proposition 4.1 does not hold in general. Indeed, let R be a non-2-nil-clean ring (For instance, take $R := A[[X]]$ where A is 2-nil-clean). It is easy to see that A is 2-nil-clean. However, $R := A[[X]]$ is never 2-nil-clean by Proposition 2.4. Also, note that in the assertion (3) of Proposition 4.1, the assumption " I is nil" is necessary for the equivalence. Indeed, Let $I = (X)$ be an ideal of $R := A[[X]]$, where A is 2-nil-clean. Observe that I is not nil. Consider the canonical surjection $\theta : A[[X]] \rightarrow A[[X]]/(X)$. Clearly, R is not 2-nil-clean. However, $\theta(R) = R/(X) = A[[X]]/(X) \simeq A$ is 2-nil-clean.

The following example illustrates Proposition 4.1 by providing a new original class of 2-nil-clean rings which are not nil-clean.

Example 4.3. Let $R = \mathbb{Z}_6$ be the ring of integers modulo 6. Consider the ring $T := \mathbb{Z}_6 \times \mathbb{Z}_3$. Consider the following pullback:

$$\begin{array}{ccc} R = \pi^{-1}(D) = \mathbb{Z}_6 & \xrightarrow{\pi/R} & D = \mathbb{Z}_3 \\ i \downarrow & & \downarrow j \\ T = \mathbb{Z}_6 \times \mathbb{Z}_3 & \xrightarrow{\pi} & \mathbb{Z}_3 \end{array}$$

One can easily check that T is 2-nil-clean which is not nil-clean. Hence, by Proposition 4.1(2), it follows that R is 2-nil-clean. Moreover, by assertion (1) of Proposition 4.1(1), R is not nil-clean, as D is not nil-clean.

Next, we examine the 2-nil-clean (resp. nil-clean) property in pullback when T is a ring, M is a maximal ideal of T , $\phi : T \rightarrow T/M$ is the natural surjection and D is a subring of T/M . Let R be the pullback of the following diagram:

$$\begin{array}{ccc} R = \phi^{-1}(D) & \xrightarrow{\phi/R} & D = R/M \\ i \downarrow & & \downarrow j \\ T & \xrightarrow{\phi} & T/M \end{array} \quad (\square)$$

where i and j are the natural injections. We assume that $R \subset T$ and we refer to this diagram as diagram of type $(\square)$.

Now, we examine the 2-nil-clean (resp. nil-clean) property in pullback, where M is a maximal ideal of T and Q is a maximal ideal of R .

Theorem 4.4. For the diagram of type $(\square)$, with M (resp., Q) a maximal ideal of T (resp., R). Then the following assertions are equivalent:

- (1) R is 2-nil-clean (resp., nil-clean) ring.
- (2) $R \setminus Q$ is 2-nil-clean (resp., nil-clean) multiplicative set.
- (3) $R \setminus M$ is 2-nil-clean (resp., nil-clean) multiplicative set.

Recall that $R \setminus Q$ (resp., $R \setminus M$) is 2-nil-clean if any element of $R \setminus Q$ (resp., $R \setminus M$) is 2-nil-clean.

Proof.

(1) $\implies$ (2) By [7 Corollary 2.4], we have the desired result.

(2) $\implies$ (3) Let $x \in R \setminus M$. If $x \in R \setminus Q$, then we are done. If $x \in Q$, then $1 - x \notin Q$. Then $1 - x = e + f + n$ for two idempotents e, f and a nilpotent n in $R \setminus Q$. Then $x = 1 - e - f - n$ is 2-nil-clean by [7 Lemma 2.2].

(3) $\implies$ (1) Let $x \in R$. If $x \in R \setminus M$, then we are done. If $x \in M$, then $1 - x \notin M$. Hence, with a similar argument as previously, it follows that x is 2-nil-clean.

The proof for nil-clean rings is similar. $\square$

Recall that a ring R is UU if $U(R) = 1 + \text{Nilp}(R)$. In the case R is a local ring, we obtain the following result:

Corollary 4.5. Let R be a commutative local ring. Then the following assertions hold:

1. R is 2-nil-clean (resp., nil-clean) if and only if every unit of R is 2-nil-clean (resp., nil-clean).
2. R is nil-clean if and only if R is UU .

Proof.

(1) This follows from Theorem 4.4 with Q is the unique maximal ideal of R .

(2) Assume that R is nil-clean and let $u \in U(R)$. Then $u = e + n$ where e (resp., n) is idempotent (resp., nilpotent) of R . Then $e = u - n \in \text{Idem}(R) \cap U(R) = \{1\}$. Hence $u = 1 + n$. Conversely, assume that R is UU . Then in virtue of statement (1), it suffices to show that every unit is nil-clean. Indeed, since R is UU , then every unit $u \in R$ can be written as $u = 1 + b$ for some nilpotent b of R which completes the proof of the corollary. $\square$

References

- [1] D. D. Anderson and M. Winders, *Idealization of a module*, J. Commut. Algebra 1 (1) (2009), 3-56.
- [2] C. Bakkari, M. Es-Saidi, N. Mahdou and M. A. S. Moutui, *Extensions of semiclean rings*, Czechoslovak Math. J. 72(147) (2022), no. 2, 461-476.
- [3] C. Bakkari, M. Es-Saidi, N. Mahdou and M. A. S. Moutui, *On clean-like conditions in some commutative ring extensions*, Indian J Pure Appl Math (2024), <https://doi.org/10.1007/s13226-024-00677-2>.
- [4] C. Bakkari and H. El-Mzaiti, *Rings in which every nonzero S -weakly prime ideal is weakly prime*, Moroccan Journal of Algebra and Geometry with Applications Vol. 3(2) (2024), 338-344.
- [5] S. Breaz, P. Danchev, Y. Zhou, *Rings in which every element is either a sum or a difference of a nilpotent and an idempotent*, J. Algebra Appl. 15 (2016), no. 8, 1650148, 11 pp.
- [6] G. Calugareanu and H. F. Pop, *On stable range one matrices*, submitted (2020), <https://arxiv.org/abs/2012.13909>.

- [7] H. Chen and M. Sheibani, *Strongly 2-nil-clean rings*, J. Algebra Appl., Vol. 16, No. 8 (2017), DOI: 10.1142/S021949881750178X.
- [8] M. Chhiti, N. Mahdou and M. Tamekkante, *Clean property in amalgamated algebras along an ideal*, Hacet. J. Math. Stat. 44 (2015), no. 1, 41-49.
- [9] P. V. Danchev and W. Wm. McGovern, *Commutative weakly nil clean unital rings*, J. Algebra 425(2015), 410-422.
- [10] A. J. Diesl, *Nil clean rings*, J. Algebra 383 (2013), 197-211.
- [11] M. D'Anna, C. A. Finocchiaro and M. Fontana, *Amalgamated algebras along an ideal*, Comm Algebra and Applications, Walter De Gruyter (2009), 241-252.
- [12] M. D'Anna, C. A. Finocchiaro and M. Fontana, *Properties of chains of prime ideals in amalgamated algebras along an ideal*, J. Pure Appl. Algebra 214(2010), 1633-1641.
- [13] M. D'Anna and M. Fontana, *An amalgamated duplication of a ring along an ideal: the basic properties*, J. Algebra Appl., 6(3)(2007), 443-459.
- [14] A. El Khalfi, H. Kim and N. Mahdou, *Amalgamation extension in commutative ring theory, a survey*, Moroccan Journal of Algebra and Geometry with Applications, Vol. 1(1) (2022), 139-182.
- [15] E. Ghashghaei and W. Wm. McGovern, *Fusible rings*, Comm. Algebra 45(3)(2017) 1151-1165.
- [16] S. Glaz, *Commutative coherent rings*, Lecture Notes in Mathematics, 1371 (1989), Springer-Verlag, Berlin, 3-540-51115-6.
- [17] Y. Hirano, H. Tominaga and A. Yaqub, *On rings in which every element is uniquely expressible as a sum of a nilpotent element and a certain potent element*, Math. J. Okayama Univ. 30(1988), 33-40.
- [18] J. A. Huckaba, *Commutative rings with zero divisors*, Marcel Dekker, New York, 1988.
- [19] T. Koşan, Z. Wang, Y. Zhou, *Nil-clean and strongly nil-clean rings*, J. Pure Appl. Algebra 220 (2016), 633-646.
- [20] A. Kostić, Z. Z. Petrović, Z. S. Pucanović and M. Roslavcev, *A generalization of nil-clean rings*, Miskolc Math. Notes 19 (2018), no. 2, 969-981.
- [21] P. Krylov and A. Tuganbaev, *Formal matrices*, Algebra and Applications, 23. Springer, Cham, 2017. viii+156 pp. ISBN: 978-3-319-53906-5.
- [22] A. Mimouni, *Note on UN-rings*, Moroccan Journal of Algebra and Geometry with Applications, Vol. 2(1) (2023), 154-161.
- [23] W. K. Nicholson and Y. Zhou, *Clean general rings*, J. Algebra 291 (2005), no. 1, 297-311.



ISSN: 2820-7114

Moroccan Journal of Algebra and Geometry with Applications

Supported by Sidi Mohamed Ben Abdellah University, Fez, Morocco

Volume 4, Issue 1 (2025), pp 90-108

Title :

A New Public Key Encryption Scheme Based on the Cubic Pell Curve Using Encoding Functions

Author(s):

Abderrahmane Nitaj and Michel Seck

A New Public Key Encryption Scheme Based on the Cubic Pell Curve Using Encoding Functions

Abderrahmane Nitaj¹ and Michel Seck²

¹Normandie Univ, UNICAEN, CNRS, LMNO, 14000 Caen, France.

email: abderrahmane.nitaj@unicaen.fr

²Ecole Polytechnique de Thies, LTISI, Senegal.

email: mseck@ept.sn

Communicated by Najib Mahdou

(Received 20 October 2024, Revised 30 November 2024, Accepted 19 December 2024)

Abstract. RSA is a public key encryption scheme introduced by Rivest, Shamir, and Adleman in 1978. Its security relies on the difficulty of factoring an integer $N = pq$ which is the product of two large prime numbers p and q . In 2018, Murru and Saettone proposed a variant of RSA, based on the cubic Pell curve with a modulus of the same form. Recently, Seck and Nitaj extended the scheme of Murru and Saettone to a prime power modulus of the form $N = p^r q^s$ where the ciphertexts C are represented as elements of $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$, with a size of $3\log_2(N)$. In addition to the difficulty of factoring composite integers, the security of the scheme of Seck and Nitaj is based on Rabin's trapdoor one-way function. In this paper, we propose a new variant of the scheme of Seck and Nitaj where the ciphertext size is reduced to a size $2\log_2(N)$ instead of $3\log_2(N)$ for a fixed modulus N . This achievement is made possible through the incorporation of encoding and compression functions.

Key Words: Public Key Cryptography, cubic Pell curve, RSA variants, Encoding functions.

2020 MSC: Primary 94A60.

Dedicated to our Professor David E. Dobbs for his 80th Birthday.

1 Introduction

In 1976, Diffie and Hellman introduced the notion of a trapdoor one-way function, which allows two different entities to share the same secret key via a non-secure channel [14]. In 1978, the RSA cryptosystem was published by Rivest, Shamir, and Adleman [33]. RSA is suitable for both encryption and digital signature. In RSA, the public key is represented as $pk = (N, e)$, and the private key as $sk = (N, d)$, where $N = pq$ is the product of two prime numbers p and q . The public exponent $e \geq 3$ and the private exponent d are chosen so that $ed \equiv 1 \pmod{(p-1)(q-1)}$. To encrypt a message $m \in \mathbb{Z}/N\mathbb{Z}$ with the public key $pk = (N, e)$ or to decrypt a ciphertext c using the private key $sk = (N, d)$, the function $f_s(y) = y^s \pmod{N}$ is applied, where $(s, y) = (e, m)$ for encryption and $(s, y) = (d, c)$ for decryption.

The security of RSA is based on the difficulty of factoring large composite integers of the form $N = pq$. Certain vulnerabilities of RSA are known for specific forms of the prime factors p and q , or for the public exponent e and the secret exponent d [45, 29, 5, 7, 8, 9, 12, 44, 43]. For example, one can use Wiener's attack [45] to efficiently recover the private exponent d when $q < p < 2q$ and

$d < \frac{1}{3}N^{1/4}$. Using Coppersmith's method [12], Boneh and Durfee [9] have improved the bound up to $d < N^{0.292}$. On the other hand, RSA is vulnerable to Håstad's broadcast attack [18, 5] when e is small.

To design more efficient, and more resistant schemes than the standard RSA, numerous variants have been proposed. For instance, Takagi [42] proposed a variant of RSA with the modulus $N = p^k q$ to achieve a faster decryption process than RSA. This construction was later generalized by Lim, Kim, and Lee [25] with the modulus $N = p^r q^s$. Other variants of RSA have been proposed over non-singular or singular curves when a certain ring can be defined. Koyama, Maurer, Okamoto, and Vanstone [22] proposed three RSA-like cryptosystems, called KMOV, based on supersingular elliptic curves $E_b : y^2 = x^3 + b$ over $\mathbb{Z}/N\mathbb{Z}$ with $N = pq$ and $p \equiv q \equiv 2 \pmod{3}$. In 1993, Demytko [13] proposed an RSA variant over elliptic curves in Weierstrass form $E_{a,b} : y^2 = x^3 + ax + b$ where only the x coordinates instead of the full points are used in the computations. A fast RSA type scheme based on the singular cubic curve $y^2 + axy = x^3 \pmod{N}$ was proposed by Koyama [21] in 1995. In the same year, Kuwakado, Koyama, and Tsuruoka [23] proposed another RSA-type scheme based on singular cubic curves $y^2 \equiv x^3 + bx^2 \pmod{N}$. Later on, Boudabra and Nitaj [10, 11] have proposed two variants with a multi-power modulus $N = p^r q^s$, the first one is based on supersingular elliptic curves $E_b : y^2 = x^3 + b$ and the second one on Edwards curves $E_d : -dx^2 + y^2 = 1 + dx^2 y^2$. In 2018, Murru and Saettone [28] proposed an RSA-like cryptosystem over the cubic Pell curve $C_r : x^3 + ry^3 + r^2 z^3 - 3rxyz \equiv 1 \pmod{N}$ with a modulus $N = pq$. Their scheme was recently generalized by Seck and Nitaj [39] over the cubic Pell curve with a prime power modulus $N = p^r q^s$. In the scheme of Seck and Nitaj, the ciphertext has size $3\log_2(N)$, and its security is based on the difficulty of factoring composite integers, and on Rabin's trapdoor one way function [31].

Our Contributions : In this paper, we propose a new RSA-like cryptosystem using the arithmetic of the cubic Pell curve $C_a(N) : x^3 + ay^3 + a^2 z^3 - 3axyz \equiv 1 \pmod{N}$ where $N = p^r q^s$. The advantage of the new scheme over the scheme of Seck and Nitaj is that the bit-size of the ciphertext is minimized from $3\log_2(N)$ to $2\log_2(N)$. This bit-size reduction is possible by using encoding functions. Notice that, for several applications and design of cryptographic primitives, various encoding functions over finite fields have been proposed in the last decade for both elliptic and hyperelliptic curves [6, 20, 16, 4, 37, 38].

We summarize our contributions as follows.

- First encoding functions : For a modulus $N = \prod_{i=1}^l p_i$ where, for $i = 1, 2, \dots, l$, p_i is a prime number, $p_i \neq p_j$ if $i \neq j$, and $p_i \equiv 2 \pmod{3}$, we construct an injective and invertible encoding from $\mathbb{Z}/N\mathbb{Z}$ into the cubic Pell curve $C_a(N) : x^3 + ay^3 + a^2 z^3 - 3axyz = 1$ over $\mathbb{Z}/N\mathbb{Z}$. To this end, we adapt the cube-root encoding technique of Boneh and Franklin [6] as well as the technique of Icart [20] for elliptic curves to the cubic Pell curve.
- Second encoding functions : For the modulus $N = p^r q^s$ with $r, s \geq 1$, and $p \equiv q \equiv 1 \pmod{3}$, we construct an efficient injective and invertible encoding that sends an element $(m_x, m_y) \in (\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})$ into a point $(x, y, z) \in C_a(N)$ using the isomorphism constructed by Dutto and Murru [15] for the cubic Pell curve. This encoding function is used in our new scheme, especially in the reduction of the ciphertext.
- A new cryptosystem : We propose a new public key encryption scheme which is a generalization of the scheme of Murru and Saettone [28]. In the new scheme, we use a modulus of the form $N = p^r q^s$. The main advantages of our construction over the scheme of Seck and Nitaj [39] are two folds. (i) For a fixed modulus N , the ciphertexts of our scheme are of size $2\log_2(N)$ while they are of size $3\log_2(N)$ in the scheme of Seck and Nitaj. This improvement is possible by using injective and invertible encoding functions into the cubic Pell curve. (ii) Our scheme

can be used as a digital signature scheme while no such transformation is known for Seck and Nitaj cryptosystem.

- Security analysis : We analyze the security of the new scheme, specifically by studying its resistance to algebraic attacks based on the continued fraction algorithm and Coppersmith's technique. We also discuss how to get the CCA security using the OAEP transformation [3, 17, 40].

A proof of concept implementation of our scheme with SimulaMath [41] and SageMath [35] is provided in [36].

Paper Organization : The rest of this paper is organized as follows.

In Section 2 we recall some properties related to cubic residue modulo a prime, encoding functions and the arithmetic of the cubic Pell curve, especially over the ring $\mathbb{Z}/n\mathbb{Z}$. In Section 3, we construct encoding functions into the cubic Pell curve over $\mathbb{Z}/n\mathbb{Z}$ when $N = \prod_{i=1}^l p_i$, $p_i \equiv 2 \pmod{3}$. In Section 4, we present our new scheme. The security analysis of our scheme is presented in Section 5. We conclude the paper in Section 6.

2 Preliminaries

In this section, we revisit some properties concerning cubic residues modulo prime powers and encoding functions into elliptic curves, with a particular emphasis on the Boneh and Franklin encoding [6]. Additionally, we explore properties associated with the cubic Pell curve $C_a : x^3 + ay^3 + a^2z^3 - 3axyz = 1$ over a field $\mathbb{F}$ or the ring $\mathbb{Z}/N\mathbb{Z}$ where $N = p^r q^s$ is a prime power modulus.

2.1 Cubic residues modulo prime powers and encoding functions

Definition 2.1 (cubic residue). Let p be a prime number. We say that an integer a is a cube (or cubic residue) modulo p if the equation $x^3 \equiv a \pmod{p}$ has at least one solution; otherwise, a is a cubic non-residue modulo p .

Theorem 2.2 ([34]). Let $n = p^r$ be a prime power integer. If k is a positive integer and a is an integer relatively prime to n , then the congruence $x^k \equiv a \pmod{n}$ has a solution if and only if

$$a^{\phi(n)/d} \equiv 1 \pmod{n},$$

where $d = \gcd(k, \phi(n))$ and $\phi(n) = p^{r-1}(p-1)$. If the congruence has a solution, then it actually has d incongruent solutions modulo n .

Corollary 2.3. Let p be a prime number. An integer a is a cubic residue modulo p if and only if $a^{(p-1)/\gcd(3, p-1)} = 1$ in $\mathbb{Z}/p\mathbb{Z}$.

Lemma 2.4 ([6, 20]). Let $q = p^n$ be a prime power with $p \equiv 2 \pmod{3}$ and $\mathbb{F}_q$ be a finite field with q elements. Then the map

$$\mathbb{F}_q \rightarrow \mathbb{F}_q : x \mapsto x^3$$

is a bijection and the inverse function is given by

$$\mathbb{F}_q \rightarrow \mathbb{F}_q : y \mapsto y^{1/3} = y^{\frac{2q-1}{3}}.$$

The previous map allows to construct injection encoding functions into elliptic curve $E_{a,b} : y^2 = x^3 + ax + b$ over $\mathbb{F}_q$.

An elliptic curve E over $\mathbb{F}_p$ is called supersingular if it has exactly $p+1$ points. When $p \equiv 2 \pmod{3}$, the following result shows a first encoding in elliptic curves.

Lemma 2.5 (Boneh-Franklin encoding [6]). Let $E_b : y^2 = x^3 + b$ be a supersingular elliptic curve over $\mathbb{F}_q$ with $q = p^n$, $p > 3$, and $p \equiv 2 \pmod{3}$. Then the map

$$\phi_1 : \mathbb{F}_q \rightarrow E_b : u \mapsto \left((u^2 - b)^{\frac{2q-1}{3}}, u \right)$$

is a one-to-one encoding and its inverse is given by $(x, y) \in E_b \mapsto y \in \mathbb{F}_q$.

2.2 The cubic Pell Curve over fields

The Pell hyperbola $H_d : x^2 - dy^2 = 1$ can be generalized in the cubic setting as

$$\mathcal{C}_a : x^3 + ay^3 + a^2z^3 - 3axyz = 1.$$

Let $\mathbb{F}$ be a field and let $a \in \mathbb{F}$. Define the quotient ring $R_a = \mathbb{F}[t]/(t^3 - a)$ where an element $w \in R_a$ is represented as $w = x + yt + zt^2$ with $(x, y, z) \in \mathbb{F}^3$. The product of two elements $w_1 = x_1 + y_1t + z_1t^2$ and $w_2 = x_2 + y_2t + z_2t^2$ of R_a is defined by (see [1])

$$w_1 \oplus w_2 = (x_1x_2 + a(y_2z_1 + y_1z_2)) + (x_2y_1 + x_1y_2 + az_1z_2)t + (y_1y_2 + x_2z_1 + x_1z_2)t^2.$$

The norm of $w = x + yt + zt^2$ is defined by

$$N_a(w) = x^3 + ay^3 + a^2z^3 - 3axyz.$$

Consider the set $\mathcal{U}_a$ of unit elements defined as

$$\mathcal{U}_a = \{x + yt + zt^2 \in R_a : x^3 + ay^3 + a^2z^3 - 3axyz = 1\},$$

and consider the cubic Pell curve over $\mathbb{F}$

$$\mathcal{C}_a = \{(x, y, z) \in \mathbb{F}^3 : x^3 + ay^3 + a^2z^3 - 3axyz = 1\}.$$

The natural product on $\mathcal{U}_a$ induces the generalized Brahmagupta product on $\mathcal{C}_a$ that we also denote by $\oplus$. This product is defined as follows:

$$w_1 \oplus w_2 = (x_1x_2 + a(y_2z_1 + y_1z_2), x_2y_1 + x_1y_2 + az_1z_2, y_1y_2 + x_2z_1 + x_1z_2),$$

where $w_1 = (x_1, y_1, z_1) \in \mathcal{C}_a$ and $w_2 = (x_2, y_2, z_2) \in \mathcal{C}_a$. Notice that $(\mathcal{C}_a, \oplus)$ is a group with neutral element $(1, 0, 0)$, and the inverse of $w = (x, y, z)$ is given by $w^{-1} = (x^2 - ayz, az^2 - xy, y^2 - xz)$.

Consider the quotient ring $\mathbb{B}_a = R_a^*/\mathbb{F}^*$. Then, an element $w = [x + yt + zt^2] = (x : y : z) \in \mathbb{B}_a$ is an equivalent class defined by

$$(x : y : z) = w = \{\lambda x + \lambda y t + \lambda z t^2 \in \mathbb{F}[t] : \lambda \in \mathbb{F}^*\}.$$

Any element $(x : y : z) \in \mathbb{B}_a$ can be rewritten as follows

$$(x : y : z) = \begin{cases} (x_1 : y_1 : 1) & \text{if } z \neq 0, \\ (x_2 : 1 : 0) & \text{if } z = 0 \text{ and } y \neq 0, \\ (1 : 0 : 0) & \text{if } y = z = 0. \end{cases}$$

With the product $\oplus$, $\mathbb{B}_a$ is a commutative group with identity $(1 : 0 : 0)$ and inverse of $(x : y : z)$ is given by $(x^2 - ayz : az^2 - xy : y^2 - xz)$.

Theorem 2.6 ([15]). Let $\mathbb{F}_q$ be a finite field with $q \equiv 1 \pmod{3}$. Let b a non zero element of $\mathbb{F}_q$ and $a = b^3$. The map

$$\begin{aligned} \psi_b : (\mathbb{B}_a, \oplus) &\rightarrow (\mathcal{C}_a, \oplus) \\ (l : m : n) &\mapsto \left(\frac{l^3 + 2b^2l(m^2 + bmn + b^2n^2) + b^4mn(m + bn)}{N_a((l, m, n))}, \right. \\ &\quad \frac{b^2m^3 + 2m(l^2 + b^2ln + b^4n^2) + bln(l + b^2n)}{N_a((l, m, n))}, \\ &\quad \left. \frac{b^5n^3 + 2bn(l^2 + blm + b^2m^2) + lm(l + bm)}{bN_a((l, m, n))} \right) \end{aligned}$$

is a group isomorphism and the inverse ψ_b^{-1} is given by :

$$\begin{aligned} \psi_b^{-1} : (\mathcal{C}_a, \oplus) &\rightarrow (\mathbb{B}_a, \oplus) \\ (x, y, z) &\mapsto (b^2(1 + 2x - by - b^2z) : b(1 - x + 2by - b^2z) : 1 - x - by + 2b^2z) \end{aligned}$$

2.3 The cubic Pell Curve over $\mathbb{Z}/n\mathbb{Z}$ with $n = p^r q^s$

Proposition 2.7 ([39]). Let N be integer greater than 3. Let a be an element of $\mathbb{Z}/N\mathbb{Z}$. The cubic Pell curve

$$\mathcal{C}_a(N) : x^3 + ay^3 + a^2z^3 - 3axyz \equiv 1 \pmod{N},$$

is nonsingular.

Theorem 2.8 ([39]). Let p, q be two prime numbers with $p, q \equiv 1 \pmod{3}$, $p \neq q$. Let r and s be two positive integers and $N = p^r q^s$. Define the values

$$\begin{aligned} \psi_1(N) &= p^{2(r-1)} q^{2(s-1)} (p^2 + p + 1) (q^2 + q + 1), \\ \psi_2(N) &= p^{2(r-1)} q^{2(s-1)} (p - 1)^2 (q - 1)^2, \\ \psi_3(N) &= p^{2(r-1)} q^{2(s-1)} (p^2 + p + 1) (q - 1)^2, \\ \psi_4(N) &= p^{2(r-1)} q^{2(s-1)} (p - 1)^2 (q^2 + q + 1). \end{aligned} \tag{1}$$

For $a \in \mathbb{Z}/N\mathbb{Z}$ with $\gcd(a, N) = 1$, the number of solutions of the cubic Pell curve equation $x^3 + ay^3 + a^2z^3 - 3axyz \equiv 1 \pmod{N}$ is then

$$|\mathcal{C}_a(N)| = \begin{cases} \psi_1(N) & \text{if } a \notin \mathcal{R}^3(p) \text{ and } a \notin \mathcal{R}^3(q), \\ \psi_2(N) & \text{if } a \in \mathcal{R}^3(p) \text{ and } a \in \mathcal{R}^3(q), \\ \psi_3(N) & \text{if } a \notin \mathcal{R}^3(p) \text{ and } a \in \mathcal{R}^3(q), \\ \psi_4(N) & \text{if } a \in \mathcal{R}^3(p) \text{ and } a \notin \mathcal{R}^3(q). \end{cases}$$

where $\mathcal{R}^3(p)$ is the set of the cubic residues modulo p , and $\mathcal{R}^3(q)$ is the set of the cubic residues modulo q .

A scalar multiplication $\otimes$ can be defined over $\mathcal{C}_a(N)$ as follows. For a solution $w = (x, y, z) \in \mathcal{C}_a(N)$ and an integer $n \geq 1$,

$$n \otimes (x, y, z) = \underbrace{(x, y, z) \oplus (x, y, z) \oplus (x, y, z) \dots \oplus (x, y, z)}_{n \text{ times}}.$$

Lemma 2.9 ([39]). Let $\mathcal{C}_a(N)$ be the set of the solutions of the cubic Pell curve $x^3 + ay^3 + a^2z^3 - 3axyz = 1$ in $(\mathbb{Z}/N\mathbb{Z})^3$. Then $(\mathcal{C}_a(N), \oplus)$ is an abelian group with order $|\mathcal{C}_a(N)|$. The neutral element of $\mathcal{C}_a(N)$ is $(1, 0, 0)$ and the inverse of a solution $(x, y, z) \in \mathcal{C}_a(N)$ is $(x^2 - ayz, az^2 - xy, y^2 - xz) \pmod{N}$. Furthermore for any positive integer k , and any solution $(x, y, z) \in \mathcal{C}_a(N)$,

$$(1 + k|\mathcal{C}_a(N)|) \otimes (x, y, z) = (x, y, z).$$

In $\mathcal{C}_a(N)$, the addition $(x_1, y_1, z_1) \oplus (x_2, y_2, z_2)$, the doubling $2 \otimes (x_1, y_1, z_1)$, and the scalar multiplication by an integer $n \otimes (x_1, y_1, z_1)$ are summarized in the following algorithms [39].

Algorithm 1 Addition in $\mathcal{C}_a(N)$

Input: $N = p^r q^s$, $a \in \mathbb{Z}/N\mathbb{Z} \setminus \{0\}$, and $(x_1, y_1, z_1), (x_2, y_2, z_2) \in \mathcal{C}_a(N)$.

Output: $(x_3, y_3, z_3) = (x_1, y_1, z_1) \oplus (x_2, y_2, z_2) \in \mathcal{C}_a(N)$.

- 1: $x_3 \equiv x_1 x_2 + a(y_2 z_1 + y_1 z_2) \pmod{N}$.
 - 2: $y_3 \equiv x_2 y_1 + x_1 y_2 + a z_1 z_2 \pmod{N}$.
 - 3: $z_3 \equiv y_1 y_2 + x_2 z_1 + x_1 z_2 \pmod{N}$.
 - 4: Return (x_3, y_3, z_3) .
-

Algorithm 2 Doubling in $\mathcal{C}_a(N)$

Input: $N = p^r q^s$, $a \in \mathbb{Z}/N\mathbb{Z} \setminus \{0\}$, and $(x_1, y_1, z_1) \in \mathcal{C}_a(N)$.

Output: $(x_3, y_3, z_3) = 2 \otimes (x_1, y_1, z_1) \in \mathcal{C}_a(N)$.

- 1: $x_3 \equiv x_1^2 + 2ay_1 z_1 \pmod{N}$.
 - 2: $y_3 \equiv 2x_1 y_1 + az_1^2 \pmod{N}$.
 - 3: $z_3 \equiv y_1^2 + 2x_1 z_1 \pmod{N}$.
 - 4: Return (x_3, y_3, z_3) .
-

Algorithm 3 Left-to-right scalar multiplication in $\mathcal{C}_a(N)$

Input: $N = p^r q^s$, $a \in \mathbb{Z}/N\mathbb{Z} \setminus \{0\}$, $(x_1, y_1, z_1) \in \mathcal{C}_a(N)$, and an integer $n \geq 2$.

Output: $(x_2, y_2, z_2) = n \otimes (x_1, y_1, z_1) \in \mathcal{C}_a(N)$.

- 1: $n := (n_{k-1} n_{k-2} \dots n_1 n_0)_2$.
 - 2: $(x_2, y_2, z_2) = (1, 0, 0)$.
 - 3: **for** i from $k-1$ **downto** 0 **do**
 - 4: $(x_2, y_2, z_2) = 2 \otimes (x_2, y_2, z_2)$.
 - 5: **if** $n_i = 1$ **then**
 - 6: $(x_2, y_2, z_2) = (x_2, y_2, z_2) \oplus (x_1, y_1, z_1)$.
 - 7: Return (x_2, y_2, z_2) .
-

3 Encoding into the cubic Pell curve

In this section, we construct two encoding functions into the cubic Pell curve

$$\mathcal{C}_a(N) : x^3 + ay^3 + a^2z^3 - 3axyz = 1$$

over $\mathbb{Z}/N\mathbb{Z}$.

3.1 Encoding into the cubic Pell curve when $N = \prod_{i=1}^l p_i$ with $p_i \equiv 2 \pmod{3}$

The following result will be used to construct the first encoding.

Lemma 3.1. *Let $N = \prod_{i=1}^l p_i$ with distinct prime factors, and $\phi(N) = \prod_{i=1}^l (p_i - 1)$. Then, for all $a \in \mathbb{Z}/N\mathbb{Z}$ and all $k \geq 1$,*

$$a^{k\phi(N)+1} \equiv a \pmod{N}.$$

Proof. For $a = 0$, we have $0^{k\phi(N)+1} \equiv 0 \pmod{N}$. Suppose that $a \in \mathbb{Z}/N\mathbb{Z}$ with $0 < a < N$. Then $a = a_1 a_2$ where $\gcd(a_1, N) = 1$, and $\gcd(a_2, N) = q_1 \dots q_r$ where each q_i is a divisor of N . Set $Q = q_1 \dots q_r$, and $P = \frac{N}{Q}$. Let k be a positive integer. We have

$$a^{k\phi(N)+1} \equiv a_1^{k\phi(N)+1} a_2^{k\phi(N)+1} \equiv a_1 a_2^{k\phi(N)+1} \pmod{N}. \quad (2)$$

Since $\gcd(P, a_2) = 1$, then

$$a_2^{k\phi(N)} \equiv \left(a_2^{k\phi(P)}\right)^{\phi(Q)} \equiv 1 \pmod{P},$$

or equivalently $a_2^{k\phi(N)} = 1 + Pz$ with an integer z . Since $a_2 \equiv 0 \pmod{Q}$, then

$$a_2^{k\phi(N)+1} \equiv a_2(1 + Pz) \equiv a_2 + Pa_2 z \equiv a_2 \pmod{N}.$$

Plugging this in (2), we get $a^{k\phi(N)+1} \equiv a_1 a_2 \equiv a \pmod{N}$. □

The following result concerns the cube map.

Proposition 3.2. *Let $N = \prod_{i=1}^l p_i$ with distinct prime factors, $p_i \equiv 2 \pmod{3}$, and $\phi(N) = \prod_{i=1}^l (p_i - 1)$. The function*

$$\psi : \mathbb{Z}/N\mathbb{Z} \rightarrow \mathbb{Z}/N\mathbb{Z} : x \mapsto x^3,$$

is a bijection and its inverse is given by

$$\psi^{-1} : \mathbb{Z}/N\mathbb{Z} \rightarrow \mathbb{Z}/N\mathbb{Z} : y \mapsto y^{\frac{2\phi(N)+1}{3}}.$$

Proof. Since $N = \prod_{i=1}^l p_i$ with $p_i \equiv 2 \pmod{3}$, then $p_i - 1 \equiv 1 \pmod{3}$, and

$$\phi(N) = \prod_{i=1}^l (p_i - 1) \equiv 1 \pmod{3}.$$

Hence $2\phi(N) + 1 \equiv 0 \pmod{3}$, and $\frac{2\phi(N)+1}{3}$ is an integer. This shows that ψ^{-1} is well defined.

To show that ψ is bijective, it suffices to show that $\psi \circ \psi^{-1} = 1_{\mathbb{Z}/N\mathbb{Z}}$ and that $\psi^{-1} \circ \psi = 1_{\mathbb{Z}/N\mathbb{Z}}$. Using Lemma 3.1, we get

$$\psi^{-1} \circ \psi(y) \equiv \psi \circ \psi^{-1}(y) \equiv y^{2\phi(N)+1} \equiv y \pmod{N}.$$

□

The following result shows how to encode from $\mathbb{Z}/N\mathbb{Z}$ into the cubic Pell curve $\mathcal{C}_a(N)$. It employs a technique similar to the Boneh-Franklin encoding defined in Lemma 2.5.

Proposition 3.3. *Let $N = \prod_{i=1}^l p_i$ with distinct prime factors, $p_i \equiv 2 \pmod{3}$, and $\phi(N) = \prod_{i=1}^l (p_i - 1)$. For $a \in \mathbb{Z}/N\mathbb{Z}$ with $a \neq 0$, let $\mathcal{C}_a(N) : x^3 + ay^3 + a^2z^3 - 3axyz = 1$ be a cubic Pell curve over $\mathbb{Z}/N\mathbb{Z}$. The map*

$$f_a : \mathbb{Z}/N\mathbb{Z} \rightarrow \mathcal{C}_a(N) : u \mapsto \left((1 - au^3)^{\frac{2\phi(N)+1}{3}}, u, 0 \right).$$

is an injective and invertible encoding.

Proof. For $u \in \mathbb{Z}/N\mathbb{Z}$, let $x = (1 - au^3)^{\frac{2\phi(N)+1}{3}} \pmod{N}$, $y = u \pmod{N}$ and $z = 0 \pmod{N}$. Then, using Lemma 3.1, we get

$$x^3 + ay^3 + a^2z^3 - 3axyz \equiv (1 - au^3)^{2\phi(N)+1} + au^3 \equiv 1 - au^3 + au^3 \equiv 1 \pmod{N}.$$

Thus f_a is well defined. Clearly f_a is injective, and for any $(m, u, 0) \in \text{Im}(f_a)$, $f_a(u) = (m, u, 0)$. This show that f_a is invertible. $\square$

Notice that in the previous Proposition, we have encoded an element $u \in \mathbb{Z}/N\mathbb{Z}$ into a point in the form $(x_u, y_u, 0) \in \mathcal{C}_a(N)$. One can also encode an element $v \in \mathbb{Z}/N\mathbb{Z}$ into a point in the form $(x_v, 0, z_v) \in \mathcal{C}_a(N)$ by the map

$$g_a : \mathbb{Z}/N\mathbb{Z} \rightarrow \mathcal{C}_a(N) : v \mapsto \left((1 - a^2v^3)^{\frac{2\phi(N)+1}{3}}, 0, v \right).$$

Similarly, an element $w \in \mathbb{Z}/N\mathbb{Z}$ can be encoded into a point in the form $(0, y_w, z_w) \in \mathcal{C}_a(N)$ by the map

$$h_a : \mathbb{Z}/N\mathbb{Z} \rightarrow \mathcal{C}_a(N) : w \mapsto \left(0, \left(a^{-1} (1 - a^2w^3) \right)^{\frac{2\phi(N)+1}{3}}, w \right).$$

3.2 Encoding into the cubic Pell curve when $p_i \equiv 1 \pmod{3}$

In this section, we consider the situation where the modulus is in the form $N = p^r q^s$ with small positive integers r and s , where p, q are two distinct primes satisfying $p, q \equiv 1 \pmod{3}$.

An encoding function. Let $N = p^r q^s$ be a prime power modulus, and $b \in \mathbb{Z}/N\mathbb{Z}$ with $b \neq 0$. The map ψ_b in Theorem 2.6 can be used to encode into the cubic Pell curve $\mathcal{C}_a(N) : x^3 + ay^3 + a^2z^3 - 3axyz \equiv 1 \pmod{N}$ where $a = b^3 \pmod{N}$. In Algorithm 4, we show how to encode an element $(m_x, m_y) \in (\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})$ into a point $(x, y, z) \in \mathcal{C}_a(N)$ using ψ_b .

Algorithm 4 The encoding algorithm **Encode2Curve** $((m_x, m_y), b, N)$

Input: An integer N , an element $b \in \mathbb{Z}/N\mathbb{Z}$, a couple $(m_x, m_y) \in (\mathbb{Z}/N\mathbb{Z})^2$

Output: A point $(x, y, z) \in \mathcal{C}_a(N)$ with $a \equiv b^3 \pmod{N}$.

- 1: $a := b^3 \pmod{N}$;
 - 2: $(l, m, n) := (m_x, m_y, 1)$; $\triangleright (l : m : n) \in \mathbb{B}_a$
 - 3: $x_2 := l^3 + 2b^2l(m^2 + bmn + b^2n^2) + b^4mn(m + bn) \pmod{N}$;
 - 4: $y_2 := b^2m^3 + 2m(l^2 + b^2ln + b^4n^2) + bln(l + b^2n) \pmod{N}$;
 - 5: $z_2 := b^5n^3 + 2bn(l^2 + blm + b^2m^2) + lm(l + bm) \pmod{N}$;
 - 6: $g := (l^3 + am^3 + a^2n^3 - 3almn) \pmod{N}$
 - 7: $x := (x_2g^{-1}) \pmod{N}$; $y := (y_2g^{-1}) \pmod{N}$; $z := (z_2(bg)^{-1}) \pmod{N}$;
 - 8: **return** (x, y, z)
-

A straightforward calculation shows that

$$x^3 + ay^3 + a^2z^3 - 3axyz = 1,$$

and that Algorithm 4 is correct. Moreover, this algorithm is well defined if and only if $g := x_m^3 + ay_m^3 + a^2 - 3ax_my_m \pmod{N}$ and b are invertible in $\mathbb{Z}/N\mathbb{Z}$, that is $\gcd(bg, N) = 1$. This condition is satisfied with overwhelming probability since otherwise, a factor of N can be found. So as well as the problem of factoring large composite integers is difficult, we can assume that g and b are invertible modulo N .

Decoding function. The map ψ_b^{-1} in Theorem 2.6 can be used to decode from the cubic Pell curve $C_a(N) : x^3 + ay^3 + a^2z^3 - 3axyz \equiv 1 \pmod{N}$ where $a = b^3 \pmod{N}$. In Algorithm 5, we show how to decode a point $(x, y, z) \in C_a(N)$ to get the corresponding point $(m_x, m_y) \in (\mathbb{Z}/N\mathbb{Z})^2$ using ψ_b^{-1} .

Algorithm 5 The decoding algorithm **DecodeFromCurve** $((x, y, z), b, N)$

Input: An integer N , $b \in \mathbb{Z}/N\mathbb{Z}$, $(x, y, z) \in C_a(N)$ with $a = b^3$.

Output: $(m_x, m_y) \in (\mathbb{Z}/N\mathbb{Z})^2$.

- 1: $a := b^3 \pmod{N}$;
 - 2: $x_2 := b^2(1 + 2x - by - b^2z) \pmod{N}$;
 - 3: $y_2 := b(1 - x + 2by - b^2z) \pmod{N}$;
 - 4: $z_2 := 1 - x - by + 2b^2z \pmod{N}$;
 - 5: $g := z_2^{-1} \pmod{N}$
 - 6: $m_x := (x_2g) \pmod{N}$; $m_y := (y_2g) \pmod{N}$; $\triangleright (m_x : m_y : 1) \in \mathbb{B}_a$
 - 7: **return** (m_x, m_y)
-

Notice that in the computation of **DecodeFromCurve** $((x, y, z), b, N)$, the point $(x_2 : y_2 : z_2) \in \mathbb{B}_a$ can be uniquely represented in the form $(x_2/z_2 : y_2/z_2 : 1)$ as well as z_2 is invertible modulo N , which will happen with overwhelming probability. Also the following properties hold, with overwhelming probability

$$\text{DecodeFromCurve}(\text{Encode2Curve}((m_x, m_y), b, N), b, N) = (m_x, m_y), \quad (3)$$

and

$$\text{Encode2Curve}(\text{DecodeFromCurve}((x, y, z), b, N), b, N) = (x, y, z). \quad (4)$$

4 A New RSA-like Scheme

In this section, we propose a new public key encryption scheme as an RSA variant. It could be also categorized as a variant of the scheme of Murru and Saettone [28] for two reasons.

- In our scheme, the modulus is $N = p^r q^s$, while it is $N = pq$ in the scheme of Murru and Saettone.
- In our scheme, we use cubic residues $a \equiv b^3 \pmod{N}$ to construct the cubic Pell curve, while in the scheme of Murru and Saettone, a is a cube non-residue. As a consequence, in our scheme, the public and the private exponents satisfy $ed \equiv 1 \pmod{p^{2(r-1)}q^{2(s-1)}(p-1)^2(q-1)^2}$ while they satisfy $ed \equiv 1 \pmod{(p^2 + p + 1)(q^2 + q + 1)}$ in the scheme of Murru and Saettone.

4.1 The new scheme

In the following Figure 1, we describe the template of our scheme. It uses encoding/decoding functions and compression/decompression functions.

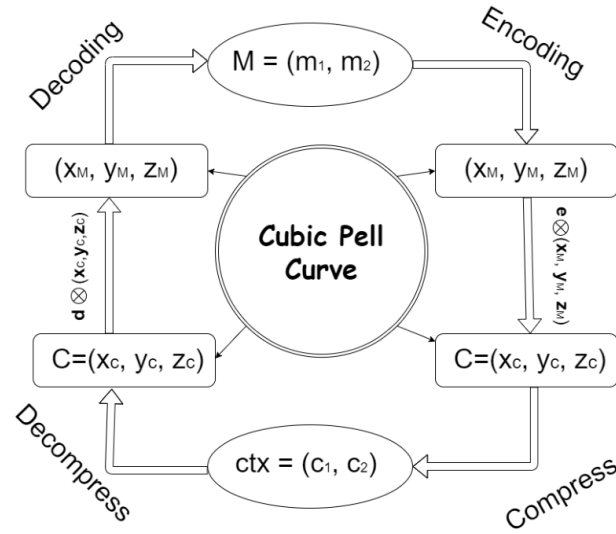


Figure 1: Template of our public key encryption scheme with compression

The key generation, encryption, and decryption phases are described in Algorithm 6, 7, and 8 respectively.

Algorithm 6 Key Generation

Input: A security parameter λ , and two small positive integers r and s .

Output: A public key pk and a private key sk .

- 1: Choose randomly a prime number p of λ bits with $p \equiv 1 \pmod{3}$.
- 2: Choose randomly a prime number q of λ bits with $q \equiv 1 \pmod{3}$.
- 3: Compute $N = p^r q^s$.
- 4: Choose randomly an integer $b \in \mathbb{Z}/N\mathbb{Z}$ such that $a = b^3 \pmod{N}$ is nonzero cubic residue modulo p and modulo q .
- 5: Choose an integer $e \in \mathbb{Z}/N\mathbb{Z}$ with $\gcd(e, pq(p-1)(q-1)) = 1$.
- 6: Compute

$$d \equiv e^{-1} \pmod{p^{2(r-1)}q^{2(s-1)}(p-1)^2(q-1)^2}.$$

- 7: The public key is $pk = (N, b, e)$.
 - 8: The private key is $sk = (N, b, d)$.
 - 9: Return the key pair (pk, sk) .
-

Algorithm 7 Encryption Process

Input: A message $M = (x_M, y_M) \in (\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})$ and a public key $pk = (N, b, e)$.

Output: The ciphertext of M .

- 1: Compute $a := b^3 \pmod{N}$;
 - 2: $(x, y, z) := \text{Encode2Curve}((x_M, y_M), b, N)$; ▷ Encoding of M into $\mathcal{C}_a(N)$
 - 3: Compute $C = (x_C, y_C, z_C) := e \otimes (x, y, z)$ on the cubic Pell curve $\mathcal{C}_a(N)$;
 - 4: $(c_x, c_y) := \text{DecodeFromCurve}(C, b, N)$; ▷ Compression of C
 - 5: Return the ciphertext $ctx = (c_x, c_y)$.
-

Algorithm 8 Decryption Process

Input: A ciphertext $ctx = (c_x, c_y) \in (\mathbb{Z}/N\mathbb{Z})^2$ and a private key $sk = (N, b, d)$.

Output: The decryption of C .

- 1: Compute $a := b^3 \pmod{N}$;
- 2: $(x_C, y_C, z_C) := \text{Encode2Curve}((c_x, c_y), b, N)$; ▷ Decompression of the ciphertext
- 3: Compute $(x, y, z) := d \otimes (x_C, y_C, z_C)$ on the cubic Pell curve $\mathcal{C}_a(N)$;
- 4: $(x_m, y_m) := \text{DecodeFromCurve}((x, y, z), b, N)$; ▷ Decoding of the point (x, y, z)
- 5: Return the plaintext (x_m, y_m)

Notice that at Line 4 in the encryption Algorithm 7, the compression function specified in the template of our scheme (Figure 1) is instantiated by the decoding function `DecodeFromCurve` which is the inverse of encoding function `Encode2Curve`. It means that in our scheme, the compression function and the decoding function are the same as well as the decompression function and the encoding function.

Encryption/Decryption Failures : The encryption process of a message $M = (x_M, y_M) \in (\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})$ fails when the encoding into $\mathcal{C}_a(N)$ of (x_M, y_M) or the compression process `DecodeFromCurve`(C, b, N) in Line 4 of Algorithm 7 fails. This occurs only when g defined in Algorithm 4 and 5 are not invertible modulo N . We know that with overwhelming probability $\gcd(g, N) = 1$; otherwise, a factor of N can be efficiently found. Similarly, the decryption process of a ciphertext $ctx = (c_x, c_y) \in (\mathbb{Z}/N\mathbb{Z})^2$ will be done correctly; otherwise, a factor of N can be found. Therefore, we can assume that the encryption and decryption process will be error-free whenever the problem of factoring large composite integers N is difficult.

4.2 A numerical example for the new scheme

In this subsection, we present a numerical example with all computation details. Notice that a proof of concept implementation of our scheme with SimulaMath [41] and SageMath [35] is provided in [36].

- **Key Generation :** Let $p = 877636073161$, $q = 427943630539$, $r = 1$ and $s = 2$. Then

$$N = p \times q^2 = 160726541291854510481081390266346881.$$

Consider the parameters

$$e = 130172055750281760449762497750803727,$$

$$b = 8919653598497184929883898221860016.$$

We can then compute

$$\begin{aligned} \psi(N) &= p^{2(r-1)} q^{2(s-1)} (p-1)^2 (q-1)^2 \\ &= 2583302107546261247071351601005913162322110106588 \backslash \\ &\quad 6025452264850972934400, \\ d &\equiv e^{-1} \pmod{\psi(N)} \\ &= 22008866449633569589025354096989208167393276780961 \backslash \\ &\quad 045235918145369812463. \end{aligned}$$

The public key is $pk = (N, b, e)$ and the private key is $sk = (N, b, d)$.

- **Encryption :** Consider the plaintext $M = (m_1, m_2)$ with

$$\begin{aligned} m_1 &= 30119327069956535343293582428481497, \\ m_2 &= 87449607717583963216974038660591367. \end{aligned}$$

To encrypt using the public key $pk = (N, b, e)$, one first computes

$$a \equiv b^3 \pmod{N} \equiv 110984846909034778402177655906954357,$$

and defines the cubic Pell curve

$$C_a(N) : x^3 + ay^3 + a^2z^3 - 3axyz \equiv 1 \pmod{N}.$$

One then encodes the message (m_1, m_2) into $C_a(N)$ using Algorithm 4. This gives (x_M, y_M, z_M) with

$$\begin{aligned} x_M &= 140951064022017564592779260398752129, \\ y_M &= 148299166162508601153120654776829594, \\ z_M &= 145736964847022157345025797688945229. \end{aligned}$$

Then, one computes $(x_C, y_C, z_C) = e \otimes (x_M, y_M, z_M)$ on $C_a(N)$ using Algorithm 3. This gives

$$\begin{aligned} x_C &= 61400146515021299784450682204296604, \\ y_C &= 11022542566060599320035499687366642, \\ z_C &= 61507634494621967923675058386448309. \end{aligned}$$

To compress (x_C, y_C, z_C) , one uses Algorithm 3. This gives (c_1, c_2) where

$$\begin{aligned} c_1 &= 119272817221858365069165947063984272, \\ c_2 &= 108837536797780384448758029507481222. \end{aligned}$$

Then (c_1, c_2) is the ciphertext to be transmitted to the recipient.

- **Decryption :** To decrypt the ciphertext (c_x, c_y) using the private key $sk = (N, b, d)$, one first decodes it to (x_C, y_C, z_C) using Algorithm 4, and obtain

$$\begin{aligned} x_C &= 61400146515021299784450682204296604, \\ y_C &= 11022542566060599320035499687366642, \\ z_C &= 61507634494621967923675058386448309. \end{aligned}$$

Then, using Algorithm 3, one computes $(x_M, y_M, z_M) = d \otimes (x_C, y_C, z_C)$ on $C_a(N)$, and obtain

$$\begin{aligned} x_M &= 140951064022017564592779260398752129, \\ y_M &= 148299166162508601153120654776829594, \\ z_M &= 145736964847022157345025797688945229. \end{aligned}$$

Finally, one decodes (x_M, y_M, z_M) using Algorithm 5 to get the plaintext $M = (m_1, m_2)$ with

$$\begin{aligned} m_1 &= 30119327069956535343293582428481497, \\ m_2 &= 87449607717583963216974038660591367. \end{aligned}$$

5 Security Analysis

In this section, we analyze the security of the new scheme by presenting two possible attacks. The first attack is based on the continued fraction algorithm, and the second is based on Coppersmith's method [12]. Both attacks are based on the modular relation $ed \equiv 1 \pmod{p^{2(r-1)}q^{2(s-1)}(p-1)^2(q-1)^2}$ between the public exponent e and the private exponent d .

5.1 A possible attack with the continued fraction algorithm

In [39], Seck and Nitaj studied the equation

$$ed - kp^{2(r-1)}q^{2(s-1)}(p-1)^2(q-1)^2 = 1,$$

and showed that, when d is sufficiently small, it can be found among the denominators of the convergents of the continued fraction expansion of $\frac{e}{N^2}$. The bound of d is presented in the following result.

Theorem 5.1. [39] Let $N = p^r q^s$ be a prime power modulus with $q < p < 2q$. Let e be a public exponent, and d be the private exponent satisfying $d \equiv e^{-1} \pmod{\psi(N)}$ where $\psi(N) = p^{2(r-1)}q^{2(s-1)}(p-1)^2(q-1)^2$. If $e < \psi(N)$, and

$$d < \frac{\sqrt{2}}{4} N^{\frac{1}{2(r+s)}},$$

then one can find d and factor N in polynomial time.

5.2 A possible attack with Coppersmith's method

Coppersmith's method [12] is a technique based on lattice basis reduction used to find the small solutions of polynomial equations. It is intensively deployed for the cryptanalysis of RSA and its variants. For univariate polynomial equations, it relies on the following two important results.

Theorem 5.2 (LLL [24, 27]). Let $\mathcal{L}$ be a lattice with a basis $(u_1, \dots, u_\omega)$. The LLL algorithm outputs a new basis $(b_1, \dots, b_\omega)$ of $\mathcal{L}$ satisfying

$$\|b_1\| \leq \dots \leq \|b_i\| \leq 2^{\frac{\omega(\omega-1)}{4(\omega+1-i)}} \det(\mathcal{L})^{\frac{1}{\omega+1-i}},$$

for $i = 1, 2, \dots, \omega$.

Theorem 5.3 (Howgrave-Graham [19]). Let $h(x) = \sum a_i x^i \in \mathbb{Z}[x]$ be a polynomial with at most ω monomials and norm

$$\|h(x)\| = \sqrt{\sum a_i^2}.$$

Let M be a positive integer. If $|y| < X$, and

$$h(y) \equiv 0 \pmod{M}, \quad \|h(Xx)\| < \frac{M}{\sqrt{\omega}},$$

then $h(y) = 0$ holds over the integers.

Using the former two theorems, the following result gives a lower bound for d in our scheme. Note that, in [26, 30], related methods have been used to solve the equations $ed \equiv 1 \pmod{p^{r-1}q^{l-1}}$ and $ex \equiv z \pmod{p^{r-1}q^{s-1}}$ respectively.

Theorem 5.4. Let $N = p^r q^s$ be an RSA prime power modulus with $r > s \geq 1$ where p and q are of the same bit-size. Let e be a public exponent satisfying $ed \equiv 1 \pmod{p^{2(r-1)}q^{2(s-1)}(p-1)^2(q-1)^2}$ with $d < N^\delta$. Then, one can factor N in polynomial time if

$$\delta < 2 - \frac{2(3r+s)}{(r+s)^2}.$$

Proof. Let $N = p^r q^s$ with $r > s \geq 1$, and $\psi(N) = p^{2(r-1)}q^{2(s-1)}(p-1)^2(q-1)^2$. The equation $ed \equiv 1 \pmod{\psi(N)}$ implies that $ed-1 \equiv 0 \pmod{p^{2(r-1)}q^{2(s-1)}}$. Let $a \equiv e^{-1} \pmod{N^2}$. Then $x_0 = d$ is solution of the equation $f(x) = x - a$ modulo $p^{2(r-1)}q^{2(s-1)}$.

Let m , t_1 , and t_2 be three parameters to be optimized later with $t_1 < t_2$. Let

$$k_0 = \left\lceil \frac{s(r-1)t_1 - r(s-1)t_2}{r-s} \right\rceil,$$

be the smallest integer k such that

$$\left\lceil \frac{2(s-1)(t_2-k)}{s} \right\rceil \geq \left\lceil \frac{2(r-1)(t_1-k)}{r} \right\rceil.$$

We can check that $k_0 \leq t_1 < t_2$.

For $k = 0, \dots, m$, consider the polynomials

$$G_k(x) = \begin{cases} f(x)^k & \text{if } t_2 \leq k, \\ f(x)^k N^{\left\lceil \frac{2(s-1)(t_2-k)}{s} \right\rceil} & \text{if } k_0 \leq k < t_2, \\ f(x)^k N^{\left\lceil \frac{2(r-1)(t_1-k)}{r} \right\rceil} & \text{if } k < k_0. \end{cases}$$

Since $f(x_0) \equiv 0 \pmod{p^{2(r-1)}q^{2(s-1)}}$, then we get

$$G_k(x_0) \equiv 0 \pmod{p^{2(r-1)t_1}q^{2(s-1)t_2}}.$$

Let $X = N^\delta$ be an upper bounds for $x_0 = d$. Consider the lattice $\mathcal{L}$ generated by the matrix where the rows are spanned by the coefficients of the polynomials $G_k(xX)$. The matrix is triangular if we consider the ordering $G_k(xX) < G_{k'}(xX)$ if $k < k'$. Similarly, the columns are ordered following the rule that $x^k < x^{k'}$ if $k < k'$.

Since the matrix of the lattice is triangular, its determinant is the product of the diagonal terms, that is

$$\det(\mathcal{L}) = X^{e_X} N^{e_N}, \quad (5)$$

where $e_X = \sum_{k=0}^m k = \frac{1}{2}m(m+1)$. The dimension of the lattice is $\omega = \sum_{k=0}^m 1 = m+1$. Using k_0 , the exponent e_N can be computed as

$$e_N = \sum_{k=0}^{k_0-1} \left\lceil \frac{2(r-1)(t_1-k)}{r} \right\rceil + \sum_{k=k_0}^{t_2} \left\lceil \frac{2(s-1)(t_2-k)}{s} \right\rceil.$$

We set $t_1 = \tau_1 m$, and $t_2 = \tau_2 m$. Then, the dominant parts in e_X and e_N are

$$e_X = \frac{1}{2}m^2 + o(m^2), \quad (6)$$

$$e_N = \frac{r-1}{r(r-s)} \left(rs(\tau_1 - \tau_2)^2 + 2r\tau_1\tau_2 - r\tau_2^2 - s\tau_1^2 \right) m^2 + o(m^2). \quad (7)$$

Next, apply the LLL algorithm to the lattice $\mathcal{L}$. It outputs a new matrix with reduced vectors. Collecting the rows of the new matrix, we build ω polynomials $h_j(xX)$ with $j = 1, \dots, \omega$ satisfying $h_j(x_0) \equiv 0 \pmod{p^{2(r-1)t_1}q^{2(s-1)t_2}}$. Taking $i = 1$ in Theorem 5.2 we get

$$\|h_1(xX)\| \leq 2^{\frac{\omega-1}{4}} \det(L)^{\frac{1}{\omega}}.$$

Then, to use Theorem 5.3, we let

$$2^{\frac{\omega-1}{4}} \det(\mathcal{L})^{\frac{1}{\omega}} < \frac{p^{2(r-1)t_1}q^{2(s-1)t_2}}{\sqrt{\omega}}.$$

Since p and q are of the same bit size, then $p \approx q \approx N^{\frac{1}{r+s}}$. Using this with $\det(\mathcal{L}) = X^{e_X} N^{e_N}$ where $X = N^\delta$, the former inequality becomes

$$2^{\frac{\omega-1}{4}} (N^{\delta e_X} N^{e_N})^{\frac{1}{\omega}} < \frac{N^{\frac{2(r-1)t_1 + 2(s-1)t_2}{r+s}}}{\sqrt{\omega}}.$$

Then, using $t_1 = m\tau_1$, $t_2 = m\tau_2$, (6), (7), and solving the former inequality, we get $\delta < F(\tau_1, \tau_2)$ where

$$F(\tau_1, \tau_2) = \frac{4((r-1)\tau_1 + (s-1)\tau_2)}{r+s} - \frac{2(r-1)}{r(r-s)} (rs(\tau_1 - \tau_2)^2 + 2r\tau_1\tau_2 - r\tau_2^2 - s\tau_1^2).$$

The optimal values for τ_1 and τ_2 are obtained by solving the system of equations

$$\frac{\partial F}{\partial \tau_1}(\tau_1, \tau_2) = 0, \quad \frac{\partial F}{\partial \tau_2}(\tau_1, \tau_2) = 0.$$

This gives the following values

$$\tau_1^{(0)} = \frac{r(r+s-2)}{r^2 + rs - r - s}, \quad \tau_2^{(0)} = 1.$$

Plugging these values in the bound of δ , we get

$$\delta < F(\tau_1^{(0)}, \tau_2^{(0)}) = 2 - \frac{2(3r+s)}{(r+s)^2}.$$

Under this condition, one can solve the equation $h_1(x) = 0$ over the integers and get the root $x_0 = d$. Then, using d , we get

$$g = \gcd(ed - 1, N^2) = p^{2(r-1)}q^{2(s-1)}, \quad pq = \sqrt{\frac{N^2}{g}},$$

and finally

$$p = \left(\frac{N^{s-1}}{g^{\frac{s}{2}}} \right)^{\frac{1}{s-r}}, \quad q = \left(\frac{N^{r-1}}{g^{\frac{r}{2}}} \right)^{\frac{1}{r-s}}.$$

This completes the proof. □

5.3 On IND-CPA and CCA Security

It is well known that deterministic public key encryption schemes, including plain RSA, are not secure neither under the chosen-ciphertext attack (CCA) [2] nor meet the indistinguishability under chosen-plaintext attack (IND-CPA) [2]. Bellare and Rogaway [3] published the Optimal Asymmetric Encryption Padding (OAEP) framework at Eurocrypt 1994, which can transform a partial-domain one-way trapdoor permutation scheme into a CCA [2] secure cryptosystem in the random oracle model. When the OAEP transformation is instantiated with plain RSA, we get the RSA-OAEP cryptosystem which is shown to be CCA2 secure [17] in the random oracle model under the RSA assumption. Later Shoup [40, 32] proposed OAEP+ transformation, a slight modification of OAEP which allows to get a CCA secure cryptosystem from a one-way trapdoor permutation scheme.

To transform our scheme into an IND-CPA and CCA secure public key encryption scheme, we apply the OAEP+ framework as follows.

Let $N = p^r q^s$ be a $k + 1$ bit integer with p and q prime. Let $(\text{KGen}, \mathcal{E}, \mathcal{D})$ our public key encryption scheme defined by Algorithms [6, 7] and [8]. Let n, k_0 and k_1 be integers such that $n + k_1 = k$ and $k_0 \leq k$. Define the random functions $G : \{0, 1\}^{k_0} \rightarrow \{0, 1\}^n$, $H : \{0, 1\}^{n+k_1} \rightarrow \{0, 1\}^{k_0}$ and $H' : \{0, 1\}^{n+k_0} \rightarrow \{0, 1\}^{k_1}$. For a binary vector $b = b_0 b_1 b_2 \dots b_i b_{i+1} \dots b_j b_{j+1} \dots b_k$, we denote by $b[i \dots j]$ the partial binary vector $b_i b_{i+1} \dots b_j$.

- Key Generation: Generate (pk, sk) with Algorithm [6]. Then the public key is the function $\mathcal{E}_{pk} : (x_1, x_2) \mapsto \mathcal{E}((x_1, x_2), pk)$, and the private key is the function $\mathcal{D}_{sk} : (y_1, y_2) \mapsto \mathcal{D}((y_1, y_2), sk)$.
- Encryption process: To encrypt a message $m \in \{0, 1\}^n$ with the public key $\mathcal{E}_{pk}$, proceed as follows. First, pick a random value $r \in \{0, 1\}^{k_0}$. Then compute $s = (G(r) \oplus m) \parallel H'(r \parallel m)$ and $t = r \oplus H(s)$ where $\parallel$ means concatenation. Finally, output $c = \mathcal{E}_{pk}(s, t)$.
- Decryption process: To decrypt a ciphertext c with the secret key $\mathcal{D}_{sk}$, compute $(s, t) = \mathcal{D}_{sk}(c)$, then $r = t \oplus H(s)$, $m = s[0 \dots n-1] \oplus G(r)$ and $y = s[n \dots n+k_1-1]$. If $y = H'(r \parallel m)$ return m ; otherwise return $\perp$.

6 Conclusion

We presented a study of three topics related to the cubic Pell curve $\mathcal{C}_a(N) : x^3 + ay^3 + a^2z^3 - 3axyz \equiv 1 \pmod{N}$ where N is a composite integer, and $a \in \mathbb{Z}/N\mathbb{Z}$. The first topic shows how to encode and decode from $\mathbb{Z}/N\mathbb{Z}$ into $\mathcal{C}_a(N)$ when $N = \prod_{i=1}^l p_i$ with distinct prime factors, $p_i \equiv 2 \pmod{3}$. The second topic shows how to encode and decode from $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ into $\mathcal{C}_a(N)$ when $N = p^r q^s$, $p \equiv q \equiv 1 \pmod{3}$. The third topic presents a new scheme based on the arithmetic of the cubic Pell equation, and on encoding and decoding functions for efficiency reasons. The security of the new scheme is analyzed.

References

- [1] E. J. Barbeau, Pell equation, Chapter 7: The Cubic Analogue of Pell Equation. Springer, New York (2003).
- [2] M. Bellare, A. Desai, D. Pointcheval and P. Rogaway, Relations among notions of security for public-key encryption schemes. In: Crypto '98, Lect. Notes Comput. Sci., 1462, Springer-Verlag, Berlin (1998), 26–45.
- [3] M. Bellare and P. Rogaway, Optimal asymmetric encryption: how to encrypt with RSA. In: Eurocrypt '94, Lect. Notes Comput. Sci., 950, Springer-Verlag, Berlin (1995), 92–111.

- [4] D. J. Bernstein, M. Hamburg, A. Krasnova and T. Lange, Elligator: elliptic-curve points indistinguishable from uniform random strings. In: V. Gligor, M. Yung (eds.) CCS, ACM (2013).
- [5] D. Boneh, Twenty years of attacks on the RSA cryptosystem. Notices Amer. Math. Soc., 46(2) (1999), 203–213.
- [6] D. Boneh and M. K. Franklin, Identity-based encryption from the Weil pairing. In: J. Kilian (ed.), CRYPTO, Lect. Notes Comput. Sci., 2139, Springer (2001), 213–229.
- [7] D. Boneh, G. Durfee and Y. Frankel, An attack on RSA given a small fraction of the private key bits. In: ASIACRYPT (1998), 25–34.
- [8] D. Boneh, G. Durfee and N. Howgrave-Graham, Factoring $N = p^r q$ for large r . In: CRYPTO (1999), 326–337.
- [9] D. Boneh and G. Durfee, Cryptanalysis of RSA with private key d less than $N^{0.292}$. In: Eurocrypt '99, Lect. Notes Comput. Sci., 1592, Springer-Verlag (1999), 1–11.
- [10] M. Boudabra and A. Nitaj, A new generalization of the KMOV cryptosystem. J. Appl. Math. Comput., 57(1–2) (2017), 229–245.
- [11] M. Boudabra and A. Nitaj, A new public key cryptosystem based on Edwards curves. J. Appl. Math. Comput., 61 (2019), 431–450.
- [12] D. Coppersmith, Small solutions to polynomial equations, and low exponent RSA vulnerabilities. J. Cryptol., 10(4) (1997), 233–260.
- [13] N. Demytko, A new elliptic curve based analogue of RSA. In: T. Hellesteth (ed.), Eurocrypt 1993, Lect. Notes Comput. Sci., 765, Springer-Verlag (1994), 40–49.
- [14] W. Diffie and M. Hellman, New directions in cryptography. IEEE Trans. Inf. Theory, 22(6) (1976), 644–654.
- [15] S. Dutto and N. Murru, On the cubic Pell equation over finite fields. arXiv:2203.05290 (2022).
- [16] P. A. Fouque, A. Joux and M. Tibouchi, Injective encodings to elliptic curves. In: Information Security and Privacy, 18th Australasian Conference, ACISP 2013, Lect. Notes Comput. Sci., Springer, Berlin Heidelberg (2013), 203–218.
- [17] E. Fujisaki, T. Okamoto, D. Pointcheval and J. Stern, RSA-OAEP is secure under the RSA assumption. In: Annual Int. Cryptology Conf., Lect. Notes Comput. Sci., Springer, Berlin Heidelberg (2001), 260–274.
- [18] J. Hastad, Using RSA with low exponent in a public key network. In: Advances in Cryptology—CRYPTO '85, Lect. Notes Comput. Sci., 5, Springer-Verlag (1986), 403–408.
- [19] N. Howgrave-Graham, Finding small roots of univariate modular equations revisited. In: Cryptography and Coding, Lect. Notes Comput. Sci., 1355, Springer-Verlag (1997), 131–142.
- [20] T. Icart, How to hash into elliptic curves. In: Annual Int. Cryptology Conf., Lect. Notes Comput. Sci., Springer, Berlin Heidelberg (2009), 303–316.
- [21] K. Koyama, Fast RSA type scheme based on singular cubic curve $y^2 + axy = x^3 \pmod{n}$. Lect. Notes Comput. Sci., 921 (1995), 329–339.

- [22] K. Koyama, U. M. Maurer, T. Okamoto and S. A. Vanstone, New public-key schemes based on elliptic curves over the ring $\mathbb{Z}_n$. *Lect. Notes Comput. Sci.*, 576 (1991), 252–266.
- [23] H. Kuwakado, K. Koyama and Y. Tsuruoka, A new RSA-type scheme based on singular cubic curves $y^2 \equiv x^3 + bx^2 \pmod{n}$. *IEICE Trans. Fundam.*, E78-A (1995), 27–33.
- [24] A. K. Lenstra, H. W. Lenstra and L. Lovász, Factoring polynomials with rational coefficients. *Math. Ann.*, 261 (1982), 513–534.
- [25] S. Lim, S. Kim, I. Yie and H. Lee, A generalized Takagi-cryptosystem with a modulus of the form p^rqs . In: *Indocrypt*, Springer (2000), 283–294.
- [26] Y. Lu, L. Peng and S. Sarkar, Cryptanalysis of an RSA variant with moduli $N = p^r q^l$. 9th Int. Workshop Coding Cryptogr. (2015), Paris, France. <https://inria.hal.science/hal-01276463/document>.
- [27] A. May, New RSA vulnerabilities using lattice reduction methods. PhD Thesis, Univ. Paderborn (2003). <https://digital.ub.uni-paderborn.de/ubpb/urn/urn:nbn:de:hbz:466-20030101205>.
- [28] N. Murru and F. M. Saettone, A novel RSA-like cryptosystem based on a generalization of the Rédei rational functions. *Lect. Notes Comput. Sci.*, 10737 (2018), Springer, Cham.
- [29] A. Nitaj, Another generalization of Wiener’s attack on RSA. *Lect. Notes Comput. Sci.*, 5023 (2008), 174–190.
- [30] A. Nitaj, W. Susilo and J. Tonien, A generalized attack on the multi-prime power RSA. *Lect. Notes Comput. Sci.*, 13503 (2022), 537–549.
- [31] M. O. Rabin, Digitalized signatures and public key functions as intractable as factorisation. *MIT/LCS/TR-212* (1979).
- [32] D. Pointcheval, How to encrypt properly with RSA. *CryptoBytes*, 5(1) (2002), 10–19.
- [33] R. Rivest, A. Shamir and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2) (1978), 120–126.
- [34] K. H. Rosen, *Elementary Number Theory and Its Applications*. Addison-Wesley, 3rd ed. (1993), 285–302.
- [35] SageMath, The Sage Mathematics Software System (Version 10.1). Sage Developers (2023). <https://www.sagemath.org>.
- [36] M. Seck, Proof of concept implementation of the proposed encryption scheme. GitHub Repository. <https://github.com/mseckkept/pkeencodingsecknitaj.git>.
- [37] M. Seck, H. Boudjou, N. Diarra and A. Y. O. C. Khlil, On indifferentiable hashing into the Jacobian of hyperelliptic curves of genus 2. *Lect. Notes Comput. Sci.* (2017), 205–222.
- [38] M. Seck and N. Diarra, Unified formulas for some deterministic almost-injective encodings into hyperelliptic curves. *Lect. Notes Comput. Sci.* (2018), 183–202.
- [39] M. Seck and A. Nitaj, A new public key cryptosystem based on the cubic Pell curve. *Cryptol. ePrint Arch.* (2024).
- [40] V. Shoup, OAEP reconsidered. *J. Cryptol.*, 15 (2002), 223–249.

- [41] SimulaMath, A software for learning, teaching and research in mathematics (Version 1.1). SimulaMath Developers (2023). <https://simulamath.org>.
- [42] T. Takagi, Fast RSA-type cryptosystem modulo p^kq . *Lect. Notes Comput. Sci.*, 1462 (1998), 318–326.
- [43] G. Teseleanu and P. Cotan, Small private key attack against a family of RSA-like cryptosystems. *Cryptol. ePrint Arch.* (2023). <https://eprint.iacr.org/2023/1356>.
- [44] B. de Weger, Cryptanalysis of RSA with small prime difference. *Appl. Algebra Eng. Commun. Comput.*, 13(1) (2002), 17–28.
- [45] M. Wiener, Cryptanalysis of short RSA secret exponents. *IEEE Trans. Inf. Theory*, 36 (1990), 553–558.



ISSN: 2820-7114

Moroccan Journal of Algebra and Geometry with Applications

Supported by Sidi Mohamed Ben Abdellah University, Fez, Morocco

Volume 4, Issue 1 (2025), pp 109-137

Title :

Survey on Side-Channel Attacks on Code-Based Key Encapsulation Mechanism

Author(s):

Pierre-Louis Cayrel, Mohamed Fall, Laila Mesmoudi, and Cheikh Tiecoumba Gueye

Survey on Side-Channel Attacks on Code-Based Key Encapsulation Mechanism

Pierre-Louis Cayrel¹, Mohamed Fall², Laila Mesmoudi² and Cheikh Tiecoumba Gueye²

¹ Universitan Monnet Saint-Etienne, CNRS, Institut d Optique Graduate School,
Laboratoire Hubert Curien UMR 5516, F-42023, SAINT-ETIENNE, France.

email: pierre.louis.cayrel@univ-st-etienne.fr

² Universiteikh Anta Diop, Laboratoire d'Alge de Cryptologie de Gie algique et Application,
Dakar, Sgal.

email: fall13.edu@gmail.com

email: laila.mesmoudi@ucad.edu.sn

email: cheikht.gueye@ucad.edu.sn

Communicated by Abderrahmane Nitaj

(Received 21 October 2024, Revised 25 November 2024, Accepted 31 December 2024)

Abstract. Code-based Key Encapsulation Mechanisms (KEM) represent a promising solution in the field of post-quantum cryptography, providing security guarantees rooted in well-studied mathematical problems, such as decoding linear codes with or without errors. This survey offers an in-depth analysis of the main code-based KEM constructions, including Classic McEliece, BIKE, and HQC. We describe their theoretical foundations, key algorithms (key generation, encapsulation, and decapsulation), as well as their strengths and weaknesses in terms of security and efficiency.

Particular attention is given to the practical vulnerabilities of these schemes against cryptanalytic attacks, such as side-channel attacks, fault injection attacks, and specific techniques for key and message recovery. We also highlight the countermeasures proposed in the literature to strengthen their security, including constant-time algorithms, hardware protections, and improvements to decoding mechanisms.

Furthermore, we discuss the challenges related to the implementation and adoption of these systems in constrained environments, such as the Internet of Things (IoT), while evaluating their potential in contexts where quantum security becomes a critical necessity. This work aims to provide a clear and comprehensive overview of recent advances and future directions for the development of robust and efficient code-based KEMs, contributing to the transition toward post-quantum cryptographic standards.

Key Words: Post-quantum cryptography, Code-based cryptography, Key encapsulation mechanisms (KEMs), Classic McEliece, BIKE, HQC, Cryptanalysis, Countermeasures.

2020 MSC: Primary 94A60; Secondary 14G50.

Dedicated to our Professor David E. Dobbs for his 80th Birthday.

1 Introduction

In the era of quantum computers, the foundations of modern cryptography, which have long been considered secure against classical computing attacks, are being profoundly challenged. Algorithms such as RSA, DSA, or elliptic curve-based cryptographic systems, which have underpinned the security of digital communications for several decades, face a new and formidable threat from quantum computing. Specifically, quantum algorithms, especially Shor's algorithm [79], can efficiently solve

mathematical problems based on these systems, such as integer factorization and the discrete logarithm problem. These problems, which are infeasible to solve within a reasonable timeframe using classical computers, can be solved in polynomial time with a sufficiently large quantum computer. As a result, the security of many widely deployed cryptosystems is severely undermined by the advent of quantum computing technologies. This imminent risk has galvanized the cryptographic community into searching for new cryptographic algorithms that can resist both classical and quantum attacks, giving rise to the burgeoning field of post-quantum cryptography.

Among the various candidates proposed for post-quantum cryptography, cryptosystems based on error-correcting codes stand out as particularly promising. These systems derive their security from the intrinsic difficulty of decoding linear codes, a problem that has been studied for many years and is believed to be hard, even for quantum computers. Error-correcting codes have a long history in both cryptography and communication theory, where they are used to correct transmission errors. However, their cryptographic strength lies in the complexity of the decoding problem. Problems like the syndrome decoding problem, which asks one to find the closest codeword to a given vector, are believed to be NP-hard, making them resistant to both classical and quantum attacks. Unlike systems based on number-theoretic problems (such as RSA), no efficient quantum algorithm has yet been found to solve the hardest problems in coding theory. This natural resistance to quantum attacks makes code-based cryptosystems an attractive option for post-quantum security.

One of the most well-known and extensively studied code-based cryptosystems is the McEliece cryptosystem [87], which was proposed as early as 1978 by Robert McEliece. Despite its age, the McEliece scheme remains one of the most secure post-quantum cryptosystems, largely due to its reliance on the hardness of decoding a general linear code. The scheme uses a family of algebraic codes known as Goppa codes, which are well suited to cryptographic applications due to their structure and resistance to known attacks. Over the years, various attempts have been made to break the McEliece cryptosystem, both from a classical and a quantum perspective, but it has consistently demonstrated remarkable resilience. This durability, combined with the performance advantages that come with well-understood decoding algorithms, ensures that the McEliece cryptosystem continues to be a central pillar in post-quantum cryptography research. Its proven security and efficiency in resisting attacks, even with the potential capabilities of quantum computers, have positioned it as one of the leading candidates for long-term cryptographic security.

In the ongoing efforts to standardize post-quantum cryptographic algorithms, several code-based key encapsulation mechanisms (KEMs) have emerged as front-runners. The National Institute of Standards and Technology (NIST), which is leading the global effort to define post-quantum cryptography standards, has recognized several code-based KEMs as highly promising candidates. These include Classic McEliece [87], BIKE (Bit Flipping Key Encapsulation) [82], and HQC (Hamming Quasi-Cyclic) [81]. Each of these schemes is grounded in variants of hard problems in coding theory, and they have been designed with a focus on achieving an optimal balance between security, efficiency, and practicality for real-world deployment.

Classic McEliece, in particular, is notable for its long-standing reputation as a highly secure cryptosystem. The scheme is based on the difficulty of decoding random linear codes, and it employs Goppa codes to ensure both robustness and efficiency. However, a common critique of the McEliece cryptosystem is the relatively large size of its public keys, which can present challenges in terms of storage and transmission, especially in resource-constrained environments. Nonetheless, ongoing research efforts are focused on mitigating this issue by exploring alternative code families and optimization techniques to reduce key sizes without compromising security.

The BIKE and HQC schemes are more recent developments in the landscape of code-based cryptography, and they introduce innovative approaches to key encapsulation. BIKE, for instance, utilizes quasi-cyclic codes and employs a bit-flipping decoding algorithm, which enables it to achieve competitive performance in both encryption and decryption operations. Its construction leverages the

cyclic structure of the underlying codes to reduce the size of public keys, while maintaining strong security guarantees based on the hardness of decoding quasi-cyclic codes. Similarly, HQC combines the use of quasi-cyclic codes with the syndrome decoding problem, a well-established hard problem in coding theory. This combination allows HQC to offer strong security against quantum attacks, while also achieving high efficiency in key generation and message encryption processes.

Despite the theoretical strengths of these code-based KEMs, cryptography in practice is rarely immune to real-world challenges. One of the most significant concerns for any cryptosystem is its vulnerability to side-channel attacks [84, 5, 85, 77, 74, 76, 83, 86]. These attacks exploit indirect information leaked during the execution of cryptographic algorithms, such as variations in power consumption, electromagnetic emissions, or timing variations, to recover secret information like private keys. For example, recent studies have demonstrated that timing attacks on the decoding process of code-based KEMs, including Classic McEliece, BIKE, and HQC, can reveal sensitive information that compromises their security. Such findings emphasize the importance of implementing cryptographic algorithms in a way that minimizes or eliminates these side-channel leakages, through techniques such as constant-time operations, randomization of processing steps, and masking.

In addition to side-channel attacks, fault injection attacks (FIA) [56, 14] pose another serious threat to the practical security of code-based cryptosystems. These attacks involve deliberately inducing faults in the hardware or software implementation of a cryptosystem, with the goal of causing errors that can be exploited to recover private keys or other sensitive data. Fault injection attacks can be highly effective against code-based KEMs if countermeasures are not carefully implemented. For example, by causing specific errors in the decoding process, an attacker might be able to gather enough information to perform a key-recovery attack, which would otherwise be impossible through conventional means.

In the case of Classic McEliece, BIKE, and HQC, several cryptanalytic studies have highlighted potential vulnerabilities related to the decapsulation process or the key generation routines. In particular, some recent attacks have identified timing leaks in the decoding algorithms used by these schemes, which could potentially allow an attacker to recover the secret key by analyzing the time it takes to process different inputs. These findings illustrate that while code-based cryptosystems are theoretically resistant to quantum attacks, they must still contend with the practical vulnerabilities that arise from their implementation in real-world devices and systems.

The ongoing research into these attacks underscores the need for robust countermeasures that address both theoretical and practical vulnerabilities. Cryptographic engineers must develop and deploy secure implementations that defend against side-channel and fault injection attacks, ensuring that these post-quantum cryptosystems can withstand not only the computational power of future quantum computers but also the more immediate threats posed by real-world attackers. By understanding and addressing these challenges, we can ensure that code-based KEMs like Classic McEliece, BIKE, and HQC will provide the long-term security required for the post-quantum era.

Organization. The remaining of the survey is described as follows. In **Section 2**, we provide a general presentation of the Classic McEliece, BIKE, and HQC key encapsulation mechanisms. In **Section 3**, we present various cryptanalysis on these different candidates. **Section 4** discusses the main results. Finally, in **Section 5**, we conclude the document.

2 General presentation of candidates

2.1 Classic McEliece

McEliece is one of the oldest and most established code-based cryptosystems, originally proposed by Robert McEliece in 1978. It is a public-key cryptosystem that relies on the hardness of decoding

random linear codes, a problem widely believed to be resistant not only to classical attacks but also to quantum attacks [80]. At the heart of the McEliece cryptosystem is its use of Goppa codes, a type of algebraic error-correcting linear code that is particularly suited to cryptographic purposes due to its efficient decoding algorithms. The core idea behind the McEliece scheme is that while decoding a randomly generated linear code is NP-hard, the problem becomes tractable when using structured codes like Goppa codes, which can be efficiently decoded by the legitimate user. This clever distinction between the public key, which appears to be a random linear code, and the private key, which allows for efficient decoding, is what provides the security and functionality of the scheme.

The security of the McEliece cryptosystem is derived from the inherent complexity of the decoding problem. In more technical terms, the challenge is to recover the original message from the received codeword when only the public key is known. This problem is computationally infeasible for an attacker because it involves finding the closest codeword to a given vector in a large-dimensional vector space, a problem known as the *syndrome decoding problem*. Unlike cryptosystems based on number-theoretic problems such as RSA, the McEliece cryptosystem is considered quantum-resistant. This is primarily due to the fact that no efficient quantum algorithm, including Shors algorithm, has been found that can solve the hard problems underlying code-based cryptography in polynomial time.

One of the strengths of the McEliece scheme is its resilience to a broad range of attacks. Over the past several decades, McEliece has resisted cryptanalytic efforts, including both classical and quantum attacks. This remarkable durability has earned McEliece a prominent place in the NIST post-quantum cryptography standardization process, where it is considered one of the leading candidates for future cryptographic standards in the quantum era. However, McEliece is not without its challenges. The size of its public key is relatively large, often on the order of several megabytes, which presents challenges for its implementation, particularly in memory-constrained environments such as embedded systems, IoT devices, and mobile platforms. Despite these practical limitations, its robustness against quantum threats makes McEliece one of the most reliable and trusted options for long-term secure communication.

The McEliece key encapsulation mechanism (KEM) is designed to provide secure encryption in post-quantum environments. It consists of three distinct phases: *key generation*, *encapsulation*, and *decapsulation*. Each phase plays a crucial role in ensuring the overall security of the system, with interdependent operations that collectively enable secure key exchange. The structure of these phases ensures that even if an attacker intercepts the encapsulated key, they will not be able to reverse the encapsulation without access to the private key.

2.1.1 Classic McEliece - key generation

The **key generation** process creates a public-private key pair based on the security parameters (m, n, t) . During this phase, a random set of elements in $\mathbb{F}_{2^m}$ is generated, along with an irreducible monic polynomial of degree t . This enables the calculation of the parity-check matrix, which is later used to encapsulate data. Once the parity-check matrix is converted into a binary matrix and put into standard form, the public key is defined by the public matrix T , while the private key consists of the polynomial g and the set $\mathcal{L}$.

Algorithm 1 The key-generation algorithm of the *Classic McEliece* KEM.

Input: The *Classic McEliece* security parameters (m, n, t) ,

Output: The private key $\text{sk} = (g, \mathcal{L})$ and the public key $\text{pk} = T$

- 1: Generate a set $\mathcal{L} = \{\alpha_0, \dots, \alpha_{n-1}\}$ of random elements of $\mathbb{F}_{2^m}$ with $\#\mathcal{L} = n$
- 2: Generate an irreducible monic polynomial $g \in \mathbb{F}_{2^m}[x]$ of degree t
- 3: Compute the $t \times n$ parity-check matrix H

$$H = \begin{pmatrix} (g(\alpha_0))^{-1} & \dots & (g(\alpha_{n-1}))^{-1} \\ \vdots & \ddots & \vdots \\ \alpha_0^{t-1}(g(\alpha_0))^{-1} & \dots & \alpha_{n-1}^{t-1}(g(\alpha_{n-1}))^{-1} \end{pmatrix}$$

- 4: Transform H to an $mt \times n$ binary matrix H' $\triangleright \mathbb{F}_{2^m} \rightarrow \mathbb{F}_2^m$ mapping
 - 5: Transform H' in standard-form $H_{\text{pub}} = (I_{mt} \mid T)$
 - 6: Return the private key $\text{sk} = (g, \mathcal{L})$ and the public key $\text{pk} = T$
-

2.1.2 Classic McEliece - encapsulation

During the **encapsulation** phase, a random vector e is generated with a Hamming weight of t , corresponding to the number of errors the code can correct. This error vector is encapsulated into a ciphertext z , obtained by multiplying the public matrix T with e . Finally, a session key K is derived by hashing e and z , ensuring the confidentiality of the transmitted data

Algorithm 2 The encapsulation algorithm of the *Classic McEliece* KEM.

Input: The public key $\text{pk} = T$

Output: The ciphertext z and the session key K

- 1: Generate a random vector $e \in \mathbb{F}_2^n$ with $\text{wt}(e) = t$
 - 2: Compute $z = (I_{mt} \mid T) e^T$
 - 3: Compute $K = \text{hash}(1 \parallel e \parallel z)$
 - 4: Return the ciphertext z and the session key K
-

2.1.3 Classic McEliece - decapsulation

To the **decapsulation** phase, the receiver uses the private key to recover the encapsulated error. By computing the syndrome from the received ciphertext z and employing the Berlekamp-Massey algorithm, the error is located and corrected. This allows for the recovery of the original vector e , and consequently, the same session key K as the sender.

Algorithm 3 The decapsulation algorithm of the *Classic McEliece* KEM.

Input: The ciphertext $\mathbf{z}$ and the private key $\text{sk} = (g, \mathcal{L})$

Output: The session key K

- 1: Compute the vector $\mathbf{v} = (\mathbf{z}, 0, \dots, 0)$ by padding $\mathbf{z}$ with $n - mt$ zeros
- 2: Compute the parity-check matrix

$$\mathbf{H}_{\text{priv}} = \begin{pmatrix} (g(\alpha_0))^{-2} & \dots & (g(\alpha_{n-1}))^{-2} \\ \vdots & \ddots & \vdots \\ \alpha_0^{2t-1}(g(\alpha_0))^{-2} & \dots & \alpha_{n-1}^{2t-1}(g(\alpha_{n-1}))^{-2} \end{pmatrix}$$

- 3: Compute the syndrome $\mathbf{s} = \mathbf{H}_{\text{priv}} \mathbf{v}^T$
 - 4: Compute the error locator pol. $\sigma(x)$ with Berlekamp-Massey algorithm
 - 5: Compute $(\sigma(\alpha_0), \dots, \sigma(\alpha_{n-1}))$ and recover the error vector $\mathbf{e}$
 - 6: Compute $K = \text{hash}(1|\mathbf{e}|\mathbf{z})$
 - 7: Return the session key K
-

2.2 BIKE (Bit Flipping Key Encapsulation)

BIKE is a KEM scheme based on binary quasicyclic codes and uses a bit-flipping decoding algorithm. Proposed within the NIST standardization process. BIKE relies on the hardness of decoding QC-MDPC (Quasi-Cyclic Moderate Density Parity Check) codes, a variant of LDPC (Low-Density Parity Check) codes, to encapsulate a session key. Errors are corrected using bit-flipping algorithms, which flip the erroneous bits in the received codeword [82]. The keys and ciphertexts are relatively compact compared to systems such as McEliece. BIKE benefits from fast and efficient implementations. The scheme is still vulnerable to practical attacks, such as side-channel attacks. Due to its efficiency and relatively small key sizes, BIKE is suitable for environments where memory and time constraints are critical, such as the Internet of Things (IoT). In terms of its structure, BIKE uses parameters based on QC-MDPC codes, denoted as $[n, r, w]$, where:

r is prime, $n = 2r$, $w = 2d$, with $w = \mathcal{O}(\sqrt{n})$ and d odd.

To elaborate the algebraic framework of BIKE, the system operates in the cyclic polynomial ring $\mathcal{R} = \mathbb{F}_2[X]/(X^r - 1)$, where each element h in $\mathcal{R}$ has a Hamming weight $|h|$. Furthermore, $\mathcal{H}_w$ defines the set of elements in $\mathcal{R}^2$ with specific weight properties, expressed as follows:

$$\mathcal{H}_w = \{(h_0, h_1) \in \mathcal{R}^2 \text{ s.t. } |h_0| = |h_1| = d\}$$

In cryptographic operations, BIKE uses hash functions L and K to generate and encapsulate keys. These functions produce outputs of appropriate lengths, and another hash function, H , produces a weight vector t , where t represents the error correction capability of the decoding process [77].

2.2.1 BIKE (Bit Flipping Key Encapsulation) - key generation

The key generation process in BIKE is straightforward, but it plays a critical role in ensuring the security of the scheme. First, a random secret σ is generated. Then, two polynomials, h_0 and h_1 , are randomly selected from the set $\mathcal{H}_w$. The public key h is calculated as the product of h_1 and the inverse of h_0 . At the end of this process, the private key consists of (h_0, h_1, σ) , while the public key is the polynomial h .

Algorithm 4 The key-generation algorithm of the BIKE KEM.

Input: The BIKE security parameters (ℓ) ,

Output: The private key $sk = (h_0, h_1, \sigma)$ and the public key $pk = h$

- 1: Pick $\sigma \xleftarrow{\$} \{0,1\}^\ell$
 - 2: Pick $(h_0, h_1) \xleftarrow{\$} \mathcal{H}_w$
 - 3: Compute $h \leftarrow h_1 h_0^{-1}$
 - 4: Return the private key $sk = (h_0, h_1, \sigma)$ and the public key $pk = h$
-

2.2.2 BIKE - encapsulation

Once the keys are established, encapsulation involves using the public key to generate a ciphertext and a shared session key. The process starts by picking a random message m . From m , an error vector (e_0, e_1) is computed using the hash function H . Then, the ciphertext is formed by combining the error vector and the public key, producing two components (c_0, c_1) . The shared secret $\mathcal{K}$ is derived from the message m and the ciphertext through the hash function K , which ensures the secure encapsulation of the session key.

Algorithm 5 The encapsulation algorithm of the BIKE KEM.

Input: The public key $pk = h$ and ℓ

Output: The ciphertext $c = (c_0, c_1)$ and the session key $\mathcal{K}$

- 1: Pick $m \xleftarrow{\$} \{0,1\}^\ell$
 - 2: Compute $(e_0, e_1) \leftarrow H(m)$
 - 3: Compute $(c_0, c_1) \leftarrow (e_0 + e_1 h, m \oplus L(e_0, e_1))$
 - 4: Compute the shared secret $\mathcal{K} \leftarrow K(m, c_0, c_1)$
 - 5: Return the ciphertext $c = (c_0, c_1)$ and the session key $\mathcal{K}$
-

2.2.3 BIKE - decapsulation

The decapsulation process reverses the encapsulation using the private key. The bit-flip decoding algorithm is applied to recover the error vector e' from the ciphertext component c_0 using the private polynomials h_0 and h_1 . Once e' is recovered, the original message m' is derived by XORing c_1 with the hash of e' . If the recovered error vector e' matches the one derived from m' , the session key $\mathcal{K}$ is reconstructed. If decoding fails, an alternative session key is computed using the private random value σ .

Algorithm 6 The decapsulation algorithm of the BIKE KEM.

Input: The ciphertext c and the private key $sk = (h_0, h_1, \sigma)$

Output: The session key $\mathcal{K}$

- 1: Compute $e' \leftarrow \text{Decoder}(c_0 h_0, h_0, h_1)$
 - 2: Compute $m' \leftarrow c_1 \oplus L(e')$
 - 3: If $e' = H(m')$ Then Compute $\mathcal{K} = K(m', c)$
 - 4: Else Compute $\mathcal{K} = K(\sigma, c)$
 - 5: Return the session key $\mathcal{K}$
-

2.3 HQC (Hamming Quasi-Cyclic)

HQC is a scheme that combines the principles of linear codes and quasicyclic structures to ensure its security. Similarly to the Learning with Errors (LWE) problem, HQC is based on the difficulty of

decoding linear codes with added noise. Noise makes decoding difficult for an attacker, while the legitimate receiver, possessing the private key, can efficiently recover the message. This mechanism encapsulates a key by introducing noise into the encoded vectors, ensuring that the legitimate recipient can recover the original data while an attacker faces an intractable problem.

The HQC scheme operates with a decodable $[n, k]$ code C , generated by a matrix $\mathbf{G} \in \mathbb{F}_2^{k \times n}$, which can correct at least δ errors via an efficient decoding algorithm, denoted as $C.Decode(\cdot)$. Like other post-quantum schemes, HQC employs hash functions $\mathcal{G}$, $\mathcal{H}$, and $\mathcal{K}$ for secure key generation and encapsulation [81]. Compared to the McEliece scheme, HQC offers more reasonable key sizes while maintaining strong security guarantees. It is also highly resistant to quantum attacks. However, as with BIKE, HQC faces challenges from practical security attacks, such as side-channel attacks. HQC is particularly appealing in applications requiring a balance between security, efficiency, and key size, such as secure communication infrastructures.

2.3.1 HQC (Hamming Quasi-Cyclic) - key generation

The key generation process in HQC involves selecting random elements from a cyclic polynomial ring. First, a polynomial h is randomly chosen from $\mathcal{R} = \mathbb{F}_2[X]/(X^n - 1)$. Then, two polynomials, x and y , are selected such that their Hamming weights are equal to the security parameter w . The public key is computed as the pair (h, s) , where $s = x + h \cdot y$, and the private key is (x, y) . This process ensures that the legitimate user has the required parameters for both encryption and decryption, while the structure of the public key maintains the security of the scheme.

Algorithm 7 The key-generation algorithm of the HQC KEM.

Input: The HQC security parameters (w)

Output: The private key $sk = (x, y)$ and the public key $pk = (h, s = x + h \cdot y)$

- 1: $h \xleftarrow{\$} \mathcal{R}$ $\triangleright \mathcal{R} = \mathbb{F}_2[X]/(X^n - 1) : \text{Cyclic polynomial ring}$
 - 2: $(x, y) \xleftarrow{\$} \mathcal{R}^2$ such that $w(x) = w(y) = w$
 - 3: Return the private key $sk = (x, y)$ and the public key $pk = (h, s = x + h \cdot y)$
-

In addition to the key generation, encapsulation and decapsulation algorithms, we will present the encryption and decryption algorithms that will be used in the encapsulation and decapsulation phases.

2.3.2 HQC - Encryption

During encryption, the sender generates random error and randomness vectors. Specifically, a random error vector e and randomness vectors $\mathbf{r}_1$ and $\mathbf{r}_2$ are chosen, where the Hamming weights of these vectors match the predefined security parameters. The ciphertext is then formed as two components, $\mathbf{u} = \mathbf{r}_1 + h \cdot \mathbf{r}_2$ and $\mathbf{v} = \mathbf{m} \cdot \mathbf{G} + \mathbf{s} \cdot \mathbf{r}_2 + \mathbf{e}$, where $\mathbf{m}$ is the encoded message. This process ensures that the legitimate recipient, who knows the private key, can correctly decrypt the message, while an attacker without the private key will struggle to do so.

Algorithm 8 The encryption algorithm of the HQC.

Input: The public key $pk, \mathbf{m}, w_e, w_r$

Output: The ciphertext c

- 1: generates $e \xleftarrow{\$} \mathcal{R}, \mathbf{r} = (\mathbf{r}_1, \mathbf{r}_2) \xleftarrow{\$} \mathcal{R}^2$ such that $w(e) = w_e, w(\mathbf{r}_1) = w(\mathbf{r}_2) = w_r$
 - 2: Sets $\mathbf{u} = \mathbf{r}_1 + h \cdot \mathbf{r}_2$ and $\mathbf{v} = \mathbf{m} \mathbf{G} + \mathbf{s} \cdot \mathbf{r}_2 + \mathbf{e}$
 - 3: Return the ciphertext $c = (\mathbf{u}, \mathbf{v})$
-

2.3.3 HQC - Decryption

The decryption process reverses the encryption operation using the private key (x, y) . The receiver computes the plaintext by subtracting the product of $\mathbf{u}$ and y from $\mathbf{v}$, followed by decoding the resulting value using the algorithm *C.Decode*. This allows the legitimate recipient to recover the original message $\mathbf{m}$ efficiently. The decoding algorithm ensures that even with the added noise, the message can be correctly recovered.

Algorithm 9 The decryption algorithm of the HQC.

Input: The ciphertext $(\mathbf{u}, \mathbf{v})$ and the private key $\text{sk} = (x, y)$

Output: The plaintext $\mathbf{m}$

- 1: Return the plaintext $\mathbf{m} = \text{C.Decode}(\mathbf{v} - \mathbf{u} \cdot y)$
-

2.3.4 HQC - encapsulation

Encapsulation in HQC follows a structure similar to other KEM schemes. The sender first generates a random message $\mathbf{m}$, which is then used to derive randomness θ through the hash function $\mathcal{G}$. The ciphertext c is generated by encrypting the message $\mathbf{m}$ using the derived randomness and the public key. Simultaneously, the shared key $\mathcal{K}$ is derived using the hash function $\mathcal{K}$, which takes the message and the ciphertext as inputs. To ensure the integrity of the message, a hash value $d = \mathcal{H}(\mathbf{m})$ is computed and returned alongside the ciphertext.

Algorithm 10 The encapsulation algorithm of the HQC KEM.

Input: The public key $\text{pk} = (h, s = x + h \cdot y)$

Output: The ciphertext (c, d) and shared key $\mathcal{K}$

- 1: Generate a random message $\mathbf{m} \in \mathbb{F}_2^k$
 - 2: Derive the randomness $\theta \leftarrow \mathcal{G}(\mathbf{m})$
 - 3: Generate the ciphertext $c = \text{Encrypt}(\text{pk}, \mathbf{m}, \theta)$ ▷ θ uses to generate $\mathbf{r}$ and e
 - 4: Derive the symmetric key $K \leftarrow \mathcal{K}(\mathbf{m}, c)$
 - 5: Let $d \leftarrow \mathcal{H}(\mathbf{m})$
 - 6: Return (c, d) and shared key $\mathcal{K}$
-

2.3.5 HQC - decapsulation

The decapsulation process mirrors the encapsulation in reverse. The recipient uses the private key to decrypt the ciphertext and recover the original message $\mathbf{m}'$. Using this message, the randomness θ' is recomputed, and a new ciphertext c' is generated. The recipient then checks the integrity of the ciphertext by comparing c' with the received ciphertext c and verifying the hash value d . If the integrity check passes, the shared key $\mathcal{K}$ is derived from the decrypted message and the ciphertext, completing the decapsulation process.

Algorithm 11 The decapsulation algorithm of the HQC KEM.

Input: (c, d) and the private key $sk = (x, y)$
Output: The Shared key $\mathcal{K}$

- 1: Decrypt $m' \leftarrow \text{Decrypt}(sk, c)$
 - 2: $\theta' \leftarrow \mathcal{G}(m')$
 - 3: $c' \leftarrow \text{Encrypt}(pk, m', \theta')$
 - 4: If $c \neq c'$ or $d \neq \mathcal{H}(m')$ then abort. Otherwise, derive the shared key $K \leftarrow \mathcal{K}(m, c)$
 - 5: Return the Shared key $\mathcal{K}$
-

2.4 Comparison of the three KEMs

KEM	Quantum Security	Key Sizes	Efficiency	Vulnerabilities
Classic McEliece	Very high	Very large	Slow	SCA, FIA, Algebraic Attack
BIKE	High	Medium	Fast	SCA, FIA
HQC	High	Medium	Balanced	SCA, FIA

Table 1: Comparison of Classic McEliece, BIKE , and HQC

3 Cryptanalysis of the different candidates

3.1 Cryptanalysis on Classic McEliece

In this section, we examine the key-recovery and message-recovery attacks on *Classic McEliece*, one of the most prominent candidates in the field of code-based post-quantum cryptography. Over the years, various side-channel attacks have been developed, targeting both the decapsulation and key generation phases of this cryptosystem. These attacks highlight the ongoing challenges of ensuring the security of McEliece-based systems in real-world implementations.

3.1.1 Key-recovery

Several key-recovery side-channel attacks have been proposed, demonstrating the continuous evolution of cryptographic vulnerabilities and the sophisticated techniques used to exploit these weaknesses in *Classic McEliece*.

Guo et al. presented a highly impactful key-recovery side-channel attack focusing on the decapsulation step of *Classic McEliece* [9]. This attack is significant due to its ability to exploit the decapsulation of n invalid ciphertexts, where n represents the security parameter of *Classic McEliece*. By carefully observing the decapsulation process, attackers can deduce secret information, such as the private key. This attack emphasizes the necessity of implementing robust countermeasures, including the use of constant-time operations and secure memory management techniques, to prevent such vulnerabilities from being exploited.

Similarly, Seck et al. introduced a partial key-recovery attack during the decapsulation phase [5]. This attack focuses on recovering the private polynomial g by leveraging side-channel information while the polynomial's coefficients are loaded into the system. Although this attack does not fully recover the private key, it exposes critical weaknesses in how certain cryptographic operations are implemented, highlighting the potential for future improvements in the protection of side-channel information.

Expanding the scope of side-channel vulnerabilities, Brinkmann et al. described a key-recovery side-channel attack that occurs during the key generation process [24]. Their method relies on simulated leakages arising during Gaussian elimination, introducing a new class of vulnerabilities in *Classic McEliece*. This attack shows that not only the decapsulation process but also the key generation stage is susceptible to side-channel attacks, stressing the importance of securing all stages of the cryptographic pipeline.

In addition to these practical attacks, theoretical approaches have been explored by Kirshanova and May, who proposed algorithms for full key recovery assuming an attacker has access to "hints" partial information about the secret key [18]. While their work is theoretical, it underscores the potential vulnerabilities in McEliece-based cryptosystems if any secret information is leaked, reinforcing the need for careful design and secure implementation practices.

In summary, these studies illustrate the diverse range of key-recovery attacks that target different phases of the *Classic McEliece* cryptosystem. The complexity and effectiveness of these attacks highlight the importance of continuously developing countermeasures to protect against both classical and quantum threats.

Table 2: Comparison of key-recovery attacks on the *Classic McEliece* KEM.

Article	Step (Algorithm)	Scenario	Attack Type	Implementation and Hardware
[24]	Gaussian Elimination (KeyGen)	1 trace	Side-channel (sim.) Full key recovery	Ref. & Botan N/A
[9]	FFT $\sigma(x)$ (Decaps.)	n traces $\text{wt}(e) = 1$	Side-channel Full key recovery	Ref. & optimized FPGA & ARM
[5] (Decaps.)	load(g)	1 trace	Side-channel Partial key recovery	Optimized ARM
[12]	$\sigma(x)$ / Validation (Decaps.)	No CCA2 Faults in σ	Fault injection (sim.) Alternate key recovery	Reference RISC-V RTL

3.1.2 Message-recovery

Message-recovery side-channel attacks target the decryption process of cryptographic systems like *Classic McEliece*, often leveraging physical vulnerabilities to recover secret information. These attacks are particularly concerning as they can recover entire messages without directly attacking the private key.

Lahr et al. demonstrated a notable message-recovery attack that enhances the syndrome by adding random columns from the parity-check matrix [10]. This enhanced syndrome is then used in a decoding oracle, where side-channel analysis is performed to detect changes in the weight of the input message. This method effectively reveals whether the bits corresponding to the modified columns are predominantly 0 or 1, allowing the attacker to recover the message efficiently. Additionally, the use of Information Set Decoding (ISD) further reduces the number of oracle calls needed, enhancing the attack's practicality.

Cayrel et al. expanded on this approach with a laser-induced fault injection attack during the encryption process [14]. By manipulating the instructions within the cryptographic operation, they converted an XOR operation into an ADD operation, causing the matrix-vector multiplication to be performed over $\mathbb{N}$ (the set of natural numbers) instead of $\mathbb{F}_2$ (the binary field). This alteration modified the syndrome decoding problem and allowed for message recovery within minutes, demonstrating the practical feasibility of such attacks.

Another approach described by Danner et al. [44] proposes a framework for fault injection attacks that specifically targets the secret key, rather than the message. This attack, although theoretical, highlights how fault injection techniques can be extended to compromise the cryptographic key itself, revealing vulnerabilities in the protection of private key material during decryption.

Xagawa et al. presented a generic attack on the Fujisaki-Okamoto transformation, widely used in various post-quantum cryptographic schemes [56]. This attack exploits an instruction-skipping vulnerability during decapsulation, allowing the attacker to recover the message with a single fault. The attack's effectiveness was experimentally demonstrated, but it has not yet been applied to *Classic McEliece*, making it a future research avenue for potential vulnerabilities.

Finally, the concept of augmenting the Syndrome Decoding Problem (SDP) with additional information obtained through physical attacks has been further explored [73]. The introduction of the Integer Syndrome Decoding Problem (IN-SDP) [68], and the use of integer linear programming techniques, represents a promising new approach to solving SDP-based cryptosystems. However, while this method significantly reduces the problem's complexity, it still faces challenges related to error tolerance and physical attack repeatability, limiting its practical applicability.

Table 3: Comparison of message-recovery attacks on the *Classic McEliece* KEM.

Article	Step (Algorithm)	Scenario	Attack Type	Implem. and Hardware
[14]	Compute Syndrome (Encrypt)	1 trace	Laser fault / ILP Full message recovery	ARM Cortex-M3 core
[10]	Modified syndrome (Decrypt)	$\leq k$ traces Iterative Chunking	Side-channel / ISD Full message recovery	FPGA implementation EM side channel
[44]	d -th coefficient of $\sigma_p(x)$ (Decrypt)	Fault injection ($d = 0$ and $d = 2$)	Fault Injection Alternate key recovery	FPGA implementation CoCoA-5

3.1.3 Countermeasures

To address countermeasures against cryptanalytic attacks on the *Classic McEliece* scheme, it is essential to introduce protective techniques while highlighting their relevance in the context of past attacks. Although the scheme has proven robust against classical attacks, particularly due to the difficulty of decoding linear codes, recent attack vectors require new strategies.

The first set of countermeasures targets side-channel attacks, which exploit information leakage during the decoding process. The use of hardware countermeasures, such as adding noise to critical operations, or software techniques like masking, helps limit these leaks. Masking transforms sensitive data into protected data using random operations, so that an attacker cannot extract any useful information.

Another threat comes from algebraic and structural attacks, which aim to exploit the particular structure of the Goppa codes used in *Classic McEliece*. To counter these attacks, several researchers have proposed masking the schemes internal parameters, notably by using generator or parity-check matrices that do not reveal information about the code structure. This significantly complicates the attacker's task in identifying algebraic vulnerabilities.

Furthermore, performance optimizations, especially through specific hardware implementations, must be accompanied by precautions to prevent timing attacks. Here, the objective is to ensure that sensitive operations, such as error decoding, are performed in constant time to prevent the observation of exploitable timing variations.

Finally, recent countermeasure proposals include diversifying the scheme instances, such as using

alternative code families or introducing random perturbations in the public key. These strategies aim to make structural cryptanalysis, specific to Goppa codes, more challenging.

In conclusion, while Classic McEliece has withstood numerous theoretical and practical attacks, these countermeasures reinforce security against evolving cryptanalytic techniques. The effectiveness of these protection techniques depends on their proper implementation, and it is crucial to remain vigilant about emerging vulnerabilities, particularly in the context of quantum computing.

3.2 Cryptanalysis on BIKE

The Bit Flipping Key Encapsulation (BIKE) mechanism is an important candidate in the field of post-quantum cryptography, designed to provide secure key encapsulation in quantum-resistant environments. Despite its theoretical robustness, BIKE has been shown to exhibit practical vulnerabilities, particularly through key-recovery and message-recovery attacks that exploit decryption failures, timing leaks, and side-channel information.

3.2.1 Key-recovery

Key-recovery attacks against BIKE have highlighted critical weaknesses in its decryption mechanisms, particularly those involving rejection-sampling routines and timing information leaks. These vulnerabilities expose the system to significant risks, enabling attackers to recover the private key in certain scenarios.

In [77], a significant vulnerability is identified in the rejection-sampling routines used during BIKE's decapsulation. These routines, which rely on secret-dependent information, can inadvertently leak timing data, allowing an attacker to determine whether the decoding step in BIKE was successful. By analyzing the timing differences, the authors were able to infer critical information about the secret keys distance spectrum, leading to a key-recovery attack using approximately 5.8×10^7 oracle queries. This underscores the importance of implementing robust countermeasures to protect sampling routines from timing analysis.

Another notable key-recovery attack, combining power analysis with information set decoding (ISD), is described in [74]. This attack targets the decapsulation process of BIKE and leverages power consumption traces. By analyzing a single trace of power consumption, the authors were able to recover the complete private key. The attack exploits the manipulation of coordinates in the private key and uses clustering techniques to extract partial information, which is then expanded using ISD to recover the full key. Both C and assembly implementations of BIKE were found to be vulnerable to this attack. For the C version, the complete key is recoverable, while for the assembly version, a large proportion of the keys could still be retrieved.

Further attacks exploiting decryption failures in QC-MDPC (Quasi-Cyclic Moderate Density Parity-Check) schemes are presented in [78]. The authors demonstrate that these failures can reveal whether a target's secret key satisfies a specific property known as "gathering." This information is used to perform a modified decoding algorithm that recovers the secret key. For BIKE with 128-bit security parameters, the complexity of the attack is estimated to be $2^{116.61}$ when ciphertext reuse is not allowed, and it decreases to $2^{98.77}$ when reuse is permitted. This illustrates how decryption failures, particularly in QC-MDPC-based schemes, can significantly weaken security under specific conditions.

In conclusion, these key-recovery attacks reveal the practical limitations of BIKE despite its theoretical strength. To mitigate these vulnerabilities, it is crucial to implement robust countermeasures that minimize information leakage and protect the decryption process from timing, power, and side-channel analysis.

Table 4: Comparison of key-recovery attacks on the BIKE KEM.

Article	Step (Algorithm)	Scenario	Attack Type	Impl. and Hardware
[77]	Compute $H(m')$ (Decapsulation)	5.8×10^7 queries	Side-channel (sim.) Full key recovery	BIKE-L1, Intel x86
[74]	Decoder (c_0, h_0, h_1) (Decapsulation)	1 trace	Power analysis / ISD Full key recovery	Optimized, ARM Cortex-M4
[78]	Decoder (c_0, h_0, h_1) (Decapsulation)	Decryption failure	Side-channel Full key recovery	N/A

3.2.2 Message-recovery

Message-recovery attacks exploit both algorithmic and hardware vulnerabilities in BIKE, typically through side-channel techniques such as timing analysis. These attacks target the cryptographic systems ability to reveal partial or complete messages during the decryption process.

One such attack targets a vulnerability introduced by the weight verification step in recent implementations of BIKE, including those found in the liboqs library and the new GitHub implementation. The study [77] describes a timing attack that exploits variations in execution time caused by the rejection-sampling process. In this modified version of BIKE, an additional weight check is performed after the decoding function is called. If the returned error vectors weight does not match the expected value, a random value is assigned. Although this step was introduced to improve security, it inadvertently introduced a new side-channel vulnerability. By repeatedly submitting the same ciphertext and measuring the timing differences in the weight check, attackers can determine whether the weight was correctly verified or not.

This timing attack allows attackers to construct a distinguishing tool that forms the basis of a message-recovery attack. The process involves flipping certain bits in the ciphertext and observing their impact on the weight verification. This information, combined with iterative decoding techniques like ISD, enables the attacker to reconstruct the original message with a high probability of success. Although millions of oracle queries may be required, this attack remains computationally less complex than traditional key-recovery attacks.

Optimizations in BIKE implementations have been proposed to reduce the risk of such attacks. These include binding the public key to the message during encapsulation to mitigate certain forms of manipulation, as well as adjusting encryption parameters to make it more difficult for attackers to exploit these vulnerabilities. However, as highlighted by [77], even countermeasures aimed at improving security can unintentionally introduce new weaknesses, underscoring the need for a holistic approach to cryptographic security.

Table 5: Message-recovery attack on the BIKE KEM.

Article	Step (Algorithm)	Scenario	Attack Type	Impl. and Hardware
[77]	Weight verification (Decapsulation)	Timing variations	Timing attack Message recovery	BIKE-L1, GitHub implementation

In conclusion, these results demonstrate that even with additional security measures, BIKE is still susceptible to message-recovery attacks. A comprehensive approach addressing both hardware vulnerabilities and algorithmic weaknesses is essential to ensure the security of modern cryptographic systems, particularly in the face of side-channel threats.

3.2.3 Countermeasures

Despite the robustness of BIKE, several vulnerabilities have been identified, particularly concerning decoding failures, side-channel attacks, and fault injections. Addressing these challenges requires a combination of techniques to enhance security and resilience.

One primary concern is decoding failures. BIKE's reliance on bit-flipping algorithms for decoding makes it vulnerable when the number of errors approaches the algorithm's correction capacity. When decoding fails, it may inadvertently leak information about the private key. To mitigate this risk, it is possible introducing randomness into the decoding process. By randomizing certain steps, the decoding behavior becomes less predictable, making it harder for attackers to exploit failure patterns. Additionally, improvements to the bit-flipping algorithm, such as incorporating adaptive flipping or increasing the number of decoding rounds, can further enhance error tolerance without significantly impacting performance.

Another significant area of vulnerability is side-channel attacks, where an attacker leverages physical signals, such as timing or power consumption, to gather information about the private key. BIKes iterative and data-dependent decoding can expose it to these attacks. A key countermeasure here is the use of constant-time implementations, ensuring that operations like syndrome computation and bit-flipping decoding are executed with no variation in time, thus preventing attackers from deducing sensitive information based on timing discrepancies. Furthermore, masking techniques, which involve randomizing intermediate values during computations, can be employed to reduce leakage. By masking key-dependent operations, such as bit-flipping, BIKE can defend against power analysis attacks by obscuring the values an attacker might observe.

In addition to side-channel vulnerabilities, fault injection attacks pose a significant risk. These attacks involve deliberately introducing faults into the system to expose sensitive information. BIKes error-correction mechanisms are particularly susceptible to this form of attack. To counter this, it is important to introduce redundant checks during the decoding process. Verifying the decoded message multiple times before using it ensures that malicious faults are detected and mitigated. Another effective approach involves incorporating error-detection mechanisms, such as checksums, to identify and handle injected faults. If discrepancies are detected, the decryption process can abort, preventing the leakage of critical information.

Though BIKE is designed to resist quantum attacks, the evolving nature of quantum cryptanalysis, including attacks leveraging Grover's algorithm, still presents a potential threat. Strengthening resistance to quantum-based attacks can be achieved by adjusting the key size and parameters used in BIKE. Larger keys provide greater protection against quantum search algorithms by making brute-force attacks less feasible. Additionally, the use of hybrid schemes, which combine BIKE with other quantum-resistant KEMs, can further bolster security. This hybrid approach ensures that even if one scheme becomes vulnerable, the other can still provide protection.

Finally, additional considerations include regularly analyzing and hardening BIKes parameters to keep up with evolving cryptanalytic techniques. This involves adjusting code lengths and bit-flipping thresholds in response to new attacks, ensuring that BIKE remains secure in the face of emerging threats. Equally important is ensuring that BIKE is implemented in secure environments. Protecting the hardware and using robust random number generators can mitigate many attack vectors that rely on exploiting weaknesses in implementation rather than the cryptographic scheme itself.

3.3 Cryptanalysis on HQC

The Hamming Quasi-Cyclic (HQC) Key Encapsulation Mechanism (KEM) is a post-quantum cryptographic scheme known for its theoretical robustness. However, key-recovery and message-recovery attacks have exposed significant vulnerabilities in its practical implementations. These attacks ex-

exploit flaws in how HQC handles decoding operations, timing information, and side-channel leakage, underscoring the importance of securing both the algorithm and the hardware implementations.

3.3.1 Key-recovery

Key-recovery attacks on HQC have highlighted critical weaknesses in its decoding process and side-channel resistance, especially when implemented on hardware platforms like microcontrollers. Below, we explore several key-recovery attacks that reveal the practical vulnerabilities of this cryptosystem.

The first key-recovery attack, described in [75], exploits timing variations during the BCH decoding step in HQC. The authors observed a correlation between the weight of the error vector and the time taken to decode using BCH codes. By exploiting this timing side-channel, attackers can infer information about the secret key with a high degree of accuracy. The attack requires 5441 decoding queries and has a success probability of 93%, making it highly efficient. This demonstrates the need for implementing constant-time operations in cryptographic routines to mitigate timing-based side channels.

In [76], a power side-channel attack is presented, marking the first such attack on HQC. The authors created an oracle using power consumption traces, which allowed them to determine whether an error was corrected during BCH decoding. Using a pattern matching approach based on the sum of squared differences, the attack requires fewer than 10000 measurements to recover most of the secret key. This attack highlights the vulnerability of HQC when implemented on embedded devices like microcontrollers, where power analysis can be used to extract sensitive information.

A third key-recovery attack is discussed in [77]. This attack exploits timing leaks during deterministic re-encryption in the decapsulation process. The rejection-sampling mechanism used in HQC leads to timing variations that can be observed by an attacker, allowing for the recovery of the secret key after around 866000 queries. Despite the high number of queries, this attack demonstrates that even advanced security mechanisms like deterministic re-encryption are not immune to timing biases, making it critical to address these issues in future implementations.

In summary, while HQC provides strong theoretical security, these key-recovery attacks reveal significant practical challenges. Effective countermeasures, such as constant-time implementations, masking techniques, and protection against power side-channel attacks, are crucial to securing HQC in real-world environments.

Table 6: Comparison of key-recovery attacks on the HQC KEM.

Article	Step (Algorithm)	Scenario	Attack Type	Impl. and Hardware
[75]	C.Decode($\mathbf{v} - \mathbf{u} \cdot \mathbf{y}$) (Decryption)	$\mathcal{O}(n^{5/2})$	Timing attack Full key recovery	Optimized impl.
[76]	C.Decode($\mathbf{v} - \mathbf{u} \cdot \mathbf{y}$) (Decryption)	< 10000 measurements	Power side-channel Full key recovery	ARM Cortex-M4
[77]	Encrypt(pk, m', θ') (Decapsulation)	Around 866000 queries	Timing attack Full key recovery	Ref. impl.

3.3.2 Message-recovery

Message-recovery attacks exploit the vulnerabilities in the HQC decoding process, specifically targeting weaknesses in the RS (Reed-Solomon) decoder. These attacks often rely on side-channel informa-

tion, such as the Hamming Weight (HW) leakage model, which can reveal the contents of exchanged messages during the decapsulation phase.

In [83], the authors present the first horizontal Access Correlation Side-channel (ACS) attack against the HQC RMRS KEM. This attack targets the RS decoder and uses the HW leakage model to infer the message being exchanged. During the decapsulation process, each byte of the codeword is manipulated multiple times, allowing correlation analysis to be performed on the side-channel data. By analyzing the correlation between the manipulated bytes and their Hamming weights, the attacker can infer the message contents.

A key advantage for the attacker in this scenario is that the HQC decoder is public and can be used to correct erroneous side-channel inferences. While the decoder has limited error correction capability, the authors enhance the attack by using more sophisticated RS decoders, which improve the success rate of message recovery. The attack is first simulated using controlled noise to analyze the impact of signal-to-noise ratio (SNR) on the attack's success. The results from simulated traces are then compared with practical results, showing that a real-world attack is feasible with fewer than 296 Galois field operations.

In conclusion, this message-recovery attack highlights the importance of securing side-channel leakages, especially in decoding routines. Implementing noise-resilient decoders and incorporating hardware countermeasures, such as obfuscation techniques, can significantly reduce the risk of successful message-recovery attacks.

Table 7: Message-recovery attack on the HQC KEM.

Article	Step (Algorithm)	Scenario	Attack Type	Impl. and Hardware
[83]	RS decoding (Decapsulation)	Hamming Weight (HW)	ACS attack Message recovery	Simulated traces and practical impl.

3.3.3 Countermeasures

While HQC is theoretically strong, offering resistance to quantum attacks and leveraging hard decoding problems, practical implementations of the scheme remain vulnerable to various types of attacks. Key recovery and message recovery attacks, which target the weaknesses in the implementation rather than the cryptographic structure itself, are significant concerns. To ensure optimal security, appropriate countermeasures must be applied, especially focusing on side-channel attacks and decoding vulnerabilities.

Side-channel attacks, which exploit leaks such as execution time or power consumption during the decoding process, pose a major threat to HQC. To mitigate these attacks, special attention must be paid to the design of the decoding algorithms. It is advisable to implement constant-time algorithms, ensuring that the execution time remains consistent, regardless of the data being processed. This approach greatly reduces the amount of exploitable information available to an attacker. Moreover, masking techniques can be employed to minimize information leaks related to power consumption or electrical fluctuations. By masking intermediate calculations during decoding, these techniques make side-channel analyses significantly more complex for the attacker.

Fault injection attacks, where deliberate errors are introduced into the system to reveal information about the private key, are another type of threat that must be addressed. To counter these attacks, HQC implementations should incorporate fault detection mechanisms, such as consistency checks during decoding. For instance, redundancy checks on the decoded messages can help identify malicious alterations and respond accordingly, either by resetting the decryption process or by halting execution to prevent information leakage.

In addition to these measures, it is crucial to design hardware-level countermeasures. Side-channel attacks based on timing and power consumption, such as power analysis or electromagnetic fluctuation analysis, can be mitigated with hardware protections. For example, adding random noise to power consumption, or using dedicated circuits designed to obscure cryptographic operations, can significantly hinder the exploitation of these channels by attackers.

Finally, HQCs security also depends on the proper implementation of its decoding algorithms. Poorly designed decoding algorithms can introduce vulnerabilities that allow attackers to exploit errors during the decoding process to recover sensitive information. Therefore, it is essential to continually assess and improve decoding techniques to minimize potential information leaks, particularly by adopting approaches that make decoding less predictable and more resistant to attacks.

In conclusion, while HQC offers robust theoretical security, its practical security depends heavily on the implementation of effective countermeasures. By combining secure decoding algorithms, hardware protections against side-channel attacks, and fault detection mechanisms, HQC can provide enhanced resistance to cryptanalyses, ensuring reliable security in post-quantum environments.

4 Discussion

4.1 Synthesis of Key Findings

This section provides a synthesis of the cryptanalysis results on three major code-based Key Encapsulation Mechanisms (KEMs): Classic McEliece, BIKE, and HQC. These candidates have been extensively analyzed for post-quantum cryptographic systems, and this synthesis highlights the key-recovery and message-recovery attacks reported in the literature.

4.1.1 Classic McEliece

1. Key-Recovery Attacks:

Several side-channel key-recovery attacks have been proposed against Classic McEliece, focusing on both decapsulation and key generation phases:

- [9] demonstrated a significant key-recovery attack by observing the decapsulation of invalid ciphertexts, exploiting vulnerabilities in the process.
- [5] introduced a partial key-recovery attack targeting side-channel leaks during the loading of private polynomial coefficients.
- [24] published an attack during the key generation phase, simulating leakage from Gaussian elimination.
- [18] proposed methods for full key recovery based on the presence of secret information "hints," although the practical feasibility of obtaining these hints remains uncertain.

2. Message-Recovery Attacks:

Message-recovery attacks against Classic McEliece exploit physical vulnerabilities during decryption:

- [10] leveraged syndrome enhancements combined with decoding oracle analysis to recover messages using Information Set Decoding (ISD).
- [14] described a fault injection attack modifying matrix-vector multiplication, allowing message recovery by altering decryption operations.
- [56] demonstrated a fault-based attack on the Fujisaki-Okamoto transformation, reducing the complexity of message recovery.

4.1.2 BIKE

1. Key-Recovery Attacks

BIKE is vulnerable to key-recovery attacks due to decryption failures and timing side-channels:

- [77] exploited timing information in rejection-sampling routines to reveal key information from the decapsulation process.
- [74] combined power analysis with ISD to recover the full private key, demonstrating BIKE's susceptibility to side-channel attacks.
- [78] presented attacks leveraging decryption failures to recover secret keys by analyzing error-handling mechanisms in BIKE's decoding process.

2. Message-Recovery Attacks

Message-recovery attacks on BIKE target both hardware and algorithmic weaknesses: Timing attacks on weight verification in BIKE's implementations enable attackers to infer message bits through time variation analysis [77].

4.1.3 HQC

1. Key-Recovery Attacks

Key-recovery attacks on HQC target timing and side-channel vulnerabilities:

- [75] demonstrated a timing attack exploiting correlations between error weight and execution time in BCH code decoding, recovering key information with high probability.
- [76] introduced a power side-channel attack that used power consumption during BCH decoding to efficiently extract secret key information.
- [77] revealed a timing leak in the rejection sampling routine during decapsulation, exposing HQC to key-recovery attacks.

2. Message-Recovery Attacks

Message-recovery attacks on HQC focus on hardware and algorithmic flaws: [83] presented the first horizontal ACS (Access Correlation Side-channel) attack on the HQC RMRS KEM, recovering message information via Hamming weight leakage during decapsulation.

Each of these KEMs presents distinct cryptographic challenges, with key-recovery and message-recovery attacks exploiting various aspects of their respective decapsulation, key generation, or decoding processes. These results emphasize the need for continued research into countermeasures that can mitigate side-channel vulnerabilities and protect against both software and hardware attacks.

4.2 Implications for Future Research

The cryptanalysis results on Classic McEliece, BIKE, and HQC reveal significant vulnerabilities in both theoretical and practical implementations. These findings open avenues for research aimed at strengthening the security of code-based Key Encapsulation Mechanisms (KEM) in the post-quantum era.

1. **Strengthening Resistance to Side-Channel Attacks:** side-channel attacks, such as key-recovery attacks on Classic McEliece [9] or power analysis attacks on HQC [76], demonstrate recurring vulnerabilities in code-based cryptographic schemes. These attacks exploit information leaks during decryption or key generation processes.

Future research must focus on developing and implementing effective countermeasures to mitigate these vulnerabilities, including:

- **Constant-time implementations:** to prevent leaks related to the execution of sensitive operations vulnerable to the attack proposed in [75].
- **Masking techniques:** designed to make sensitive information less accessible to physical and software-based attacks like in [76].
- **Operation obfuscation:** to obscure signals emitted during cryptographic processes, particularly on embedded devices vulnerable to side-channel attacks as with [77].

These measures could also be combined with hardware approaches to protect embedded and IoT devices.

2. **Improving Fault Injection Resilience:** fault injection attacks, such as those exposed in the work on Classic McEliece [14], reveal the ability of attackers to induce errors in computation to recover sensitive information. Future research should focus on:

- **Fault detection:** utilizing redundancy or error-correcting codes to identify and correct faults in real-time to protect systems against attacks like in [44].
- **Fault tolerance:** to protect cryptographic schemes from malicious disturbances during decryption and key generation operations as in [14].

These techniques would aim to make fault injection attacks significantly more complex and costly.

3. **Exploring New Decoding Algorithms:** Cryptanalysis of schemes such as Classic McEliece and BIKE show that current decoding algorithms are often the targets of attacks as in [10, 78]. Future research could explore:

- **Development of more resistant decoders:** to prevent attacks using timing or power consumption analysis such as in [75, 74].
- **Securing decapsulation processes:** specifically by enhancing the robustness of decoders against attacks combining side-channel and Information Set Decoding (ISD) like in [77].

This could include decoding algorithms that reduce leaks and minimize the impact of errors.

4. **Hybrid Approaches for Post-Quantum Security:** despite improvements, cryptanalysis reveals persistent vulnerabilities in code-based schemes. One potential solution lies in **hybrid schemes**, which combine code-based cryptography with other post-quantum techniques (such as lattice-based cryptography) to balance security and efficiency.

Hybrid approaches could address the weaknesses of individual schemes, providing enhanced security against various types of attacks like in [78].

5. **Formalizing Security Models:** the cryptanalysis results suggest that current security models, often based on theoretical assumptions, need to be expanded to include implementation vulnerabilities, such as those identified in side-channel or fault injection attacks [77, 14].

Future research must explore **extended security proofs** that account for these practical attacks, providing better assurance of the robustness of post-quantum schemes in real-world environments.

6. **Continuous Cryptanalysis of NIST Candidates:** ongoing cryptanalysis of candidates for the NIST standardization process, such as Classic McEliece, BIKE, and HQC, is crucial to ensure these schemes withstand new classical and post-quantum attacks. As demonstrated by the

vulnerabilities discovered in BIKE [77] and HQC [83], future research must focus on continuous improvement of these schemes before widespread adoption.

7. **New Directions in Attack Methodologies:** finally, attack methodologies are evolving rapidly, as evidenced by recent attacks combining power analysis and decoding techniques as in [74]. Future research should:

- **Develop new attack strategies:** targeting previously unexplored weaknesses in post-quantum schemes.
- **Leverage automation and machine learning:** to facilitate cryptanalysis, especially in the context of side-channel attacks like in [73].

These approaches will provide a deeper understanding of the limitations of current schemes and help design more resilient systems against emerging threats.

5 Conclusion

5.1 Summary of Key Points

In this survey, we have conducted a comprehensive examination of code-based key encapsulation mechanisms (KEMs), focusing on **Classic McEliece**, **BIKE**, and **HQC**, three of the most prominent candidates in the ongoing NIST post-quantum standardization process. We have highlighted the theoretical security of these systems, grounded in the hardness of coding theory problems such as the Syndrome Decoding Problem (SDP) and its variants, which are believed to be resistant to quantum attacks.

Despite their strong theoretical underpinnings, several cryptanalytic studies have shown that these systems remain vulnerable in practical implementations. In the case of Classic McEliece, key-recovery and message-recovery attacks have demonstrated that information leakage during key generation or decoding can potentially compromise the system's security [83, 5]. Similarly, BIKE has been shown to be vulnerable to attacks that exploit decryption failures and timing leaks during the rejection sampling process [78]. Finally, HQC is susceptible to side-channel attacks, particularly those that leverage power consumption and timing leaks [76, 75]. These vulnerabilities highlight the importance of carefully analyzing and securing both theoretical constructs and their practical implementations.

5.2 Importance and Practical Applications

As quantum computing continues to advance, the need for secure cryptographic systems that can withstand quantum attacks becomes increasingly urgent. Code-based cryptosystems, such as the ones discussed in this survey, are crucial candidates for ensuring the confidentiality, integrity, and authenticity of digital communications in the post-quantum era. Their resistance to attacks from quantum computers, especially those leveraging Shors and Grovers algorithms, makes them essential for securing sensitive sectors like finance, defense, healthcare, and critical infrastructure.

Moreover, the resilience of these cryptosystems against quantum threats ensures long-term protection for data requiring extended confidentiality, such as government secrets and private records. However, as current cryptanalytic results demonstrate, the practical implementation of these systems presents several challenges. **Practical attacks**, such as side-channel and fault-injection attacks, underscore the need for robust countermeasures and careful system design. This requires a coordinated effort from both academia and industry to ensure that cryptographic solutions not only hold up against theoretical attacks but also withstand real-world adversarial scenarios.

5.3 Suggestions for Researchers

The findings presented in this work suggest several promising avenues for future research aimed at improving the security and performance of code-based KEMs. Given the importance of these cryptosystems in the post-quantum world, the following research directions are proposed:

- **Development of Robust Countermeasures:** One of the primary areas of focus for future research should be the development of countermeasures that mitigate the risks posed by side-channel and fault-injection attacks. Techniques such as *timing masking*, *random noise injection*, and *fault detection and correction* have shown promise in protecting cryptosystems from such attacks. These countermeasures must be carefully integrated into implementations without significantly impacting performance.
- **In-depth Study of Key Generation:** The key generation phase has been identified as a critical point of vulnerability. Attacks targeting this phase, such as those described in [24], reveal that even small information leaks can compromise security. Therefore, it is essential to enhance the robustness of key generation algorithms through techniques that minimize leakage while maintaining computational efficiency. Additionally, the randomness and unpredictability of key generation should be further analyzed to ensure resilience against both classical and quantum attacks.
- **Optimizing Performance Without Compromising Security:** Balancing security and efficiency is a central challenge in post-quantum cryptography. For instance, the BIKE KEM [77] has been shown to be vulnerable to attacks that exploit rejection sampling mechanisms. Future research should aim to optimize the decapsulation and verification routines of such systems to reduce their susceptibility to timing leaks or decryption failures. This could involve exploring new algorithmic approaches that streamline performance without weakening the cryptosystems security.
- **Deepening Attack Methodologies:** Researchers should continue to investigate advanced cryptanalytic techniques that combine multiple attack vectors, such as power consumption analysis, electromagnetic emissions, and fault injection, with sophisticated decoding strategies. Attacks combining these vectors, as explored in studies on BIKE [74], can expose new vulnerabilities and help researchers better anticipate future threats. A deeper understanding of these multi-vector attacks will lead to the development of more robust cryptographic defenses.
- **Post-Quantum Security in Constrained Environments:** As many practical applications of cryptography involve resource-constrained devices such as IoT, embedded systems, and mobile platforms, research should focus on adapting post-quantum algorithms like McEliece, BIKE, and HQC for such environments. Efficient implementations, reduced key sizes, and hardware-based optimizations are essential for ensuring that code-based cryptosystems can be deployed on a wide scale without sacrificing security.

By addressing these challenges, the cryptographic community can help ensure that code-based cryptosystems remain secure and practical in the face of emerging threats. These research directions will not only enhance the resilience of current systems but also lay the groundwork for cryptographic solutions capable of withstanding the evolving landscape of quantum computing and cryptanalysis.

5.4 Final Thoughts

The transition to a post-quantum world will require a paradigm shift in how cryptographic systems are designed, implemented, and evaluated. Code-based cryptography, with its long history and

proven resilience against quantum threats, offers a promising path forward. However, as this survey has shown, theoretical security alone is not sufficient. Practical implementations must be fortified against a broad range of attack vectors, particularly in real-world scenarios where side-channel and fault-injection attacks pose significant risks.

In conclusion, while much progress has been made in the development of secure code-based KEMs, continued research and innovation are necessary to ensure their long-term viability. By focusing on both the theoretical and practical aspects of cryptographic security, we can build a future where digital communication remains secure in the face of rapidly advancing quantum technologies.

References

- [1] Elwyn R. Berlekamp, Robert J. McEliece and Henk C. A. van Tilborg, *On the inherent intractability of certain coding problems (Corresp.)*, Trans. Inf. Theory, 24(3) (1978), 384–386.
- [2] Sidelnikov, VM and Shestakov, SO, *On insecurity of cryptosystems based on generalized Reed-Solomon codes*, Discrete Math. Appl., 2(4) (1992), 439–444.
- [3] Wen Wang, Jakub Szefer and Ruben Niederhagen, *FPGA-Based Niederreiter Cryptosystem Using Binary Goppa Codes*, Post-Quantum Cryptography - 9th International Conference, PQCrypto 2018, Fort Lauderdale, FL, USA, April 9-11, (2018), 77–98.
- [4] Tanja Lange and Rainer Steinwandt, *Post-Quantum Cryptography - 9th International Conference, PQCrypto 2018, Fort Lauderdale, FL, USA, April 9-11, 2018, Proceedings*, Lecture Notes in Computer Science, 10786 (2018).
- [5] Nadia El Mrabet, Luca De Feo and Sylvain Duquesne, *Progress in Cryptology - AFRICACRYPT 2023 - 14th International Conference on Cryptology in Africa, Sousse, Tunisia, July 19-21, 2023, Proceedings*, Lecture Notes in Computer Science, 14064 (2023).
- [6] Brice Colombier, Vlad-Florin Dragoi, Pierre-Louis Cayrel and Vincent Grosso, *Profiled Side-Channel Attack on Cryptosystems Based on the Binary Syndrome Decoding Problem*, Trans. Inf. Forensics Secur., 17 (2022) 3407–3420.
- [7] Vincent Grosso Pierre-Louis Cayrel, Brice Colombier and Vlad-Florin Dragoi, *Punctured Syndrome Decoding Problem - Efficient Side-Channel Attacks Against Classic McEliece*, Constructive Side-Channel Analysis and Secure Design - 14th International Workshop, COSADE 2023, Munich, Germany, April 3-4, 2023, Proceedings (2023) 170–192.
- [8] Elif Bilge Kavun and Michael Pehl, *Constructive Side-Channel Analysis and Secure Design - 14th International Workshop, COSADE 2023, Munich, Germany, April 3-4, 2023, Proceedings*, Lecture Notes in Computer Science, 13979 (2023).
- [9] Qian Guo Andreas Johansson and Thomas Johansson, *A Key-Recovery Side-Channel Attack on Classic McEliece Implementations*, Trans. Cryptogr. Hardw. Embed. Syst., 2022(4) (2022) 800–827.
- [10] Norman Lahr and Ruben Niederhagen, Richard Petri and Simona Samardjiska, *Side Channel Information Set Decoding Using Iterative Chunking - Plaintext Recovery from the "Classic McEliece" Hardware Reference Implementation*, Advances in Cryptology - ASIACRYPT 2020 - 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7-11, 2020, Proceedings, Part I, (2020) 881–910.

- [11] Shiho Moriai and Huaxiong Wang, *Advances in Cryptology - ASIACRYPT 2020 - 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7-11, 2020, Proceedings, Part I*, Lecture Notes in Computer Science, 12491 (2020).
- [12] Sabine Pircher, Johannes Geier, Julian Danner, Daniel Mueller-Gritschneider and Antonia Wachter-Zeh, *Key-Recovery Fault Injection Attack on the Classic McEliece KEM*, Code-Based Cryptography - 10th International Workshop, CBCrypto 2022, Trondheim, Norway, May 29-30, 2022, Revised Selected Papers, (2022) 37–61.
- [13] Jean-Christophe Deneuville, *Code-Based Cryptography - 10th International Workshop, CBCrypto 2022, Trondheim, Norway, May 29-30, 2022, Revised Selected Papers*, Lecture Notes in Computer Science, 13839 (2023).
- [14] Pierre-Louis Cayrel, Brice Colombier, Vlad-Florin Dragoi, Alexandre Menu and Lilian Bossuet, *Message-Recovery Laser Fault Injection Attack on the Classic McEliece Cryptosystem*, Advances in Cryptology - EUROCRYPT 2021 - 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17-21, 2021, Proceedings, Part II, (2021) 438–467.
- [15] Sebastian Bitzer, Jeroen Delvaux, Elena Kirshanova, Sebastian Maan, Alexander May and Antonia Wachter-Zeh, *How to Lose Some Weight - A Practical Template Syndrome Decoding Attack*, Cryptology ePrint Archive, Paper 2024/621, (2024).
- [16] Sebastian Bitzer, Jeroen Delvaux, Elena Kirshanova, Sebastian Maan, Alexander May and Antonia Wachter-Zeh, *How to Lose Some Weight - A Practical Template Syndrome Decoding Attack*, Cryptology ePrint Archive, Paper 2024/621, (2024).
- [17] Anne Canteaut and François-Xavier Standaert, *Advances in Cryptology - EUROCRYPT 2021 - 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17-21, 2021, Proceedings, Part II*, Lecture Notes in Computer Science, 12697 (2021).
- [18] Elena Kirshanova and Alexander May, *Breaking Goppa-based McEliece with hints*, Inf. Comput., 293 (2023) 105045.
- [19] Yuanxing Li, Robert H. Deng and Xinmei Wang, *On the equivalence of McEliece's and Niederreiter's public-key cryptosystems*, Trans. Inf. Theory, 40(1) (1994) 271–273.
- [20] Colin O'Flynn and Zhizhang (David) Chen, *ChipWhisperer: An Open-Source Platform for Hardware Embedded Security Research*, Constructive Side-Channel Analysis and Secure Design - 5th International Workshop, COSADE 2014, Paris, France, April 13-15, 2014. Revised Selected Papers, (2014) 243–260.
- [21] Emmanuel Prouff, *Constructive Side-Channel Analysis and Secure Design - 5th International Workshop, COSADE 2014, Paris, France, April 13-15, 2014. Revised Selected Papers*, Lecture Notes in Computer Science, 8622 (2014).
- [22] Suresh Chari, Josyula R. Rao and Pankaj Rohatgi, *Template Attacks*, Cryptographic Hardware and Embedded Systems - CHES 2002, 4th International Workshop, Redwood Shores, CA, USA, August 13-15, 2002, Revised Papers, (2002) 13–28.
- [23] Burton S. Kaliski Jr., Çetin Kaya Koç and Christof Paar, *Cryptographic Hardware and Embedded Systems - CHES 2002, 4th International Workshop, Redwood Shores, CA, USA, August 13-15, 2002, Revised Papers*, Lecture Notes in Computer Science, 2523 (2003).

- [24] Marcus Brinkmann, Chitchanok Chuengsatiansup, Alexander May, Julian Nowakowski and Yuval Yarom, *Leaky McEliece: Secret Key Recovery From Highly Erroneous Side-Channel Information*, Cryptol. ePrint Arch., 1536 (2003).
- [25] Anna-Lena Horlemann, Sven Puchinger, Julian Renner, Thomas Schamberger and Antonia Wachter-Zeh, *Information-Set Decoding with Hints*, Code-Based Cryptography - 9th International Workshop, CBCrypto 2021, Munich, Germany, June 21-22, 2021 Revised Selected Papers, (2021) 60–83.
- [26] Antonia Wachter-Zeh, Hannes Bartz and Gianluigi Liva, *Code-Based Cryptography - 9th International Workshop, CBCrypto 2021, Munich, Germany, June 21-22, 2021 Revised Selected Papers*, Lecture Notes in Computer Science, 13150 (2022).
- [27] Eugene Prange, *The use of information sets in decoding cyclic codes*, Trans. Inf. Theory, 8(5) (1962) 5–9.
- [28] Jacques Stern, *A method for finding codewords of small weight*, Coding Theory and Applications, 3rd International Colloquium, Toulon, France, November 2-4, 1988, Proceedings, (1998) 106–113.
- [29] Gérard D. Cohen and Jacques Wolfmann, *Coding Theory and Applications, 3rd International Colloquium, Toulon, France, November 2-4, 1988, Proceedings*, Lecture Notes in Computer Science, 388 (1989).
- [30] Alexander Barg, *Complexity Issues in Coding Theory*, Electron. Colloquium Comput. Complex., TR97-046 (1997).
- [31] Goppa, Valerii Denisovich, *A new class of linear correcting codes*, Problemy Peredachi Informatsii, 6(3) (1970).
- [32] Bernstein, Daniel J., *Understanding binary-Goppa decoding*, IACR Communications in Cryptology, 1(1) (2024).
- [33] Patterson, N., *The algebraic decoding of Goppa codes*, IEEE Transactions on Information Theory, 21(2) (1975) 203-207.
- [34] Berlekamp, Elwyn R., *Algebraic Coding Theory - Revised Edition*, World Scientific Publishing Co., Inc., (2015).
- [35] James L. Massey, *Shift-register synthesis and BCH decoding*, IEEE Trans. Inf. Theory, 1969(15) (1969) 122–127.
- [36] Lothaire, M., *Algebraic Combinatorics on Words* Cambridge University Press (2002).
- [37] Matthias J. Kannwischer, Peter Schwabe, Douglas Stebila and Thom Wiggers, *Improving Software Quality in Cryptography Standardization Projects* IEEE European Symposium on Security and Privacy, EuroS&P 2022 - Workshops, Genoa, Italy, June 6-10, (2022) 19–30.
- [38] Sendrier, N., *Finding the permutation between equivalent linear codes: the support splitting algorithm* IEEE Transactions on Information Theory 46(4) (2000) 1193-1203.
- [39] Shivam Bhasin, Jean-Luc Danger, Sylvain Guilley and Zakaria Najm, *Side-channel leakage and trace compression using normalized inter-class variance* Hardware and Architectural Support for Security and Privacy, Minneapolis, MN, USA, June 15, 2014 46(4) 1–7.

- [40] Ruby B. Lee and Weidong Shi, *Hardware and Architectural Support for Security and Privacy*, Minneapolis, MN, USA, June 15, 2014, ACM (2014).
- [41] Minjoo Sim, Hyeokdong Kwon, Siwoo Eum, Gyeongju Song, Minwoo Lee and Hwajeong Seo, *Efficient Implementation of the Classic McEliece on ARMv8 Processors*, Information Security Applications - 24th International Conference, WISA 2023, Jeju Island, South Korea, August 23-25, 2023, Revised Selected Papers, 14402 (2023) 324–337.
- [42] Vastitas Kostalabros, Jordi Ribes-González, Oriol Farràs, Miquel Moretó and Carles Hernández, *HLS-Based HW/SW Co-Design of the Post-Quantum Classic McEliece Cryptosystem*, IEEE (2021) 52–59.
- [43] Shaofen Chen, Haiyan Lin, Wenjin Huang and Yihua Huang, *Hardware Design and Implementation of Classic McEliece Post-Quantum Cryptosystem Based on FPGA*, High Performance Extreme Computing Conference, HPEC 2022, Waltham, (2022) 1–6.
- [44] Julian Danner and Martin Kreuzer, *A fault attack on the Niederreiter cryptosystem using binary irreducible Goppa codes*, CoRR, abs/2002.01455 (2020).
- [45] Johannes Roth, Evangelos G. Karatsiolis and Juliane Krämer, *Classic McEliece Implementation with Low Memory Footprint*, Smart Card Research and Advanced Applications - 19th International Conference, CARDIS 2020, Virtual Event, November 18-19, 2020, Revised Selected Papers, Lecture Notes in Computer Science 12609 (2020) 34–49.
- [46] Mullen, Gary L. and Wan, Daqing and Wang, Qiang, *VALUE SETS OF POLYNOMIAL MAPS OVER FINITE FIELDS*, The Quarterly Journal of Mathematics, 64(4) (2012) 1191–1196.
- [47] Reed, I. S. and Solomon, G., *Polynomial Codes Over Certain Finite Fields*, Journal of the Society for Industrial and Applied Mathematics, 8(2) (1960) 300–304.
- [48] Stefan Heyse, Amir Moradi and Christof Paar, *Practical Power Analysis Attacks on Software Implementations of McEliece*, Third International Workshop on Post-Quantum Cryptography, 6061 (2010) 108–125.
- [49] Cong Chen, Thomas Eisenbarth, Ingo von Maurich and Rainer Steinwandt, *Horizontal and Vertical Side Channel Analysis of a McEliece Cryptosystem*, Transactions on Information Forensics and Security, 11(6) (2016) 1093–1105.
- [50] Roberto Avanzi, Simon Hoerder, Dan Page and Michael Tunstall, *Side-channel attacks on the McEliece and Niederreiter public-key cryptosystems*, Journal of Cryptographic Engineering, 1(4) (2011) 271–281.
- [51] H. Gregor Molter, Marc Stöttinger, Abdulhadi Shoufan and Falko Strenzke, *A simple power analysis attack on a McEliece cryptoprocessor*, Journal of Cryptographic Engineering, 1(1) (2011) 29–36.
- [52] Leif Both and Alexander May, *Decoding Linear Codes with High Error Rate and Its Impact for LPN Security*, Post-Quantum Cryptography - 9th International Conference, PQCrypto 2018, Fort Lauderdale, FL, USA, April 9-11, 2018, Proceedings, Lecture Notes in Computer Science, 10786 (2018) 25–46.
- [53] Léo Ducas, Andre Esser, Simona Etinski and Elena Kirshanova, *Asymptotics and Improvements of Sieving for Codes*, Advances in Cryptology - EUROCRYPT 2024 - 43rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zurich, Switzerland, May 26-30, 2024, Proceedings, Part VI, 14656 (2024) 151–180.

- [54] Anja Becker, Antoine Joux, Alexander May and Alexander Meurer, *Decoding Random Binary Linear Codes in $2^{n/20}$: How $1 + 1 = 0$ Improves Information Set Decoding*, Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings, Lecture Notes in Computer Science, 7237 (2012) 520–536.
- [55] Eliya Nachmani and Lior Wolf, *Autoregressive Belief Propagation for Decoding Block Codes*, CoRR, abs/2103.11780 (2021).
- [56] Keita Xagawa, Akira Ito, Rei Ueno, Junko Takahashi and Naofumi Homma, *Fault-Injection Attacks Against NIST's Post-Quantum Cryptography Round 3 KEM Candidates*, 13091 (2021) 33–61.
- [57] Andre Esser and Alexander May and Floyd Zweydinger, *McEliece needs a Break Solving McEliece-1284 and Quasi-Cyclic-2918 with Modern ISD*, Cryptology ePrint Archive, Report 2021/1634 (2021).
- [58] Daniel Augot and Matthieu Finiasz and Nicolas Sendrier, *Daniel Augot and Matthieu Finiasz and Nicolas Sendrier*, IACR Cryptol. ePrint Arch., 230 (2003).
- [59] Harald Niederreiter, *Knapsack-type cryptosystems and algebraic coding theory*, Problems of Control and Information Theory 15, (1986) 159–166.
- [60] Gaborit, Philippe, Lauradoux, Cedric and Sendrier, Nicolas, *SYND: a Fast Code-Based Stream Cipher with a Security Reduction*, Gaborit, Philippe and Lauradoux, Cedric and Sendrier, Nicolas, (2007) 186–190.
- [61] Jacques Stern, *A New Identification Scheme Based on Syndrome Decoding*, Advances in Cryptology - CRYPTO '93, 13th Annual International Cryptology Conference, Santa Barbara, California, USA, August 22-26, 1993, Proceedings, 773 (1993) 13–21.
- [62] Andre Esser, Alexander May and Floyd Zweydinger, *McEliece Needs a Break - Solving McEliece-1284 and Quasi-Cyclic-2918 with Modern ISD*, Lecture Notes in Computer Science, 13277 (2022) 433–457.
- [63] Esser, Andre, Bellini, Emanuele, Hanaoka, Goichiro, Shikata, Junji and Watanabe, Yohei, *Syndrome Decoding Estimator*, Public-Key Cryptography – PKC, (2022) 112–141.
- [64] Baldi, Marco and Barengi, Alessandro and Chiaraluce, Franco and Pelosi, Gerardo and Santini, Paolo, *A Finite Regime Analysis of Information Set Decoding Algorithms*, Algorithms, 12(10) (2019) 1999–4893.
- [65] Kirshanova, Elena and Laarhoven, Thijs, *Lower Bounds on Lattice Sieving and Information Set Decoding*, Springer-Verlag, (2021) 791–820.
- [66] Jeffrey S. Leon, *A probabilistic algorithm for computing minimum weights of large error-correcting codes*, Trans. Inf. Theory, 34(5) (1988) 1354–1359.
- [67] Donald E. Knuth, *The Art of Computer Programming, Volume II: Seminumerical Algorithms*, Addison-Wesley, (1969).
- [68] Vlad-Florin Dragoi, Pierre-Louis Cayrel, Brice Colombier, Dominic Bucerzan and Sorin Hoara, *Solving a Modified Syndrome Decoding Problem using Integer Programming*, International Journal of Computers Communications & Control, 15(5) (2020).

- [69] Robert Dorfman, *The Detection of Defective Members of Large Populations*, Annals of Mathematical Statistics, 14 (1943) 436–440.
- [70] Kangwook Lee, Kabir Chandrasekher, Ramtin Pedarsani and Kannan Ramchandran, *The Detection of Defective Members of Large Populations*, Transactions on Signal Processing, 67(17) (2019) 4649–4664.
- [71] Oliver Gebhard, Max Hahn-Klimroth, Dominik Kaaser and Philipp Loick, *Quantitative Group Testing in the Sublinear Regime*, arXiv. 1905.01458 (2019).
- [72] Leo Breiman, *Random Forests*, Machine Learning, 45(1) (2001) 5–32.
- [73] Anna-Lena Horlemann-Trautmann, Sven Puchinger, Julian Renner, Thomas Schamberger and Antonia Wachter-Zeh, *Information-Set Decoding with Hints*, Cryptology ePrint Archive, Report 2021/279 (2021).
- [74] Cheriére, Agathe, Aragon, Nicolas, Richmond, Tania and Gérard, Benoît, *BIKE Key-Recovery: Combining Power Consumption Analysis and Information-Set Decoding*, Applied Cryptography and Network Security, (2023) 725–748.
- [75] Guillaume Wafo-Tapa, Slim Bettaieb, Loic Bidoux, Philippe Gaborit and Etienne Marcatel, *A Practicable Timing Attack Against HQC and its Countermeasure*, Cryptology ePrint Archive, Paper 2019/909 (2019).
- [76] Thomas Schamberger, Julian Renner, Georg Sigl and Antonia Wachter-Zeh, *A Power Side-Channel Attack on the CCA2-Secure HQC KEM*, Cryptology ePrint Archive, Paper 2020/910 (2020).
- [77] Qian Guo, Clemens Hlauschek, Thomas Johansson, Norman Lahr, Alexander Nilsson and Robin Leander Schröder, *Don't Reject This: Key-Recovery Timing Attacks Due to Rejection-Sampling in HQC and BIKE*, Cryptology ePrint Archive, Paper 2021/1485 (2021).
- [78] Tianrui Wang, Anyu Wang and Xiaoyun Wang, *Exploring Decryption Failures of BIKE: New Class of Weak Keys and Key Recovery Attacks*, Cryptology ePrint Archive, Paper 2023/659 (2023).
- [79] Shor, Peter W., *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, SIAM Journal on Computing, 26(5) (1997) 1484–1509.
- [80] McEliece, R. J., *A Public-Key Cryptosystem Based On Algebraic Coding Theory*, Deep Space Network Progress Report, 44 (1978) 114–116.
- [81] Melchor, Carlos Aguilar, Aragon Nicolas, Bettaieb Slim, Bidoux Loic, Blazy Olivier, Deneuville Jean-Christophe, Gaborit Philippe, Persichetti Edoardo, Zémor Gilles and Bourges IC, *Hamming quasi-cyclic (HQC)*, NIST PQC Round, 2(4) (2018).
- [82] Aragon Nicolas, Barreto Paulo, Bettaieb Slim, Bidoux Loïc, Blazy Olivier, Deneuville Jean-Christophe, Gaborit Philippe, Ghosh Santosh, Gueron Shay, Güneysu Tim and others, *BIKE: bit flipping key encapsulation*, (2022).
- [83] Goy Guillaume, Loiseau Antoine and Gaborit Philippe, *Estimating the strength of horizontal correlation attacks in the hamming weight leakage model: A side-channel analysis on HQC KEM*, WCC 2022: The Twelfth International Workshop on Coding and Cryptography, (2022).

- [84] Colombier Brice, Dragoi Vlad-Florin, Cayrel Pierre-Louis and Grosso Vincent, *Message-recovery Profiled Side-channel Attack on the Classic McEliece Cryptosystem*, IACR Cryptol. ePrint Arch., 2022 (2022).
- [85] Colombier Brice, Grosso Vincent, Cayrel Pierre-Louis and Drăgoi Vlad-Florin, *Horizontal correlation attack on classic McEliece*, Cryptology ePrint Archive, (2023).
- [86] Goy Guillaume, Maillard Julien, Gaborit Philippe and Loiseau Antoine, *IACR Transactions on Cryptographic Hardware and Embedded Systems*, IACR Transactions on Cryptographic Hardware and Embedded Systems, 2 (2024) 64–87.
- [87] Martin R. Albrecht, Daniel J. Bernstein, Tung Chou, Carlos Cid, Jan Gilcher, Tanja Lange, Varun Maram, Ingo von Maurich, Rafael Misoczki, Ruben Niederhagen, Kenneth G. Paterson, Edoardo Persichetti, Christiane Peters, Peter Schwabe, Nicolas Sendrier, Jakub Szefer, Cen Jung Tjhai, Martin Tomlinson and Wen Wang, *Classic McEliece*, National Institute of Standards and Technology (2022).



ISSN: 2820-7114

Moroccan Journal of Algebra and Geometry with Applications

Supported by Sidi Mohamed Ben Abdellah University, Fez, Morocco

Volume 4, Issue 2 (2025), pp 138-151

Title :

On nonnil-u-S-coherent rings

Author(s):

Najib Mahdou and El Houssaine Oubouhou

On nonnil-u-S-coherent rings

Najib Mahdou¹ and El Houssaine Oubouhou²

¹Laboratory of Modelling and Mathematical Structures,
Department of Mathematics, Faculty of Science and Technology of Fez, Box 2202,
University S.M. Ben Abdellah Fez, Morocco.
e-mail: mahdou@hotmail.com

²Laboratory of Modelling and Mathematical Structures,
Department of Mathematics, Faculty of Science and Technology of Fez, Box 2202,
University S.M. Ben Abdellah Fez, Morocco.
e-mail: hossineoubouhou@gmail.com

Communicated by Mohamed Yousif

(Received 20 November 2024, Revised 25 December 2024, Accepted 01 January 2025)

Abstract. Let R be a commutative ring with identity. If the nilpotent radical $\text{Nil}(R)$ of R is a divided prime ideal, then R is called a ϕ -ring. Let R be a ϕ -ring and S be a multiplicative subset of R . In this paper, we introduce and study the notions of uniformly nonnil-S-coherent ring, which is “uniform” version of nonnil-S-coherent ring. We give the ideal-theoretic characterizations of uniformly nonnil-S-coherent rings. Besides, we characterize uniformly nonnil-S-coherent rings in terms of ϕ -u-S-flat modules and nonnil-u-S-injective modules. Finally, we obtain a strongly uniformly S-versions of the Chase Theorem and Matlis Theorem.

Key Words: nonnil-S-coherent ring, ϕ -S-coherent ring, S-coherent ring, nonnil-coherent ring, ϕ -S-flat module.

2020 MSC: Primary 13E99, 13A15.

Dedicated to our Professor David E. Dobbs for his 80th Birthday

1 Introduction

Throughout this paper, it is assumed that all rings are commutative with nonzero identity and all modules are unitary. If R is a ring, then we denote by $\text{Nil}(R)$ and $Z(R)$ the ideal of all nilpotent elements and the set of all zero-divisors of R respectively. A nonempty subset S of R is said to be a multiplicative subset if $1 \in S$ and for each $a, b \in S$ we have $ab \in S$. A prime ideal P of R is called *divided prime* if it is comparable to every ideal of R . Set $\mathcal{H} = \{R \mid R \text{ is a commutative ring and } \text{Nil}(R) \text{ is a divided prime ideal of } R\}$. If $R \in \mathcal{H}$, then R is called a ϕ -ring. Let R be a ϕ -ring with a total quotient ring T . As in [5], we define $\phi : T \longrightarrow K := R_{\text{Nil}(R)}$ such that $\phi(\frac{a}{b}) = \frac{a}{b}$ for each $a \in R$ and every $b \in R \setminus Z(R)$. Then ϕ is a ring homomorphism from T into K , and ϕ restricted to R is also a ring homomorphism from R into K given by $\phi(x) = \frac{x}{1}$ for every $x \in R$.

In [4], Bacem and Benhissi introduced two versions of coherent rings that are in the class $\mathcal{H}$. A ϕ -ring R is called *nonnil-coherent* if every finitely generated nonnil ideal of R is finitely presented and R is said to be ϕ -coherent if $\phi(R)$ is a nonnil-coherent ring. Among other things, they proved the Chase Theorem for nonnil-coherent rings using ϕ -flat modules. Next, the authors of [21] showed that any nonnil-coherent ring is ϕ -coherent, and they gave an example to show that the converse does not hold (see [21, Example 1.5]).

On the other hand, in [1], Anderson and Dumitrescu introduced the notion of S-Noetherian rings as a generalization of Noetherian rings; i.e., every ideal of R is S-finite. Recall from [1] that an

R -module M is said to be S -finite if there exists a finitely generated submodule F of M and $s \in S$ such that $sM \subseteq F$. However, the element $s \in S$ in the definition of S -Noetherian rings is not “uniform” in general. This situation make it difficult to study S -Noetherian rings via module-theoretic methods. To overcome this difficulty, the authors in [19] introduced the uniformly S -Noetherian (u - S -Noetherian for short) ring. A ring is said to be u - S -Noetherian if there exist an element $s \in S$ such that for any ideal I of R , $sI \subseteq K$ for some finitely generated subideal K of I . The u - S -Noetherian ring has been studied in [19] by using the trivial ring extension and the amalgamation of rings along an ideal, in addition to the Eakin-Nagata-Formanek theorem for u - S -Noetherian rings and the Cartan-Eilenberg-Bass theorem for u - S -Noetherian rings. In [13], Kwon and Lim introduced the notion of nonnil- S -Noetherian rings as a generalization of both nonnil-Noetherian rings and S -Noetherian rings. Let R be a ring and S be a multiplicative set of R . Then R is said to be a *nonnil- S -Noetherian* ring if each nonnil ideal of R is S -finite. The nonnil- S -Noetherian rings was studied in [13, 18] using the Cohen-type theorem, the flat extension, the faithfully flat extension, Eakin-Nagata-Formanek theorem, the polynomial ring extension, the power series ring extension and the amalgamated algebra.

In 2018, Bennis and El Hajoui [7] introduced S -finitely presented modules and S -coherent rings, which are S -versions of finitely presented modules and coherent rings. They also gave an S -version of Chase’s result to characterize S -coherent rings using ideals. After that, the authors of [20] investigate the open question: “How to give an S -version of flatness that characterizes S -coherent rings similarly to the classical case?”, and they proved that a ring R is an S -coherent ring, if and only if any product of flat R -modules is S -flat, if and only if, any product of R is S -flat (cf. [20, Theorem 4.4]), where an R -module M is called S -flat if $S^{-1}M$ is a flat $S^{-1}R$ -module. In [23] Zhang introduce and study the “uniform” version of S -coherent rings for extending uniformly S -Noetherian rings. In [17] Mahdou and Oubouhou introduced the notion of nonnil- S -coherent rings as a generalization of both nonnil-coherent rings and S -coherent rings. Let R be a ϕ -ring and S be a multiplicative set of R . Then R is said to be a *nonnil- S -coherent* ring if each nonnil ideal of R is S -finitely presented.

The main purpose of this paper is to integrate the concepts of nonnil-coherent rings and u - S -coherent rings. Then we construct a new class of rings that contains the class of nonnil-coherent rings. Let R be a ϕ -ring and S be a multiplicative subset of R . We define R to be a *nonnil- u - S -coherent* if there is $s \in S$ such that any finitely generated nonnil ideal of R is u - S -finitely presented with respect to s , and R is said to be a *ϕ - u - S -coherent* ring if $\phi(R)$ is a nonnil- u - $\phi(S)$ -coherent ring. Note that if S consists of units of R , then the concept of u - S -finitely presented modules is the same as that of finitely presented module; so if S consists of units of R , then the notion of nonnil- u - S -coherent (resp., ϕ - S -coherent) rings coincides with that of nonnil-coherent (resp., ϕ -coherent) rings. Furthermore, if R is a domain, then the concepts of nonnil- u - S -coherent and ϕ - u - S -coherent rings are precisely the same as that of u - S -coherent domains. Clearly, if $S_1 \subseteq S_2$ are multiplicative subsets, then any nonnil- u - S_1 -coherent ring (resp., ϕ - u - S_1 -coherent) is nonnil- u - S_2 -coherent (resp., ϕ - u - S -coherent); and if S^* is the saturation of S in R , then R is a nonnil- u - S -coherent (resp., ϕ - u - S -coherent) ring if and only if R is a nonnil- u - S^* -coherent (resp., ϕ - u - S^* -coherent) ring.

The organization of the paper is as follows: In Section 2, we introduce uniformly nonnil- S -coherent and ϕ - u - S -coherent rings. In particular, we study the ideal-theoretic characterizations of uniformly nonnil- S -coherent rings (see Theorem 2.1). Moreover we provide an example of nonnil- S -coherent rings and nonnil- c - S -coherent rings which are not nonnil- u - S -coherent (see Example 2.11). In Section 3, Strong version of Chase Theorem and Matlis Theorem for uniformly S -coherent rings are obtained (see Theorem 3.7 and Theorem 3.8). We continue to characterize nonnil- u - S -coherent rings in terms of nonnil- u - S -injective modules and ϕ - u - S -flat modules (see Theorem 3.5).

2 On nonnil- S -coherent rings

Recall from [7], that an R -module M is said to be S -finitely presented, if there exist an exact sequence of R -modules $0 \rightarrow K \rightarrow F \rightarrow M \rightarrow 0$, where K is S -finite and F is a finitely generated free R -module; equivalently there exist an exact sequence of R -modules $0 \rightarrow T_1 \rightarrow N \rightarrow M \rightarrow 0$ with N finitely presented and $sT_1 = 0$ for some $s \in S$. In [23] Zhang give the notion of uniformly S -finitely presented modules which generalize both S -finitely presented modules and c - S -finitely presented modules. Following [23, Definition 2.1] an R -module M is called u - S -finitely presented (abbreviates uniformly S -finitely presented) (with respect to s) provided that there is an exact sequence $0 \rightarrow T_1 \rightarrow F \rightarrow M \rightarrow T_2 \rightarrow 0$ with F finitely presented and $sT_1 = sT_2 = 0$; equivalently M is u - S -isomorphic to a finitely presented R -module.

The following theorem is a characterization of nonnil- u - S -coherent rings.

Theorem 2.1. Let R be a ϕ -ring and S be a multiplicative subset of R . Then the following assertions are equivalent:

1. R is nonnil- u - S -coherent;
2. There exist $s \in S$ such that $(I : b)$ is S -finite with respect to s for every non-nilpotent element $b \in R$ and any finitely generated ideal I of R ;
3. There exist $s \in S$ such that $(0 : a)$ is S -finite with respect to s for every non-nilpotent element $a \in R$, and the intersection of two finitely generated nonnil ideals of R is S -finite with respect to s .

Proof. (1) $\Rightarrow$ (2) Let I be a finitely generated ideal of R and b a non-nilpotent element in R . So $J = I + Rb$ is a finitely generated nonnil ideal of R , and so it is u - S -finitely presented with respect to s . Thus, there exist an exact sequence $0 \rightarrow K \rightarrow R^{n+1} \rightarrow J \rightarrow 0$, where K is S -finite with respect to s by [23, Theorem 2.2]. Following [15, Lemma 2.3.1], there exist a surjective homomorphism $g : K \rightarrow (I : b)$ which shows that $(I : b)$ is S -finite with respect to s .

(2) $\Rightarrow$ (1) Let I be a finitely generated nonnil ideal of R generated by $\{a_1, \dots, a_n\}$ where each a_i is non-nilpotent. We will show I is S -finitely presented with respect to s by induction on n . The case $n = 1$ follows from the exact sequence $0 \rightarrow (0 : a_1) \rightarrow R \rightarrow Ra_1 \rightarrow 0$ according to [23, Theorem 2.2(4)]. For $n > 1$; let $L = \langle a_1, \dots, a_{n-1} \rangle$ and consider the exact sequence

$$0 \rightarrow (L : a_n) \rightarrow R \rightarrow (Ra_n + L)/L \rightarrow 0.$$

Then $(Ra_n + L)/L = I/L$ is S -finitely presented by [23, Theorem 2.2(4)]. Again, consider the exact sequence $0 \rightarrow L \rightarrow I \rightarrow I/L \rightarrow 0$. Since L and I/L are S -finitely presented with respect to s , I is also S -finitely presented with respect to s by [23, Theorem 2.2 (2)].

(1) $\Rightarrow$ (3) Let a a non-nilpotent element in R , so Ra is S -finitely presented with respect to s . Consider the exact sequence $0 \rightarrow (0 : a) \rightarrow R \rightarrow aR \rightarrow 0$, so the ideal $(0 : a)$ is S -finite with respect to s by [23, Theorem 2.2(4)]. Now, let I and J be two finitely generated nonnil ideals of R . Since $\text{Nil}(R) \subseteq I \cap J \subseteq I + J$, $I + J$ is a finitely generated nonnil ideal, and so it is S -finitely presented with respect to s . Consider the following exact sequence

$$0 \rightarrow I \cap J \rightarrow I \oplus J \rightarrow I + J \rightarrow 0.$$

Since $I + J$ and $I \oplus J$ are S -finitely presented with respect to s according to [23, Theorem 2.2(3)], we get that $I \cap J$ is S -finite with respect to s by [23, Theorem 2.2(4)].

(3) $\Rightarrow$ (1) Let I be a finitely generated nonnil ideal of R . Write $I = Rx_1 + \dots + Rx_n$ with all $a_i \in R \setminus \text{Nil}(R)$, and we will prove the result by induction on n . For $n = 1$ we have $I = Rx_1$, since x_1

is non-nilpotent $(0, x_1)$ is S-finite. Hence I is S-finitely presented with respect to s . For $n > 1$, set $J = Rx_1 + \dots + Rx_{n-1}$ is a finitely generated nonnil ideal of R . Then we have the following exact sequence

$$0 \longrightarrow J \cap Rx_n \longrightarrow J \oplus Rx_n \longrightarrow I \longrightarrow 0.$$

Note that $J \oplus Rx_n$ is S-finitely presented with respect to s by [23, Theorem 2.2(3)]. On the other hand, since $J \cap Rx_n$ is the intersection of two finitely generated nonnil ideals of R , $J \cap Rx_n$ is S-finitely generated with respect to s . So I is S-finitely presented with respect to s according to [23, Theorem 2.2(4)]. $\square$

Let p be a prime ideal of R , an R -module M is (simply) u- p -finitely presented provided R is u- $(R \setminus p)$ -finitely presented. Following [23, Proposition 2.6], an R -module M is a finitely presented, if and only if, M is u- p -finitely presented for every $p \in \text{Spec}(R)$, if and only if, M is u- m -finitely presented for every $m \in \text{Max}(R)$.

Corollary 2.2. *Let R be a ϕ -ring. Then the following conditions are equivalent:*

1. R is a nonnil-coherent ring;
2. R is a nonnil-u- p -coherent ring for every prime ideals p of R ;
3. R is a nonnil-u- m -coherent ring for every maximal ideals m of R .

The following result gives us a criterion to u-S-finitely presented nonnil ideal.

Theorem 2.3. *Let R be a ϕ -ring, S a multiplicative subset of R and I an u-S-finitely presented nonnil ideal of R . Then $I/\text{Nil}(R)$ is a u- T -finitely presented nonzero ideal of $R/\text{Nil}(R)$ with $T = S + \text{Nil}(R)$.*

Proof. Let $0 \longrightarrow \text{Ker}(\pi_1) \xrightarrow{i_1} R^n \xrightarrow{\pi_1} I \longrightarrow 0$ be an exact sequence of R -modules with $\text{Ker}(\pi_1)$ is S-finite with respect to s . Since I is a finitely generated nonnil ideal of R , $I/\text{Nil}(R)$ is a finitely generated nonzero ideal of $R/\text{Nil}(R)$. Then there is an epimorphism $\pi_2 : (R/\text{Nil}(R))^n \longrightarrow I/\text{Nil}(R)$. Therefore,

$$0 \longrightarrow \text{Ker}(\pi_2) \xrightarrow{i_2} (R/\text{Nil}(R))^n \xrightarrow{\pi_2} I/\text{Nil}(R) \longrightarrow 0$$

is an exact sequence of $(R/\text{Nil}(R))$ -module. We can take as an exact sequence of R -modules with $(R/\text{Nil}(R))^n$ is finitely generated R -module. Consider the following commutative diagram:

$$\begin{array}{ccccccc} 0 & \xrightarrow{i_1} & \text{Ker}(\pi_1) & \longrightarrow & R^n & \xrightarrow{\pi_1} & I \longrightarrow 0 \\ & & \downarrow \alpha & & \downarrow \beta & & \downarrow \nu \\ 0 & \xrightarrow{i_2} & \text{Ker}(\pi_2) & \longrightarrow & (R/\text{Nil}(R))^n & \xrightarrow{\pi_2} & I/\text{Nil}(R) \longrightarrow 0 \end{array}$$

We have $\pi_1(\text{Nil}(R)^n) = \text{Nil}(R)$. Indeed, let $m' \in \text{Nil}(R)^n$, therefore, $\pi_2 \circ \beta(m') = 0 = \gamma \circ \pi_1(m')$. Then $\pi_1(m') \in \text{Ker}(\gamma) = \text{Nil}(R)$. Conversely, let $m \in \text{Nil}(R)$, and let $a \in I \setminus \text{Nil}(R)$, so $\text{Nil}(R) \subseteq Ra$. Therefore $m = ar$ with $r \in \text{Nil}(R)$ since $\text{Nil}(R)$ is a prime ideal of R . Thus $m = ar = r\pi_1(x) = \pi_1(rx) \in \pi_1(\text{Nil}(R)^n)$.

Our aim is to show that α is an epimorphism, therefore $\alpha(K_1) = \beta(K_1) = K_2$. For this, let $k \in \text{Ker}(\pi_1)$. Then $\nu \circ \pi_1(k) = 0 = \pi_2 \circ \beta(k)$ and hence $\beta(k) \in \text{Ker}(\pi_2)$. Conversely, let $k_2 = \beta(k) \in \text{Ker}(\pi_2)$. Then $\pi_2 \circ \beta(k) = 0 = \nu \circ \pi_1(k)$ and consequently $\pi_1(k) \in \text{Ker}(\gamma) = \text{Nil}(R) = \pi_1(\text{Nil}(R)^n)$. So there exist $j \in \text{Nil}(R)^n$ such that $\pi_1(k) = \pi_1(j)$. Then $k - j \in \text{Ker}(\pi_1) = K_1$. Hence $\beta(k) = \beta(k - j) + \beta(j) = \beta(k - j) \in \beta(K_1)$. Then α is an epimorphism, therefore, $\text{Ker}(\pi_2)$ is S-finite with respect to s . Hence, $I/\text{Nil}(R)$ is a u- T -finitely presented with respect to $s + \text{Nil}(R)$ nonzero ideal of $R/\text{Nil}(R)$ according to [23, Theorem

2.2(4)]. □

In light of Theorem 2.3, we give a new characterization of nonnil- u - S -coherent rings using the domain $R/\text{Nil}(R)$.

Theorem 2.4. Let R be a ϕ -ring and S a multiplicative subset of R . Then the following conditions are equivalent:

1. R is a nonnil- u - S -coherent ring;
2. $R/\text{Nil}(R)$ is a u - T -coherent domain with $T = S + \text{Nil}(R)$ and there exist $s \in S$ such that $(0 : r)$ is an S -finite ideal with respect to s for every non-nilpotent element $r \in R$.

Proof. Assume that R is nonnil- u - S -coherent ring, there exist $s \in S$ such that $(0 : r)$ is an S -finite ideal with respect to s for every non-nilpotent element $r \in R$ by Theorem 2.1. Now, let $I/\text{Nil}(R)$ be a finitely generated ideal of $R/\text{Nil}(R)$. So I is a finitely generated nonnil ideal of R . Since R is nonnil- u - S -coherent, we conclude that I is u - S -finitely presented with respect to s . Hence, by Theorem 2.3 $I/\text{Nil}(R)$ is u - T -finitely presented nonzero ideal of $R/\text{Nil}(R)$ with respect to $s + \text{Nil}(R)$. Therefore $R/\text{Nil}(R)$ is a u - T -coherent domain.

Conversely, let I and J be two finitely generated nonnil ideals of R , so $I/\text{Nil}(R)$ and $J/\text{Nil}(R)$ are finitely generated nonzero ideals of $R/\text{Nil}(R)$. Thus $(I \cap J)/\text{Nil}(R) = I/\text{Nil}(R) \cap J/\text{Nil}(R)$ is T -finite with respect to $s + \text{Nil}(R)$, therefore there exist a finitely generated nonnil ideal K of R such that $s(I \cap J)/\text{Nil}(R) \subseteq K/\text{Nil}(R) \subseteq I \cap J/\text{Nil}(R)$. Hence $s(I \cap J) \subseteq K \subseteq I \cap J$, so $I \cap J$ is S -finite with respect to s . Whence R is a nonnil- u - S -coherence according to Theorem 2.1. □

Corollary 2.5. Let R be a ϕ -ring with $Z(R) = \text{Nil}(R)$ and S be a multiplicative subset of R . Then R is a nonnil- u - S -coherent ring if and only if $R/\text{Nil}(R)$ is a u - T -coherent domain with $T = S + \text{Nil}(R)$.

Corollary 2.6. Let R be a ϕ -ring and S a multiplicative subset of R . Then R is a ϕ - u - S -coherent ring if and only if $\phi(R)/\text{Nil}(\phi(R))$ is u - S' -coherent domain, with $S' = \phi(S) + \text{Nil}(\phi(R))$.

Proof. Note that by definition R is a ϕ - u - S -coherent ring if and only if $\phi(R)$ is nonnil- u - $\phi(S)$ -coherent ring. Since $\phi(R)$ is a ϕ -ring with $\text{Nil}(\phi(R)) = Z(\phi(R))$ and, according to Corollary 2.5, we have the result. □

Recall from [6, Lemma 1.1] $R/\text{Nil}(R) \cong \phi(R)/\text{Nil}(\phi(R))$ for every ϕ -ring R . Then, we have the following corollary as a direct consequence of this result and the previous Theorem 2.4.

Corollary 2.7. Let R be a ϕ -ring and S a multiplicative subset of R , such that $(0 : r)$ is an S -finite ideal with respect to $s \in S$ for every non-nilpotent element $r \in R$. Then the following statements are equivalent:

1. R is a nonnil- u - S -coherent ring;
2. $R/\text{Nil}(R)$ is a u - T -coherent domain, with $T = S + \text{Nil}(R)$;
3. $\phi(R)/\text{Nil}(\phi(R))$ is an S' - u -coherent domain, with $S' = \phi(S) + \text{Nil}(\phi(R))$;
4. R is a ϕ - u - S -coherent ring.

Following [7, Definition 4.1] an R -module M is called c - S -finitely presented provided that there exist a finitely presented submodule N of M such that $sM \subseteq N \subseteq M$ for some $s \in S$. Trivially, an R -module M is called c - S -finitely presented if and only if there exist an exact sequence of R -modules $0 \rightarrow N \rightarrow M \rightarrow T_2 \rightarrow 0$ with N finitely presented and $sT_2 = 0$ for some $s \in S$. A ϕ -ring R is said to be nonnil- c - S -coherent provided that any finitely generated nonnil ideal is c - S -finitely presented. Recall from [17] that a ϕ -ring R is nonnil- S -coherent provided that any finitely generated nonnil ideal is S -finitely presented.

Proposition 2.8. *Let R be a ϕ -ring and S a multiplicative subset of R . If R is a nonnil- u - S -coherent ring, then R is both nonnil- S -coherent and nonnil- c - S -coherent.*

Proof. Let I be a finitely generated nonnil ideal and $0 \rightarrow K \rightarrow R^n \rightarrow I \rightarrow 0$ an exact sequence. Then K is S -finite by [19, Theorem 2.2(4)]. Thus I is S -finitely presented, and so R is nonnil- S -coherent. Consider the exact sequence $0 \rightarrow T_1 \rightarrow N \rightarrow I \rightarrow T_2 \rightarrow 0$ with N finitely presented and $sT_1 = sT_2 = 0$. Localizing at S we get

$$0 \rightarrow 0 = S^{-1}T_1 \rightarrow S^{-1}N \rightarrow S^{-1}I \rightarrow S^{-1}T_2 = 0 \rightarrow 0.$$

Hence $S^{-1}I \cong S^{-1}N$, since I is finitely generated, I is c - S -finitely presented according to [7, Proposition 4.3(2)]. $\square$

Proposition 2.9. *Let R be a ϕ -ring and S a multiplicative subset of R consisting of finite elements. Then the following statements are equivalent:*

1. R is a nonnil- u - S -coherent ring;
2. R is a nonnil- S -coherent ring;
3. R is a nonnil- c - S -coherent ring.

Proof. Suppose $S = \{s_1, \dots, s_n\}$ and set $s = s_1 \cdots s_n$.

(1) $\Rightarrow$ (2) and (1) $\Rightarrow$ (3) Follows from Proposition 2.8.

(2) $\Rightarrow$ (1) Let I be a finitely generated nonnil ideal of R . Then there is an exact sequence $0 \rightarrow K \rightarrow R^n \rightarrow I \rightarrow 0$ with K is S -finite. Let X be a submodule of K such that $s_i K \subseteq X$ for some $s_i \in S$, whence $sK/X = 0$. Then the exact sequence

$$0 \rightarrow K/X \rightarrow R^n/X \rightarrow I \rightarrow 0$$

makes I u - S -finitely presented with respect to s . So R is a nonnil- u - S -coherent ring.

(3) $\Rightarrow$ (1) Let I be a finitely generated nonnil ideal of R . Then there is a finitely presented sub-ideal J of R such that $s_i I \subseteq J = 0$. So $s(I/J) = 0$. Then the exact sequence $0 \rightarrow I \rightarrow J \rightarrow I/J \rightarrow 0$ makes I S -finitely presented with respect to s . So R is a nonnil- u - S -coherent ring. $\square$

Let R be a ring, M an R -module and S a multiplicative subset of R . For any $s \in S$, $S_s = \{1, s, s^2, \dots\}$ is a multiplicative subset of S . We denote by M_s the localization of M at S_s .

Proposition 2.10. *Let R be a ϕ -ring and S a multiplicative subset of R . If R is a nonnil- u - S -coherent ring with respect to some $s \in S$, then R_s is a nonnil-coherent ring.*

Proof. Assume that R is u - S -coherent ring with respect to $s \in S$. Let J be a finitely generated nonnil ideal of R_s . Since R is a ϕ -ring, $\text{Nil}(R)$ is a prime ideal of R . Hence $J \cong I_s$ for some finitely generated nonnil ideal I of R . Then there is an exact sequence $0 \rightarrow T_1 \rightarrow K \rightarrow I \rightarrow T_2 \rightarrow 0$ with K finitely presented and $sT_1 = sT_2 = 0$. Localizing at S_s , we have $(T_1)_s = (T_2)_s = 0$. So $J \cong I_s \cong K_s$ which is finitely presented over R_s . Thus R_s is a nonnil-coherent ring. $\square$

Let R be a ring, M be an R -module. Then $R \ltimes M$, the set of pairs (r, m) with component-by-component addition and multiplication defined by: $(r, m)(b, f) = (rb, rf + bm)$, is a unitary commutative ring, called the *trivial extension* (or *idealization*) of R by M . For a suitable background on the commutative trivial ring extensions, see [2]. Now we will give an example of a nonnil- S -coherent and nonnil- c - S -coherent ring which is not nonnil- u - S -coherent.

Example 2.11. Let D be a domain that is not a field, Q its quotient field. Let $R = D \ltimes Q$ be the trivial extension construction and $S = S_0 \ltimes 0$ with $S_0 = D^*$. Then R is a nonnil- S -coherent and nonnil- c - S -coherent ring which is not nonnil- u - S -coherent.

Proof. Let I be a finitely generated nonnil ideal of R . Suppose $r \in I \setminus \text{Nil}(R)$. Then we have $rI \subseteq Rr \subseteq I$. Since $r \notin \text{Nil}(R) = Z(R)$, $Rr \cong R$ is finitely presented, R is a nonnil- c - S -coherent ring. On the other hand Since $R/\text{Nil}(R)$ is not S_0 -coherent according to [23, Example 3.15], R is not nonnil- S -coherent by [17, Corollary 2.8]. Since $R/\text{Nil}(R)$ is not u - S_0 -coherent by [23, Example 3.15], R is not nonnil- u - S -coherent by Corollary 2.5. $\square$

3 Module-theoretic characterizations of u - S -coherent and nonnil- u - S -coherent rings

Since the rest of the paper involves uniformly torsion theory, we give a quick review (see [22] for more details). Recall from [22] that an R -module M is called a u - S -torsion module if there exist an element $s \in S$ such that $sM = 0$. An R -sequence $M \xrightarrow{f} N \xrightarrow{g} L$ is called u - S -exact (at N) if there is an element $s \in S$ such that $s\text{Ker}(g) \subseteq \text{Im}(f)$ and $s\text{Im}(f) \subseteq \text{Ker}(g)$. An R -homomorphism $f : M \rightarrow N$ is an S -monomorphism (resp., S -epimorphism, S -isomorphism) if $\text{Ker}(f)$ is u - S -torsion (resp., $\text{Coker}(f)$ is u - S -torsion, both $\text{Ker}(f)$ and $\text{Coker}(f)$ are u - S -torsion modules).

Let R be a ring and M an R -module. We denote by ψ_M the canonical homomorphism

$$\psi_M : M \bigotimes_R \prod R \rightarrow \prod \left(M \bigotimes_R R \right)$$

Lemma 3.1. Let M be an R -module. Then

1. If ψ_M is a u - S -epimorphism with respect to s , then M is S -finite with respect to s .
2. Moreover, if M is finitely generated and ψ_M is a u - S -isomorphism with respect to s , then M is u - S -finitely presented with respect to s .

Proof. (1) According to the proof of [23, Theorem 4.4].

(2) Let $0 \rightarrow K = \text{ker}(\pi_M) \rightarrow R^n \xrightarrow{\pi_M} M \rightarrow 0$ be an exact sequence. Consider the following commutative diagram of exact sequences:

$$\begin{array}{ccccccc} K \bigotimes \prod R & \longrightarrow & R^n \bigotimes \prod R & \longrightarrow & M \bigotimes \prod R & \longrightarrow & 0 \\ \psi_K \downarrow & & \cong \downarrow & & \psi_M \downarrow & & \\ 0 \longrightarrow & \prod (J \bigotimes R) & \longrightarrow & \prod (R \bigotimes R) & \longrightarrow & \prod (R/J \bigotimes R) & \longrightarrow 0. \end{array}$$

Since ψ_M is a u - S -isomorphism with respect to s , ψ_K is a u - S -epimorphism with respect to s . Hence M is S -finite with respect to s by (1). $\square$

Theorem 3.2. Let M be a finitely generated R -module. Then M is u - S -finitely presented with respect to s if and only if ψ_M is a u - S -isomorphism with respect to s .

Proof. The following exact sequence $0 \rightarrow A = \text{ker}(\pi_M) \rightarrow R^n \xrightarrow{\pi_M} M \rightarrow 0$ shows that A is S -finite with respect to s according [23, Theorem 2.2(4)]. So there exist a finitely generated submodule K of A such that $sA \subseteq K \subseteq A$. Consider the following commutative diagram:

$$\begin{array}{ccc}
K \otimes_R \prod_{i \in I} R & \xrightarrow{g} & A \otimes_R \prod_{i \in I} R \\
\psi_K \downarrow & & \psi_A \downarrow \\
\prod_{i \in I} (K \otimes_R R) & \xrightarrow{f} & \prod_{i \in I} (A \otimes_R R).
\end{array}$$

Since $sA \subseteq K$, f is a u - S -epimorphism with respect to s . As K is a finitely generated R -module, ψ_K is an epimorphism. Hence ψ_A is a u - S -epomorphism with respect to s . On the other hand, consider the following commutative diagram with exact arrow:

$$\begin{array}{ccccccc}
A \otimes \prod R & \longrightarrow & R^n \otimes \prod R & \longrightarrow & M \otimes \prod R & & \\
\psi_A \downarrow & & \cong \downarrow & & \psi_M \downarrow & & \\
\prod(A \otimes R) & \longrightarrow & \prod(R^n \otimes R) & \longrightarrow & \prod(M \otimes R) & \longrightarrow & 0.
\end{array}$$

Since ψ_A is a u - S -epimorphism with respect to s , we get ψ_M is a u - S -monomorphism with respect to s by [24] Theorem 1.3].

Conversely, consider the following exact sequence $0 \rightarrow A \rightarrow R^n \xrightarrow{\pi_M} M \rightarrow 0$, then there is a commutative diagram of exact sequences,

$$\begin{array}{ccc}
K \otimes_R \prod_{i \in I} R & \xrightarrow{g} & A \otimes_R \prod_{i \in I} R \\
\psi_K \downarrow & & \psi_A \downarrow \\
\prod_{i \in I} (K \otimes_R R) & \xrightarrow{f} & \prod_{i \in I} (A \otimes_R R).
\end{array}$$

Since ψ_M is a u - S -isomorphism with respect to s , ψ_K is a u - S -epimorphism with respect to s . Hence K is S -finite with respect to s according to Lemma 3.1(1). $\square$

Corollary 3.3. *Let R be a ring. Then R is u - S -coherent ring with respect to s if and only if ψ_I is u - S -isomorphism with respect to s for each finitely generated ideal I of R .*

Corollary 3.4. *Let R be a ϕ -ring. Then R is nonnil- u - S -coherent ring with respect to s if and only if ψ_I is u - S -isomorphism with respect to s for each finitely generated nonnil ideal I of R .*

Let R be a ring and M be an R -module. Set

$$\phi\text{-tor}(M) := \{x \in M \mid tx = 0 \text{ for some } t \in R \setminus \text{Nil}(R)\}.$$

If $\phi\text{-tor}(M) = M$, then M is called a ϕ -torsion module, and if $\phi\text{-tor}(M) = 0$, then M is called a ϕ -torsion-free module. Recall from [10] that an R -module F is ϕ - u - S -flat (abbreviates ϕ -uniformly S -flat) provided that for any u - S -exact sequence $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$ with C is ϕ -torsion, the induced sequence $0 \rightarrow A \otimes_R F \rightarrow B \otimes_R F \rightarrow C \otimes_R F \rightarrow 0$ is u - S -exact. An R -module M is ϕ - u - S -flat if and only if $\text{Tor}_1^R(M, F)$ is u - S -torsion for any ϕ -torsion R -module M if and only if there exist $s \in S$ satisfying that for any nonnil ideal I of R , $s \text{Tor}_1^R(R/I, F) = 0$ (see [10] Theorems 1 and 2]). In this case we say that M is ϕ - u - S -flat with respect to s .

Now, we are ready to give a “uniform” S -version of Chase Theorem for nonnil- u - S -coherent rings.

Theorem 3.5. (Chase Theorem for nonnil- u - S -coherent rings) Let R be a ϕ -ring and S a multiplicative subset of R . The following statements are equivalent:

1. R is a nonnil- u - S -coherent ring;

2. There exist an $s \in S$ such that every direct product of ϕ -u- S -flat R -modules with respect to s is ϕ -u- S -flat with respect to s^2 ;
3. There exist an $s \in S$ such that every direct product of R is ϕ -u- S -flat with respect to s .

Proof. (1) $\Rightarrow$ (2) Assume that R is a nonnil-u- S -coherent ring with respect to $s \in S$, let $\{F_i\}_{i \in I}$ be a family of ϕ -u- S -flat R -modules with respect to s and J be a finitely generated nonnil ideal of R . Then J is u- S -finitely presented with respect to s . The following exact sequence $0 \rightarrow A = \ker(\pi_J) \rightarrow R^n \xrightarrow{\pi_J} J \rightarrow 0$ shows that A is S -finite with respect to s according [23 Theorem 2.2(4)]. So there exist a finitely generated submodule K of A such that $sA \subseteq K \subseteq A$. Consider the following commutative diagram:

$$\begin{array}{ccc} K \otimes_R \prod_{i \in I} F_i & \xrightarrow{g} & A \otimes_R \prod_{i \in I} F_i \\ \nu \downarrow & & \beta \downarrow \\ \prod_{i \in I} (K \otimes_R F_i) & \xrightarrow{f} & \prod_{i \in I} (A \otimes_R F_i). \end{array}$$

Since $sA \subseteq K$, f is a u- S -epimorphism with respect to s . As K is a finitely generated R -module, ν is an epimorphism. Hence β is a u- S -epimorphism with respect to s . On the other hand, consider the following commutative diagram with exact arrow:

$$\begin{array}{ccccccc} A \otimes \prod_{i \in I} F_i & \longrightarrow & R^n \otimes \prod_{i \in I} F_i & \longrightarrow & J \otimes \prod_{i \in I} F_i & & \\ \beta \downarrow & & \cong \downarrow & & \alpha \downarrow & & \\ \prod_{i \in I} (A \otimes F_i) & \longrightarrow & \prod_{i \in I} (R^n \otimes F_i) & \longrightarrow & \prod_{i \in I} (J \otimes F_i) & \longrightarrow & 0. \end{array}$$

Since β is a u- S -epimorphism with respect to s , we get α is a u- S -monomorphism with respect to s by [24 Theorem 1.3]. Consider the following commutative diagram with exact arrow:

$$\begin{array}{ccccccc} 0 & \longrightarrow & \text{Tor}_1^R(R/J, \prod_{i \in I} F_i) & \longrightarrow & J \otimes \prod_{i \in I} F_i & \longrightarrow & R \otimes \prod_{i \in I} F_i \\ & & \downarrow & & \alpha \downarrow & & \cong \downarrow \\ & & \prod_{i \in I} \text{Tor}_1^R(R/J, F_i) & \longrightarrow & \prod_{i \in I} (J \otimes F_i) & \longrightarrow & \prod_{i \in I} (R \otimes F_i). \end{array}$$

Since all F_i are ϕ -u- S -flat R -modules with respect to s and J is a nonnil ideal of R , $s\text{Tor}_1^R(R/J, F_i) = 0$ for every $i \in I$. Hence $s\prod_{i \in I} \text{Tor}_1^R(R/J, F_i) = 0$. Therefore $s^2\text{Tor}_1^R(R/J, \prod_{i \in I} F_i) = 0$, consequently $\prod_{i \in I} F_i$ is ϕ -u- S -flat R -module with respect to s^2 .

(2) $\Rightarrow$ (3) Straightforward.

(3) $\Rightarrow$ (1) Let J be a nonnil ideal of R , the following exact sequence $0 \rightarrow J \rightarrow R \rightarrow R/J \rightarrow 0$ induce the following commutative diagram with exact arrow:

$$\begin{array}{ccccccc} J \otimes \prod R & \xrightarrow{f} & R \otimes \prod R & \longrightarrow & R/J \otimes \prod R & \longrightarrow & 0 \\ \beta \downarrow & & \cong \downarrow & & \cong \downarrow & & \\ 0 & \longrightarrow & \prod (J \otimes R) & \longrightarrow & \prod (R \otimes R) & \longrightarrow & \prod (R/J \otimes R) \longrightarrow 0. \end{array}$$

Since $\prod R$ is ϕ -u- S -flat module, then f is a u- S -monomorphism, so β is also a u- S -monomorphism with respect to s . Now consider the following exact sequence $0 \rightarrow A = \ker(i) \rightarrow R^n \xrightarrow{i} J \rightarrow 0$, then there is a commutative diagram of exact sequences:

$$\begin{array}{ccccccc}
A \otimes \prod R & \xrightarrow{f} & R^n \otimes \prod R & \longrightarrow & J \otimes \prod R & \longrightarrow & 0 \\
\alpha \downarrow & & \cong \downarrow & & \beta \downarrow & & \\
0 \longrightarrow & \prod(A \otimes R) & \longrightarrow & \prod(R^n \otimes R) & \longrightarrow & \prod(J \otimes R) & \longrightarrow 0.
\end{array}$$

Since β is a u - S -monomorphism with respect to s , α is a u - S -epimorphism with respect to s . Hence A is S -finite by [20, Lemma 4.1]. Therefore, I is S -finitely presented. $\square$

In [22], Zhang introduced the class of u - S -flat (abbreviates uniformly S -flat) modules F for which the functor $F \otimes_R -$ preserves u - S -exact sequences; equivalently $\text{Tor}_1^R(M, F)$ is u - S -torsion for any module M by [23, Theorem 3.2]. At this point, it is interesting to note that if $\text{Tor}_1^R(R/I, F)$ is u - S -torsion for any ideal I of R it does not necessarily apply that F is u - S -flat (see [22, Example 3.3]). Moreover, if S is composed of nonzero divisors, then F is u - S -flat if and only if there exist $s \in S$ satisfying that for every ideal I of R , $s\text{Tor}_1^R(R/I, F) = 0$ by [23, Proposition 4.3]. Without making the assumption that S has nonzero divisors, the following theorem shows that the above statement is true in the general case.

Proposition 3.6. *Let R be a ring, S be a multiplicative subset of R , and F be an R -module. Then the following statements are equivalent:*

1. F is u - S -flat;
2. There exist $s \in S$ satisfying that $s\text{Tor}_1^R(R/I, F) = 0$ for every ideal I of R ;
3. There exist $s \in S$ satisfying that for every ideal I of R , the natural homomorphism $\sigma_I : I \otimes_R F \longrightarrow IF$ is a u - S -isomorphism with respect to s ;
4. There exist $s \in S$ satisfying that $s\text{Tor}_1^R(R/K, F) = 0$ for every finitely generated ideal K of R ;
5. There exist $s \in S$ satisfying that, for every finitely generated ideal K of R , the natural homomorphism $\sigma_K : K \otimes_R F \longrightarrow KF$ is a u - S -isomorphism with respect to s .

Proof. (2) $\Leftrightarrow$ (3), (4) $\Leftrightarrow$ (5) and (2) $\Rightarrow$ (4) These are simple.

(5) $\Rightarrow$ (3) Follows from [23, Proposition 4.3].

(1) $\Leftrightarrow$ (2) Follows from [24, Proposition 2.3] (take $n=0$ in the proof of (4) $\Leftrightarrow$ (3)). $\square$

In 1960, Chase characterized coherent rings in terms of flat modules. In [23] Zhang give Chase Theorem for u - S -coherent rings: Let R be a ring and S is a regular multiplicative subset of R . Then R is u - S -coherent, if and only if, R is a u - S -coherent ring if and only if there is $s \in S$ such that any direct product of flat modules (resp, R) is u - S -flat with respect to s . The following theorem clarifies that their conclusion is true in general (without requiring that S has nonzero divisors).

Theorem 3.7. (Chase Theorem for u - S -coherent rings) Let R be a ring and S a multiplicative subset of R . The following statements are equivalent:

1. R is a u - S -coherent ring;
2. There exist $s \in S$ such that every direct product of u - S -flat R -modules with respect to s is u - S -flat with respect to s^2 ;
3. There exist $s \in S$ such that every direct product of flat R -modules is u - S -flat with respect to s ;
4. There exist $s \in S$ such that every direct product of R is u - S -flat with respect to s .

Proof. Analogue to Theorem [3.5](#).

In 1982, Matlis showed that a ring R is coherent if and only if $\text{Hom}_R(M, E)$ is flat for any injective modules M and E . In [\[23\]](#) Zhang give Chase Theorem for u - S -coherent rings: Let R be a ring and S is a regular multiplicative subset of R . Then R is u - S -coherent if and only there is $s_1, s_2 \in S$ such that if E is injective cogenerators, then $\text{Hom}_R(M, E)$ is u - S -flat with respect to s_1 for any u - S -injective module M with respect to s_2 . The following theorem shows that their result holds in general (without requiring that S have nonzero divisors).

Theorem 3.8. (Matlis Theorem for u - S -coherent rings) Let R be a ring and S is a multiplicative subset of R . Then the following statements are equivalent:

1. R is a u - S -coherent ring;
2. There exists $s_1, s_2 \in S$ such that $\text{Hom}_R(M, E)$ is u - S -flat with respect to s_1 for any u - S -injective module M with respect to s_2 and any injective module E ;
3. There exists $s_1, s_2 \in S$ such that if E is injective cogenerators, then $\text{Hom}_R(M, E)$ is u - S -flat with respect to s_1 for u - S -injective module M with respect to s_2 ;
4. There exists $s_1, s_2 \in S$ such that $\text{Hom}_R(\text{Hom}_R(M, E_1), E_2)$ is u - S -flat with respect to s_1 for any M a u - S -flat module with respect to s_2 and any injective modules E_1, E_2 ;
5. There exists $s_1, s_2 \in S$ such that if E_1 and E_2 are injective cogenerators, then $\text{Hom}_R(\text{Hom}_R(M, E_1), E_2)$ is u - S -flat with respect to s_1 for any M a u - S -flat module with respect to s_2 .

Proof. (2) $\Rightarrow$ (3) and (4) $\Rightarrow$ (5) Are straightforward.

(3) $\Rightarrow$ (4) Follows from [\[23\]](#) Proposition 4.3].

(1) $\Rightarrow$ (2) Assume that R is a u - S -coherent ring with respect to some element $s \in S$. Let I be a finitely generated ideal of R . Then we have an exact sequence $0 \rightarrow T' \rightarrow K \xrightarrow{f} I \rightarrow T \rightarrow 0$ with K finitely presented and $sT = sT' = 0$. Set $\text{Im}(f) = K'$. Consider the following commutative diagram with exact rows ($(-, -)$ is instead of $\text{Hom}_R(-, -)$):

$$\begin{array}{ccccccc} (M, E) \otimes T' & \longrightarrow & (M, E) \otimes K & \longrightarrow & (M, E) \otimes K' & \longrightarrow & 0 \\ \Psi_{T'} \downarrow & & \Psi_K \downarrow & & \Psi_{K'} \downarrow & & \\ ((T', M), E) & \longrightarrow & ((K, M), E) & \longrightarrow & ((K', M), E) & \longrightarrow & 0. \end{array}$$

Since K is finitely presented, Ψ_K is an isomorphism by [\[3\]](#) Proposition 8.14(1)] and [\[14\]](#) Theorem 2], $\Psi_{K'}$ is a u - S -isomorphism with respect to s . Now consider the following commutative diagram with exact rows:

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & \text{Tor}_1^R((M, E), R/K') & \longrightarrow & (M, E) \otimes K' & \longrightarrow & (M, E) \otimes R & \longrightarrow & (M, E) \otimes R/K' & \longrightarrow & 0 \\ & & \Psi_{R/K'}^1 \downarrow & & \Psi_{K'} \downarrow & & \Psi_R \downarrow & & \Psi_{R/K'} \downarrow & & \\ 0 & \longrightarrow & (\text{Ext}_R^1(R/K', M), E) & \longrightarrow & ((K', M), E) & \longrightarrow & ((R, M), E) & \longrightarrow & ((R/K', M), E) & \longrightarrow & 0. \end{array}$$

Since Ψ_R is an isomorphism and $\Psi_{K'}$ is a u - S -isomorphism with respect to s , $\Psi_{R/K'}^1$ so is. Then the following commutative diagram with exact rows:

$$\begin{array}{ccccccc}
Tor_1^R((M, E), T) & \longrightarrow & Tor_1^R((M, E), R/K') & \longrightarrow & Tor_1^R((M, E), R/I) & \longrightarrow & (M, E) \otimes T \\
\downarrow & & \Psi_{R/K'}^1 \downarrow & & \Psi_{R/I}^1 \downarrow & & \downarrow \\
(Ext_R^1(T, M), E) & \longrightarrow & (Ext_R^1(R/K', M), E) & \longrightarrow & (Ext_R^1(R/I, M), E) & \longrightarrow & ((T, M), E),
\end{array}$$

shows that $\Psi_{R/I}^1$ is a u-S-isomorphism with respect to s^3 by the proof of [24 Theorem 1.3]. Since M is u-S-injective with respect to s_2 , $s_2 Ext_R^1(R/I, M) = 0$. Then $s_1 Tor_1^R((M, E), R/I) = 0$ with $s_1 = s^3 s_2$. Therefore (M, E) is a u-S-flat with respect to s_1 .

(5) $\Rightarrow$ (1) Since R is a flat R -module, $\bigoplus R$ is flat. Then

$$\text{Hom}_R(\text{Hom}_R(\bigoplus R, E_1), E_2) \cong \text{Hom}_R(\prod \text{Hom}_R(R, E_1), E_2)$$

is u-S-flat with respect to s by (5). Note that $\bigoplus \text{Hom}_R(R, E_1)$ is the pure submodule of $\prod \text{Hom}_R(R, E_1)$. Thus the natural epimorphism

$$\text{Hom}_R(\prod \text{Hom}_R(R, E_1), E_2) \longrightarrow \text{Hom}_R(\bigoplus \text{Hom}_R(R, E_1), E_2)$$

splits by [16 Lemma 2.19]. It follows that

$$\prod \text{Hom}_R(\text{Hom}_R(R, E_1), E_2) \cong \text{Hom}_R(\bigoplus \text{Hom}_R(R, E_1), E_2)$$

is u-S-flat with respect to s . By [16 Corollary 2.21] $\prod R$ is the pure submodule of $\prod \text{Hom}_R(\text{Hom}_R(R, E_1), E_2)$. Using long exact sequence of Tor , we can easily prove that $(\prod \text{Hom}_R(\text{Hom}_R(R, E_1), E_2))/\prod R$ is u-S-flat with respect to s . Thus $\prod R$ is u-S-flat with respect to s^2 . Therefore R is u-S-coherent according to Theorem 3.7 $\square$

Theorem 3.9. Let R be a ring and S is a multiplicative subset of R . Then the following statements are equivalent:

1. R is u-S-coherent;
2. There exists $s_1, s_2 \in S$ such that $\text{Hom}(F, M)$ is u-S-flat with respect to s_2 for all free modules F and for all u-S-flat modules M with respect to s_1 ;
3. There exists $s_1, s_2 \in S$ such that $\text{Hom}(P, M)$ is u-S-flat with respect to s_2 for all projective modules P and for all u-S-flat modules M with respect to s_1 .

Proof. (1) $\Rightarrow$ (2) Let F be free and for all u-S-flat modules M with respect to s_1 . Write $F = \bigoplus_{i \in I} R_i$, where I is an index set, and for each $i \in I$, R_i is a copy of the R -module R . Then

$$\text{Hom}(F, M) = \prod_{i \in I} \text{Hom}(R, M) = \prod_{i \in I} M$$

is u-S-flat with respect to s_2 by Theorem 3.7 since R is u-S-coherent.

(2) $\Rightarrow$ (1) Let $(M_i)_{i \in I}$ be any family of u-S-flat modules M with respect to s_1 . Then

$$\prod_{i \in I} M_i = \prod_{i \in I} \text{Hom}(R, M_i) = \text{Hom}\left(\bigoplus_{i=1}^{\infty} R, M_i\right)$$

is u-S-flat with respect to s_2 by (2). Hence (1) follows by Theorem 3.7

(2) $\Leftrightarrow$ (3) This is simple. $\square$

References

- [1] D. D. Anderson and T. Dumitrescu, *S-Noetherian rings*, Comm. Algebra, 30(9) (2002), 4407–4416.
- [2] D. D. Anderson and M. Winders, *Idealization of a module*, J. Comm. Algebra, 1(1) (2009), 3–56.
- [3] L. Angeleri Hügel and D. Herbera, *Mittag-Leffler conditions on modules*, Indiana Univ. Math. J., 57 (2008), 2459–2517.
- [4] K. Bacema and A. Benhissi, *nonnil-coherent rings*, Beitr. Algebra Geom., 57(2) (2016), 297–305. 725–736.
- [5] A. Badawi, *On divided commutative rings*, Comm. Algebra, 27(3) (1999), 1465–1474.
- [6] A. Badawi, *On nonnil-Noetherian rings*, Comm. Algebra, 31(4) (2003), 1669–1677.
- [7] D. Bennis, M. El Hajoui, *On S-coherence*, J. Korean Math. Soc., 55(6) (2018), 1499–1512.
- [8] S. Kabbaj, *Matlis' semi-regularity and semi-coherence in trivial ring extensions: a survey*, Moroccan Journal of Algebra and Geometry with Applications, 1(1) (2021), 1–17.
- [9] H. Kim, N. Mahdou and E. H. Oubouhou, *When every ideal is ϕ -P-flat*, Hacettepe J. Math. Stat, 52(3) (2023), 708–720.
- [10] H. Kim, N. Mahdou and E. H. Oubouhou, *On ϕ -u-S-flat modules and nonnil-u-S-injective modules*, Georgian Math. J., 31(5) (2024), 819–834.
- [11] H. Kim, N. Mahdou and E. H. Oubouhou, *ϕ -rings from a module-theoretic point of view: a survey*, Moroccan Journal of Algebra and Geometry with Applications 3(1) (2024), 78–114
- [12] H. Kim, N. Mahdou, E. H. Oubouhou and X. Zhang, *Uniformly S-projective modules and uniformly S-projective uniformly S-covers*, Kyungpook Math. J., 64 (2024), 607–618.
- [13] M. J. Kwon and J. W. Lim *On nonnil-S-Noetherian rings*, Mathematics, 8(9) (2020), 1428.
- [14] E. Lenzing, *Endlich präsentierbare Moduln*, Archiv Der Mathematik 20(3) (1969), 262–266.
- [15] S. Glaz, *Commutative Coherent Rings*, Springer-Verlag, Lecture Notes in Mathematics, 1371 (1989).
- [16] R. Gobel, J. Trlifaj, *Approximations and endomorphism algebras of modules*, De Gruyter Exp. Math., vol. 41, Berlin: Walter de Gruyter GmbH Co. KG, 2012.
- [17] N. Mahdou and E. H. Oubouhou, *Nonnil-S-coherent rings*, Commun. Korean Math. Soc., 39(1) (2024), 45–58.
- [18] N. Mahdou, E. H. Oubouhou and E. Yetkin Celikel, *On nonnil-S-Noetherian and nonnil-u-S-Noetherian rings*, An. S. t. Univ. Ovidius Constanta., 32(1) (2024), 201–219.
- [19] W. Qi, H. Kim, F. G. Wang, M. Z. Chen and W. Zhao, *Uniformly S-Noetherian rings*, Quaest. Math., 47(5) (2023), 1019–1038.
- [20] W. Qi, X. L. Zhang, W. Zhao, *New characterizations of S-coherent rings*, J. Algebra Appl., (2021), 2350078.
- [21] W. Qi, X. L. Zhang, *Some remarks on nonnil-coherent rings and ϕ -IF rings* J. Algebra Appl., (2021), 2250211.

- [22] X. Zhang *Characterizing S -flat modules and S -von Neumann regular rings by uniformity*, Bull. Korean Math. Soc., 59(3) (2022), 643–657.
- [23] X. Zhang *On uniformly S -coherent rings*, Rocky Mountain J. Math., to appear.
- [24] X. Zhang *The u - S -weak global dimension of commutative rings*, Commun. Korean Math. Soc., 38(1) (2023), 97–112.



ISSN: 2820-7114

Moroccan Journal of Algebra and Geometry with Applications

Supported by Sidi Mohamed Ben Abdellah University, Fez, Morocco

Volume 4, Issue 2 (2025), pp 152-167

Title :

On graded 1-absorbing primary ideals and graded weakly 1-absorbing primary ideals

Author(s):

Mohammed Issoual and Emel Aslankarayigit Ugurlu

On graded 1-absorbing primary ideals and graded weakly 1-absorbing primary ideals

Mohammed Issoual¹ and Emel Aslankarayigit Ugurlu²

¹ CRMEF Fès, Morocco.

e-mail: issoual2@yahoo.fr

² Department of Mathematics, Marmara University, Istanbul, Turkey.

e-mail: emelakyugurlu@gmail.com

Communicated by Najib Mahdou

(Received 20 June 2024, Revised 04 January 2025, Accepted 20 January 2025)

Abstract. Let G be a group with identity e and R a G -graded commutative ring with $1 \neq 0$. In this paper, we study the concepts of graded 1-absorbing primary and graded weakly 1-absorbing primary ideals within G -graded rings. We aim to compare them with other ideal types, such as graded primary (graded weakly primary) and graded 2-absorbing primary (graded weakly 2-absorbing primary). Additionally, we examine their primary properties and investigate their behavior under G -graded ring homomorphisms. We also provide characterizations of these classes of ideals in contexts such as localizations of graded rings, graded trivial ring extensions, and graded amalgamation algebras along an ideal.

Key Words: Graded ring, graded ideal, graded 1-absorbing primary ideal, graded weakly 1-absorbing primary, graded primary ideal, graded prime ideal, trivial ring extension, graded module, graded submodule.

2020 MSC: 13A15, 13A02, 13C05, 13H05.

Dedicated to our Professor David E. Dobbs for his 80th Birthday.

1 Introduction

Throughout this paper (unless otherwise stated), all rings are commutative with $1 \neq 0$. The concept of 1-absorbing primary ideals was introduced by Badawi and Yetkin Celikel in [6]. A proper ideal I of R is called a 1-absorbing primary ideal, if for any nonunit $a, b, c \in R$ with $abc \in I$, then either $ab \in I$ or $c \in \sqrt{I}$. The concept of weakly 1-absorbing primary ideal was introduced by Badawi and Yetkin Celikel [7]. A proper ideal I of R is called weakly 1-absorbing primary ideal if for any nonunit $a, b, c \in R$ with $0 \neq abc \in I$, then either $ab \in I$ or $c \in \sqrt{I}$.

In this paper, we study graded 1-absorbing primary ideals and graded weakly 1-absorbing primary ideals of graded rings. First, we review some basic properties of graded rings and modules that will be used in subsequently the sequel. For further details and more information on graded rings and modules, we refer to [17, 18]. Let G be a multiplication group with identity e . A ring R is called to be G -graded ring (or G -graded ring) if there exist additive subgroups R_g of R indexed by the elements $g \in G$ such that $R = \bigoplus_{g \in G} R_g$ and $R_g R_h \subseteq R_{gh}$ for all $g, h \in G$. If the inclusion is equality, then the ring R is called strongly graded. The elements of R_g are called homogeneous of degree g and R_e is a subring of R and $1 \in R_e$. For $x \in R$, x can be written uniquely as $x = \sum_{g \in G} x_g$ where x_g is the component of x in R_g . Also we write $h(R) = \bigcup_{g \in G} R_g$ the set of all homogeneous elements. Moreover, if $r \in R_g$ and r is unit, then $r^{-1} \in R_{g^{-1}}$. A G -graded ring $R = \bigoplus_{g \in G} R_g$ is called a crossed product if R_g contains a unit for every $g \in G$. Note that a G -crossed product $R = \bigoplus_{g \in G} R_g$ is a strongly graded ring. Let R be a

G -graded ring and I be an ideal of R . Then I is called G -graded ideal if $I = \bigoplus_{g \in G} (I \cap R_g) = \bigoplus_{g \in G} I_g$, i.e, if $x \in I$ and $x = \sum_{g \in G} x_g$, then $x_g \in I$ for all $g \in G$. If $R = \bigoplus_{g \in G} R_g$ and $R' = \bigoplus_{g \in G} R'_g$ are two G -graded rings, then a mapping $f : R \rightarrow R'$ with $f(1_R) = 1_{R'}$ is called a gr-homomorphism if $f(R_g) \subseteq R'_g$ for all $g \in G$. Let $R = \bigoplus_{g \in G} R_g$ be a G -graded ring and let I be a graded ideal of R . Then the Quotient ring R/I is also a G -graded ring. Indeed, $R/I = \bigoplus_{g \in G} (R/I)_g$ where $(R/I)_g = \{x + I : x \in R_g\}$, with this grading, $(R/I)_e \cong R_e/I_e$. By the equality $I = \bigoplus_{g \in G} (I \cap R_g) = \bigoplus_{g \in G} I_g$, we obtain that an ideal I of R is a graded ideal if and only if I is generated by homogeneous elements of R . Recall that a G -graded ring is called *graded integral domain* if for element $a \in h(R)$, a is not a divisor of zero. In particular, R is said to be a *graded field* if every nonzero homogeneous element has a multiplicative inverse.

Let R be G -graded ring and let $S \subseteq h(R)$ be a multiplicatively closed subset of R . The the ring of fractions $S^{-1}R$ is a G -graded ring which is called the gr-ring of fractions. Indeed $S^{-1}R = \bigoplus_{g \in G} (S^{-1}R)_g$ where

$$(S^{-1}R)_g = \left\{ \frac{r}{s}, s \in R, s \in S \quad \text{and} \quad g = (\deg s)^{-1}(\deg r) \right\}.$$

Consider the ring gr-homomorphism $f : R \rightarrow S^{-1}R$ defined by $f(r) = \frac{r}{1}$. For any graded ideal I of R , the ideal of $S^{-1}R$ generated by $f(I)$ is denoted by $S^{-1}I$. Similar to non graded case, we can prove that

$$S^{-1}R = \{ \beta \in S^{-1}R : \beta = \frac{r}{s}, r \in I, s \in S \}.$$

Note that a proper graded ideal I of R is said to be graded prime if whenever $a, b \in h(R)$ such that $ab \in I$, then either $a \in I$ or $b \in I$. Let R be a G -graded ring. The *graded radical* of a graded ideal I , denoted by $\text{Gr}(I)$ is the set of all $x \in R$ such that for each $g \in G$ there exists $n_g > 0$ with $x^{n_g} \in I$. Note that, if r is a homogeneous element, then $r \in \text{Gr}(I)$ if and only if $r^n \in I$ for some positive integer n . In particular, we denotes $N(R) = \text{Gr}\{0\}$. A graded R -module is an R -module M such that $M = \bigoplus_{g \in G} M_g$ where M_g is an additive subgroup of M , and for every $g, h \in G$ we have $R_g M_h \subseteq M_{hg}$. Since $R_e M_h \subseteq M_h$, we can see that M_h is an R_e -submodule of M . The elements of $h(M) = \bigcup_{g \in G} M_g$ are called the homogeneous elements of M . A non zero element $m \in M_g$ is said to be a homogeneous element of degree g . Every $m \in M$ can be uniquely represented as a sum $m = \sum_{g \in G} m_g$ with $m_g \in M_g$ and finitely many nonzero m_g . The nonzero elements m_g in this sum are called the homogeneous components of m . An R -submodule N of M is said to be a graded submodule if for every $n \in N$, all its homogeneous components are also in N , i.e, $N = \sum_{g \in G} (N \cap M_g)$. If $I = \bigoplus_{g \in G} I_g$ is a graded ideal of R , then I_g is an R_e -module for every $g \in G$. A graded submodule N is called graded primary submodule if whenever $a \in h(R)$ and $m \in h(M)$ with $am \in N$, then either $m \in N$ or $a^k \in (N : M)$ for some positive integer. Therefore, if $P := (N : M)$ is a graded prime ideal, we say that N is a graded P -primary submodule [10, 19].

Let R be a commutative ring and M be a R -module. Then the trivial extension $R(+)M$ with the coordinate-wise addition and multiplication given by $(r_1, m_1)(r_2, m_2) = (r_1 r_2, r_1 m_2 + r_2 m_1)$ is a commutative ring with unity $(1, 0)$ (even R -algebra) is called the idealization of M or the trivial extension of R by M . Note that R naturally embeds into $R(+)M$ by $r \mapsto (r, 0)$, if N is a submodule of M , then $0(+)N$ is an ideal of $R(+)M$, $0(+)M$ is a nilpotent ideal of $R(+)M$ of index 2. It is well known that if I is an ideal of R and N is a submodule of M such that $IM \subseteq N$, then $I(+)N$ is an ideal of $R(+)M$. We recall that $U(R(+)M) = U(R)(+)M$, see [3].

Suppose that $R = \bigoplus_{g \in G} R_g$ be a G -graded ring and $M = \bigoplus_{g \in G} M_g$ be a G -graded R -module. Then $R(+)M$ is a G -graded ring with $(M(+)R)_g = R_g \oplus M_g$ for every $g \in G$. Consequently, $h(R(+)M) = \{(a, x) : a \in h(R), x \in h(M)\}$, see [3, 21].

In this paper, we aim to investigate the notions of graded 1-absorbing primary and graded weakly primary ideals in G -graded rings. In Section 2, we study the concept of graded primary, graded 2-absorbing primary, and graded 1-absorbing primary ideals. After examining the relationships

among these concepts, we provide a counterexample (see Examples 2.3). In addition to some main properties of graded 1-absorbing primary in the Cartesian product of G -graded commutative rings. We also investigate the attitude of the notion of graded 1-absorbing primary ideals under a G -graded ring homomorphism. Moreover, we obtain some characterizations of this notion in the localization of graded rings, the graded trivial extension rings, and the graded amalgamation algebras along an ideal. In Section 3, we study the concept of graded weakly 1-absorbing primary ideals in G -graded rings. It is clear that every graded 1-absorbing primary ideal is a graded weakly 1-absorbing primary ideal, but the converse is not true, see Example 3.2. As well as some characterizations of graded weakly 1-absorbing primary ideals, we compare them with other classes of ideals, such as graded weakly primary, graded weakly 2-absorbing primary, and graded 1-absorbing primary ideals. Finally, similar to Section 2, we characterize the class of graded weakly 1-absorbing primary ideals in the localization of graded rings, the graded trivial extension rings, and the graded amalgamation algebras along an ideal.

2 Graded 1-absorbing primary ideals

We remind the reader with the following definitions.

Definition 2.1. (cf. [15]) Let $R = \bigoplus_{g \in G} R_g$ be a G -graded ring, $I = \bigoplus_{g \in G} I_g$ be a graded ideal of R .

1. I is said to be a graded primary ideal of R if $I \neq R$, and whenever $r, s \in h(R)$ with $rs \in I$, then either $r \in I$ or $s \in Gr(I)$.
2. I is said to be a graded 2-absorbing primary ideal of R if $I \neq R$, and whenever $r, s, t \in h(R)$ with $rst \in I$, then either $rs \in I$ or $rt \in Gr(I)$ or $st \in Gr(I)$.
3. I is said to be a graded 1-absorbing primary ideal of R if $I \neq R$, and whenever $r, s, t \in h(R)$ nonunit homogeneous elements with $rst \in I$, then either $rs \in I$ or $t \in Gr(I)$.

Since the proof of the following result is elementary, we omit its proof.

Theorem 2.2. Let R be a G -graded ring and I be a proper graded ideal of R . Then:

1. If I is graded primary ideal of R , then I is graded 1-absorbing primary ideal of R .
2. If I is a graded 1-absorbing primary ideal of R , then I is graded 2-absorbing primary ideal of R .

The following example provide a graded 1-absorbing primary ideal that is not graded primary ideal.

Example 2.3. (A graded 1-absorbing primary ideal which is not graded primary) In Theorem 2.9, we will show that there exist a graded 1-absorbing ideal which is not a graded primary ideal. Precisely, if R is not a graded local ring, there exist a graded 1-absorbing primary ideal which is not graded primary ideal.

Theorem 2.4. Let R be a G -graded ring. If I is a graded 1-absorbing primary ideal of R , then $Gr(I)$ is a graded prime ideal of R .

Proof. Let r, s be homogeneous elements in $h(R)$ such that $rs \in Gr(I)$, we can assume that s, t are nonunits. Let $n \geq 2$ be a positive integer such that $(rs)^n \in I$. Then $n = 2m$ for some positive integer $m \geq 1$. Since $(rs)^n = r^m r^m s^n \in I$ and r^m, s^n are nonunit homogeneous elements of $h(R)$ and I is a graded 1-absorbing primary ideal, we conclude that either $r^m \cdot r^m = r^n \in I$ or $s^n \in Gr(I)$. That is $r \in Gr(I)$ or $Gr(I)$. Hence $Gr(I)$ is a graded prime ideal of R . $\square$

Recall that for graded ideal M of a G -graded ring R is said to be a graded maximal ideal, if there is no graded ideal K such that $M \subset K \subset R$. Also, note that a G -graded commutative ring R is said to be a G -graded local ring, if R has a one graded maximal ideal M which is the ideal generated by noninvertible homogeneous elements.

Lemma 2.5. [12 Lemma 2.7] *Let R be a G -graded crossed product ring. Then R is a graded local ring if and only if R_e is a local ring.*

Lemma 2.6. [6 Lemma 1] *Let R be a ring. Suppose that for every nonunit element w of R and for every unit element u of R , we have $u + w$ is a unit element of R . Then R is a local ring.*

Let I be a graded ideal of a G -graded ring R . Then I is said to be a graded primary ideal if for every $a, b \in h(R)$ with $ab \in I$, then either $a \in I$ or $b \in Gr(I)$. It is clear that a graded primary ideal is a graded 1-absorbing primary ideal, but the converse is not true. In the next result, we give some examples of graded 1-absorbing primary which are not graded primary ideals. Also, we show that if R is G -graded ring which is not a graded local ring, then the concept of graded 1-absorbing primary ideals and graded primary ideals collapse.

Theorem 2.7. *Let R be a G -graded crossed product ring which admits a proper ideal which is graded 1-absorbing primary ideal that is not a graded primary. Then R is G -graded local ring.*

Proof. We will show that R_e is a local ring. Let c be a nonunit element of R_e . Suppose that I is a proper graded 1-absorbing primary ideal of R that is not a graded primary ideal of R . Hence there exist $a, b \in h(R)$ with $ab \in I$ and neither $a \in I$ nor $b \in Gr(I)$. Since c is homogeneous, $b \notin Gr(I)$ and $abc \in I$, then $ac \in I$. Now, let $d \in R_e$ be a unit homogeneous element of R . Assume that $d + c$ is nonunit which is in $R_e \subseteq h(R)$, we have $(d + c)ab \in I$. The fact that $b \notin Gr(I)$ and I is a graded 1-absorbing primary ideal give that $(d + c)a \in I$, since $ca \in I$ and I is an ideal. This implies $da \in I$. The fact that d is a unit element in R_e gives $a \in I$, a contradiction. Thus $d + c$ is unit. By Lemma 2.6, we deduce that R_e is local ring, and by Lemma 2.5, R is G -graded local ring. $\square$

Corollary 2.8. *Suppose that R is G -graded ring which is not a G -graded local ring. Then every proper graded ideal is a graded 1-absorbing primary ideal if and only if I is a graded primary ideal of R .*

Proof. Follows directly from the Theorem 2.7. $\square$

Let R_1 and R_2 be two G -graded rings, then $R_1 \times R_2$ is a G -graded ring with $(R_1 \times R_2)_g = (R_1)_g \times (R_2)_g$ for every $g \in G$. In the following result, we give a characterization of graded 1-absorbing primary ideals of a graded ring $R_1 \times R_2$.

Theorem 2.9. *Let R_1 and R_2 be G -graded commutative rings. Let $R = R_1 \times R_2$, and $K = I \times J$ be a nonzero proper graded ideal of R . Then the followings are equivalent:*

1. K is a graded 1-absorbing primary ideal of R ;
2. K is a graded primary ideal of R ;
3. $K = I \times R_2$, where I is a graded primary ideal of R_1 or $K = R_1 \times J$, where J is a graded primary ideal of R_2 .

Before proving Theorem 2.9, we first establish the following lemmas.

Lemma 2.10. *Let R_1 and R_2 be a G -graded commutative rings with identity. Let $K := I \times J$ a graded ideal of $R_1 \times R_2$, where I, J are graded ideals of R_1 and R_2 respectively. K is a graded prime ideal of $R_1 \times R_2$ if and only if $K = I \times R_2$ where I is a graded prime ideal of R_1 or $K = R_1 \times J$, where J is a graded prime ideal of R_2 .*

Proof. Assume that K is a graded prime ideal of $R_1 \times R_2$. Since $(1,0)(0,1) = (0,0) \in K$, then either $(1,0) \in I \times J$ or $(0,1) \in I \times J$. Thus $K = R_1 \times J$ or $K = I \times R_2$. Without loss the generality, assume that $K = I \times R_2$. Let $ab \in I$ for some homogeneous elements $a, b \in h(R)$, then $(a,0)(b,0) \in K$, with $(a,0), (b,0) \in h(R_1) \times h(R_2)$ and K is a graded prime ideal of $R_1 \times R_2$, we conclude that either $(a,0) \in K$ or $(b,0) \in K$. Hence $a \in I$ or $b \in I$. Thus I is a graded prime ideal of R_1 . Conversely assume that $K = I \times R_2$ and I is graded prime ideal of R_1 . Let $(a,a')(b,b') = (ab, a'b') \in I \times R_2$, for some $(a,a'), (b,b') \in h(R_1) \times h(R_2)$. Since $ab \in I$ and I is a graded prime of R_1 , we conclude either $a \in I$ or $b \in I$. Hence either $(a,a') \in K$ or $(b,b') \in K$. That is K is a graded prime ideal of $R_1 \times R_2$. Similarly, one can see the claim if $K = R_1 \times J$ and J is a graded prime ideal of R_2 . $\square$

Lemma 2.11. Let R_1 and R_2 be two G -graded commutative rings with identity. Let $K := I \times J$ be a graded ideal of $R_1 \times R_2$, where I, J are graded ideals of R_1 and R_2 , respectively. Then K is a graded primary ideal of $R_1 \times R_2$ if and only if $K = I \times R_2$, where I is a graded primary ideal of R_1 or $K = R_1 \times J$, where J is a graded primary ideal of R_2 .

Proof. Assume that K is a graded primary ideal of $R_1 \times R_2$, then by [20, Lemma 1.8], $Gr(K)$ is a graded prime ideal of $R_1 \times R_2$. By Lemma 2.10, we have $Gr(K) = P \times R_2$, where P is a graded prime ideal of R_1 or $Gr(K) = R_1 \times Q$, where Q is a graded prime ideal of R_2 . Without loss the generality, we may assume that $Gr(K) = P \times R_2$. Let $a \in h(R_1) \setminus P$, so $(a,0) \notin Gr(K)$. Let $b \in R_2$, then $(0,b)(a,0) = (0,0) \in K$ and $(a,0) \notin Gr(K)$, this implies $(a,b) \in K$, thus $J = R_2$. Hence $K = I \times R_2$ with $Gr(I) = P$, and it is easy to see that I is a graded primary ideal of R_1 . Conversely, if $K = I \times R_2$, where I is a graded primary ideal of R_1 , it is clear that K is a graded primary ideal of $R_1 \times R_2$. $\square$

Proof of Theorem 2.9

- (1) $\Leftrightarrow$ (2) Follows from the Corollary 2.8 since $R_1 \times R_2$ is not a G -graded local ring.
 (2) $\Leftrightarrow$ (3) Follows from the Lemma 2.11. $\square$

The following result gives us a method to construct a graded 1-absorbing primary ideal.

Theorem 2.12. Let R be a graded local ring with a graded maximal ideal M . Let P a graded prime ideal such that $P \subset M$. Then PM is a graded 1-absorbing primary ideal of R .

Proof. It is clear that PM is a graded ideal of R . On the other hand, we have $Gr(PM) = P$. Let r, s, t be nonunit homogeneous elements in $h(R)$ with $rst \in PM$. Since rs, t are homogeneous nonunit elements of $h(R)$ and P be a graded prime, we have either $rs \in P$ or $t \in P$. If $rs \in P$, we are done. Otherwise, $t \in P$. Since $P \subseteq Gr(P)$, we conclude that $t \in Gr(P) = Gr(PM)$. Thus, PM is a graded 1-absorbing primary ideal of R . $\square$

Theorem 2.13. Let I be a graded 1-absorbing primary ideal of a G -graded ring R . Let $c \in h(R) \setminus I$ be a nonunit homogeneous element of $h(R)$. Then $(I : c) := \{r \in R : rc \in I\}$ is a graded primary ideal of R .

Proof. Let $c \in h(R) \setminus I$. First, we prove that $(I : c)$ is a graded ideal of R . Let $r \in (I : c)$. Then $r \in R$ such that $rc \in I$. Since R is graded, $r = \sum_{g \in G} r_g$, where $r_g \in R_g$ and then $rc = \sum_{g \in G} r_g c$. Since $r_g c \in h(R)$ for all $g \in G$ and I is a graded ideal, we deduce that $r_g c \in I$, so $r_g \in (I : c)$ for all $g \in G$. Hence $(I : c)$ is a graded ideal of R . Now let $rs \in (I : c)$ for some nonunit homogeneous elements $r, s \in h(R)$, then $rsc \in I$. Assume that $s \notin (I : c)$. As I is graded 1-absorbing primary and $rc \notin I$, we have $s \in Gr(I)$. Since $Gr(I) \subseteq Gr((I : c))$ we obtain that $(I : c)$ is a graded primary ideal of R . $\square$

Recall that a G -graded ring R is called *graded divided* if for every graded prime ideal P and for every $x \in h(R) \setminus P$, we have $x|p$ for every $p \in h(R) \cap P$. Recall that a ring is called a *graded chained* if

for every $x, y \in h(R)$, either $x|y$ or $y|x$. Also, note that a G -graded ring is said to be a *graded valuation domain*, if for every nonzero homogeneous elements a, b of R , then either $a|b$ or $b|a$.

Theorem 2.14. Let R be a G -graded divided ring. Then a proper graded ideal I is a graded 1-absorbing primary ideal of R if and only if I is a graded primary ideal.

Proof. Let I be a graded primary ideal of R , and let $(rs).t = rst \in I$ for some nonunit homogeneous elements of $h(R)$ with $rs \notin I$, then $s \in Gr(I)$. Hence I is a graded 1-absorbing primary ideal of R . Conversely, assume that I is a graded 1-absorbing primary ideal of R and let $rs \in I$ for some nonunit homogeneous elements of R and $r \notin Gr(I)$. By Theorem 2.4, $Gr(I)$ is a graded prime ideal of R , thus $s \in Gr(I)$. Since R is a graded divided ring and $Gr(I)$ is a graded prime ideal and $r \notin Gr(I)$, we deduce that $r|s$. Thus $s = rt$ for some homogeneous element $t \in h(R)$. Since $rs = rtr \in I$ and $r \notin Gr(I)$ and I is a graded 1-absorbing primary ideal, we conclude $s = rt \in I$. Thus I is a graded primary ideal of R . $\square$

Corollary 2.15. Let R be a G -graded valuation domain. Then a proper graded ideal I is a graded 1-absorbing primary ideal of R if and only if I is a graded primary ideal.

Proof. Every graded valuation domain is a graded divided ring. Indeed, let P be a graded prime ideal and x be a homogeneous element in $h(R) \setminus P$. Assume that $y \in h(R) \cap P$. Since R is a graded valuation domain, then either $x|y$ or $y|x$. As $x \notin P$, we have $x|y$ for every $y \in h(R) \cap P$. Then R is a graded divided ring. Thus the result follows from the Theorem 2.14. $\square$

Theorem 2.16. Let R be a G -graded ring and $I = \bigoplus_{g \in G} (I \cap R_g) = \bigoplus_{g \in G} I_g$ be a graded ideal of R . Then the following statements hold:

1. If I is a graded 1-absorbing primary ideal of R , then I_e is a 1-absorbing primary ideal of R_e .
2. If I_e is a 1-absorbing primary ideal of R_e and R is a crossed product, then I is a graded 1-absorbing primary ideal of R .

Proof. (1) It is clear that I_e is an ideal of the ring R_e . Now let r, s, t nonunit elements in R_e such that $rst \in I_e \subseteq I$. Since I is a graded ideal and r, s, t are homogeneous nonunit elements, we get either $rs \in I$ or $t \in Gr(I)$. Assume $rs \in I$, then $rs \in R_e \cap I = I_e$. Now let $t \in Gr(I)$, there exists a positive integer $n \geq 1$ such that $t^n \in I$. Since $t^n \in R_e \cap I = I_e$, we conclude that $t^n \in R_e \cap I = I_e$, then $t \in Gr(I_e)$. Hence, I_e is a 1-absorbing primary ideal of R_e .

(2) Suppose that R is a crossed product and I_e is a 1-absorbing primary ideal of R_e . Let r, s, t be nonunit homogeneous elements in $h(R)$ such that $rst \in I$. There exist $g, h, k \in G$ such that $r \in R_g, s \in R_h, t \in R_k$. Since R is a crossed product, also $R_{g^{-1}}$ contains a unit, say s' and $R_{h^{-1}}$ contains a unit, say r' and $R_{k^{-1}}$ contains a unit, say t' . Thus $(rr')(ss')(tt') \in I_e$, since I_e is a 1-absorbing primary and rr', ss', tt' are nonunit elements in R_e , we conclude either $(rr')(ss') \in I_e$ or $tt' \in Gr(I_e)$. then either $rs \in I_{g^{-1}h^{-1}}$ or $tt' \in Gr(I_{k^{-1}})$. Hence either $rs \in I$ or $t \in Gr(I)$. Therefore, I is a graded 1-absorbing primary ideal of R . $\square$

For G -graded rings R and R' , a G -graded ring homomorphism $\varphi : R \rightarrow R'$ is a ring homomorphism such that $\varphi(R_g) \subseteq R'_g$ for every $g \in G$. The following result is an analogue of [6, Theorem 17].

Theorem 2.17. Let R and R' be two G -graded rings and $\varphi : R \rightarrow R'$ be a G -graded ring homomorphism with $\varphi(1) = 1$. Then the following statements hold:

1. Assume that for every nonunit homogeneous element r of $h(R)$, we have $\varphi(r)$ is nonunit elements of $h(R')$. Then if I' is graded 1-absorbing primary ideal of R' , then $\varphi^{-1}(I')$ is a graded 1-absorbing primary ideal of R .
2. If φ is a graded epimorphism and I is a graded 1-absorbing primary ideal of R containing $\ker(\varphi)$, then $\varphi(I)$ is a graded 1-absorbing primary ideal of R' .

Proof. (1) Suppose that I' is a graded 1-absorbing primary ideal of R' and let r, s, t be nonunit homogeneous elements of $h(R)$ such that $rst \in \varphi^{-1}(I')$, then $\varphi(rst) = \varphi(r)\varphi(s)\varphi(t) \in I'$. Since $\varphi(r), \varphi(s), \varphi(t)$ are nonunit homogeneous elements of $h(R')$ by assumption (1) and I' is a graded 1-absorbing primary ideal of R' , we conclude that either $\varphi(r)\varphi(s) \in I'$ or $\varphi(t) \in Gr(I')$, and hence either $rs \in \varphi^{-1}(I')$ or $t \in \varphi^{-1}(Gr(I')) = Gr(\varphi^{-1}(I'))$. Therefore $\varphi^{-1}(I')$ is a graded 1-absorbing primary ideal of R .

(2) Suppose that I is a graded 1-absorbing primary ideal of R containing $\ker(\varphi)$ and $r's't' \in \varphi(I)$ for some nonunits $r', s', t' \in h(R')$. Since φ is a graded epimorphism, there exist $r, s, t \in h(R)$ such that $r' = \varphi(r), s' = \varphi(s)$ and $t' = \varphi(t)$. Since $\varphi(1) = 1$, we have $\varphi(r), \varphi(s), \varphi(t)$ are nonunit homogeneous elements of $h(R')$. Now we have $\varphi(rst) = r's't' \in \varphi(I)$. Since $\ker(\varphi) \subseteq I$, we have $rst \in I$. Since I is a graded 1-absorbing primary ideal of R , we obtain either $rs \in I$ or $t \in Gr(I)$. So either $r's' \in \varphi(I)$ or $t' \in \varphi(Gr(I)) = Gr(\varphi(I))$. Thus $\varphi(I)$ is a graded 1-absorbing primary ideal of R' . $\square$

Let I be a proper graded ideal of a G -graded ring R . Then we define $G - Z_I(R) := \{r \in h(R) : rs \in I \text{ for some } s \in h(R) - Z_I(R)\}$. The following result is an analogue of [6 Theorem 18].

Theorem 2.18. Let I be a proper graded ideal of a G -graded ring R . Then the following statements hold:

1. If J is a proper graded ideal of R with $J \subseteq I$ and I is a graded 1-absorbing primary ideal of R , then I/J is a graded 1-absorbing primary ideal of a G -graded ring R/J .
2. Let J be a proper graded ideal of R with $J \subseteq I$ such that $U(R/J) \cap h(R/J) = \{r + J, r \in h(R) \cap U(R)\}$. If J is a graded 1-absorbing ideal of R and I/J is a graded 1-absorbing ideal of R/J . Then I is a graded 1-absorbing primary of R .

Proof. (1) Follows from Theorem 2.17 (2).

(2) Suppose that $rst \in I$ for some nonunit homogeneous elements of R . If $rst \in J$, then either $rs \in J \subseteq I$ or $t \in Gr(J) \subseteq Gr(I)$. Now assume that $rst \notin J$, then $(r+J)(s+J)(t+J) \in I/J$, where $r+J, s+J, t+J$ are nonunit elements of R/J by hypothesis. Thus either $(r+J)(s+J) \in I/J$ or $t+J \in Gr(I/J)$. If $(r+J)(s+J) \in I/J$, then $rs \in I$. If $t+J \in Gr(I/J)$, there exists a positive integer n with $(t+J)^n \in I/J$, so $t^n \in I$ and hence $t \in Gr(I)$. $\square$

Theorem 2.19. Let R be a G -graded ring, $S \subseteq h(R)$ be a multiplicatively closed subset of R , and I be a proper graded ideal of R . Then the followings hold:

1. If I is a graded 1-absorbing primary ideal of R such that $I \cap S = \emptyset$, then $S^{-1}I$ is a graded 1-absorbing primary ideal of a graded ring $S^{-1}R$.
2. If $S^{-1}I$ is a graded 1-absorbing primary ideal of a graded ring $S^{-1}R$ such that $S \cap G - Z_I(R) = \emptyset$, then I is a graded 1-absorbing primary ideal of R .

Proof. (1) Suppose that $\frac{r_1 r_2 r_3}{s_1 s_2 s_3} \in S^{-1}R$ for some nonunit homogeneous elements of $S^{-1}R$. Then there exist $v \in S$ such that $0 \neq vr_1 r_2 r_3 \in I$. Since I is a graded 1-absorbing primary ideal of R and $vr_1 \in h(R)$, then either $vr_1 r_2 \in I$ or $r_3 \in Gr(I)$, then $\frac{vr_1 r_2}{vs_1 s_2} \in S^{-1}I$ or $\frac{r_3}{s_3} \in S^{-1}Gr(I) = Gr(S^{-1}I)$. Hence $S^{-1}I$ is a graded 1-absorbing primary ideal of $S^{-1}R$.

(2) Suppose that $r_1 r_2 r_3 \in I$ for some nonunit homogeneous elements of R . Then $\frac{r_1}{1} \frac{r_2}{1} \frac{r_3}{1} \in S^{-1}R$. Since $S^{-1}I$ is a graded 1-absorbing primary ideal of $S^{-1}R$, we deduce that either $\frac{r_1}{1} \frac{r_2}{1} \in S^{-1}I$ or $\frac{r_3}{1} \in Gr(S^{-1}I) = S^{-1}Gr(I)$. If $\frac{r_1}{1} \frac{r_2}{1} \in S^{-1}I$, then $vr_1 r_2 \in I$ for some $v \in S$. Since $S \cap G - Z_I(R) = \emptyset$ and $v \in S$, we conclude that $r_1 r_2 \in I$. If $\frac{r_3}{1} \in S^{-1}Gr(I)$, then $(tr_3)^n \in I$ for some $t \in S$ and some positive integer $n \geq 1$. The fact that $t \in S$, gives $t^n \notin G - Z_I(R)$ and hence $r_3^n \in I$. Thus $r_3 \in Gr(I)$. Therefore, I is a graded 1-absorbing primary ideal of R . $\square$

Definition 2.20. Let I be a graded 1-absorbing primary ideal of a G -graded ring. Then $Gr(I) = P$ is a graded prime ideal of R , by Theorem 2.4. Hence we call I as a graded P -1-absorbing primary ideal of R .

Theorem 2.21. Let $I_1, \dots, I_n$ be graded P -1-absorbing primary ideals of a G -graded ring R . Then $I := \cap_{i=1}^n I_i$ is a graded P -1-absorbing primary ideal of R .

Proof. First observe that I is a graded ideal of R and $Gr(I) = P$. Let r, s, t nonunit homogeneous elements such that $rst \in I$ and $rs \notin I$. We may assume that $rs \notin I_1$. Since I_1 is a graded P -1-absorbing primary ideal, we obtain $t \in P$. Hence I is a graded P -1-absorbing primary ideal of R . $\square$

Lemma 2.22. (cf. [21] Proposition 3.3 and Corollary 3.5]) Let $R = \bigoplus_{g \in G} R_g$ be G -graded ring and $M = \bigoplus_{g \in G} M_g$ be a G -graded R -module. Let I be a graded ideal of R and N be a graded submodule of M such that $IM \subseteq N$. Then the following statements hold:

1. $I(+)N$ is a graded ideal of $R(+)M$.
2. $Gr(I(+)N) = Gr(I)(+)M$.

Theorem 2.23. Let $R = \bigoplus_{g \in G} R_g$ be G -graded ring and $M = \bigoplus_{g \in G} M_g$ be a G -graded R -module. Let I be a graded ideal of R . Then I is a graded 1-absorbing primary ideal of R if and only if $I(+)M$ is a graded 1-absorbing primary of $R(+)M$.

Proof. Assume that $I(+)M$ is a graded 1-absorbing primary ideal of $R(+)M$. Let $abc \in I$ for some nonunit homogeneous elements of R . Since $U(R(+)M) = U(R)(+)M$, we get $(a, 0), (b, 0), (c, 0)$ are nonunit homogeneous elements of $R(+)M$. Then $(a, 0)(b, 0)(c, 0) \in I(+)M$ and $I(+)M$ is a graded 1-absorbing primary of $R(+)M$ imply that either $(a, 0)(b, 0) \in I(+)M$ or $(c, 0) \in Gr(I(+)M) = Gr(I)(+)M$. Thus, we have either $ab \in I$ or $c \in Gr(I)$, that is, I is a graded 1-absorbing primary ideal of R . Conversely, let $(a, e)(b, f)(c, g) \in I(+)M$ for some nonunit homogeneous elements of $R(+)M$. Since $U(R(+)M) = U(R)(+)M$, we have a, b, c are nonunit homogeneous elements of R and $abc \in I$. Since I is a graded 1-absorbing primary ideal of R , either $ab \in I$ or $c \in Gr(I)$. Hence we conclude either $(a, e)(b, f) \in I(+)M$ or $(c, g) \in Gr(I)(+)M = Gr(I(+)M)$. Thus, $I(+)M$ is a graded 1-absorbing primary ideal of $R(+)M$. $\square$

Theorem 2.24. Let $R = \bigoplus_{g \in G} R_g$ be G -graded ring and $M = \bigoplus_{g \in G} M_g$ be a G -graded R -module. Let I be a graded ideal of R and N be a graded submodule of M . Then $I(+)N$ is a graded 1-absorbing primary ideal of $R(+)M$ if and only if either:

1. $N = M$ and I is a graded 1-absorbing primary ideal of R or
2. $N \subsetneq M, IM \subseteq N, I$ is a graded 1-absorbing primary of R and N is graded P -primary submodule of M , where $P = Gr(I)$ is a graded prime ideal of R .

Proof. ($\Rightarrow$). Assume that $I(+)N$ is a graded 1-absorbing primary ideal. Let $abc \in I$ for some nonunit homogeneous elements of R . Since $(a, 0), (b, 0), (c, 0)$ are nonunit homogeneous elements of $R(+)M$ and $(a, 0)(b, 0)(c, 0) \in I(+)N$, we conclude that either $(a, 0)(b, 0) \in I(+)M$ or $(c, 0) \in Gr(I(+)N) = Gr(I)(+)M$. Thus, we obtain either $ab \in I$ or $c \in Gr(I)$, so I is a graded 1-absorbing primary ideal of R . Now by

the Theorem 2.4, we have $Gr(I(+)N)$ is a graded prime ideal of $R(+)M$. By [9 Proposition 3.1], we get $Gr(I(+)N) = P(+)M$ for some graded prime ideal P of R , and with Lemma 2.22, we deduce $Gr(I) = P$.

($\Leftarrow$). If $N = M$ see Theorem 2.23. Assume that $N \subsetneq M$. Since $IM \subseteq N$, and I is a graded ideal of R , we conclude that $I(+)N$ is a graded ideal of $R(+)M$. Now let $(a, e), (b, f), (c, g)$ be nonunit homogeneous elements of $R(+)M$ such that $(a, e)(b, f)(c, g) = (abc, abg + acf + bce) \in I(+)N$. Since $U(R(+)M) = U(R)(+)M$ we have $a, b, c \in h(R) \setminus U(R)$ and $abc \in I$. As I is a graded 1-absorbing primary ideal of R , we conclude either $ab \in I$ or $c \in Gr(I)$. If $c \in Gr(I)$, then $(c, f) \in Gr(I(+)N) = Gr(I)(+)M$ and so we are done. We may assume that $c \notin Gr(I) = P$. On the one hand, we have $ab \in I$ and $acf + bce \in N$ since $IM \subseteq N$, on the other hand, $c(af + be) \in N$ and $c \notin P = (M : N)$, hence $af + be \in N$ since N is a graded P -primary submodule of M . Thus $(a, e)(b, f) = (ab, af + be) \in I(+)N$. This implies that $I(+)N$ is a graded ideal of $R(+)M$. $\square$

3 Graded weakly 1-absorbing primary ideals

Definition 3.1. Let $R = \bigoplus_{g \in G} R_g$ be a G -graded ring, $I = \bigoplus_{g \in G} I_g$ be a graded ideal of R .

1. I_g is called a prime subgroup of R_g , if $I_g \neq R_g$; and whenever $a, b \in R_g$ with $ab \in I_g$, then either $a \in I_g$ or $b \in I_g$.
2. I is called a graded weakly 1-absorbing primary ideal of R if $I \neq R$ and whenever $r, s, t \in h(R)$ nonunit homogeneous elements with $0 \neq rst \in I$, then either $rs \in I$ or $t \in Gr(I)$.

It is clear that every graded 1-absorbing primary ideal is a graded weakly 1-absorbing primary ideal. The following example shows that the converse is not true.

Example 3.2. (cf. [8 Example 2.2]) **(A graded weakly 1-absorbing primary ideal which is not graded 1-absorbing primary)** Let $R = \mathbb{Z}_6[i]$ and $G = \mathbb{Z}_2$. Then R is graded by $R_0 = \mathbb{Z}_6$ and $R_1 = i\mathbb{Z}_6$. Let $I = \{0\}$ which is a graded ideal of R . We have $2.2.3 \in I$ but neither $2.2 \in I$ nor $3 \in Gr(I)$. On the other hand, I is graded weakly 1-absorbing primary ideal by the definition.

Now, let us continue with the following result:

Theorem 3.3. Let $R = \bigoplus_{g \in G} R_g$ be a G -graded ring, $I = \bigoplus_{g \in G} I_g$ be a graded ideal of R .

1. If I is a graded weakly primary ideal of R , then I is a graded weakly 1-absorbing primary ideal.
2. If I is a graded weakly 1-absorbing primary ideal, then I is a graded weakly 2-absorbing primary ideal.
3. If $\{0\}$ is a graded 1-absorbing primary ideal, then I is a graded weakly 1-absorbing primary ideal if and only if I is a graded 1-absorbing primary ideal.
4. If R is a graded integral domain, then I is graded weakly 1-absorbing primary ideal if and only if I is a graded 1-absorbing primary ideal.
5. Let R be a graded local ring with graded maximal ideal $Gr(0)$. Then every graded proper ideal of R is a graded weakly 1-absorbing primary ideal of R .

Proof. (1) Straightforward.

(2) Let $0 \neq rst$ for some homogeneous elements $r, s, t \in h(R)$. If one of r, s, t is unit, we are done. We can assume that r, s, t nonunits elements, as I is graded weakly 1-absorbing, we get either $rs \in I$ or $t \in Gr(I)$, this implies $rs \in I$ or $st \in Gr(I)$ or $tr \in Gr(I)$. Hence I is a graded weakly 2-absorbing primary ideal of R .

Let $rst \in I$ for some nonunit homogeneous elements of $h(R)$. If $0 \neq rst$, as I is graded weakly 1-absorbing primary ideal of R , we get that either $rs \in I$ or $t \in Gr(I)$. If $0 = rst \in \{0\}$, by assumption, we have either $0 = rs \in I$ or $t \in Gr(0) \subset Gr(I)$. Hence I is a graded 1-absorbing primary ideal of R .

(3) It is clear that R is graded integral domain if and only if $\{0\}$ is graded prime ideal. Thus, the result follows from (3).

(4) Let I be a graded ideal of R . Since R is graded local ideal with graded maximal ideal $Gr(0)$, then $Gr(I) = Gr(0)$. Then by the [20, Proposition 1.11], we get I is graded primary ideal, and so graded weakly 1-absorbing primary ideal of R . $\square$

Theorem 3.4. Let $R = \bigoplus_{g \in G} R_g$ be a graded ring and I be a graded weakly 1-absorbing primary which is not graded 1-absorbing primary ideal of R . Then $Gr(I)$ is not graded maximal ideal of R .

Proof. Let I be graded weakly 1-absorbing primary ideal such that $Gr(I) = M$ is a graded maximal ideal, by the [20, Proposition 1.11], we get I is graded primary ideal. Thus I is a graded 1-absorbing primary ideal, a contradiction. $\square$

Recall that R is called a graded reduced ring if R is a G -graded ring and $Gr(0) = 0$.

Theorem 3.5. Let R be a G -graded reduced ring. If I is a nonzero graded weakly 1-absorbing primary ideal of R , then $Gr(I)$ is a graded weakly prime ideal of R and there exists $g \in G$ such that I_g is not prime subgroup of R_g .

Proof. Suppose that $0 \neq rs \in Gr(I)$ for some nonunit homogeneous elements of $h(R)$. Then there exists a positive integer $n = 2m$ such that $(rs)^n \in I$. Since R is a graded reduced ring and $I \neq 0$, we have $0 \neq r^n s^n \in I$. Hence $0 \neq r^m r^m s^n \in I$. Since r^m, s^n are nonunit homogeneous elements of R and I is a graded weakly 1-absorbing primary ideal of R , we obtain either $r^m, r^m = r^n \in I$ or $s^n \in Gr(I)$. Thus $Gr(I)$ is a graded weakly prime ideal of R . Now, suppose by way of contradiction that for every $g \in G$ that I_g is prime subgroup of R_g . Thus by [4, Theorem 2.4], we get $Gr(I) = Gr(0)$. Since R is graded reduced, we conclude that $I = 0$, a contradiction. $\square$

A G -graded ring $R = \bigoplus_{g \in G} R_g$ is called a crossed product if R_g contain a unit for every $g \in G$. Note that a G -crossed product $R = \bigoplus_{g \in G} R_g$ is a strongly graded ring, that is, $R_{gh} = R_g R_h$ for every $g, h \in G$.

Theorem 3.6. Let R be a G -graded ring and $I = \bigoplus_{g \in G} (I \cap R_g) = \bigoplus_{g \in G} I_g$ be a graded ideal of R . Then the following statements hold:

1. If I is a graded weakly 1-absorbing primary ideal of R , then I_e is a weakly 1-absorbing primary ideal of R_e .
2. If I_e is a weakly 1-absorbing primary ideal of R_e and R is a crossed product, then I is a graded weakly 1-absorbing primary ideal of R .

Proof. (1) It is clear that I_e is an ideal of the ring R_e . Now let r, s, t nonunit elements in R_e such that $0 \neq rst \in I_e \subseteq I$. Since I is a graded weakly 1-absorbing primary ideal and r, s, t are homogeneous nonunit elements, we get either $rs \in I$ or $t \in Gr(I)$. Let $rs \in I$, then $rs \in R_e \cap I = I_e$. Now, assume that $t \in Gr(I)$, then $t^n \in I$ for some positive integers n , thus $t^n \in I \cap R_e = I_e$. This yields $t \in \sqrt{I_e}$. Hence I_e is a weakly 1-absorbing prime ideal of R_e .

(2) Suppose that R is a crossed product and I_e is a weakly 1-absorbing primary ideal of R_e . Let r, s, t be nonunit homogeneous elements in $h(R)$ such that $0 \neq rst \in I$. There exist $g, h, k \in G$ such that $r \in R_g, s \in R_h, t \in R_k$. Since R is a crossed product, also $R_{g^{-1}}$ contains a unit, say s' and $R_{h^{-1}}$ contains a unit, say r' and $R_{k^{-1}}$ contains a unit, say t' . Thus $0 \neq (rr')(ss')(tt') \in I_e$, since I_e is a weakly 1-absorbing primary ideal and rr', ss', tt' are nonunit elements in R_e , we conclude either $(rr')(ss') \in I_e$

or $tt' \in \sqrt{I_e}$. Then either $rs \in I_{g^{-1}h^{-1}}$ or $t^n \in I_{k^{-n}}$ for some positive integer n . Hence either $rs \in I$ or $t \in Gr(I)$. Therefore, I is a graded weakly 1-absorbing primary ideal of R . $\square$

Definition 3.7. Let $R = \oplus_{g \in G} R_g$ be a G -graded ring, $I = \oplus_{g \in G} I_g$ be a graded ideal of R and $g \in G$.

1. I is called a g -1-absorbing primary (resp., g weakly 1-absorbing primary) ideal of R , if $I_g \neq R_g$ and whenever r, s, t nonunit elements in R_g with $rst \in I$ (resp., $0 \neq rst \in I$), then $rs \in I$ or $t \in Gr(I)$.
2. Let $r, s, t \in R_g$. We say that (r, s, t) is a g -1-triple-zero of I if $rst = 0, rs \notin I$ and $t \notin Gr(I)$.

Theorem 3.8. Let $R = \oplus_{g \in G} R_g$ be a G -graded ring and $I = \oplus_{g \in G} I_g$ be a graded weakly 1-absorbing primary ideal of R . Let $g \in G$. If (r, s, t) is a g -1-triple-zero of I , then

1. $rsI_g = 0$.
2. If $rt \notin I$ and $st \notin I$, then $rtI_g = stI_g = rI_g^2 = sI_g^2 = tI_g^2 = 0$.
3. If $rt \notin I$ and $st \notin I$, then $I_g^3 = 0$.

Proof. (1) Suppose that $rsI_g \neq 0$. Then $rsu \neq 0$ for some nonunits $u \in I_g$. Hence $0 \neq rs(t+u) \in I$. Since $rs \notin I$, we conclude that $t+u \in R_g$ nonunit element. Since I is graded weakly 1-absorbing and $rs \notin I$, we conclude that $u+t \in Gr(I)$. Since $u \in I_g \subseteq I \subseteq Gr(I)$, we have $t \in Gr(I)$, a contradiction. Thus, we have $rsI_g = 0$.

(2) Suppose that $rtI_g \neq 0$. Then $rtw \neq 0$ for some $w \in I_g$. Hence $0 \neq rtw = r(s+w)t \in I$. Since $rt \notin I$, we conclude that $s+w$ is nonunit element of R_g . Since I is a graded weakly 1-absorbing primary ideal of R and $rs \notin I$ and $rw \in I$. We conclude that $r(s+w) \notin I$, and hence $t \in Gr(I)$, a contradiction. Thus $rtI_g = 0$. By a similarly argument, we obtain that $stI_g = 0$. Now, we prove that $rI_g^2 = 0$. Suppose $ruv \neq 0$ for some nonunit elements u, v of I_g . Since $rsI_g = 0$ by (1) and $rtI_g = 0$ by (2), $0 \neq auv = r(u+s)(v+t) \in I$. As $ab \notin I$, we conclude that $(v+t)$ is nonunit element of R_g . Since I is graded weakly 1-absorbing primary of R , we have either $r(u+s) \in I$ or $(v+t) \in Gr(I)$. By $u, v \in I_g \subseteq I$, we conclude that either $rs \in I$ or $t \in Gr(I)$, a contradiction. Thus $rI_g^2 = 0$. By the same argument above, we conclude that $sI_g^2 = tI_g^2 = 0$.

(3) Assume that $uvw \neq 0$ for some nonunits $u, v, w \in I_g$. Then $0 \neq uvw = (r+u)(s+v)(t+w) \in I$, by (1) and (2). Since $rs \notin I$, we conclude that $(t+w)$ is nonunit element of R_g . Since neither $rt \in I$ nor $st \in I$, we conclude that $r+u$ and $s+v$ are nonunit of R_g . As I is a graded weakly 1-absorbing primary ideal of R , we have $(r+u)(s+v) \in I$ or $s+w \in Gr(I)$. Since $u, v, w \in I_g \subseteq I$, we conclude that $rs \in I$ or $t \in Gr(I)$, a contradiction. Thus $I_g^3 = 0$. $\square$

Theorem 3.9. Let $R = \oplus_{g \in G} R_g$ be a G -graded ring, $I = \oplus_{g \in G} I_g$ be a graded weakly 1-absorbing primary ideal of R , which is not g -1-absorbing primary ideal of R for every $g \in G$. If For each $g \in G$, I admits a g -1-triple-zero $(r, s, t) \in (R_g)^3$ such that neither $rt \in I$ nor $st \in I$. Then $Gr(I) = Gr(0)$.

Proof. Suppose for every $g \in G$, there exists $(r, s, t) \in (R_g)^3$ which is a g -1-triple-zero of I such that neither $rt \in I$ nor $st \in I$. By Theorem 3.6 we have $I_g^3 = 0$ for every $g \in G$. Let $x \in Gr(I)$. For every $g \in G$, we have $x_g^3 = 0$, then $x_g \in Gr(0)$ and hence $x \in Gr(0)$. Thus $Gr(I) \subseteq Gr(0)$. Since $Gr(0) \subseteq Gr(I)$, we conclude that $Gr(I) = Gr(0)$. $\square$

Corollary 3.10. Let $R = \oplus_{g \in G} R_g$ be a G -graded reduced ring, $I = \oplus_{g \in G} I_g$ be a graded weakly 1-absorbing primary ideal of R wick is not g -1-absorbing primary ideal of R for every $g \in G$. If For each $g \in G$, I admits a g -1-triple-zero $(r, s, t) \in (R_g)^3$ such that neither $rt \in I$ nor $st \in I$. Then $I = 0$.

Proof. Since R is a graded reduced ring, we get $Gr(0) = 0$. Thus $Gr(I) = 0$ and $I = 0$. $\square$

Let R and R' be two G -graded rings, $\varphi : R \rightarrow R'$ be a G -graded ring homomorphism such that $\varphi(R_g) \subseteq R'_g$ for every $g \in G$. The following result is an analogue of [6] Theorem 17].

Theorem 3.11. Let R and R' be two G -graded rings and $\varphi : R \rightarrow R'$ be a G -graded ring homomorphism with $\varphi(1) = 1$. Then the following statements hold:

1. Suppose that φ is injective. Then if I' is graded weakly 1-absorbing primary ideal of R' , then $\varphi^{-1}(I')$ is a graded weakly 1-absorbing primary ideal of R .
2. If φ is a graded epimorphism and I is a graded weakly 1-absorbing primary ideal of R containing $\ker(\varphi)$, then $\varphi(I)$ is a graded weakly 1-absorbing primary ideal of R' .

Proof. (1) Suppose that I' is a graded weakly 1-absorbing primary ideal of R' and let r, s, t be nonunit homogeneous elements of $h(R)$ such that $0 \neq rst \in \varphi^{-1}(I')$. Since $\ker(\varphi) = 0$, then $0 \neq \varphi(rst) = \varphi(r)\varphi(s)\varphi(t) \in I'$. As $\varphi(r), \varphi(s), \varphi(t)$ are nonunit homogeneous elements of $h(R')$ and I' is a graded weakly 1-absorbing primary ideal of R' , we conclude that either $\varphi(r)\varphi(s) \in I$ or $\varphi(t) \in Gr(I')$, and hence either $rs \in \varphi^{-1}(I')$ or $t \in \varphi^{-1}(Gr(I')) = Gr(\varphi^{-1}(I'))$. Therefore $\varphi^{-1}(I')$ is a graded 1-absorbing primary ideal of R .

(2) Follows immediately from [8] Proposition 2.22]. $\square$

Theorem 3.12. Let R be a G -graded ring, $S \subseteq h(R)$ be a multiplicatively closed subset of R , and I be a proper graded ideal of R . Then the following statements hold:

1. If I is a graded 1-absorbing primary ideal of R such that $I \cap S = \emptyset$, then $S^{-1}I$ is a graded 1-absorbing primary ideal of a G -graded ring $S^{-1}R$.
2. If $S^{-1}I$ is a graded weakly 1-absorbing primary ideal of a G -graded ring $S^{-1}R$ and $S \cap G - Z_I(R) = \emptyset$ and $S \cap G - Z(R) = \emptyset$, then I is a graded weakly 1-absorbing primary ideal of R .

Proof. (1) Suppose that $0 \neq \frac{r_1}{s_1} \frac{r_2}{s_2} \frac{r_3}{s_3} \in S^{-1}I$ for some $\frac{r_1}{s_1}, \frac{r_2}{s_2}, \frac{r_3}{s_3}$ of $S^{-1}R$ as $S \cap G - Z(R) = \emptyset$. Then there exists $v \in S$ such that $0 \neq vr_1r_2r_3 \in I$. Since I is a graded weakly 1-absorbing primary ideal of R and $vr_1 \in h(R)$, then either $vr_1r_2 \in I$ or $r_3 \in Gr(I)$, then $\frac{vr_1r_2}{vs_1s_2} \in S^{-1}I$ or $\frac{r_3}{s_3} \in S^{-1}Gr(I) = Gr(S^{-1}I)$. Hence $S^{-1}I$ is a graded weakly 1-absorbing primary ideal of $S^{-1}R$.

(2) Assume that $0 \neq r_1r_2r_3 \in I$ for some nonunit homogeneous elements of R . Then $\frac{r_1}{1} \frac{r_2}{1} \frac{r_3}{1} \in S^{-1}I$. Since $S^{-1}I$ is a graded weakly 1-absorbing primary ideal of $S^{-1}R$, we deduce that either $\frac{r_1}{1} \frac{r_2}{1} \in S^{-1}I$ or $\frac{r_3}{1} \in G(S^{-1}I) = S^{-1}Gr(I)$. If $\frac{r_1}{1} \frac{r_2}{1} \in S^{-1}I$, then $vr_1r_2 \in I$ for some $v \in S$. Since $S \cap G - Z_I(R) = \emptyset$ and $v \in S$, we conclude that $r_1r_2 \in I$. If $\frac{r_3}{1} \in S^{-1}Gr(I)$, then $(tr_3)^n \in I$ for some $t \in S$ and some positive integer $n \geq 1$. The fact that $t \in S$ gives $t^n \notin G - Z_I(R)$ and hence $r_3^n \in I$. Thus $r_3 \in Gr(I)$. Therefore I is a graded weakly 1-absorbing primary ideal of R . $\square$

Definition 3.13. Let I be a graded weakly 1-absorbing ideal of a graded ring A . Let a, b, c be nonunit homogeneous elements of $h(A)$. We say that (a, b, c) is a 1-triple-zero of I , if $abc = 0$ but neither $ab \in I$ nor $c \in Gr(I)$.

Theorem 3.14. Let $R = \bigoplus_{g \in G} R_g$ be G -graded ring and $M = \bigoplus_{g \in G} M_g$ be a G -graded R -module. Let I be a graded ideal of R . Then the followings are equivalent:

1. $I(+)M$ is a graded weakly 1-absorbing primary of $R(+)M$;
2. I is a graded weakly 1-absorbing primary ideal of R and for 1-triple zero (a, b, c) nonunit homogeneous of R , we have $ab, bc, ac \in \text{ann}(M)$.

Proof. $\Rightarrow$. Assume that $I(+)M$ is graded weakly 1-absorbing primary, and let $0 \neq abc \in I$ for some nonunit homogeneous elements of R , then $0 \neq (a, 0)(b, 0)(c, 0) \in I(+)M$. Thus either $(a, 0)(b, 0) = (ab, 0) \in I(+)M$ or $(c, 0) \in Gr(I(+)M) = Gr(I)(+)M$. Thus either $ab \in I$ or $c \in Gr(I)$, that is, I is a graded weakly 1-absorbing primary ideal of R . Let $a, b, c \in H(R) \setminus U(R)$ with $abc = 0$, and neither $ab \in I$ nor $c \in Gr(I)$. Without loss the generality assume that $ab \notin \text{ann}(M)$, so there exists $e \in M$ such that $abe \neq 0$, since M is a graded R module, there exists $g \in G$ with $abe_g \neq 0$. Hence $0 \neq (a, 0)(b, 0)(c, e_g) = (0, abe_g) \in I(+)M$, the fact that $I(+)M$ is a graded weakly 1-absorbing gives that either $(ab, 0) \in I(+)M$ or $(c, e_g) \in Gr(I)(+)M$. Consequently, we obtain that either $ab \in I$ or $c \in Gr(I)$, a contradiction.

$\Leftarrow$. Let $(a, e), (b, f), (c, g)$ are nonunit homogeneous elements of $R(+)M$ with $(a, e)(b, f)(c, g) = (abc, abg + acf + bce) \in I(+)M$. If $abc \neq 0$, then I is a graded weakly 1-absorbing primary ideal of R . Then either $ab \in I$ or $c \in Gr(I)$. Thus we have either $(a, e)(b, f) \in I(+)M$ or $(c, g) \in Gr(I)(+)M = Gr(I(+)M)$. Now assume that $abc = 0$, if we have either $ab \in I$ or $c \in Gr(I)$ we are done, otherwise we have $ab, ac, bc \in \text{ann}(M)$ by assumption, then $(a, e)(b, f)(c, g) = (0, 0)$, a contradiction. Thus $I(+)M$ is a graded weakly 1-absorbing primary ideal of $R(+)M$. $\square$

Let $A = \bigoplus_{g \in G} A_g$ and $B = \bigoplus_{g \in G} B_g$ be two rings graded by an arbitrary group G . Also, let $J = \bigoplus_{g \in G} J_g$ be a graded ideal of B and let $f : A \longrightarrow B$ be a graded ring homomorphism. Then

$$R := A \bowtie^f J := \{(a, f(a) + j) / a \in A, j \in J\}$$

called amalgamation of A with B along J respect to f , see [10], [11]. Therefore, according to [13], $R = \bigoplus_{g \in G} R_g$ is a graded ring, with $h(R) = \bigcup_{\alpha \in \Gamma} R_\alpha$, where for every $g \in G$,

$$R_g = (A \bowtie^f J)_g = \{(a_g, f(a_g) + j_g) / a_g \in A, j_g \in J\}.$$

Also, note that the set $h(R) = \bigcup_{g \in G} R_g$ is the homogeneous element of the graded ring $R := A \bowtie^f J$. This construction, first introduced and studied in [13, 14], allows us to meet the challenges posed by providing rich examples that enrich the current literature of graded ring theory. One of the key tools for studying $A \bowtie^f J$ is based on the fact that the graded amalgamation can be studied in the frame of the pullback constructions [14 Section 3]. Other classical constructions, such as the graded amalgamated duplication of a ring along an ideal denoted by $A \bowtie I$ and the graded trivial ring extension of A by E [21] ($A \ltimes E$), can be interpreted as a particular cases of the general graded amalgamation construction [13 Examples 3.3 & 3.4].

Lemma 3.15. Let $A = \bigoplus_{g \in G} A_g$ and $B = \bigoplus_{g \in G} B_g$ be two rings graded by an arbitrary group G . Let $J = \bigoplus_{g \in G} J_g$ be a graded ideal of B and let $f : A \longrightarrow B$ be a graded ring homomorphism. Let K be a graded ideal of $A \bowtie^f J$ which contains $0 \times J$. Then $Gr(K) = Gr(I) \bowtie^f J$, for a graded ideal

$$I := \{a \in A : (a, f(a) + j) \in K \text{ for some } j \in J\}.$$

Proof. Note that I is clearly an ideal of A . Now, we will show that I is a graded ideal of A . Take $a = \sum_{g \in G} a_g$ for $a_g \in A_g$. Then there exists $j \in J$ such that $(a, f(a) + j) \in K$. Since $(a, f(a) + j) = \sum_{g \in G} (a_g, f(a_g) + j_g)$ and K is a graded ideal of $A \bowtie^f J$, we have $(a_g, f(a_g) + j_g) \in K$ for all $g \in G$. This implies $a_g \in I$ for all $g \in G$. Hence I is a graded ideal of A . Now, take $(a, f(a) + j) \in Gr(K)$. Then for all $g \in G$ there exists $n_g > 0$ such that $(a_g, f(a_g) + j_g)^{n_g} = (a_g^{n_g}, f(a_g^{n_g}) + \sum_{k=0}^{n_g-1} \binom{n_g}{k} f(a_g^k) j_g^{n_g-k})$. By definition of I , we get $a_g^{n_g} \in I$ and this yields $a \in Gr(I)$. Consequently, we have $(a, f(a) + j) \in Gr(I) \bowtie^f J$.

Conversely, assume $(a, f(a) + j) \in Gr(I) \bowtie^f J$ for some $a \in A$ and $j \in J$. Since $0 \times J \subseteq K \subseteq Gr(K)$, it is sufficient to show that $(a, f(a)) \in Gr(K)$. As $a \in Gr(I)$, then for all $g \in G$, there exists $n_g > 0$ such

that $a_g^{n_g} \in I$. Then we get $(a_g^{n_g}, f(a_g^{n_g}) + j') \in K$ for some $j' \in J$. Moreover, $(a_g^{n_g}, f(a_g^{n_g})) = (a_g, f(a_g))^{n_g} \in Gr(K)$ and this yields $(a_g, f(a_g)) \in Gr(Gr(K)) = Gr(K)$. Hence, we conclude that $(a, f(a)) \in Gr(K)$, which completes the proof. $\square$

Corollary 3.16. Let $A = \bigoplus_{g \in G} A_g$ and $B = \bigoplus_{g \in G} B_g$ be two rings graded by an arbitrary group G . Let $J = \bigoplus_{g \in G} J_g$ be a graded ideal of B and let $f : A \rightarrow B$ be a graded ring homomorphism. Let I be a graded ideal of A . Then $Gr(I \bowtie^f J) = Gr(I) \bowtie^f J$.

Proof. It follows from Lemma 3.15 since $I \bowtie^f J$ is a graded ideal of $A \bowtie^f J$ such that $0 \times J \subseteq I \bowtie^f J$. $\square$

Theorem 3.17. Let A and B be two rings graded by an arbitrary group G . Let J a graded ideal of B and let $f : A \rightarrow B$ be a graded ring homomorphism. Let I be a proper ideal of A . Then the following statements hold:

1. If $I \bowtie^f J$ is a graded weakly 1-absorbing primary not a graded 1-absorbing primary ideal of $A \bowtie^f J$, then I is a graded weakly 1-absorbing primary not a graded 1-absorbing primary ideal of A .
2. If I is a graded weakly 1-absorbing primary not a graded weakly 1-absorbing primary ideal of A and for every 1-triple-zero (a, b, c) nonunit homogeneous elements, we have $f(a)f(b)J = f(a)f(c)J = f(b)f(c)J = 0$ and $J^3 = 0$. Then $I \bowtie^f J$ is a graded weakly 1-absorbing primary which is not a graded 1-absorbing primary ideal of $A \bowtie^f J$.

Proof. (1) Assume that $I \bowtie^f J$ is a graded weakly 1-absorbing primary not graded 1-absorbing primary ideal of $A \bowtie^f J$. Let $0 \neq abc \in I$ for some nonunit homogeneous elements $a, b, c \in h(A)$. Then $(0, 0) \neq (a, f(a))(b, f(b))(c, f(c)) \in I \bowtie^f J$. Since f is a graded homomorphism of graded rings, we have $(a, f(a)), (b, f(b))$ and $(c, f(c))$ are nonunit homogeneous elements of $A \bowtie^f J$. By assumption, we get either $(a, f(a))(b, f(b)) \in I \bowtie^f J$ or $(c, f(c)) \in Gr(I \bowtie^f J)$. By the Lemma 3.15 we have either $ab \in I$ or $c \in Gr(I)$. Hence I is a graded weakly 1-absorbing primary ideal of A . By [15, Theorem 2.18], I is not a graded 1-absorbing primary ideal. Thus I is a graded weakly 1-absorbing primary ideal which is not a graded 1-absorbing primary ideal of a graded ring A . Then there exists a 1-triple-zero $(r, s, t) \in h(A)^3$ of I , that is, $rst = 0$ but neither $rs \in I$ nor $t \in Gr(I)$. Without loss the generality we can assume that $0 \neq f(r)f(s)J$. Then $f(r)f(s)j_g \neq 0$ for some homogeneous element j_g of J . Thus $0 \neq (r, f(r))(s, f(s))(t, f(t) + j_g) = (0, f(r)f(t)j_g) \in I \times J_g \subseteq I \bowtie^f J$, which implies either $rs \in I$ or $t \in Gr(I)$, a contradiction. Hence $f(r)f(s)J = f(r)f(t)J = f(s)f(t)J = 0$.

(2) Let $0 \neq (a, f(a) + j)(b, f(b) + k)(c, f(c) + l) \in I \bowtie^f J$ for some nonunit homogeneous elements $(a, f(a) + j), (b, f(b) + k), (c, f(c) + l)$ of $h(A \bowtie^f J)$. It is clear that $a, b, c \in h(A)$ are nonunit homogeneous elements of A . Let $0 \neq abc$. By assumption we get either $ab \in I$ or $c \in Gr(I)$, which implies $(a, f(a) + j)(b, f(b) + k) \in I \bowtie^f J$ or $(c, f(c) + l) \in Gr(I \bowtie^f J) = Gr(I \bowtie^f J)$. Then $I \bowtie^f J$ is graded weakly 1-absorbing primary ideal of $A \bowtie^f J$. We can assume that $abc = 0$. By the way of contradiction, suppose that neither $(a, f(a) + j)(b, f(b) + k) \in I \bowtie^f J$ nor $(c, f(c) + l) \in Gr(I \bowtie^f J)$. We have necessarily ab is not in I and c is not in $Gr(I)$. Thus (a, b, c) is a 1-triple-zero of I . Then $f(a)f(b)J = f(a)f(c)J = f(b)f(c)J = 0$ by assumption. We conclude that $(a, f(a) + j)(b, f(b) + k)(c, f(c) + l) = (0, jkl) = (0, 0)$. Since $J^3 = 0$, we deduce $jkl = 0$, and hence $(a, f(a) + j)(b, f(b) + k)(c, f(c) + l) = (0, 0)$, a contradiction. On the other hand, I is not a graded 1-absorbing primary ideal of A , then by [13, Theorem 3.5(2)], we have $I \bowtie^f J$ is not a graded 1-absorbing primary ideal. This completes the proof. $\square$

Corollary 3.18. Let $A = \bigoplus_{g \in G} A_g$ be a graded ring and $I = \bigoplus_{g \in G} I_g$ be a graded proper ideal of A . Let K be a proper graded ideal of A . Then the followings are equivalent:

1. If $K \bowtie I$ is a graded weakly 1-absorbing primary which is not graded-1-absorbing primary ideal of $A \bowtie I$, then K is graded weakly 1-absorbing primary which is a not graded 1-absorbing primary ideal of A ;
2. If K is a graded weakly 1-absorbing primary which is not graded weakly 1-absorbing primary ideal of A and for every 1-triple-zero (a, b, c) nonunit homogeneous elements, we have $ab, ac, bc \in \text{ann}(I)0$ and $I^3 = 0$. Then $K \bowtie^f I$ is a graded weakly 1-absorbing primary which is not graded 1-absorbing primary ideal of $A \bowtie I$.

Conflicts of Interest: The authors declare no conflict of interest.

References

- [1] M. T. Ahmed, M. Issoual and N. Mahdou, *Graded (m, n) -closed and graded weakly (m, n) -closed ideals*, Moroccan Journal of algebra and Geometry with applications, 1(2) (2022), 392–401.
- [2] K. Al-Zoubi and N. Sharafat, *On graded 2-absorbing primary and graded weakly 2-absorbing primary ideals*, J. Korean Math. Soc., 54(2) (2017), 675–684.
- [3] D. D. Anderson and M. Winderes, *Idealisation of a module*, J. Comm. Algebra, 1(1) (2009), 3–56.
- [4] S. E. Atani, *On Graded Weakly Prime Ideals*, Turkish J. Math., 30 (2006), 351–358.
- [5] A. Assarrar and N. Mahdou, *On graded-coherent like properties of commutative graded rings: a survey*, Moroccan Journal of algebra and Geometry with applications, 3(2) (2024), 288–320.
- [6] A. Badawi and E. Y. Celikel, *On 1-absorbing primary ideals of a commutative ring*, J. Algebra Appl., 19(06) (2020), 2050111.
- [7] A. Badawi and E. Y. Celikel, *On weakly 1-absorbing primary ideals of a commutative ring*, Algebra Colloquium, 29(2) (2022), 189–202.
- [8] M. Bataineh and R. Abu-Dawwas, *Graded weakly 1-absorbing primary ideals*, Demonstr. Math., 56(1) (2023), 20220214.
- [9] A. Y. Darani, *Graded primal submodules of graded modules*, J. Korean Math. Soc., 48(5) (2011), 927–938.
- [10] M. D’Anna, C. A. Finocchiaro and M. Fontana, *Amalgamated algebras along an ideal*. Comm. Algebra and Applications, Walter de Gruyter, Berlin, (2009), 155–172.
- [11] A. El Khalfi, H. Kim and N. Mahdou, *Amalgamation extension in commutative ring theory, a survey*, Moroccan Journal of algebra and Geometry with applications, 1(1) (2022), 139–182.
- [12] M. Issoual, *Graded 1-absorbing prime ideals on graded commutative rings*, J. Algebra Appl, 22(3) (2023), 2350058.
- [13] F. Z. Guissi, H. Kim and N. Mahdou, *Graded amalgamated algebras along an ideal*, J. Algebra Appl., 23(6) (2024), 2450116.
- [14] F. Z. Guissi, H. Kim and N. Mahdou, *The structure of prime homogeneous ideals in graded amalgamated algebra along an ideal*, J. Algebra Appl., DOI: 10.1142/S0219498825501063.

- [15] F. Z. Guissi, N. Mahdou and M. A. Salam Moutui, *Graded Amalgamated Algebras Along an Ideal Defined by Graded 1-Absorbing-Like Conditions*, J. Algebra Appl., DOI: 10.1142/S0219498825503098.
- [16] S. R. Naghani and H. F. Moghimi, *On graded 2-absorbing and graded weakly 2-absorbing ideals of a commutative ring*, Çankaya univ. j. sci. eng., 13 (2016), 11–17.
- [17] C. Nastassecu and F. Oystaeyen, *Graded Ring Theory*, Mathematical Library 28, Amesterdam: North Holland publishing company, (1982).
- [18] C. Nastassecu and F. Oystaeyen, *Methods of Graded Rings*, LNM 1836, Berlin-Heidelberg, Springer-Verlag, 2004.
- [19] K. H. Oral, U. Tekir and A. Agargun, *On graded prime and primary submodules*, Turkish J. Math., 35 (2011), 159–167.
- [20] M. Refai and K. AL-Zoubi, *On graded primary ideals*, Turkish J. Math., 28 (2004), 217–229.
- [21] R. N. Uregen , U. Tekir, K. P. Shum and S. Koc, *On graded 2-absorbing quasi primary ideals*, Southeast Asian Bull. Math., 43(4) (2019), 601–613.



ISSN: 2820-7114

Moroccan Journal of Algebra and Geometry with Applications

Supported by Sidi Mohamed Ben Abdellah University, Fez, Morocco

Volume 4, Issue 2 (2025), pp 168-175

Title :

On $\sum$ -nil-good rings

Author(s):

Moutu Abdou Salam Moutui

On Σ -nil-good rings

Moutu Abdou Salam Moutui

Department of Mathematics and Statistics St. Francis Xavier University Antigonish,
Nova Scotia, Canada B2G 2W5.
e-mail: amoutu@stfx.ca

Communicated by Hwankoo Kim

(Received 30 June 2024, Revised 10 January 2025, Accepted 22 January 2025)

Abstract. In this paper, we introduce a new concept of ring called Σ -nil-good ring as a generalization of the notion of nil-good ring, in the context of commutative rings. We study some basic properties of this ring. We investigate this notion to various context of commutative ring extensions such as homomorphic image, direct product, power series ring and amalgamation ring, with application on the transfer of this property to trivial ring extension. Our goal is to generate a new original class of rings satisfying the above property.

Key Words: Σ -nil-good, nil-good, 2-nil-good, homomorphic image, direct product, amalgamation, trivial ring extension.

2020 MSC: Primary 13F05, 13A15, 13E05, 13F20, 13C10, 13C11, 13F30, 13D05.

1 Introduction

Throughout the whole paper, all rings considered are commutative with unity and all modules are unital. In [32], Vámos introduced the concept of 2-good ring which is a ring for which any element can be written as a sum of two units. He showed that the endomorphism ring of a free module of rank at least 2 is 3-good and that every ring can be embedded in a 2-good ring. Answering a question of Skornjakov, he showed that a (right) self-injective von Neumann regular ring is 2-good provided it has no 2-torsion. This generalizes a result of Zelinsky's on the ring of linear transformations of a vector space. A significant work has been done on generalizations of 2-good rings. A more general concept of 2-good ring is the notion of k -good ring which is a ring for which any element can be written as a sum of k units. In [10], the authors defined a new class of unital rings called nil-good ring, as a ring for which each of its elements can be written as sum $u + b$ where u is a unit or equal 0 and b is a nilpotent. Also, the authors studied the structure as well as the behavior of this property with respect to subrings, matrix extensions and direct products. Later, in [1], a ring R is defined to be 2-nil-good if every element in R is the sum of two units and a nilpotent. Fundamental properties of such rings are obtained. Among other things, the authors proved that every strongly π -regular ring is 2-nil-good if and only if the identity is the sum of two units. One of the main results of their paper is that every square matrix ring over J -fine rings is 2-nil-good. Also, they established the 2-nil-good property for Morita contexts. This implies, in particular, that every matrix ring over a 2-nil-good ring is 2-nil-good. In [4], the authors introduced new classes of rings, namely, n^* -nil clean ring, Σ -nil clean ring and BB-ring, and they studied the behavior of the above notions to several commutative ring extensions such as homomorphic image, direct product, power series ring and amalgamation ring, with applications to the transfer of these properties in trivial ring extension. Motivated by these studies on generalizations of k -good rings, we introduce a new class of rings. We call a ring R to be Σ -nil-good if for every element x of R , there is an integer $n \geq 1$ such that x can be written as a sum of n units and a nilpotent element. We study some basic properties of these rings and establish

several characterizations. In this paper, we deal with a new concept of ring called Σ -nil-good ring as a generalization of the notion of nil-good ring, in the context of commutative rings. We study some basic properties of this ring. We investigate this notion to various context of commutative ring extensions such as homomorphic image, direct product, power series ring and amalgamation ring, with application to the transfer of this property to trivial ring extension. Our goal is to generate a new original class of rings satisfying the above property.

Let (A, B) be a pair of rings, $f : A \rightarrow B$ be a ring homomorphism and J be an ideal of B . In this setting, we can consider the following subring of $A \times B$: $A \bowtie^f J := \{(a, f(a) + j) \mid a \in A, j \in J\}$, called *the amalgamation of A and B along J with respect to f* , introduced and studied by D'Anna, Finocchiaro and Fontana in [12, 13]. In particular, they have studied amalgamations in the frame of pullbacks which allowed them to establish numerous (prime) ideal and ring-theoretic basic properties for this new construction. This construction is a generalization of *the amalgamated duplication of a ring along an ideal* (introduced and studied by D'Anna and Fontana in [14] and [15]). The interest of amalgamation resides, partly, in its ability to cover several basic constructions in commutative algebra, including pullbacks and trivial ring extensions (also called Nagata's idealizations) (cf. [29, page 2]). For example, constructions such as the $A + XB[X]$, the $A + XB[[X]]$ and the $D + M$ constructions can be studied as particular cases of the amalgamation ([12, Examples 2.5 and 2.6]) and other classical constructions, such as the CPI extensions (in the sense of Boisen and Sheldon [6]) are strictly related to it ([12, Example 2.7 and Remark 2.8]). In [12], the authors studied the basic properties of this construction (e.g., characterizations for $A \bowtie^f J$ to be a Noetherian ring, an integral domain, a reduced ring) and they characterized those distinguished pullbacks that can be expressed as an amalgamation. Moreover, in [13], they pursued the investigation on the structure of the rings of the form $A \bowtie^f J$, with particular attention to the prime spectrum, to the chain properties and to the Krull dimension.

Let A be a ring and E an A -module. The trivial ring extension of A by E (also called idealization of E over A) is the ring $R := A \ltimes E$ whose underlying group is $A \times E$ with multiplication given by $(a, e)(a', e') = (aa', ae' + ea')$. Trivial ring extensions have been studied extensively; and considerable work, part of is summarized in Glaz's book [18] and Huckaba's book [23], has been concerned with these extensions. Mainly, trivial ring extensions have been useful for solving many open problems and conjectures in both commutative and non-commutative ring theory. See for instance [2, 23].

For a ring R , we denote respectively by $\text{Nilp}(R)$, $\text{Idem}(R)$, $\text{Jac}(R)$, $U(R)$ and $\text{Char}(R)$, the ideal of all nilpotent elements of R , the set of all idempotent elements of R , the Jacobson radical of R , the multiplicative group of units of R and the characteristic of R .

2 On Σ -nil-good rings

We begin this section by recalling the notion of Σ -nil-good ring defined in the introduction.

Definition 2.1.

Let R be a ring. An element x of R is said to be Σ -nil-good if there exists a positive integer $n \geq 1$ such that $x = u_1 + u_2 + \cdots + u_n + w$ with $u_1, u_2, \dots, u_n \in U(R)$ and $w \in \text{Nilp}(R)$. Then R is said to be Σ -nil-good if each of its elements is Σ -nil-good.

Example 2.2. 1. Every n -good ring is Σ -nil-good.

2. Every 2-nil-good ring is Σ -nil-good.

It is worthwhile noting from the definition that a 2-nil-good ring is Σ -nil-good. However, a Σ -nil-good ring need not be 2-nil-good, as shown in the following example:

Example 2.3. Let $R := \mathbb{Z}_6$ be the ring of integers modulo 6. Then:

1. R is Σ -nil-good.

2. R is not 2-nil-good.

Proof. (1) Notice first that $0 = 1 - 1$ and $1 = 1 + 0$ are Σ -nil-good elements of R . Since every element of $n \in \mathbb{Z}_6$ with $n \geq 2$, can be written as $n = \underbrace{1 + 1 + \cdots + 1}_{n \text{ times}}$, then R is Σ -nil-good.

(2) R is not 2-nil-good since 5 can not be expressed as a sum of two unit elements and a nilpotent element. $\square$

Recall that a ring R has unit stable range one if $\forall a \in R$, there is $u \in U(R)$ such that $a + u.1 \in U(R)$.

Proposition 2.4. *Let R be a ring. Then the following assertions hold:*

1. *If R is Σ -nil-good, then there exists a positive integer $n \geq 1$ such that $1 = v_1 + \cdots + v_n$ with $v_i \in U(R)$ for $i = 1, \dots, n$.*

2. *Assume that R has unit stable range one with $1 = u_1 + \cdots + u_n$ and $u_i \in U(R)$ for all $i = 1, \dots, n$. Then R is Σ -nil-good.*

Proof. (1) Assume that R is Σ -nil-good. Then there exist $u_1, u_2, \dots, u_n \in U(R)$ and $w \in \text{Nilp}(R)$ such that $1 = u_1 + u_2 + \cdots + u_n + w$. So, $1 - w = u_1 + u_2 + \cdots + u_n$. Since $w \in \text{Nilp}(R) \subseteq \text{Jac}(R)$, $(1 - w) \in U(R)$ and so it follows that $1 = (1 - w)^{-1}u_1 + (1 - w)^{-1}u_2 + \cdots + (1 - w)^{-1}u_n$. One can easily check that $(1 - w)^{-1}u_i \in U(R)$ for every $i = 1, 2, \dots, n$. Hence, there exist $v_1, \dots, v_n \in U(R)$ such that $1 = v_1 + \cdots + v_n$, as desired.

(2) Assume that R is unit stable range one with $1 = v_1 + \cdots + v_n$ with $v_i \in U(R)$ for all $i = 1, \dots, n$. We claim that R is Σ -nil-good. Indeed, let $a \in R$. Then there exists $u \in U(R)$ such that $a + 1.u \in U(R)$ (as R is unit stable range one). So, $a + (v_1 + \cdots + v_n)u = y \in U(R)$. Since $uv_i \in U(R)$ for every $i = 1, \dots, n$, it follows that $a = v_1u + \cdots + v_nu + y$, which is a sum of $(n + 1)$ units. Hence, R is Σ -nil-good, as desired. $\square$

Recall that a ring R is UU (i.e., every unit is unipotent) if every unit $u \in R$ is unipotent, that is, u can be expressed as $u = 1 + w$ for some nilpotent element w of R . In the next proposition, we show that in a UU -ring R containing the field of rational numbers $\mathbb{Q}$, the properties " Σ -nil-good" and "nil-good" collapse.

Proposition 2.5. *Let R be a UU -ring such that $\mathbb{Q} \subseteq R$. Then R is Σ -nil-good if and only if R is nil-good.*

Proof. Assume that R is Σ -nil-good. Let $x \in R$. Then there exists $n \geq 1$ such that $x = u_1 + u_2 + \cdots + u_n + w$ with $u_i \in U(R)$ for every $i = 1, \dots, n$ and $w \in \text{Nilp}(R)$. Since R is a UU -ring, $u_i = 1 + w_i$ with $w_i \in \text{Nilp}(R)$ for every $i = 1, \dots, n$. So, $x = 1 + w_1 + 1 + w_2 + \cdots + 1 + w_n + w = n + (w_1 + w_2 + \cdots + w_n) + w$. Set $W = w_1 + w_2 + \cdots + w_n + w$. Clearly, $W \in \text{Nilp}(R)$ and $n \in R$. Therefore, $x = n + W$. Using the fact that $W \in \text{Nilp}(R)$ and n is a unit (as $\mathbb{Q} \subseteq R$), it follows that $n + W$ is a nil-good element. Hence, R is nil-good. The converse is trivial. $\square$

Recall that in [28], the author defined the concept of strongly Σ - m -clean rings, as a ring for which each of its elements can be expressed as a sum of n units for some positive integer $n \geq 1$ and an m -potent element. The following result shows that the class of Σ -nil-good rings is included in the class of strongly Σ - m -clean rings.

Proposition 2.6. *Every Σ -nil-good ring is a strongly Σ - m -clean ring for every positive integer $m \geq 2$. The converse holds if R is an integral domain.*

Proof. Consider a Σ -nil-good ring R . Let $x \in R$. Then there exists $n \geq 1$ such that $x = u_1 + u_2 + \cdots + u_n + w$ with $u_i \in U(R)$ for each $i = 1, \dots, n$ and $w \in Nilp(R)$. Observe that $u_n + w = u_n(1 + u_n^{-1}w) \in U(R)$, as $u_n^{-1}w \in Nilp(R)$. Therefore, $x = u_1 + u_2 + \cdots + u_{n-1} + v$ with $v = u_n + w \in U(R)$. Hence, $x = u_1 + u_2 + \cdots + u_{n-1} + v + 0$ is a strongly Σ -m-clean element. Thus, R is strongly Σ -m-clean.

Conversely, assume that R is a strongly Σ -m-clean domain. Let $x \in R$. Then there exists $n \geq 1$ such that $x = u_1 + u_2 + \cdots + u_n + f$ for some $u_1, u_2, \dots, u_n \in U(R)$ and f is an m -potent element of R with $m \geq 2$. Since $f^m = f$, then $f^m - f = f(f^{m-1} - 1) = 0$. Two cases are then possible:

Case 1 : $f = 0$, then $x = u_1 + u_2 + \cdots + u_n$ which is a sum of n units and so x is an n -good element.

Case 2 : $f^{m-1} - 1 = 0$. Then $f^{m-1} = f f^{m-2} = 1$. Therefore, f is a unit of R and so $x = u_1 + u_2 + \cdots + u_n + f$ is a sum of $(n+1)$ units. Consequently, x is an $(n+1)$ -good element.

Hence, in all cases, it follows that x is a Σ -nil-good element, making R , a Σ -nil-good ring. $\square$

Proposition 2.7.

(1) Let A be a ring and I be an ideal of A . If A is Σ -nil-good, then so is A/I . The converse holds if I is a nil ideal of A .

(2) Let I be a finite index set. If $A = \prod_{\alpha \in I} A_\alpha$ is Σ -nil-good, then so is $A_\alpha \forall \alpha \in I$.

Proof. (1) If A is Σ -nil-good, then we claim that so is A/I . Indeed, this is due to the fact that any homomorphic image of a nilpotent (resp., unit) element is also a nilpotent (resp., unit) element.

Conversely, assume that A/I is Σ -nil-good and I is a nil ideal of A . We claim that A is Σ -nil-good. Let $a \in A$ such that $\bar{a} \in A/I$. Then there exists $n \geq 1$ such that $\bar{a} = \bar{u}_1 + \cdots + \bar{u}_n + \bar{b} = (u_1 + \cdots + u_n + I) + b + I = (u_1 + \cdots + u_n + b + I)$ with $\bar{b} \in Nilp(A/I)$ and $\bar{u}_i \in U(A/I)$ for every $i = 1, \dots, n$. Therefore, $a = u_1 + \cdots + u_n + b + b_1$, with $b_1 \in I$. Since $I \subseteq Nilp(A)$, then $b \in Nilp(A)$. The fact that I is nil ideal implies that $I \subseteq Jac(A)$ and so $u_i \in U(A)$ for every $i = 1, \dots, n$. Consequently, there exists $n \geq 1$ such that $a = u_1 + \cdots + u_n + w$ with $u_i \in U(A)$ for every $i = 1, \dots, n$ and $w \in Nilp(A)$. Hence, a is Σ -nil-good, making A , a Σ -nil-good ring.

(2) Assume that $A = \prod_{\alpha \in I} A_\alpha$ is a Σ -nil-good ring. Then by assertion (1) above, so is $A_\alpha \forall \alpha \in I$ (as $\forall \alpha \in I$, A_α is the homomorphic image of A under the canonical projection over A_α). $\square$

The next proposition examines the Σ -nil-good property in the formal power series ring $R[[X]]$.

Proposition 2.8. Let R be a ring. Then $R[[X]]$ is Σ -nil-good if and only if so is R .

Proof. Assume that $R[[X]]$ is Σ -nil-good. Then by assertion (1) of Proposition 2.7, $R[[X]]/X \simeq R$ is Σ -nil-good.

Conversely, assume that R is Σ -nil-good. Let $P \in R[[X]]$. We need to show that P is a Σ -nil-good element. We have $P = \sum_{i=0}^{\infty} a_i X^i$ where $a_i \in R$ for $i = 0, 1, 2, \dots$ and so $a_0 \in R$ which is a Σ -nil-good ring. So, there exists $n \geq 1$ such that $a_0 = u_1 + u_2 + \cdots + u_n + w$ such that $u_i \in U(R)$ for $i = 1, \dots, n$ and $w \in Nilp(R)$. Therefore, $P = u_1 + \sum_{i=1}^{\infty} a_i X^i + u_2 + \cdots + u_n + w$. Since $u_1 + \sum_{i=1}^{\infty} a_i X^i$ is a unit of $R[[X]]$ and $w \in Nilp(R) \subseteq Nilp(R[[X]])$, it follows that P is Σ -nil-good, making $R[[X]]$, a Σ -nil-good ring, as desired. $\square$

The next result establishes the transfer of Σ -nil-good ring property to amalgamation ring.

Theorem 2.9. Let $f : A \rightarrow B$ be a ring homomorphism and J be an ideal of B . Then the following statements hold:

1. If $A \bowtie^f J$ is Σ -nil-good, then so are A and $f(A) + J$.
2. Assume that $J \subseteq Nilp(B)$. Then $A \bowtie^f J$ is Σ -nil-good if and only if so is A .
3. Assume that $\forall a \in U(A)$, $f(a) + j \in U(f(A) + J)$. Then $A \bowtie^f J$ is Σ -nil-good if and only if so is A and $\forall x \in J$, $x = l + h$ for some $l \in J \cap Jac(B)$ and $h \in J \cap Nilp(B)$.

Proof. (1) Assume that $A \bowtie^f J$ is Σ -nil-good. By [12] Proposition 5.1], A and $f(A)+J$ are homomorphic images of $A \bowtie^f J$, and so by Proposition 2.7(1), we obtain the desired result.

(2) If $A \bowtie^f J$ is Σ -nil-good, then by assertion (1) above, so is A .

Conversely, assume that A is Σ -nil-good. We claim that $A \bowtie^f J$ is Σ -nil-good. Indeed, let $(a, f(a)+j) \in A \bowtie^f J$. Clearly, $a \in A$ which is Σ -nil-good. So, there exists $n \geq 1$ such that $a = u_1 + \dots + u_n + w$ with $u_i \in U(A)$ for each $i = 1, \dots, n$ and $w \in Nilp(A)$. Therefore, $(a, f(a)+j) = (u_1, f(u_1)) + \dots + (u_n, f(u_n)) + (w, f(w)+j)$ with $(u_i, f(u_i)) \in U(A \bowtie^f J)$ for each $i = 1, \dots, n$ and from [8] Lemma 2.10], $(w, f(w)+j) \in Nilp(A \bowtie^f J)$ as $w \in Nilp(A)$ and $j \in Nilp(B) \cap J$. Hence, $(a, f(a)+j)$ is a Σ -nil-good element, making $A \bowtie^f J$, a Σ -nil-good ring.

(3) If $A \bowtie^f J$ is Σ -nil-good, then by assertion (1) above, so is A . Let $x \in J$. Then $(0, x) \in A \bowtie^f J$ which is Σ -nil-good. So, there exists $n \geq 1$ such that $(0, x) = \sum_{i=1}^n (u_i, f(u_i) + l_i) + (w, f(w) + h)$, with $(w, f(w)+h) \in Nilp(A \bowtie^f J)$ and $(u_i, f(u_i)+l_i) \in U(A \bowtie^f J)$ for each $i = 1, 2, \dots, n$. Therefore, $\sum_{i=1}^n u_i + w = 0$ and so $x = \sum_{i=1}^n l_i + h$, with $h \in Nilp(B) \cap J$ and $l_i \in J$ for each $i = 1, 2, \dots, n$. On the other hand, for each $i = 1, 2, \dots, n$, $(u_i, f(u_i)+l_i) \in U(A \bowtie^f J)$, then $f(u_i)+l_i \in U(f(A)+J)$. So, for each $i = 1, 2, \dots, n$, there exists $f(v_i)+\alpha_i \in f(A)+J$ such that $(f(u_i)+l_i)(f(v_i)+\alpha_i) = 1$. It follows that $l_i(f(v_i)+\alpha_i) = 1 - f(u_i)(f(v_i)+\alpha_i)$ and so $1 - l_i(f(v_i)+\alpha_i) = f(u_i)(f(v_i)+\alpha_i) \in U(B)$. Consequently, $l_i \in J \cap Jac(B)$ for each $i = 1, 2, \dots, n$. Set $l = \sum_{i=1}^n l_i$. Hence, $x = l + h$ with $l \in J \cap Jac(B)$ and $h \in J \cap Nilp(B)$.

Conversely, assume that A is Σ -nil-good and $\forall x \in J$, $x = l + h$ with $l \in J \cap Jac(B)$ and $h \in J \cap Nilp(B)$. Let $(a, f(a)+j) \in A \bowtie^f J$. Then $a \in A$ which is Σ -nil-good. So, there exists $n \geq 1$ such that $a = u_1 + u_2 + \dots + u_n + w$ with $u_i \in U(A)$ for each $i = 1, 2, \dots, n$ and $w \in Nilp(A)$. Therefore, $f(a) = f(u_1 + u_2 + \dots + u_n) + f(w) = f(u_1) + f(u_2) + \dots + f(u_n) + f(w)$ with $f(w) \in Nilp(B)$. Using the fact that $j \in J$, it follows that $j = l + h$ with $h \in J \cap Nilp(B)$ and $l \in J \cap Jac(B)$. Consequently, $(a, f(a)+j) = (u_1 + u_2 + \dots + u_n + w, f(u_1) + f(u_2) + \dots + f(u_n) + f(w) + l + h) = (u_1, f(u_1)+l) + (u_2, f(u_2)+l) + \dots + (u_n, f(u_n)+l) + (w, f(w)+h)$. One can easily check that $(u_i, f(u_i)+l) \in U(A \bowtie^f J)$ as $l \in J \cap Jac(A)$ and $(u_i, f(u_i)) \in U(A \bowtie^f J)$ for each $i = 2, \dots, n$. From [8] Lemma 2.10], it follows that $(w, f(w)+h) \in Nilp(A \bowtie^f J)$. Hence, $(a, f(a)+j)$ is a Σ -nil-good element of $A \bowtie^f J$, making $A \bowtie^f J$, a Σ -nil-good ring, as desired. $\square$

The next corollary is a consequence of assertion (2) of Theorem 2.9 on the transfer of Σ -nil-good property to trivial ring extension.

Corollary 2.10.

Let A be a ring, E be an A -module and $R := A \ltimes E$ be the trivial ring extension of A by E . Then R is Σ -nil-good if and only if so is A .

Proof. Consider $f : A \hookrightarrow R$ to be the injective ring homomorphism defined by $f(a) = (a, 0)$, for every $a \in A$ and let $J := 0 \ltimes E$ be an ideal of R . Clearly, $f^{-1}(J) = 0$. Therefore, by [12] Proposition 5.1 (3)], $f(A) + J = A \ltimes 0 + 0 \ltimes E = A \ltimes E = R \simeq A \bowtie^f J$. On the other hand, $J := 0 \ltimes E \subseteq Nilp(B)$ and so by an application to assertion (2) of Theorem 2.9, we have the desired result. $\square$

The following corollary is an immediate consequence of assertion (3) of Theorem 2.9.

Corollary 2.11. Let $f : A \rightarrow B$ be a ring homomorphism and J be an ideal of B such that $J \subseteq Jac(B)$. Then $A \bowtie^f J$ is Σ -nil-good if and only if so is A and $\forall x \in J$, $x = l + h$ for some $h \in J \cap Nilp(B)$ and $l \in J \cap Jac(B)$.

The following example illustrates Theorem 2.9 by providing a new class of Σ -nil-good rings which are not 2-nil-good.

Example 2.12. Let $A := \mathbb{Z}_6$ be the ring of integers modulo 6, E be an A -module, $B := A \ltimes E$ be the trivial ring extension of A by E . Consider the injective ring homomorphism $f : A \hookrightarrow B$ defined by $f(a) = (a, 0)$ for every $a \in A$ and let $J := 0 \ltimes E$ be an ideal of B . Then:

1. $A \bowtie^f J$ is Σ -nil-good.

2. $A \bowtie^f J$ is not 2-nil-good.

Proof. (1) By assertion (2) of Theorem 2.9, $A \bowtie^f J$ is Σ -nil-good since A is Σ -nil-good and $J \subseteq \text{Nilp}(B)$.
 (2) By Proposition 2.7(1), $A \bowtie^f J$ is not 2-nil-good since the homomorphic image A of $A \bowtie^f J$ is not 2-nil-good (as 5 can not be written as a sum of two unit elements and a nilpotent element). $\square$

As another application of Theorem 2.9 we generate a new original class of Σ -nil-good rings which are not 4-good.

Example 2.13. Let $A := \mathbb{Z}$, which is a Σ -nil-good ring, $B := \mathbb{Z}_4$ be the ring of integers modulo 4, $f : A \rightarrow B$ be the canonical surjection and $J := 2\mathbb{Z}_4$ is the maximal ideal of B . Then:

1. $A \bowtie^f J$ is Σ -nil-good.

2. $A \bowtie^f J$ is not a 4-good ring.

Proof. (1) Since A is a Σ -nil-good ring and $J^2 = 0 \subseteq \text{Nilp}(B)$, then by assertion (2) of Theorem 2.9, it follows that $A \bowtie^f J$ is Σ -nil-good.

(2) By [4] Proposition 4.3(1)], $A \bowtie^f J$ is not a 4-good ring since the homomorphic image A of $A \bowtie^f J$ is not a 4-good ring (as the element 6 can not be expressed as a sum of 4 units). $\square$

Acknowledgments. The author would like to express his sincere thanks to the referee for his/her helpful suggestions and comments.

References

- [1] M. S. Abdolyousefi, N. Ashrafi and H. Chen, *On 2-nil-good rings*, J. Algebra Appl. 17 (2018), no. 6, 1850110, 13 pp.
- [2] D. D. Anderson and M. Winders, *Idealization of a module*, J. Commut. Algebra (1)(2009), 3–56.
- [3] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, 1969.
- [4] C. Bakkari, M. Es-Saidi, N. Mahdou and M. A. S. Moutui, *On clean-like conditions in some commutative ring extensions*, accepted for publication, Indian Journal of Pure and Applied Mathematics, August 2024.
- [5] C. Bakkari, M. Es-saidi, N. Mahdou and M. A. S. Moutui, *Extensions of semiclean rings*, Czechoslovak Math. J. 72(147) (2022), no. 2, 461-476.
- [6] M. B. Boisen and P.B. Sheldon; *CPI-extension: Over rings of integral domains with special prime spectrum*, Canad. J. Math. 29 (1977), 722-737.
- [7] G. Calugareanu and T. Y. Lam, *Fine rings: a new class of simple rings*, J. Algebra Appl., 15 (2015), <http://dx.doi.org/10.1142/s0219498816501735>.
- [8] M. Chhiti, N. Mahdou and M. Tamekkante, *Clean property in amalgamated algebras along an ideal*, Hacet. J. Math. Stat. 44 (2015), no. 1, 41-49.
- [9] P. V. Danchev, W. Wm. McGovern, *Commutative weakly nil clean unital rings*, J. Algebra 425(2015), 410-422.
- [10] P. V. Danchev, *Nil-Good Unital Rings*, Int. J. Algebra, Vol. 10, (2016), no. 5, 239-252.

- [11] A. J. Diesl, *Nil clean rings*, J. Algebra 383 (2013), 197-211.
- [12] M. D'Anna, C. A. Finocchiaro and M. Fontana, *Amalgamated algebras along an ideal*, Comm Algebra and Applications, Walter De Gruyter (2009), 241-252.
- [13] M. D'Anna, C. A. Finocchiaro and M. Fontana, *Properties of chains of prime ideals in amalgamated algebras along an ideal*, J. Pure Appl. Algebra 214(2010), 1633-1641.
- [14] M. D'Anna and M. Fontana; *An amalgamated duplication of a ring along an ideal: the basic properties*, Journal of Algebra and its Applications, 6(3) (2007), 443-459.
- [15] M. D'Anna and M. Fontana; *The amalgamated duplication of a ring along a multiplicative canonical ideal*, Ark. Mat. 45(2) (2007), 241-252.
- [16] A. El Khalfi, H. Kim and N. Mahdou, *Amalgamation extension in commutative ring theory, a survey*, Moroccan Journal of Algebra and Geometry with Applications, Vol. 1(1) (2022), 139-182.
- [17] D.E. Fields, *Zero divisors and nilpotent elements in power series rings*, Proc. Amer. Math. Soc., 27 (1971), pp. 427-433.
- [18] S. Glaz, *Commutative coherent rings*, Lecture Notes in Mathematics, 1371 (1989), Springer-Verlag, Berlin, 3-540-51115-6.
- [19] A. B. Gorman and W. Y. Shiao, *Nil-good and nil-good clean matrix rings*, arXiv: 1512.04640v1 [math.RA], 2015.
- [20] H. K. Grover, Z. Wang, D. Khurana, J. Chen and T. Y. Lam, *Sums of units in rings*, J. Algebra Appl. 13 (2014), Article ID: 1350072, 10 pp.
- [21] Y. Hirano, H. Tominaga and A. Yaqub, *On rings in which every element is uniquely expressible as a sum of a nilpotent element and a certain potent element*, Math. J. Okayama Univ. 30(1988), 33-40.
- [22] Y. Hirano, H. Tominaga, *Rings in which every element is the sum of two idempotents*, Bull. Austral. Math. Soc. Vol. 30(1988), 161-164.
- [23] J. A. Huckaba, *Commutative rings with zero divisors*, Marcel Dekker, New York, 1988.
- [24] T. Koşan, Z. Wang and Y. Zhou, *Nil-clean and strongly nil-clean rings*, J. Pure Appl. Algebra 220 (2016), no. 2, 633-646.
- [25] N. Mahdou, A. Mimouni and M. A. S. Moutui, *On almost valuation and almost Bézout rings*, Commun. Algebra 43 (2015), 4534-4548.
- [26] N. Mahdou and M. A. S. Moutui, *Prüfer property in amalgamated algebras along an ideal*, Ric. Mat. 69 (2020), no. 1, 111-120.
- [27] A. Mimouni, *Note on UN-rings*, Moroccan Journal of Algebra and Geometry with Applications, Vol. 2(1) (2023), 154-161.
- [28] M. A. S. Moutui, *On strongly Σ - m -clean rings*, Indian J. Pure Appl. Math. 54 (2023), no. 3, 778-788.
- [29] M. Nagata, *Local Rings*, Interscience, New York, 1962.
- [30] S. Purkait, T. K. Dutta and S. Kar, *On m -clean and strongly m -clean rings*, Comm. Algebra, published online, (2019), DOI: 10.1080/00927872.2019.1640236.

- [31] S. Purkait, *On strongly m -clean ring and m -semiperfect ring*, Comm. Algebra, published online (2020), DOI: 10.1080/00927872.2020.1766055.
- [32] P. Vámos, *2-good rings*, The Quart. J. Math, 56, (2005), 417-430.



ISSN: 2820-7114

Moroccan Journal of Algebra and Geometry with Applications

Supported by Sidi Mohamed Ben Abdellah University, Fez, Morocco

Volume 4, Issue 2 (2025), pp 176-197

Title :

On ϕ -Gorenstein homological dimensions

Author(s):

Younes El Haddaoui, Hwankoo Kim & Najib Mahdou

On ϕ -Gorenstein homological dimensions

Younes El Haddaoui¹, Hwankoo Kim² and Najib Mahdou³

¹ Department of Mathematics, Faculty of Science and Technology, Fez, Morocco.

e-mail: younes.elhaddaoui@usmba.ac.ma

² Division of Computer Engineering, Hoseo University, Asan, Republic of Korea.

e-mail: hkkim@hoseo.edu

³ Department of Mathematics, Faculty of Science and Technology, Fez, Morocco.

e-mail: mahdou@hotmail.com

Communicated by Mohammed Tamekkante

(Received 20 November 2024, Revised 19 February 2025, Accepted 28 February 2025)

Abstract. The study of Gorenstein projective and injective modules has been a cornerstone in the field of Gorenstein homological algebra since these concepts were first introduced. This paper marks a significant advancement in the field by demonstrating the integration of ϕ -torsion theory into Gorenstein homological algebra. We take this exploration further by introducing and examining the novel concepts of nonnil-Gorenstein projective and injective modules. Our study also extends to the nonnil-Gorenstein projective and injective dimensions of a module, offering a deeper insight into their structure and implications. Furthermore, we delve into the concept of nonnil-Gorenstein global dimension of a ring, unveiling its significance and potential applications. A key application of these innovative concepts is their use in characterizing ϕ von Neumann regular rings. This approach not only adds a new dimension to our understanding of these rings but also highlights the versatility and depth of Gorenstein homological algebra.

Key Words: ϕ -torsion theory, ϕ -(weak) global dimension of rings, nonnil-Gorenstein global dimension of rings.

2020 MSC: 13A15, 13A18, 13F05, 13G05, 13C20.

Dedicated to our Professor David E. Dobbs for his 80th Birthday.

1 Introduction

We devote this introductory section to some conventions and a review of some standard background material. All rings considered in this paper are assumed to be commutative with non-zero identity and prime nilradical. We use $\text{Nil}(R)$ to denote the set of nilpotent elements of R , and $Z(R)$ to denote the set of zero-divisors of R . A ring with $\text{Nil}(R)$ being divided prime (i.e., $\text{Nil}(R) \subset xR$, for every $x \in R \setminus \text{Nil}(R)$) is called a ϕ -ring. Let $\mathcal{H}$ (resp., $\overline{\mathcal{H}}$) be the set of all rings with divided prime nilradical (resp., divided prime nilradical but not maximal). A ring R is called a strongly ϕ -ring if $R \in \mathcal{H}$ and $Z(R) = \text{Nil}(R)$.

Let R be a ring and M be an R -module. We define

$$\phi\text{-tor}(M) = \{x \in M \mid sx = 0 \text{ for some } s \in R \setminus \text{Nil}(R)\}.$$

If $\phi\text{-tor}(M) = M$, then M is called a ϕ -torsion module, and if $\phi\text{-tor}(M) = 0$, then M is called a ϕ -torsion-free module. An R -module M is said to be ϕ -uniformly torsion (ϕ -u-torsion for short) if $sM = 0$ for some $s \in R \setminus \text{Nil}(R)$. An ideal I of R is called nonnil if $I \not\subseteq \text{Nil}(R)$. A ring R is said to be self-injective if it is an injective module over itself; if, in addition, R is Noetherian, then R is said to be a quasi-Frobenius ring. As usual, we use $\text{pd}_R(M)$, $\text{id}_R(M)$, and $\text{fd}_R(M)$ to denote the classical

projective, injective, and flat dimension of M , respectively. For a Noetherian ring R , Auslander and Bridger [3] introduced the G -dimension, $\text{Gdim}_R(M)$, for every finitely generated R -module M . They showed that $\text{Gdim}_R(M) \leq \text{pd}_R(M)$ for every finitely generated R -module M , and equality holds if $\text{pd}_R(M)$ is finite. Several decades later, Enochs and Jenda [15, 16] introduced the notion of the Gorenstein projective dimension (G -projective dimension for short) as an extension of G -dimension to modules that are not necessarily finitely generated, and the Gorenstein injective dimension (G -injective dimension for short) as a dual notion of the Gorenstein projective dimension. To complete the analogy with the classical homological dimension, Enochs et al. [18] introduced the Gorenstein flat dimension. Some related references are [7, 12, 13, 15, 16, 18, 21, 22]. Recall from [15] that an R -module M is said to be Gorenstein projective (G -projective for short) if there exists an exact sequence of projective R -modules

$$\mathbf{P}: \quad \cdots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow P^0 \longrightarrow P^1 \longrightarrow \cdots$$

such that $M \cong \text{Im}(P_0 \rightarrow P^0)$ and such that the functor $\text{Hom}_R(-, Q)$ leaves $\mathbf{P}$ exact whenever Q is projective. The complex $\mathbf{P}$ is called a complete projective resolution. It is known that M is G -projective if and only if M has a complete projective resolution $\mathbf{P}$ such that $\text{Ext}_R^1(L, Q) = 0$ for any syzygy L of $\mathbf{P}$ and any module Q with finite projective dimension. The Gorenstein injective (G -injective for short) modules are defined dually.

On the other hand, in [32], Tang, Wang and Zhao introduced the class of ϕ -rings, called ϕ -von Neumann regular rings. An R -module M is said to be ϕ -flat if for every R -monomorphism $f: A \rightarrow B$ with $\text{Coker}(f)$ ϕ -torsion, $f \otimes 1: A \otimes_R M \rightarrow B \otimes_R M$ is an R -monomorphism [32, Definition 3.1]. An R -module M is ϕ -flat if and only if $M_{\mathfrak{p}}$ is ϕ -flat for every prime ideal $\mathfrak{p}$ of R , if and only if $M_{\mathfrak{m}}$ is ϕ -flat for every maximal ideal $\mathfrak{m}$ of R [32, Theorem 3.5]. A ϕ -ring R is called a ϕ -von Neumann regular ring if all R -modules are ϕ -flat. This is equivalent to stating that $R/\text{Nil}(R)$ is a von Neumann regular ring [32, Theorem 4.1].

The authors of [14] introduced and defined the ϕ -(weak) global dimension of rings with prime nilradical. An R -module P is said to be ϕ -u-projective if $\text{Ext}_R^1(P, N) = 0$ for each ϕ -u-torsion R -module N [14, Definition 3.1]. The ϕ -projective dimension of M over R , denoted by $\phi\text{-pd}_R M$, is defined to be at most n (where $n \geq 1$ and $n \in \mathbb{N}$) if either $M = 0$, or $M \neq 0$ and M is not ϕ -u-projective, and if it satisfies the condition $\text{Ext}_R^{n+1}(M, N) = 0$ for any ϕ -u-torsion module N . If n is the least non-negative integer for which $\text{Ext}_R^{n+1}(M, N) = 0$ for every ϕ -u-torsion module N , then we set $\phi\text{-pd}_R M = n$. If there is no such n , we set $\phi\text{-pd}_R M = \infty$. An R -module E is said to be nonnil injective if $\text{Ext}_R^1(R/I, E) = 0$ for all nonnil ideals of R . The ϕ -injective dimension of M over R , denoted by $\phi\text{-id}_R M$, is defined to be at most n (where $n \geq 1$ and $n \in \mathbb{N}$) if either $M = 0$, or $M \neq 0$ and M is not nonnil injective, and if it satisfies the condition $\text{Ext}_R^{n+1}(R/I, M) = 0$ for any nonnil ideal I of R . If n is the least non-negative integer for which $\text{Ext}_R^{n+1}(R/I, M) = 0$ for every nonnil ideal I of R , then we set $\phi\text{-id}_R M = n$. If there is no such n , we set $\phi\text{-id}_R M = \infty$, and we easily have that an R -module M of ϕ -injective dimension 0 if and only if it is nonnil injective. For a ring R , its ϕ -global dimension is either 0 or the supremum of all $\phi\text{-pd}_R(R/I)$, where I is a nonnil ideal of R such that R/I is not ϕ -u-projective. In particular, for a ring R of $Z(R) = \text{Nil}(R)$, its ϕ -global dimension is the supremum of $\phi\text{-pd}_R(R/I)$ for all nonnil ideals I of R .

In [2], Anderson and Badawi introduced the class of ϕ -rings called ϕ -Dedekind rings. A ϕ -ring R is said to be ϕ -Dedekind if $R/\text{Nil}(R)$ is a Dedekind domain.

This paper is divided into four sections, including the introduction. In Section 2, we define nonnil-Gorenstein projective modules, nonnil-Gorenstein injective modules and nonnil-Gorenstein flat. We then present some characterizations of these modules and establish that every nonnil-Gorenstein projective (resp., nonnil-Gorenstein injective) module is Gorenstein projective (resp., Gorenstein injective). We also provide examples of Gorenstein projective (resp., Gorenstein injective) modules that are not nonnil-Gorenstein projective (resp., nonnil-Gorenstein injective). The section concludes by establishing analogs of the well-known behavior, as demonstrated in [21, 2.5. Theorem], showing

more precisely that nonnil-Gorenstein projective (resp., nonnil-Gorenstein injective) R -modules are projectively (respectively, injectively) resolving.

In Section 3, we introduce analogs of Gorenstein projective and Gorenstein injective dimensions, termed nonnil-Gorenstein projective and injective dimensions.

The final section briefly defines the nonnil-Gorenstein global dimension of a ring R as the supremum of all $\phi\text{-Gpd}_R M$, where M is an R -module. We note that $G\text{-gl.dim}(R) \leq \phi\text{-G.gl.dim}(R)$ for all rings R . We characterize rings of nonnil-Gorenstein global dimension 0 as those in which every nonnil-injective module is projective, equivalent to every ϕ -u-projective module being nonnil-injective. We also show that ϕ -rings of nonnil-Gorenstein global dimension 0 are fields. In the second part of this section, we introduce the closed nonnil-Gorenstein global dimension of rings as the supremum of all nonnil-Gorenstein projective dimensions of ϕ -u-torsion modules. We establish that ϕ -von Neumann regular rings are strongly ϕ -rings of closed nonnil-Gorenstein global dimension 0, equivalent to von Neumann regular rings being strongly ϕ -rings where every ϕ -u-projective module is nonnil-injective.

To provide examples, we discuss the trivial extension. Let R be a ring and E be an R -module. The trivial ring extension of R by E , denoted $R \ltimes E$, has the additive structure of the external direct sum $R \oplus E$ and multiplication defined by $(a, e)(b, f) := (ab, af + be)$ for all $a, b \in R$ and $e, f \in E$. This construction is also known by other terminology and notations, such as the idealization $R(+E)$ (see [6, 19, 23, 24]).

For any undefined terminology and notation, readers are referred to [12, 17, 19, 23, 33].

2 On nonnil-Gorenstein projective, injective and flat modules

We start this section by defining two new classes of modules, which we call nonnil-Gorenstein projective and nonnil-Gorenstein injective. These two classes are sub-classes of Gorenstein projective and Gorenstein injective, respectively.

Definition 2.1. An R -module M is said to be nonnil-Gorenstein projective (nonnil-G-projective for short) if there exists a complete projective resolution of M , that is an exact sequence of R -modules

$$\mathcal{P}: \quad \cdots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow P^0 \longrightarrow P^1 \longrightarrow \cdots$$

in which all P_i, P^j are projective modules and $M \cong \text{Im}(P_0 \rightarrow P^0)$ and such that the functor $\text{Hom}_R(-, Q)$ leaves $\mathcal{P}$ exact whenever Q is a ϕ -u-projective module.

The nonnil-Gorenstein injective (nonnil-G-injective for short) modules are defined dually as follows: An R -module N is said to be nonnil-G-injective if there exists a complete injective resolution of N , that is

$$\mathcal{E}: \quad \cdots \longrightarrow E^1 \longrightarrow E^0 \longrightarrow E_0 \longrightarrow E_1 \longrightarrow \cdots$$

such that all E_i, E^j are injective modules and such that both $N \cong \text{Im}(E^0 \rightarrow E_0)$ and $\text{Hom}(Q, \mathcal{E})$ is a complex exact of R -modules for every nonnil-injective module Q .

Remark 2.2. 1. It is easy to see from [17, Definition 10.2.1] that every nonnil-G-projective module is Gorenstein projective, and so the projective dimension of every nonnil-G-projective module is either zero or infinite by [17, Proposition 10.2.3]. Dually the nonnil-G-injective modules are Gorenstein injective by [17, Definition 10.1.1]. Thus, the injective dimension of any nonnil-G-injective module is either zero or infinite.

2. Every projective module P is nonnil-Gorenstein projective. In fact, the exact sequence $0 \rightarrow P \rightarrow P \rightarrow 0$ is a complete projective resolution of P , and for every ϕ -u-projective module M , we have the isomorphism of R -modules $0 \rightarrow \text{Hom}_R(P, M) \rightarrow \text{Hom}_R(P, M) \rightarrow 0$. In the same way, we establish that every injective module is nonnil-G-injective.

3. Note that a ϕ -u-projective module is not necessarily a nonnil-G-projective module. For instance, consider $R := K \propto K^n$, where $n \geq 2$ and K is a field. In this case, its Gorenstein global dimension is infinite, as shown in [27 Corollary 3.8]. Consequently, there exists no Gorenstein projective R -module M ; in particular, M is not nonnil-G-projective by (1). However, R is a ϕ -von Neumann regular ring by [14 Theorem 5.16], which implies that M is ϕ -u-projective by [14 Corollary 5.34]. Similarly, we establish that there are nonnil-injective R -modules that are not nonnil-Gorenstein injective.

Next, we may write a complete projective resolution of an R -module M as follows:

$$\mathcal{P}: \quad \cdots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow P_{-1} \longrightarrow P_{-2} \longrightarrow \cdots. \quad (1)$$

Note that $M \cong \text{Im}(P_0 \rightarrow P_{-1})$. Set $K_i := \text{Ker}(P_i \rightarrow P_{i-1})$ for the i -th syzygy of (1); in particular, $M \cong K_{-1}$.

In the same way, we may write a complete injective resolution of an R -module N as follows:

$$\mathcal{E}: \quad \cdots \longrightarrow E_{-1} \longrightarrow E_0 \longrightarrow E_1 \longrightarrow E_2 \longrightarrow \cdots. \quad (2)$$

The i -th cosyzygy K_i of (2) is defined as $K_i := \text{Im}(E_i \rightarrow E_{i+1})$; in particular, $N \cong K_{-1}$. Our first characterization of the nonnil-G-projective modules is as follows.

Theorem 2.3. The following are equivalent for an R -module M :

1. M is nonnil-Gorenstein projective,
2. M has a complete projective resolution (1) such that $\text{Ext}_R^1(K_i, Q) = 0$ for every ϕ -u-projective module Q and every i -th syzygy K_i of (1),
3. M has a complete projective resolution (1) such that $\text{Ext}_R^k(K_i, Q) = 0$ for every ϕ -u-projective module Q and every i -th syzygy K_i of (1) and every $k \geq 1$,
4. M has a complete projective resolution (1) such that $\text{Ext}_R^k(K_i, Q) = 0$ for every R -module Q of finite ϕ -projective dimension and every i -th syzygy K_i of (1) and every $k \geq 1$,
5. M has a complete projective resolution (1) such that $\text{Ext}_R^1(K_i, Q) = 0$ for every R -module Q of finite ϕ -projective dimension and every i -th syzygy K_i of (1),
6. M has a right projective resolution (i.e., $\mathcal{R}: 0 \rightarrow M \rightarrow P_{-1} \rightarrow P_{-2} \rightarrow \cdots$, where each P_i is projective) such that for every ϕ -u-projective module Q , both the complex $\text{Hom}(\mathcal{R}, Q)$ is exact and $\text{Ext}_R^k(M, Q) = 0$ for every $k > 0$.

Proof. (4) $\Rightarrow$ (6) & (4) $\Rightarrow$ (5) $\Rightarrow$ (1) They are obvious.

(1) $\Rightarrow$ (2) Assume that M is a ϕ -Gorenstein projective module and let $i \in \mathbb{Z}$ and Q be a ϕ -u-projective module. Then there exists a complete projective resolution of M as (1). Starting by the exact sequence $P_{i+2} \rightarrow P_{i+1} \rightarrow K_i \rightarrow 0$, we get the exact sequence $0 \rightarrow \text{Hom}_R(K_i, Q) \rightarrow \text{Hom}_R(P_{i+1}, Q) \xrightarrow{d} \text{Hom}_R(P_{i+2}, Q)$, this shows that $\ker(d) = \text{Hom}_R(K_i, Q)$. Now, considering the exact sequence $0 \rightarrow K_i \rightarrow P_i \rightarrow K_{i-1} \rightarrow 0$, we get the exact sequence $0 \rightarrow \text{Hom}_R(K_{i-1}, Q) \rightarrow \text{Hom}_R(P_i, Q) \xrightarrow{d} \text{Hom}_R(K_i, Q) \rightarrow \text{Ext}_R^1(K_{i-1}, Q) \rightarrow 0$. Since $\ker(d) = \text{Im}(d) = \text{Hom}_R(K_i, Q)$, we get immediately $\text{Ext}_R^1(K_{i-1}, Q) = 0$. Since $i \in \mathbb{Z}$, we get (2), as desired.

(2) $\Rightarrow$ (1) If (2) holds, then by considering the short exact sequences $0 \rightarrow K \rightarrow P_i \rightarrow K \rightarrow 0$ for every $i \in \mathbb{Z}$, so we have $0 \rightarrow \text{Hom}_R(K, Q) \rightarrow \text{Hom}_R(P_i, Q) \rightarrow \text{Hom}_R(K, Q) \rightarrow 0$ is exact for any ϕ -u-projective module Q . By linking these short exact sequences, we get a long exact sequence $\cdots \rightarrow \text{Hom}_R(P_{i+1}, Q) \rightarrow \text{Hom}_R(P_i, Q) \rightarrow \text{Hom}_R(P_{i-1}, Q) \rightarrow \cdots$, as desired M is ϕ -Gorenstein projective.

(2) $\Rightarrow$ (3) It follows from the short exact sequences $0 \rightarrow K \rightarrow P_i \rightarrow K \rightarrow 0$ that $\text{Ext}_R^{k+1}(K, Q) \cong \text{Ext}_R^k(K, Q)$ where K is the syzygies of the complete projective resolution. Now the assertion follows by induction on k .

(3) $\Rightarrow$ (4) Let $n = \phi\text{-pd}_R Q$. If $n = 0$, then Q is ϕ -u-projective and so (4) holds by hypothesis. Now, assume that $n \neq 0$, i.e., Q is not ϕ -u-projective. Following [14, Theorem 3.10], there exists an exact sequence $0 \rightarrow Q_n \rightarrow Q_{n-1} \rightarrow \cdots \rightarrow Q_0 \rightarrow Q \rightarrow 0$ such that Q_i is projective for all $0 \leq i \leq n-1$ and Q_n is ϕ -u-projective. But considering these short exact sequences $0 \rightarrow Q_n \rightarrow Q_{n-1} \rightarrow K \rightarrow 0, \dots, 0 \rightarrow K \rightarrow Q_0 \rightarrow Q \rightarrow 0$ where K is the syzygies of the above exact sequence, so we get for all $k \in \mathbb{N}^*$, $0 = \text{Ext}_R^k(K, Q_{n-1}) \rightarrow \text{Ext}_R^k(K, K) \rightarrow \text{Ext}_R^{k+1}(K, Q_n) = 0$. So $\text{Ext}_R^k(K, K) = 0$ for every K , in particular $\text{Ext}_R^k(K, Q) = 0$, as desired.

(6) $\Rightarrow$ (1) Let $\mathcal{P}r : \cdots \rightarrow P_1 \rightarrow P_0 \rightarrow M \rightarrow 0$ be a projective resolution of M . Since $\text{Ext}_R^k(M, Q) = 0$ for every ϕ -u-projective module Q and every $k \geq 1$, we get $\text{Hom}(\mathcal{P}r, Q)$ is an exact complex. Set $\mathcal{P}r \cup \mathcal{R}$ is the linking between $\mathcal{P}r$ and $\mathcal{R}$ through M , we get a complete projective resolution of M such that $\text{Hom}(\mathcal{P}r \cup \mathcal{R}, Q)$ is an exact complex for every ϕ -u-projective module Q , as desired M is ϕ -Gorenstein projective. $\square$

Dually with Theorem 2.3, the nonnil-G-injective modules are characterized as follows.

Theorem 2.4. The following are equivalent for an R -module N :

1. N is nonnil-G-injective,
2. N has a complete injective resolution (2) such that $\text{Ext}_R^1(Q, K_i) = 0$ for every nonnil-injective module Q and every i -th cosyzygy K_i of (2),
3. N has a complete injective resolution (2) such that $\text{Ext}_R^k(Q, K_i) = 0$ for every nonnil-injective module Q and every i -th cosyzygy K_i of (2) and every $k \geq 1$,
4. N has a complete injective resolution (2) such that $\text{Ext}_R^k(Q, K_i) = 0$ for every R -module Q of finite ϕ -injective dimension, every i -th cosyzygy K_i of (2) and every $k \geq 1$,
5. N has a complete injective resolution (2) such that $\text{Ext}_R^1(Q, K_i) = 0$ for every R -module Q of finite ϕ -injective dimension and every i -th cosyzygy K_i of (2),
6. N has a left injective resolution (i.e., $\mathcal{L} : \cdots \rightarrow E_1 \rightarrow E_0 \rightarrow N \rightarrow 0$) such that for every nonnil-injective module Q , we get the exact complex $\text{Hom}(Q, \mathcal{L})$ and $\text{Ext}_R^k(Q, N) = 0$ for every $k > 0$.

Proof. This proof is analogous to that of Theorem 2.3 above. $\square$

Remark 2.5. 1. If M is nonnil-G-projective with its complete projective resolution $\mathcal{P}$, then by symmetry all images and hence all kernels and cokernels of $\mathcal{P}$ are nonnil-G-projective modules.

2. If N is nonnil-G-injective with its complete projective resolution $\mathcal{E}$, then by symmetry all images and hence all kernels and cokernels of $\mathcal{E}$ are nonnil-G-injective modules.

From Theorem 2.3 we can easily deduce the following.

Corollary 2.6. 1. If M is a nonnil-G-projective module, then $\text{Ext}_R^k(M, Q) = 0$ for every $k \geq 1$ and every R -module Q of finite ϕ -projective dimension.

2. If N is a nonnil-G-injective module, then $\text{Ext}_R^k(Q, N) = 0$ for every $k \geq 1$ and every R -module Q of finite ϕ -injective dimension.

Recall from [32] that a ϕ -ring R is said to be ϕ -von Neumann regular if every R -module is ϕ -flat. It is shown in [14, Corollary 5.34] that every ϕ -von Neumann regular is characterized by the fact that every module over it is ϕ -u-projective and nonnil-injective, i.e., every module over a ϕ -von Neumann regular ring has both finite ϕ -projective and ϕ -injective dimension.

Corollary 2.7. Let R be a ring in which every R -module has finite ϕ -projective dimension and M be an R -module. Then M is nonnil-G-projective if and only if M is projective.

Corollary 2.8. *Let R be a ring in which every R -module has finite ϕ -injective dimension and M be an R -module.. Then N is nonnil-G-injective if and only if N is injective.*

Proof. This is easily done by Theorem 2.4. □

Remark 2.9. We now justify that the class of Gorenstein projective modules generalizes the class of nonnil-G-projective modules. In other words, the class of nonnil-G-projective modules is strictly contained in the class of Gorenstein projective modules. Let $R = K \ltimes K$, where K is a field. We claim that there exists a Gorenstein projective R -module which is not nonnil-G-projective. However, R is a ϕ -von Neumann regular ring. Thus, if every Gorenstein projective R -module is nonnil-G-projective, then R is a semisimple ring by Corollary 2.7 and [27, Corollary 3.8], a desired contradiction since $\text{Nil}(R) \neq 0$. Therefore, R contains a Gorenstein projective module which is not nonnil-G-projective. Similarly, we can justify that there exists a Gorenstein injective R -module which is not nonnil-G-injective.

Example 2.10. Let $R = \mathbb{Z} \ltimes \mathbb{Q}$. Then every nonnil-G-injective R -module is injective. In fact, R is a strongly ϕ -ring and $\phi\text{-gl.dim}(R) = 1$ by [14, Example 6.5]. Therefore, every R -module has finite ϕ -injective dimension, a conclusion supported by the fact that every nonnil ideal of R is free (see [14, Theorem 4.1]).

The ϕ -von Neumann regular rings are characterized according to the nonnil-Gorenstein projectivity or nonnil-Gorenstein injectivity as follows.

Theorem 2.11. The following are equivalent for a ϕ -ring R :

1. R is a ϕ -von Neumann regular ring,
2. R is a strongly ϕ -ring such that every R -module has finite ϕ -projective dimension and every ϕ -torsion module is nonnil-G-projective,
3. R is a strongly ϕ -ring such that every R -module has finite ϕ -projective dimension and every ϕ -u-torsion module is nonnil-G-projective,
4. R is a strongly ϕ -ring such that every R -module has finite ϕ -injective dimension and every ϕ -torsion module is nonnil-G-injective,
5. R is a strongly ϕ -ring such that every R -module has finite ϕ -injective dimension and every ϕ -u-torsion module is nonnil-G-injective.

Proof. (2) $\Rightarrow$ (3) & (4) $\Rightarrow$ (5) These are straightforward.

(1) $\Rightarrow$ (2) & (1) $\Rightarrow$ (4) These follow directly from [14, Corollary 5.15, Theorem 5.29 and Corollary 5.33] and the fact that every ϕ -torsion R -module is zero.

(3) $\Rightarrow$ (1) Let I be a nonnil ideal of R . Then R/I is a ϕ -u-torsion R -module, and so R/I is nonnil-G-projective. By Corollary 2.7, we get that R/I is projective, and so I is generated by an idempotent. From [32, Theorem 4.1], we deduce that R is a ϕ -von Neumann regular ring.

(5) $\Rightarrow$ (1) Let $s \in R \setminus \text{Nil}(R)$. Then R/sR is a ϕ -u-torsion R -module, and so R/sR is nonnil-G-injective. Thus R/sR is an injective R -module by Corollary 2.8. So we get $R = sR$, and so $s \in U(R)$. Therefore, R is a ϕ -von Neumann regular ring by [14, Theorem 5.14]. □

Proposition 2.12. *Every direct sums (resp., direct product) of nonnil-G-projective (resp., nonnil-G-injective) modules is nonnil-G-projective (resp., nonnil-G-injective).*

Proof. Let $\{M_i\}_{i \in I}$ be a family of nonnil-G-projective modules and $\mathcal{P}_i$ be a complete projective resolution of M_i for each $i \in I$. Then $\bigoplus_{i \in I} \mathcal{P}_i$ is a complete projective resolution of $\bigoplus_{i \in I} M_i$. By [33, Theorem 2.1.19], we get easily that $\bigoplus_{i \in I} M_i$ is nonnil-G-projective. Dually, we can establish the "nonnil-G-injective" case. $\square$

Next, we establish an analog of the well-known result [21, 2.5. Theorem]. More precisely, the following theorem shows that the nonnil-G-projective (resp., injective) R -modules are projectively (resp., injectively) resolving.

Theorem 2.13. Let $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$ be a short exact sequence.

1. If C is a nonnil-G-projective module, then A is nonnil-G-projective if and only if B is nonnil-G-projective.
2. If A is a nonnil-G-injective module, then B is nonnil-G-injective if and only if C is nonnil-G-injective.

Proof. (1) This follows immediately from [10, Theorem 2.3 (1)].

(2) This follows immediately from [30, 2.10. Proposition]. $\square$

Proposition 2.14. (1) Every R -module is nonnil-Gorenstein projective if and only if every ϕ - u -projective R -module is injective.

(2) Every R -module is nonnil-Gorenstein injective if and only if every nonnil-injective R -module is projective. In particular, when the above equivalent conditions are satisfied R is quasi-Frobenius.

Proof. (1) This follows immediately from [10, Proposition 2.4] by setting $\mathcal{X}$ to be the set of all ϕ - u -projective R -modules.

(2) This follows immediately from [30, 2.9. Proposition] by setting $\mathcal{Y}$ to be the set of all nonnil-injective R -modules. $\square$

Next, we will define the nonnil-Gorenstein flat R -modules as follows.

Definition 2.15. Let R be a ring and M be an R -module. We say that M is nonnil-Gorenstein flat if there exists a complete flat resolution of M , which is an exact sequence of R -modules of the form

$$\mathcal{F} : \cdots \rightarrow F_n \rightarrow F_{n-1} \rightarrow \cdots \rightarrow F_1 \rightarrow F_0 \rightarrow F^0 \rightarrow F^1 \rightarrow \cdots \rightarrow F^n \rightarrow \cdots$$

where each F_i is a flat R -module, and such that the complex $E \otimes_R \mathcal{F}$ is exact for every nonnil-injective R -module E . Furthermore, M is isomorphic to $\text{im}(F_0 \rightarrow F^0)$.

Remark 2.16. It is easy to see that every nonnil-Gorenstein flat R -module is a Gorenstein-flat.

Proposition 2.17. The class of nonnil-Gorenstein flat R -modules is closed under arbitrary direct sums.

Proof. Simply note that a (degree-wise) sum of complete flat resolutions again is a complete flat resolution (as tensorproducts commutes with sums). $\square$

Theorem 2.18. For any left R -module M , we consider the following conditions:

1. M is a nonnil-Gorenstein flat R -module,
2. The Pontryagin dual $M^+ = \text{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$ is a nonnil-Gorenstein injective R -module,

3. M admits a co-proper right flat resolution

$$\mathcal{F}_r: 0 \rightarrow M \rightarrow F^0 \rightarrow F^1 \rightarrow F^2 \rightarrow \dots.$$

such that $E \otimes_R \mathcal{F}_r$ is an exact complex of R -modules and $\text{Tor}_i^R(E, M) = 0$ for all nonnil-injective R -modules E , and all integers $i > 0$.

Then (1) $\Rightarrow$ (2). If R is a coherent ring, then the previous conditions are equivalent.

Proof. (1) $\Rightarrow$ (2) Let $\mathcal{F}: \dots \rightarrow F_1 \rightarrow F_0 \rightarrow F^0 \rightarrow F^1 \rightarrow \dots$ be a complete flat resolution, such that $M \cong \text{Im}(F_0 \rightarrow F^0)$. Then

$$\mathcal{F}^+: \dots \rightarrow F^{1+} \rightarrow F^{0+} \rightarrow F_0^+ \rightarrow F_1^+ \rightarrow \dots$$

is an exact sequence of injective R -modules, such that $M^+ \cong \text{Im}(F^{0+} \rightarrow F_0^+)$. On the other hand, we have for all nonnil-injective R -modules E ,

$$\text{Hom}_R(E, \mathcal{F}^+) = \text{Hom}_R(E, \text{Hom}_{\mathbb{Z}}(\mathcal{F}, \mathbb{Q}/\mathbb{Z})) \cong \text{Hom}_{\mathbb{Z}}(E \otimes_R \mathcal{F}, \mathbb{Q}/\mathbb{Z})$$

which is exact. Then $\mathcal{F}^+$ is a complete injective resolution and M^+ is nonnil-Gorenstein injective.

Suppose now that R is a coherent ring.

(2) $\Rightarrow$ (3) From Remark 2.16 and [21] 3.6. Theorem], M admits a co-proper right flat resolution $0 \rightarrow M \rightarrow F^0 \rightarrow F^1 \rightarrow F^2 \rightarrow \dots$.

Let's prove that $\text{Tor}_i^R(E, M) = 0$ for all $i > 0$ and injective R -module E . Let $\dots \rightarrow F_2 \rightarrow F_1 \rightarrow F_0 \rightarrow M \rightarrow 0$ be a flat resolution of M , then $0 \rightarrow M^+ \rightarrow F_0^+ \rightarrow F_1^+ \rightarrow F_2^+ \rightarrow \dots$ is an injective resolution. Let E be an R -module, we have the following commutative diagram:

$$\begin{array}{ccccccc} \dots & \longrightarrow & \text{Hom}_R(E, F_1^+) & \longrightarrow & \text{Hom}_R(E, F_0^+) & \longrightarrow & \text{Hom}_R(E, M^+) \longrightarrow 0 \\ & & \downarrow & & \downarrow \cong & & \downarrow \cong \\ \dots & \rightarrow & \text{Hom}_{\mathbb{Z}}(E \otimes_R F_1, \mathbb{Q}/\mathbb{Z}) & \rightarrow & \text{Hom}_{\mathbb{Z}}(E \otimes_R F_0, \mathbb{Q}/\mathbb{Z}) & \rightarrow & \text{Hom}_{\mathbb{Z}}(E \otimes_R M, \mathbb{Q}/\mathbb{Z}) \rightarrow 0 \end{array}$$

such that the upper row of the diagram is exact as M^+ is nonnil-Gorenstein injective, then also the lower row is exact, which means that $\text{Tor}_i^R(E, M) = 0$ for all $i > 0$ and every nonnil-injective R -module E . Now, let $\mathcal{F}_l: \dots \rightarrow F_1 \rightarrow F_0 \rightarrow M \rightarrow 0$ be a flat resolution of M . By linking $\mathcal{F}_l$ with $\mathcal{F}_r$ through M , we get the following complete flat resolution of M :

$$\dots F_1 \rightarrow F_0 \rightarrow F^0 \rightarrow F^1 \rightarrow \dots.$$

So, the following

$$\dots F^{1+} \rightarrow F^{0+} \rightarrow F_0^+ \rightarrow F_1^+ \rightarrow \dots$$

is a complete injective resolution of M^+ . Since, M^+ is assumed nonnil-Gorenstein injective, we get the following exact sequence $\dots \rightarrow \text{Hom}_R(E, F^{1+}) \rightarrow \text{Hom}_R(E, F^{0+}) \rightarrow \text{Hom}_R(E, M^+) \rightarrow 0$, that means the sequence $\dots \rightarrow (E \otimes_R F^0)^+ \rightarrow (E \otimes_R F^0)^+ \rightarrow (E \otimes_R M)^+ \rightarrow 0$ is exact. Hence, we get that $E \otimes_R \mathcal{F}_r$ is exact, as desired.

(3) $\Rightarrow$ (1) By the same way as (2) $\Rightarrow$ (3), we get a complete flat resolution by linking $\mathcal{F}_l$ with $\mathcal{F}_r$ through M . So, the assumption, $\text{Tor}_i^R(E, M) = 0$ for every nonnil-injective R -module E and every $i > 0$, implies that the complex $E \otimes_R \mathcal{F}_l$ is exact. By assumption, the complex $E \otimes_R \mathcal{F}_r$ is exact. Hence, by linking $E \otimes_R \mathcal{F}_r$ and $E \otimes_R \mathcal{F}_l$ through $E \otimes_R M$, we showed that M is a nonnil-Gorenstein flat R -module. $\square$

Remark 2.19. Let K be a field and consider $R = K \ltimes K$. There exists a Gorenstein flat R -module M which is not nonnil-Gorenstein flat: in fact, from [27 Corollary 3.8] and [29 Proposition 2.3], every R -module is a Gorenstein flat. But, R is not a von Neumann regular ring, which means that, there exists an R -module M that not flat. If M is a nonnil-Gorenstein flat R -module, then $\text{Tor}_R^k(E, M) = 0$ for every R -module E and every $k > 0$ by Theorem 2.18, [14 Corollary 5.34] and Corollary 2.6. Hence, M is flat, a contradiction.

Corollary 2.20. Let R be a coherent ring and $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$ be a short exact sequence of R -modules. If C is a nonnil-Gorenstein flat R -module, then A is a nonnil-Gorenstein flat R -module if and only if B is a nonnil-Gorenstein flat R -module.

Proof. The short exact sequence of R -modules $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$ induces the short exact sequence $0 \rightarrow C^+ \rightarrow B^+ \rightarrow A^+ \rightarrow 0$. By Theorem 2.18, if C is a nonnil-Gorenstein flat R -module then C^+ is a nonnil-Gorenstein injective R -module. So, from Theorem 2.13, A^+ is a nonnil-Gorenstein injective R -module if and only if B^+ is a nonnil-Gorenstein injective R -module. Again Theorem 2.18, A is a nonnil-Gorenstein flat R -module if and only if B is a nonnil-Gorenstein flat R -module. $\square$

Theorem 2.21. Let R be a coherent ring and consider the short exact sequence of R -modules $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$, where A and B are nonnil-Gorenstein flat R -module. If $\text{Tor}_1^R(E, C) = 0$ for every (nonnil)-injective R -module E , then C is a nonnil-Gorenstein flat R -module.

Proof. The proof follows from [30, 4.6. Proposition] if we consider E as an injective R -module. Now, assuming that E is nonnil-injective. Considering the short exact sequence of R -modules $0 \rightarrow C^+ \rightarrow B^+ \rightarrow A^+ \rightarrow 0$. By Theorem 2.18, both A^+ and B^+ are nonnil-Gorenstein injective R -modules. By assumption, we get $\text{Ext}_R^1(E, C^+) = 0$ for every nonnil-injective R -module E . But for every $k > 1$, we get the isomorphism $\text{Ext}_R^k(E, A^+) \cong \text{Ext}_R^{k+1}(E, C^+) = 0$. Therefore, C^+ is a nonnil-Gorenstein injective R -module. But R is a coherent ring, and so, C is a nonnil-Gorenstein flat R -module. $\square$

Proposition 2.22. If R is coherent, then the class of nonnil-Gorenstein flat left R -modules is closed under extensions, kernels of epimorphisms, direct sums and direct summands.

Proof. It follows immediately from [30, 4.5. Proposition] by setting $\mathcal{U}$ as the set of all nonnil-injective R -modules. $\square$

3 On nonnil-G-projective, nonnil-G-injective dimensions and nonnil-G-flat dimensions

In this section, we introduce the analogs of the Gorenstein injective dimension and the Gorenstein projective dimension.

Definition 3.1. Let M be an R -module. Then M is said to have a finite nonnil-G-projective dimension at most $n \in \mathbb{N}$ (we denote $\phi\text{-Gpd}_R M \leq n$) if there exists a finite nonnil-G-projective resolution, that is

$$0 \rightarrow P_n \rightarrow P_{n-1} \rightarrow \cdots \rightarrow P_1 \rightarrow P_0 \rightarrow M \rightarrow 0, \quad (3)$$

in which every P_i is nonnil-G-projective. If M does not have a finite length of nonnil-G-projective resolution, then we set $\phi\text{-Gpd}_R M = \infty$.

Dually, let N be an R -module. Then N is said to have a finite nonnil-G-injective dimension at most $n \in \mathbb{N}$ if there exists a nonnil-G-injective resolution, that is

$$0 \rightarrow N \rightarrow E_0 \rightarrow E_1 \rightarrow \cdots \rightarrow E_n \rightarrow 0, \quad (4)$$

in which every E_j is nonnil-G-injective. If N does not have a finite length of nonnil-G-injective resolution, then we set $\phi\text{-Gid}_R N = \infty$.

Remark 3.2. Obviously, an R -module M is nonnil-G-projective if and only if its nonnil-G-projective dimension is zero. Similarly, an R -module N is nonnil-G-injective if and only if its nonnil-G-injective dimension is zero.

Next, the following theorem is an analog of the well-known result [33, Proposition 11.3.4].

Theorem 3.3. Let $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$ be an exact sequence.

1. If $\phi\text{-Gpd}_R B > \phi\text{-Gpd}_R C$, then $\phi\text{-Gpd}_R A = \phi\text{-Gpd}_R B$.
2. If $\phi\text{-Gid}_R B > \phi\text{-Gid}_R A$, then $\phi\text{-Gid}_R B = \phi\text{-Gid}_R C$.

Proof. We will only prove (1); the case of (2) can be dually proved with (1). Write $m = \phi\text{-Gpd}_R A$, $n = \phi\text{-Gpd}_R B$, and $s = \phi\text{-Gpd}_R C$. First let $s = 0$, that is, C is a nonnil-G-projective module. If $m < \infty$, consider a nonnil-G-projective resolution

$$\mathcal{P} : \cdots \rightarrow P_m \rightarrow P_{m-1} \rightarrow \cdots \rightarrow P_0 \rightarrow A \rightarrow 0$$

of A . For $i > m$, set $P_i = 0$. Since C is nonnil-G-projective, there is an exact sequence

$$\mathcal{Q} : \cdots \rightarrow Q_m \rightarrow Q_{m-1} \rightarrow \cdots \rightarrow Q_0 \rightarrow C \rightarrow 0$$

such that each Q_i is projective and each syzygy C_i is nonnil-G-projective. So, we can prove that there exists a complex exact sequence $0 \rightarrow \mathcal{P} \rightarrow \mathcal{F} \rightarrow \mathcal{Q} \rightarrow 0$, where each term $F_i = P_i \oplus Q_i$ of $\mathcal{F}$ is a nonnil-G-projective module. Denote by B_i the i -th syzygy of the complex $\mathcal{F}$. Then there is an exact sequence $0 \rightarrow P_m \rightarrow B_m \rightarrow C_m \rightarrow 0$. By Theorem 2.13(1), B_m is nonnil-G-projective. Thus $n \leq m$. Hence if $n = \infty$, then $m = \infty$.

Let $n < \infty$. Then there is an exact sequence $0 \rightarrow F_n \rightarrow \cdots \rightarrow F_0 \rightarrow B \rightarrow 0$, where each F_i is nonnil-G-projective. Let K_0 be the kernel of the homomorphism $F_0 \rightarrow B$. Then $\phi\text{-Gpd}_R K_0 = n - 1$. Thus we have the following commutative diagram with all exact rows and columns:

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \\
 & & K_0 & \xlongequal{\quad} & K_0 & & \\
 & & \downarrow & & \downarrow & & \\
 0 & \longrightarrow & L & \longrightarrow & F_0 & \longrightarrow & C \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \parallel \\
 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & &
 \end{array}$$

By Theorem 2.13(1), L is nonnil-G-projective, and so $m \leq (n - 1) + 1 = n$. Therefore $m = n$. For $s > 0$ in the general case, we can examine a nonnil-Gorenstein projective resolution of A and a complete projective resolution of C . Now the assertion follows by applying the above discussion. $\square$

Corollary 3.4. Let M be a nonnil-G-projective (resp., nonnil-G-injective) module and N be an R -module. Then $\phi\text{-Gpd}_R(M \oplus N) = \phi\text{-Gpd}_R N$ (resp., $\phi\text{-Gid}_R(M \oplus N) = \phi\text{-Gid}_R N$).

Proof. This follows from the short exact sequence $0 \rightarrow N \rightarrow M \oplus N \rightarrow M \rightarrow 0$. If $M \oplus N$ is nonnil-G-projective, then N is also nonnil-G-projective by Theorem 2.13(1). If $\phi\text{-Gpd}_R(M \oplus N) = n > 0$, then we get $\phi\text{-Gpd}_R N = n$ by Theorem 3.3. We can prove the "nonnil-G-injective dimension" case dully. $\square$

Proposition 3.5. *Let M be an R -module with finite nonnil-Gorenstein injective dimension n . Then there exist exact sequences*

$$0 \longrightarrow M \longrightarrow I \longrightarrow F \longrightarrow 0$$

with I nonnil-Gorenstein injective, $\text{id}(F) \leq n - 1$, and

$$0 \longrightarrow I' \longrightarrow F' \longrightarrow M \longrightarrow 0$$

with I' nonnil-Gorenstein injective, $\text{id}(F') \leq n$.

Proof. It follows immediately from [30, 2.12. Proposition] by setting $\mathcal{Y}$ as the set of all nonnil-injective R -modules. $\square$

Corollary 3.6. *Let $0 \rightarrow M \rightarrow I_0 \rightarrow I_1 \rightarrow 0$ be a short exact sequence of R -modules, where I_0 and I_1 are nonnil-Gorenstein injective modules and $\text{Ext}_R^1(I, M) = 0$ for all injective R -modules I . Then M is nonnil-Gorenstein injective.*

Proof. It follows immediately from [30, 2.13. Corollary] by setting $\mathcal{Y}$ as the set of all nonnil-injective R -modules. $\square$

The following theorem is the main ingredient of the important functorial description of the nonnil-G-projective dimension.

Theorem 3.7. The following are equivalent for an R -module M of finite nonnil-G-projective dimension:

1. $\phi\text{-Gpd}_R M \leq n$.
2. $\text{Ext}_R^k(M, Q) = 0$ for every R -module Q with finite ϕ -projective dimension and every $k > n$.
3. $\text{Ext}_R^k(M, Q) = 0$ for every ϕ -u-projective R -module Q and every $k > n$.
4. If $0 \rightarrow P_n \rightarrow P_{n-1} \rightarrow \cdots \rightarrow P_0 \rightarrow M \rightarrow 0$ is an exact sequence such that every P_i , where $0 \leq i \leq n-1$, is a projective module, then P_n is nonnil-G-projective.
5. If $0 \rightarrow Q_n \rightarrow Q_{n-1} \rightarrow \cdots \rightarrow Q_0 \rightarrow M \rightarrow 0$ is an exact sequence such that every Q_i , where $0 \leq i \leq n-1$, is a nonnil-G-projective module, then Q_n is nonnil-G-projective.
6. $\text{Ext}_R^k(M, Q) = 0$ for every R -module Q with finite projective dimension and every $k > n$.
7. $\text{Ext}_R^k(M, Q) = 0$ for every projective R -module Q and every $k > n$.

Proof. Set $m = \phi\text{-Gpd}_R M$. Then there exists a nonnil-G-projective resolution

$$0 \rightarrow G_m \rightarrow G_{m-1} \rightarrow \cdots \rightarrow G_1 \rightarrow G_0 \rightarrow M \rightarrow 0 \quad (5)$$

such that each G_i is nonnil-G-projective. We set K_i to be its i -th syzygy of (5). In particular, $K_{-1} := M$. Note that if $k > m + 1$, then $K_{k-2} \cong G_{k-1}$.

(5) $\Rightarrow$ (1) This is straightforward.

(1) $\Rightarrow$ (2) Let $k > 0$ and $i \geq -1$. Then we have the short exact sequence $0 \rightarrow K_{i+1} \rightarrow G_i \rightarrow K_i \rightarrow 0$. By Theorem 2.3, we get $\text{Ext}_R^k(G_i, Q) = 0$, and so we have the isomorphism $\text{Ext}_R^k(K_{i+1}, Q) \cong \text{Ext}_R^{k+1}(K_i, Q)$. Since $\phi\text{-Gpd}_R M \leq n$, it follows that for every $k > n$, $\text{Ext}_R^k(M, Q) \cong \text{Ext}_R^{k-1}(K_0, Q) \cong \dots \cong \text{Ext}_R^1(K_{k-2}, Q) = \text{Ext}_R^1(G_{k-1}, Q) = 0$.

(2) $\Rightarrow$ (3) This is straightforward.

(3) $\Rightarrow$ (1) If $m = 0$, naturally we have $m \leq n$. Let $m > 0$ and set $L := \text{Ker}(G_0 \rightarrow M)$. Then $\phi\text{-Gpd}_R L = m - 1$. Take a projective module P and an epimorphism $P \rightarrow M$. Set $K := \text{Ker}(P \rightarrow M)$. By [33, Theorem 2.3.12], there is an exact sequence $0 \rightarrow K \rightarrow L \oplus P \rightarrow G_0 \rightarrow 0$. By Corollary 3.4, $\phi\text{-Gpd}_R(L \oplus P) = m - 1$. By Proposition 3.3, $\phi\text{-Gpd}_R K = m - 1$. Since $\text{Ext}_R^{k-1}(K, Q) = \text{Ext}_R^k(M, Q) = 0$ for any $k > n$ and any ϕ -u-projective module Q , by induction $m - 1 \leq n - 1$. Thus $m \leq n$.

(1) $\Rightarrow$ (4) Assume that $\phi\text{-Gpd}_R M \leq n$. Then there exists a nonnil-Gorenstein projective resolution of M as follows:

$$0 \rightarrow G_n \rightarrow G_{n-1} \rightarrow \dots \rightarrow G_1 \rightarrow G_0 \rightarrow M \rightarrow 0$$

in which every G_i is nonnil-G-projective. By [33, Theorem 3.2.1], we get the following commutative diagram:

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & P_n & \longrightarrow & P_{n-1} & \longrightarrow & \dots & \longrightarrow & P_0 & \longrightarrow & M & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & & & \downarrow & & \parallel & & \\ 0 & \longrightarrow & G_n & \longrightarrow & G_{n-1} & \longrightarrow & \dots & \longrightarrow & G_0 & \longrightarrow & M & \longrightarrow & 0 \end{array}$$

By [33, Lemma 11.3.3], there exists an exact sequence $0 \rightarrow P_n \rightarrow P_{n-1} \oplus G_n \rightarrow \dots \rightarrow P_1 \oplus G_2 \rightarrow P_0 \oplus G_1 \rightarrow G_0 \rightarrow 0$. Since $G_0, G_1, \dots, G_n$ are nonnil-Gorenstein projective modules, repeated application of Theorem 2.13 implies that P_n is also nonnil-G-projective.

(4) $\Rightarrow$ (5) Let $0 \rightarrow P_n \rightarrow P_{n-1} \rightarrow \dots \rightarrow P_1 \rightarrow P_0 \rightarrow M \rightarrow 0$ be an exact sequence of R -modules such that $P_0, P_1, \dots, P_{n-1}$ are projective modules. Then P_n is nonnil-G-projective. By [33, Theorem 3.2.1], we get the following commutative diagram:

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & P_n & \longrightarrow & P_{n-1} & \longrightarrow & \dots & \longrightarrow & P_0 & \longrightarrow & M & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & & & \downarrow & & \parallel & & \\ 0 & \longrightarrow & Q_n & \longrightarrow & Q_{n-1} & \longrightarrow & \dots & \longrightarrow & Q_0 & \longrightarrow & M & \longrightarrow & 0 \end{array}$$

Therefore, by [33, Lemma 11.3.3], there exists an exact sequence $0 \rightarrow P_n \rightarrow P_{n-1} \oplus Q_n \rightarrow \dots \rightarrow P_1 \oplus Q_2 \rightarrow P_0 \oplus Q_1 \rightarrow Q_0 \rightarrow 0$. Decompose this exact sequence into two exact sequences

$$0 \rightarrow P_n \rightarrow P_{n-1} \oplus Q_n \rightarrow K \rightarrow 0$$

and

$$0 \rightarrow K \rightarrow P_{n-2} \oplus Q_{n-1} \rightarrow \dots \rightarrow P_0 \oplus Q_1 \rightarrow Q_0 \rightarrow 0.$$

By Theorem 2.13, we deduce that K is nonnil-G-projective, since all Q_i are nonnil-G-projective modules. Therefore, Q_n is nonnil-G-projective, as desired.

(5) $\Leftrightarrow$ (6) $\Leftrightarrow$ (7) These follow immediately from [30, 3.14. Proposition] by setting $\mathcal{X}$ as the set of all ϕ -u-projective R -modules. $\square$

Corollary 3.8. *Let M be an R -module with finite nonnil-Gorenstein projective dimension. Then $\text{Gpd}_R M = \phi\text{-Gpd}_R M$. In particular, an R -module M is Gorenstein projective if and only if M is nonnil-Gorenstein projective.*

Proof. It follows immediately from [30, 3.15. Corollary] by setting $\mathcal{X}$ as the set of all ϕ -u-projective R -modules. $\square$

Remark 3.9. We define $\mathcal{P}r(R)$ (resp., $\overline{\mathcal{P}r(R)}$) for the class of all ϕ -u-projective modules (resp., all R -modules of finite ϕ -projective dimension). By Theorem 3.7, the nonnil-G-projective dimension of an R -module M is given as follows:

$$\begin{aligned}\phi\text{-Gpd}_R M &= \sup \{i \in \mathbb{N} \mid \exists Q \in \mathcal{P}r(R) \text{ such that } \text{Ext}_R^i(M, Q) \neq 0\} \\ &= \sup \{i \in \mathbb{N} \mid \exists Q \in \overline{\mathcal{P}r(R)} \text{ such that } \text{Ext}_R^i(M, Q) \neq 0\}.\end{aligned}$$

Dually with Theorem 3.7, we establish the following theorem.

Theorem 3.10. Let $n \in \mathbb{N}$. Then the following are equivalent for an R -module N of finite nonnil-G-projective dimension:

1. $\phi\text{-Gid}_R N \leq n$,
2. $\text{Ext}_R^k(Q, N) = 0$ for every R -module Q with finite ϕ -injective dimension and every $k > n$,
3. $\text{Ext}_R^k(Q, N) = 0$ for every nonnil-injective R -module Q and every $k > n$,
4. If $0 \rightarrow N \rightarrow E_0 \rightarrow E_1 \rightarrow \dots \rightarrow E_n \rightarrow 0$ such that every E_i , where $0 \leq i \leq n-1$, is an injective module, then E_n is nonnil-G-injective.
5. If $0 \rightarrow N \rightarrow Q_0 \rightarrow Q_1 \rightarrow \dots \rightarrow Q_n \rightarrow 0$ such that every Q_i , where $0 \leq i \leq n-1$, is nonnil-G-injective module, then Q_n is nonnil-G-injective.
6. $\text{Ext}_R^k(Q, N) = 0$ for every injective R -module Q and every $k > n$,
7. $\text{Ext}_R^k(Q, N) = 0$ for every R -module Q with finite injective dimension and every $k > n$,

Proof. The proof the first statements is similar of to that of Theorem 3.7.

(5) $\Leftrightarrow$ (6) $\Leftrightarrow$ (7) These follow immediately from [30, 2.15. Proposition]. $\square$

Remark 3.11. We define $\mathcal{I}(R)$ (resp., $\overline{\mathcal{I}(R)}$) for the class of all nonnil-injective modules (resp., all R -modules of finite ϕ -injective dimension). By Theorem 3.10, the nonnil-G-injective dimension of an R -module N is given as follows:

$$\begin{aligned}\phi\text{-Gid}_R N &= \sup \{i \in \mathbb{N} \mid \exists Q \in \mathcal{I}(R) \text{ such that } \text{Ext}_R^i(Q, N) \neq 0\} \\ &= \sup \{i \in \mathbb{N} \mid \exists Q \in \overline{\mathcal{I}(R)} \text{ such that } \text{Ext}_R^i(Q, N) \neq 0\}.\end{aligned}$$

Corollary 3.12. Let N be an R -module with finite nonnil-Gorenstein injective dimension. Then $\text{Gid}_R N = \phi\text{-Gid}_R N$. In particular, an R -module is nonnil-Gorenstein injective if and only if it is Gorenstein injective.

Proof. It follows immediately from [30, 2.16. Corollary] by setting $\mathcal{I}$ as the class of all nonnil-injective R -modules. $\square$

Corollary 3.13. Let $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$ be a short exact sequence of R -modules and let $n \in \mathbb{N}$. Then the following hold.

1. If $\phi\text{-Gpd}_R B \leq n$ and $\phi\text{-Gpd}_R C \leq n$, then $\phi\text{-Gpd}_R A \leq n$. In particular, if both B and C are nonnil-G-projective, then so is A .
2. If $\phi\text{-Gid}_R A \leq n$ and $\phi\text{-Gid}_R B \leq n$, then $\phi\text{-Gid}_R C \leq n$. In particular, if both A and B are nonnil-G-injective, then so is C .

Proof. (1) By Theorem 3.7(4) and [33, Theorem 2.6.6 (Horseshoe Lemma)], we get that $\phi\text{-Gpd}_R A < \infty$. So, for every $k > n$ and every ϕ -u-projective module Q , we get the exact sequence $\text{Ext}_R^k(B, Q) \rightarrow \text{Ext}_R^k(A, Q) \rightarrow \text{Ext}_R^{k+1}(C, Q)$. By Theorem 3.7, $\text{Ext}_R^k(A, Q) = 0$, i.e., $\phi\text{-Gpd}_R A \leq n$.

(2) The proof is similar to that of (1). $\square$

Corollary 3.14. *Let $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$ be a short exact sequence of R -modules. Then:*

1. *If both A and B are nonnil- G -projective modules, then C is projective if and only if $\text{Ext}_R^1(C, Q) = 0$ for every nonnil- G -projective module Q .*
2. *If both B and C are nonnil- G -injective modules, then A is injective if and only if $\text{Ext}_R^1(Q, A) = 0$ for every nonnil- G -injective module Q .*

Proof. (1) By Theorem 2.7, $\phi\text{-Gpd}_R C \leq 1$, and so there exists a short exact sequence $0 \rightarrow M \rightarrow F \rightarrow C \rightarrow 0$, where F is projective and M is nonnil- G -projective. Since $\text{Ext}_R^1(C, M) = 0$, it follows that $0 \rightarrow M \rightarrow F \rightarrow C \rightarrow 0$ is split, and so C is projective. The converse is straightforward.

(2) This proof is similar to that of (1). $\square$

Proposition 3.15. *Let $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$ be a short exact sequence of R -modules and let $n \in \mathbb{N}$. Then the following hold.*

1. *If $\phi\text{-Gpd}_R B < \phi\text{-Gpd}_R C$, then $\phi\text{-Gpd}_R A = \phi\text{-Gpd}_R C - 1$. In general, we get $\phi\text{-Gpd}_R C \leq 1 + \max\{\phi\text{-Gpd}_R A, \phi\text{-Gpd}_R B\}$.*
2. *If $\phi\text{-Gid}_R B < \phi\text{-Gid}_R A$, then $\phi\text{-Gid}_R C = \phi\text{-Gid}_R A - 1$. In general, we get $\phi\text{-Gid}_R A \leq 1 + \max\{\phi\text{-Gid}_R A, \phi\text{-Gid}_R C\}$.*

Proof. It follows immediately from [34, Corollary 3.7]. $\square$

Proposition 3.16. *Let R be a ring and $n \in \mathbb{N}$. Then the following properties hold:*

1. *If $\phi\text{-Gpd}_R M \leq n$ for every R -module M , then the injective dimension of any ϕ -u-projective module is at most n .*
2. *If $\phi\text{-Gid}_R N \leq n$ for every R -module N , then the projective dimension of any nonnil-injective module is at most n .*

Proof. (1) Let Q be a ϕ -u-projective module and M be an R -module. Since $\phi\text{-Gpd}_R M \leq n$, there exists an exact sequence

$$0 \rightarrow P_n \rightarrow P_{n-1} \rightarrow \cdots \rightarrow P_1 \rightarrow P_0 \rightarrow M \rightarrow 0.$$

where $P_0, P_1, \dots, P_{n-1}$ are projective modules and P_n is nonnil- G -projective. Then $\text{Ext}_R^{n+1}(M, Q) \cong \text{Ext}_R^1(P_n, Q) = 0$. Therefore, $\text{id}_R Q \leq 1$.

(2) This can be proved dually to (1). $\square$

Next, we give an analog of the well-known result [33, Theorem 11.3.14 (Holm) & Theorem 11.3.15 (Christensen-Frankild-Holm)].

Proposition 3.17. *Let M be an R -module with finite nonnil-Gorenstein projective dimension n , then there exist exact sequences*

$$0 \rightarrow H \rightarrow G \rightarrow M \rightarrow 0$$

with nonnil-Gorenstein projective and $\text{pd}(H) \leq n - 1$ and

$$0 \rightarrow M \rightarrow H' \rightarrow G' \rightarrow 0.$$

Proof. It follows immediately from [30] 3.11. Proposition] by setting $\mathcal{X}$ as the set of all ϕ -u-projective R -modules. $\square$

We next define the nonnil-Gorenstein flat dimension of modules as follows.

Definition 3.18. Let R be a ring and M be an R -module. Then M is said to have a ϕ -Gorenstein flat dimension at most $n \in \mathbb{N}$, and we write $\phi\text{-G-f}d_R M \leq n$, if there exists a resolution of nonnil-Gorenstein flat R -modules as follows

$$0 \rightarrow F_n \rightarrow F_{n-1} \rightarrow \cdots \rightarrow F_1 \rightarrow F_0 \rightarrow M \rightarrow 0.$$

If no such resolution exists, we set $\phi\text{-G-f}d_R M = \infty$.

Proposition 3.19. Let R be a ring and M be an R -module. The following hold.

1. $\phi\text{-G-id}_R M^+ \leq \phi\text{-G-f}d_R M$.
2. If R is a coherent ring, then $\phi\text{-G-id}_R M^+ = \phi\text{-G-f}d_R M$.

Proof. (1) If $\phi\text{-G-f}d_R M = \infty$, the inequality holds. Assuming that $\phi\text{-G-f}d_R M \leq n$, where $n \in \mathbb{N}$. Then, there exists a resolution of Gorenstein flat R -modules as follows

$$0 \rightarrow F_n \rightarrow F_{n-1} \rightarrow \cdots \rightarrow F_1 \rightarrow F_0 \rightarrow M \rightarrow 0.$$

The above resolution induces

$$0 \rightarrow M^+ \rightarrow F_0^+ \rightarrow \cdots \rightarrow F_1^+ \rightarrow F_{n-1}^+ \rightarrow F_n^+ \rightarrow 0$$

which is a resolution of nonnil-Gorenstein injective R -modules. So, it follows that $\phi\text{-G-id}_R M^+ \leq n$, as desired.

(2) This is obvious from Theorem 2.18. $\square$

Corollary 3.20. Let R be coherent and consider the short exact sequence of R -modules $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$, where B is nonnil-Gorenstein flat. If C is nonnil-Gorenstein flat, then so is A . If otherwise $n > 0$, then:

$$\phi\text{-G-f}d_R A = \phi\text{-G-f}d_R C - 1.$$

Proof. Considering the short exact sequence of R -modules $0 \rightarrow C^+ \rightarrow B^+ \rightarrow A^+ \rightarrow 0$, and applying Proposition 3.19 (2) in conjunction with Proposition 3.15 $\square$

Corollary 3.21. Let R be a coherent ring. If $(M_\lambda)_{\lambda \in \Lambda}$ is any family of R -modules, then we have an equality:

$$\phi\text{-G-f}d_R \left(\bigoplus M_\lambda \right) = \sup \{ \phi\text{-G-f}d_R M_\lambda \mid \lambda \in \Lambda \}.$$

Proof. This follows immediately from Proposition 3.19 (2). $\square$

Corollary 3.22. Let M be an R -module of finite ϕ -Gorenstein flat dimension with R is coherent, and let n be an integer. Then the following conditions are equivalent:

1. $\phi\text{-G-f}d_R \leq n$,
2. $\text{Tor}_i^R(L, M) = 0$ for all $i > n$, and all R -modules L with finite ϕ -injective dimension.
3. $\text{Tor}_i^R(E, M) = 0$ for all $i > n$, and all nonnil-injective R -modules E .

4. for every exact sequence $0 \rightarrow K_n \rightarrow G_{n-1} \rightarrow \dots \rightarrow G_0 \rightarrow M \rightarrow 0$, where $G_0, \dots, G_{n-1}$ are nonnil-Gorenstein flats, then also K_n is nonnil-Gorenstein flat.
5. $\text{Tor}_i^R(L, M) = 0$ for all $i > n$, and all R -modules L with finite injective dimension.
6. $\text{Tor}_i^R(E, M) = 0$ for all $i > n$, and all injective R -modules E .

Consequently, the nonnil-Gorenstein flat dimension of M is determined by the following formulas:

$$\begin{aligned} \phi\text{-Gfd}_R M &= \sup \{i \in \mathbb{N} \mid \exists L \in \overline{\phi\text{-}\mathcal{I}(R)} : \text{Tor}_i^R(L, M) \neq 0\}, \\ &= \sup \{i \in \mathbb{N} \mid \exists E \in \phi\text{-}\mathcal{I}(R) : \text{Tor}_i^R(E, M) \neq 0\}, \end{aligned}$$

where, $\phi\text{-}\mathcal{I}(R)$ (resp., $\overline{\phi\text{-}\mathcal{I}(R)}$) is the set of all nonnil-injective R -modules (resp., all R -modules with finite ϕ -injective dimension).

Proof. The equivalences of the first four statements follow immediately from Proposition 3.19 (2) and Theorem 3.10.

(4) $\iff$ (5) $\iff$ (6) These follow immediately from [30, 4.9. Proposition] by setting $\mathcal{Y}$ as the set of all nonnil-injective R -modules. $\square$

4 On nonnil-Gorenstein global dimension

In this section, we denote $\mathcal{M}_R$ (resp., $\mathcal{T}_R$) for the class of all R -modules (resp., for all ϕ -u-torsion R -modules). We start with the following definition of the nonnil-Gorenstein global dimension as follows.

Definition 4.1. For a ring R , define

$$\phi\text{-G-gl.dim}(R) := \sup \{\phi\text{-Gpd}_R M \mid M \in \mathcal{M}_R\}, \quad (6)$$

which are called the nonnil-Gorenstein global dimension of R .

Our next goal is to characterize the rings of finite nonnil-Gorenstein global dimension at most $n \in \mathbb{N}$.

Theorem 4.2. Let $n \in \mathbb{N}$. Then the following are equivalent for a ring R of finite nonnil-Gorenstein global dimension R :

1. $\phi\text{-G-gl.dim}(R) \leq n$.
2. The injective dimension of any ϕ -u-projective module is at most n .
3. The projective dimension of any nonnil-injective module is at most n .
4. $\phi\text{-Gpd}_R M \leq n$ for any finitely generated R -module M .
5. $\phi\text{-Gpd}_R(R/I) \leq n$ for any ideal I of R .
6. $\text{Ext}_R^k(M, N) = 0$ for any module M , any module N of finite ϕ -projective dimension, and any $k > n$.
7. $\phi\text{-Gid}_R N \leq n$ for every R -module N .

Proof. (3) $\Rightarrow$ (7) Let N be an R -module and E be a nonnil-injective R -module. Then for every $k > n$, we have $\text{Ext}_R^k(E, N) = 0$, since $\text{pd}_R E \leq n$. Then $\phi\text{-Gid}_R N \leq n$ by Theorem 3.10.

(7) $\Rightarrow$ (3) Let E be a nonnil-injective module and N be an R -module. Then $\text{Ext}_R^{n+1}(E, N) = 0$ by hypothesis and Theorem 3.10. Therefore, $\text{pd}_R E \leq n$.

(1) $\Rightarrow$ (4) $\Rightarrow$ (5) These are direct.

(5) $\Rightarrow$ (2) Let P be a ϕ -u-projective module. Then by Theorem 3.7, we get $\text{Ext}_R^k(R/I, P) = 0$ for every $k > n$ and every ideal I of R . Therefore, $\text{id}_R P \leq n$.

(1) $\Leftrightarrow$ (6) This follows from Theorem 3.7.

(1) $\Leftrightarrow$ (2) The necessity follows immediately from Proposition 3.16. We claim the sufficiency. Let M be an R -module and P be a ϕ -u-projective module. Then for all $k > n$, we get that $\text{Ext}_R^k(M, P) = 0$, since the injective dimension of P is at most n . By Theorem 3.7, we deduce that $\phi\text{-Gpd}_R M \leq n$.

(1) $\Leftrightarrow$ (3) This is the dual of the proof of (1) $\Leftrightarrow$ (2). $\square$

Proposition 4.3. *Let R be a ring. Then*

$$\begin{aligned}\phi\text{-G-gl.dim}(R) &= \sup \{ \phi\text{-Gid}_R N \mid N \in \mathcal{M}_R \} \\ &= \sup \{ \text{Gid}_R N \mid N \in \mathcal{M}_R \} \\ &= \sup \{ \phi\text{-Gp}_R M \mid M \text{ is a finitely generated } R\text{-module} \} \\ &= \sup \{ \phi\text{-Gp}_R \left(\frac{R}{I} \right) \mid I \text{ is an ideal of } R \}.\end{aligned}$$

Proof. It follows immediately from Theorem 4.2 and [34, Theorem 4.5]. $\square$

Proposition 4.4. *Let R be a ring. Then $\text{G-gl.dim}(R) \leq \phi\text{-G-gl.dim}(R)$, with equality if $\phi\text{-G-gl.dim}(R) < \infty$.*

Proof. This follows immediately from Remark 2.2, Corollary 3.8, [21, 2.20. Theorem], and [33, Definition 11.4.1]. $\square$

Recall that a ring R is said to be quasi-Frobenius (QF for short) if every projective module is injective.

Definition 4.5. A ring R is said to be strongly quasi-Frobenius (strongly QF for short) if its nonnil-Gorenstein global dimension is zero.

Remark 4.6. It is easy to see that every strongly QF ring is QF. The converse is not true by Remark 2.9.

The following theorem is an analog of the well-known result [33, Theorem 4.6.10 (Faith-Walker)].

Theorem 4.7. The following are equivalent for a ring R of finite nonnil-Gorenstein global dimension:

1. R is strongly QF,
2. Every nonnil-injective module is projective,
3. Every ϕ -u-projective module is injective,
4. R is QF such that every nonnil-injective module is injective,
5. R is QF such that every ϕ -u-projective module is projective,
6. Every R -module is nonnil-G-injective.

Proof. (1) $\Leftrightarrow$ (2) $\Leftrightarrow$ (3) $\Leftrightarrow$ (6) These follow immediately from Theorem 4.2

(2) $\Leftrightarrow$ (4) This follows immediately from [33] Theorem 4.6.10 (Faith-Walker)].

(3) $\Rightarrow$ (5) & (5) $\Rightarrow$ (1) These follow immediately from [33] Theorem 4.6.10 (Faith-Walker)]. $\square$

Remark 4.8. Note that a QF ring is not necessarily a strongly QF ring. In fact, for every field K , it is easy to see that the ring $R = K \ltimes K$ is a QF ring by [27] Corollary 3.8]. However, R is never a strongly QF ϕ -ring, since its nilradical is a ϕ -u-projective R -module but not projective by [33] Proposition 6.7.12].

It is natural to ask: what are the ϕ -rings of nonnil-Gorenstein global dimension 0? The following theorem answers this question.

Theorem 4.9. If $R \in \mathcal{H}$, then R is a field if and only if its nonnil-Gorenstein global dimension equals zero.

Proof. The necessity is trivial. Now we prove the sufficiency. Let $R \in \mathcal{H}$ of nonnil-Gorenstein global dimension 0. By Proposition 4.4 and [7] Proposition 2.6], R is a QF ring. In particular, $\text{Nil}(R)$ is finitely generated. By [5] Lemma 2.3], either R is an integral domain or a local Artinian ring with maximal ideal $\text{Nil}(R) \neq 0$. But if R is not an integral domain, then R is a ϕ -von Neumann regular ring. So every R -module is projective by Corollary 2.7] i.e., R is a semisimple ring, and so $\text{Nil}(R) = 0$, a desired contradiction. Therefore R is an integral domain. Consequently, R is a field. $\square$

We can give a second proof of Theorem 4.9 as follows.

Second proof of Theorem 4.9. By Theorem 4.7 and [31] Theorem 1.6], we deduce that if R is a strongly QF ϕ -ring, then R is a QF integral domain. Therefore, R must be a field. $\square$

Also, there is a third proof as follows.

Third proof of Theorem 4.9. First, if $R \in \mathcal{H}$, then $R/\text{Nil}(R)$ is a ϕ -u-projective R -module. In fact, we claim that $\text{Ext}_R^1(R/\text{Nil}(R), X) = 0$ for any ϕ -u-torsion R -module X . Let X be a ϕ -u-torsion R -module. We first show that $\text{Hom}_R(\text{Nil}(R), X) = 0$. Let $\gamma \in \text{Hom}_R(\text{Nil}(R), X)$. Since X is a ϕ -u-torsion R -module, $sX = 0$ for some $s \in R \setminus \text{Nil}(R)$. Since $R \in \mathcal{H}$, it follows that $\text{Nil}(R)$ is a ϕ -divisible R -module, and so $\text{Nil}(R) = s\text{Nil}(R)$. Then for every $n \in \text{Nil}(R)$, we can write $n = sn'$ for some $n' \in \text{Nil}(R)$, and so $\gamma(n) = s\gamma(n') \in sX = 0$. It follows that $\text{Hom}_R(\text{Nil}(R), X) = 0$. However, it follows from the short exact sequence $0 \rightarrow \text{Nil}(R) \rightarrow R \rightarrow R/\text{Nil}(R) \rightarrow 0$ that $0 = \text{Hom}_R(\text{Nil}(R), X) \rightarrow \text{Ext}_R^1(R/\text{Nil}(R), X) \rightarrow 0$. Therefore, $R/\text{Nil}(R)$ is a ϕ -u-projective R -module.

Now, if the nonnil-Gorenstein global dimension of R is zero, then by Theorem 4.7, R is a QF ring such that $R/\text{Nil}(R)$ is a projective R -module, and so $\text{Nil}(R)$ is a projective ideal of R . It follows that $\text{Nil}(R) = 0$ by [33] Proposition 6.7.12], and so R is both an integral domain and a QF-ring, that is a field. The converse is obvious. $\square$

As shown in Theorem 4.9, the ϕ -rings with nonnil-Gorenstein global dimension 0 are precisely the fields. Therefore, the class of ϕ -rings of nonnil-Gorenstein global dimension 0 is well-established. To extend this class, let us consider the following definition.

Definition 4.10. Let R be a ring. Define its closed nonnil-Gorenstein global dimension, denoted by $\overline{\phi\text{-G.gl.dim}}(R)$, as follows:

$$\overline{\phi\text{-G.gl.dim}}(R) := \sup \{ \phi\text{-Gpd}_R M \mid M \in \mathcal{T} \}. \quad (7)$$

Theorem 4.11. The following are equivalent for a ring R of finite closed nonnil-Gorenstein global dimension:

1. $\overline{\phi\text{-G.gl.dim}(R)} \leq n$,
2. The ϕ -injective dimension of any ϕ -u-projective module is at most n ,
3. The ϕ -projective dimension of nonnil-injective module is at most n ,
4. $\phi\text{-Gpd}_R M \leq n$ for any finitely generated ϕ -u-torsion R -module M ,
5. $\phi\text{-Gpd}_R(R/I) \leq n$ for any nonnil ideal I of R ,
6. $\text{Ext}_R^k(M, N) = 0$ for any ϕ -u-torsion module M , any module N of finite ϕ -projective dimension, and any $k > n$.

Proof. (1) $\Rightarrow$ (4) $\Rightarrow$ (5) These are straightforward.

(5) $\Rightarrow$ (2) Let P be a ϕ -u-projective module. Then by Theorem 3.7, we get $\text{Ext}_R^k(R/I, P) = 0$ for every $k > n$ and every nonnil ideal I of R . Therefore, $\phi\text{-id}_R P \leq n$.

(1) $\Leftrightarrow$ (6) This follows from Theorem 3.7.

(1) $\Leftrightarrow$ (2) The necessity follows immediately from Proposition 3.16. We claim the sufficiency. Let M be a ϕ -u-torsion R -module and P be a ϕ -u-projective module. Then for any $k > n$, we get $\text{Ext}_R^k(M, P) = 0$, since the ϕ -injective dimension of P is at most n . By Theorem 3.7, we deduce that $\phi\text{-Gpd}_R M \leq n$.

(1) $\Leftrightarrow$ (3) This can be proved dually with (1) $\Leftrightarrow$ (2). □

Next, a ϕ -ring R is said to be nonnil-self-injective if R is a nonnil injective module over itself. The following theorem characterizes the ϕ -von Neumann regular rings in terms of the closed nonnil-Gorenstein global dimension.

Theorem 4.12. The following are equivalent for a strongly ϕ -ring R :

1. R is a nonnil self-injective ring,
2. $\text{Nil}(R)$ and $R/\text{Nil}(R)$ are nonnil injective R -modules,
3. $\text{Nil}(R)$ is a nonnil-injective ideal of R and $R/\text{Nil}(R)$ is a self-injective ring,
4. $R/\text{Nil}(R)$ is a self injective ring,
5. R is a ϕ -von Neumann regular ring,
6. $\overline{\phi\text{-G.gl.dim}(R)} = 0$.

Proof. (1) $\Rightarrow$ (2) Assume that R is a nonnil self-injective ring. Then $\text{Nil}(R)$ is a nonnil injective ideal. In fact, it is easy to see that $R/\text{Nil}(R)$ is a ϕ -torsion-free R -module, and so for any nonnil ideal I of R , we get $\text{Hom}_R(R/I, R/\text{Nil}(R)) = 0$ by [32, Theorem 2.3]. Using the sequence $0 \rightarrow \text{Nil}(R) \rightarrow R \rightarrow R/\text{Nil}(R) \rightarrow 0$, we obtain that $\text{Ext}_R^1(R/I, \text{Nil}(R)) = 0$ since R is nonnil self-injective, and so $\text{Nil}(R)$ is a nonnil-injective ideal. Since $\text{Ext}_R^1(R/I, R/\text{Nil}(R)) \cong \text{Ext}_R^2(R/I, \text{Nil}(R))$, it follows that $\text{Ext}_R^1(R/I, R/\text{Nil}(R)) = 0$, and so $R/\text{Nil}(R)$ is a nonnil injective R -module.

(2) $\Rightarrow$ (1) If $\text{Nil}(R)$ and $R/\text{Nil}(R)$ are nonnil injective R -modules, then it is straightforward to see that R is a nonnil self-injective ring.

(2) $\Leftrightarrow$ (3) This follows from [31, Proposition 1.4].

(3) $\Rightarrow$ (5) Let $s \in R \setminus \text{Nil}(R)$. Since $R/\text{Nil}(R)$ is a nonnil-injective R -module, it is a divisible R -module by [14, Theorem 2.9], and so there exists $r \in R$ such that $1 + \text{Nil}(R) = sr + \text{Nil}(R)$. Hence $sr \in 1 + \text{Nil}(R) \subset U(R)$. Therefore, $R \setminus \text{Nil}(R) \subset U(R)$. It follows that R is a local ϕ -ring with maximal ideal $\text{Nil}(R)$. Therefore, R is a ϕ -von Neumann regular ring by [14, Theorem 5.14].

(5) $\Rightarrow$ (1) This follows from [14, Remarks 4.9 and Theorem 5.32].

(4) $\Leftrightarrow$ (5) This follows immediately from [32, Theorem 4.1] and the fact that every self-injective integral domain is a field.

(5) $\Rightarrow$ (6) If R is a ϕ -von Neumann regular ring, then each ϕ -u-torsion R -module is equal zero. Then $\overline{\phi\text{-G. gl. dim}(R)} = 0$.

(6) $\Rightarrow$ (1) Assume that R is a ϕ -ring of the closed nonnil-Gorenstein global dimension 0. By Theorem 4.11, we deduce easily that R is nonnil-self-injective. $\square$

By combining Theorem 2.11 and Theorem 4.12, we give the following corollary.

Corollary 4.13. *The following are equivalent for a ϕ -ring R :*

1. R is a ϕ -von Neumann regular ring,
2. R is a strongly ϕ -ring such that every R -module has finite ϕ -projective dimension and every ϕ -torsion module is nonnil-G-projective,
3. R is a strongly ϕ -ring such that every R -module has finite ϕ -projective dimension and every ϕ -u-torsion module is nonnil-G-projective,
4. R is a strongly ϕ -ring such that every R -module has finite ϕ -injective dimension and every ϕ -torsion module is nonnil-G-injective,
5. R is a strongly ϕ -ring such that every R -module has finite ϕ -injective dimension and every ϕ -u-torsion module is nonnil-G-injective,
6. R is a strongly ϕ -ring such that every ϕ -u-projective module is nonnil-injective,
7. R is a strongly ϕ -ring such that every nonnil-injective module is ϕ -u-projective,
8. R is a strongly ϕ -ring of $\overline{\phi\text{-G. gl. dim}(R)} = 0$.

Statements and Declarations

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Funding

H. Kim was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF), funded by the Ministry of Education (2021R111A3047469).

References

- [1] D. F. Anderson and A. Badawi, On ϕ -Prüfer rings and ϕ -Bézout rings, *Houston J. Math.*, 30(2) (2004), 331-343.
- [2] D. F. Anderson and A. Badawi, On ϕ -Dedekind rings and ϕ -Krull rings, *Houston J. Math.* 31(4) (2005), 1007-1022.
- [3] M. Auslander and M. Bridger, Stable Module Theory, *Mem. Amer. Math. Soc.* 94, (1969).
- [4] A. Badawi, On nonnil-Noetherian rings, *Comm. Algebra* 31(4) (2003), 1669-1677.

- [5] A. Badawi and T. G. Lucas, Rings with prime nilradical, in *Arithmetical Properties of Commutative Rings and Monoids*, vol. 241 of *Lect. Notes Pure Appl. Math.*, pp. 198–212, Chapman & Hall/CRC, Boca Raton, Fla, USA, 2005.
- [6] C. Bakkari, S. Kabbaj and N. Mahdou, Trivial extensions defined by Prüfer conditions, *J. Pure Appl. Algebra*, 214(1), (2010), 53–60.
- [7] D. Bennis and N. Mahdou, Global Gorenstein dimensions, *Proc. Am. Math. Soc.* 138(2) (2010), 461–465.
- [8] D. Bennis and N. Mahdou, Strongly Gorenstein projective, injective, and flat modules. *J. Pure. Appl. Algebra. Soc.*, 210(2) (2007), 437–445.
- [9] D. Bennis, N. Mahdou and K. Ouarghi, Rings over which all modules are strongly Gorenstein projective, *Rocky Mt. J. Math.*, 40(3) (2010), 749–759.
- [10] D. Bennis and K. Ouarghi, $\mathcal{X}$ -Gorenstein projective modules, *Int. Math. Forum*, 5 (10), (2010), 487–491.
- [11] M. Chhiti, N. Mahdou and M. Tamekkante, Self injective amalgamated duplication along an ideal. *J. Algebra Appl.*, 12(07) (2013), 1350033.
- [12] L. Christensen, Gorenstein Dimensions. In: *Lecture Notes in Mathematics*, vol. 1747. Springer, Berlin (2000).
- [13] L. Christensen, A. Frankild and H. Holm, On Gorenstein projective, injective and flat dimensions — a functorial description with applications. *J. Algebra* 302 (2006), 231–279.
- [14] Y. El Haddaoui and N. Mahdou, On ϕ -(weak) global dimension, *J. Algebra its Appl.*, 2023, DOI: 10.1142/S021949882450169X
- [15] E. E. Enochs and O. M. G. Jenda, Gorenstein injective and projective modules. *Math. Z.* 220 (1995), 611–633.
- [16] E. E. Enochs and O. M. G. Jenda, On Gorenstein injective modules. *Commun. Algebra* 21(10) (1993), 3489–3501.
- [17] E. E. Enochs and O. M. G. Jenda, *Relative Homological Algebra*, Walter de Gruyter, 2001.
- [18] E. E. Enochs, O. M. G. Jenda and B. Torrecillas, Gorenstein flat modules, *Nanjing Daxue Xuebao Shuxue Bannian Kan* 10 (1993), 1–9.
- [19] S. Glaz, *Commutative Coherent Rings*, *Lecture Notes in Mathematics*, Vol. 1371, Berlin: Springer-Verlag, 1989.
- [20] Z. Gao and F. G. Wang, All Gorenstein hereditary rings are coherent, *J. Algebra its Appl.*, 13(04) (2014), 1350140 (5 pages).
- [21] H. Holm, Gorenstein homological dimensions. *J. Pure Appl. Algebra*, 189 (2004), 167–193.
- [22] H. Holm, Rings with finite Gorenstein injective dimension, *Proc. Amer. Math. Soc.*, 132(5) (2003), 1279–1283.
- [23] J. A. Huckaba, *Commutative Rings with Zero Divisors*, *Monographs and Textbooks in Pure and Appl. Math.*, 117, Dekker, New York, 1988.

- [24] S. Kabbaj, Matlis' semi-regularity and semi-coherence in trivial ring extensions: a survey, *Moroccan J. Algebra Geom. Appl.*, 1(1) (2022), 1-17.
- [25] S. Kabbaj and N. Mahdou, Trivial extensions defined by coherent-like conditions, *Commun. Algebra*, 32(10) (2004), 3937-3953.
- [26] S. Kabbaj and N. Mahdou, Trivial extensions of local rings and a conjecture of Costa, *Dekker Lect. Notes Pure Appl. Math.* 231 (2003), pp. 301-312.
- [27] N. Mahdou and O. Ouarghi, Gorenstein dimensions in trivial ring extensions, *Commutative Algebra and Applications*, Walter De Gruyter, (2009), pp. 293-302.
- [28] N. Mahdou and M. Tamekkante, On (strongly) Gorenstein (semi)hereditary rings, *Arab J Sci Eng*, 36(3) ((2011)), 431-440.
- [29] N. Mahdou, M. Tamekkante and S. Yassemi, On (strongly) Gorenstein von Neumann regular rings, *Commun. Algebra*, 39 (3), (2011), 3242-3252.
- [30] F. Meng and Q. Pan, $\mathcal{X}$ -Gorenstein projective and $\mathcal{Y}$ -Gorenstein injective modules, *Hacet. J. Math. Stat.*, 40 (4) (2011), 537-554.
- [31] W. Qi and X. L. Zhang, Some remarks on ϕ -Dedekind rings and ϕ -Prüfer rings, *arXiv:2103.08278v3 [math.AC]* 15 Jan 2023
- [32] G. H. Tang, F. G. Wang and W. Zhao, On ϕ -von Neumann regular rings. *J. Korean Math. Soc.*, 50(1) (2013), 219-229.
- [33] F. G. Wang and H. Kim, *Foundations of Commutative Rings and Their Modules*, Algebra and Applications, 22, Springer, Singapore, 2016.
- [34] J. Wang, X. Xu and Z. Zhao, $\mathcal{X}$ -Gorenstein projective dimensions, *J. Math. Study*, 55 (2022), 398-414.



ISSN: 2820-7114

Moroccan Journal of Algebra and Geometry with Applications

Supported by Sidi Mohamed Ben Abdellah University, Fez, Morocco

Volume 4, Issue 2 (2025), pp 198-206

Title :

**New Eisenstein series identities for the Ramanujan-Göllnitz-Gordon continued fraction
and combinatorial partition identities**

Author(s):

Mahendra Mal Chaudhary & Ananda Rathna Kumara Vanitha

New Eisenstein series identities for the Ramanujan–Göllnitz–Gordon continued fraction and combinatorial partition identities

Mahendra Mal Chaudhary¹ and Ananda Rathna Kumara Vanitha²

¹ International Scientific Research and Welfare Organization, New Delhi, India.

e-mail: dr.m.p.chaudhary@gmail.com

² Department of Mathematics, The National Institute of Engineering, Mysuru 570008, Karnataka, India.

e-mail: a.vanitha4@gmail.com

Communicated by Bouchaïb Sodaïgui

(Received 29 August 2024, Revised 27 February 2025, Accepted 09 March 2025)

Abstract. In this paper, we establish several new Eisenstein series identities associated with Ramanujan–Göllnitz–Gordon continued fraction. We further derive inter relationships between Eisenstein series identities and combinatorial partition identities.

Key Words: Continued fraction, Eisenstein series, combinatorial partition identities.

2020 MSC: Primary 11A55, 11M36; Secondary 11P83.

1 Introduction

Throughout this paper, we assume that q is a complex number such that $|q| < 1$ and use the standard product notation

$$(a; q)_0 := 1, \quad (a; q)_n := \prod_{j=0}^{n-1} (1 - aq^j) \quad \text{and} \quad (a; q)_\infty := \prod_{n=0}^{\infty} (1 - aq^n).$$

For convenience, we sometimes use the multiple q -shifted factorial notation, which is defined as

$$(a_1, a_2, \dots, a_m; q)_\infty = (a_1; q)_\infty (a_2; q)_\infty \cdots (a_m; q)_\infty.$$

The celebrated Ramanujan–Göllnitz–Gordon continued fraction is defined as

$$G(q) = \frac{q^{1/2}}{1+q} + \frac{q^2}{1+q^3} + \frac{q^4}{1+q^5} + \frac{q^6}{1+q^7} + \cdots \quad (1)$$

An interesting product representation of $G(q)$ is recorded in [18]

$$G(q) = q^{\frac{1}{2}} \frac{(q; q^8)_\infty (q^7; q^8)_\infty}{(q^3; q^8)_\infty (q^5; q^8)_\infty}. \quad (2)$$

On page 299 of his second notebook [18], Ramanujan recorded the two identities,

$$\frac{1}{G(q)} - G(q) = \frac{(-q^2; q^4)_\infty^2 (q^4; q^4)_\infty (q^4; q^8)_\infty}{q^{1/2} (q^8; q^8)_\infty}, \quad (3)$$

and

$$\frac{1}{G(q)} + G(q) = \frac{(-q; q^2)_\infty^2 (q^2; q^2)_\infty (q^4; q^8)_\infty}{q^{1/2} (q^8; q^8)_\infty}. \quad (4)$$

The identity (2) was rediscovered and proved independently by Göllnitz [12] and Gordon [13]. The identities (3) and (4) were first proved by Berndt [3] and then rediscovered by Chan and Huang [11].

A *partition* of a positive integer n is a non-increasing sequence of positive integers whose sum is equal to n . The integers in a partition are called *parts*. We denote the number of partitions of n by $p(n)$, and follow the convention $p(0) := 1$. For instance, since the partitions of 4 are

$$4, 3+1, 2+2, 2+1+1 \text{ and } 1+1+1+1,$$

we have $p(4) = 5$. Euler established the identity

$$\sum_{n=0}^{\infty} p(n) q^n = \frac{1}{(q; q)_\infty}. \quad (5)$$

Andrews et al. [2] investigated new double summation hypergeometric q -series representations for several families of partitions and further explored the role of double series in combinatorial partition identities by introducing the following general family:

$$R(s, t, l, u, v, w) := \sum_{n=0}^{\infty} q^{s \binom{n}{2} + tn} r(l, u, v, w; n), \quad (6)$$

where

$$r(l, u, v, w; n) := \sum_{j=0}^{\left\lfloor \frac{n}{u} \right\rfloor} (-1)^j \frac{q^{uv \binom{j}{2} + (w-ul)j}}{(q; q)_{n-uj} (q^{uv}; q^{uv})_j}. \quad (7)$$

The following interesting special cases of (6) are recalled [2 p. 106]

$$R(2, 1, 1, 1, 2, 2) = (-q; q^2)_\infty; \quad (8)$$

$$R(2, 2, 1, 1, 2, 2) = (-q^2; q^2)_\infty; \quad (9)$$

$$R(m, m, 1, 1, 1, 2) = \frac{(q^{2m}; q^{2m})_\infty}{(q^m; q^{2m})_\infty}. \quad (10)$$

In [6], Chaudhary et al. have established the combinatorial partition identities for the identities (3) and (4) using (8)–(10). In [4, 5, 7, 8, 9, 10], Chaudhary et al. have established the several identities between q -product identities and combinatorial partition identities. Recently, Srivastava et al. [19, 20] established new results which depict the inter relationships between q -product identities, continued fraction identities and combinatorial partition identities.

The main purpose of this paper is to establish many new Eisenstein series identities involving the Ramanujan–Göllnitz–Gordon continued fraction. We further develop inter relationships between Eisenstein series identities and combinatorial partition identities for $G(q)$.

2 Definitions and Preliminary results

In this section, we present some basic definitions and preliminary results on Ramanujan's theta functions. Ramanujan's theta function $f(a, b)$ is defined, for $|ab| < 1$, by

$$f(a, b) = \sum_{n=-\infty}^{\infty} a^{n(n+1)/2} b^{n(n-1)/2}. \quad (11)$$

In Ramanujan's notation, Jacobi triple product identity is given by [1] Entry 19]

$$f(a, b) = (-a; ab)_{\infty} (-b; ab)_{\infty} (ab; ab)_{\infty}. \quad (12)$$

Then it is easy to verify that

$$f(a, b) = f(b, a), \quad f(1, a) = 2f(a, a^3), \quad f(-1, a) = 0.$$

If n is an integer,

$$f(a, b) = a^{n(n+1)/2} b^{n(n-1)/2} f(a(ab)^n, b(ab)^{-n}). \quad (13)$$

The three most interesting special cases of $f(a, b)$ are [1] Entry 22]

$$\varphi(q) := f(q, q) = \sum_{n=-\infty}^{\infty} q^{n^2} = (-q; q^2)_{\infty} (q^2; q^2)_{\infty}, \quad (14)$$

$$\psi(q) := f(q, q^3) = \sum_{n=0}^{\infty} q^{n(n+1)/2} = \frac{(q^2; q^2)_{\infty}}{(q; q^2)_{\infty}} \quad (15)$$

and

$$f(-q) := f(-q, -q^2) = \sum_{n=-\infty}^{\infty} (-1)^n q^{n(3n-1)/2} = (q; q)_{\infty}. \quad (16)$$

Note that $\eta(\tau) = q^{1/24} f(-q)$ where $q = e^{2\pi i \tau}$, $\text{Im} \tau > 0$, and $\eta(\tau)$ is the Dedekind-eta function. Also, after Ramanujan, define

$$\chi(q) := (-q; q^2)_{\infty}. \quad (17)$$

The following q -serie identity:

$$(-q; q)_{\infty} = \frac{1}{(q; q^2)_{\infty}} = \frac{1}{\chi(-q)} \quad (18)$$

provides the analytical equivalence of Euler's theorem: The number of partitions of a positive integer n into distinct parts is equal to the number of partitions of n into odd parts. For convenience, we define, for a positive integer n , that

$$f_n := f(-q^n) = (q^n; q^n)_{\infty}.$$

The following lemma is a consequence of the product representations (14)–(17).

Lemma 2.1. [1] We have

$$\varphi(q) = \frac{f_2^5}{f_1^2 f_4^2}, \quad \psi(q) = \frac{f_2^2}{f_1}, \quad \varphi(-q) = \frac{f_1^2}{f_2}, \quad \psi(-q) = \frac{f_1 f_4}{f_2},$$

$$f(q) = \frac{f_2^3}{f_1 f_4}, \quad \chi(q) = \frac{f_2^2}{f_1 f_4} \quad \text{and} \quad \chi(-q) = \frac{f_1}{f_2}.$$

The Jacobi theta function θ_1 , which is defined as

$$\theta_1(x|z) = 2 \sum_{n=0}^{\infty} (-1)^n q^{\frac{(2n+1)^2}{8}} \sin(2n+1)x = 2q^{\frac{1}{8}} \sum_{n=0}^{\infty} (-1)^n q^{\frac{n(n+1)}{2}} \sin(2n+1)x. \quad (19)$$

In [14], Chan et al. showed that

$$\begin{aligned} 2 \sum_{n=0}^{\infty} (-1)^n q^{\frac{n(n+1)}{2}} \sin(2n+1)x &= \sum_{n=-\infty}^{\infty} (-1)^n q^{\frac{n(n+1)}{2}} \sin(2n+1)x \\ &= 2(\sin x)(q; q)_{\infty} (qe^{2ix}; q)_{\infty} (qe^{-2ix}; q)_{\infty}. \end{aligned} \quad (20)$$

Combining (20) and (19), we find the infinite product representation of θ_1 :

$$\begin{aligned} \theta_1(x|z) &= 2q^{\frac{1}{8}} (\sin x)(q; q)_{\infty} (qe^{2ix}; q)_{\infty} (qe^{-2ix}; q)_{\infty} \\ &= iq^{\frac{1}{8}} e^{-ix} (q; q)_{\infty} (e^{2ix}; q)_{\infty} (e^{-2ix}; q)_{\infty}. \end{aligned} \quad (21)$$

Differentiating both sides of the equation (21) and then setting $x = 0$ yields

$$\theta'_1(0|z) = 2q^{1/8} (q; q)_{\infty}^3, \quad (22)$$

where θ'_1 denotes the partial derivative of θ_1 with respect to x .

3 Eisenstein series identities associated with $G(q)$

In this section, we establish many new Eisenstein series identities associated with $G(q)$ by using the Ramanujan's ${}_1\Psi_1$ summation formula and the Jacobi theta function θ_1 .

Theorem 3.1. Let $|q| < 1$. Then, we have the Eisenstein series identities

$$\sum_{\substack{n=1 \\ n \equiv 1 \pmod{2}}}^{\infty} \frac{q^n - q^{3n}}{1 - q^{8n}} + \sum_{\substack{n=1 \\ n \equiv 1 \pmod{2}}}^{\infty} \frac{q^{5n} - q^{7n}}{1 - q^{8n}} = \frac{\eta^4(16\tau)}{\eta^2(8\tau)} \left(\frac{1}{G(q^2)} - G(q^2) \right), \quad (23)$$

$$\sum_{\substack{n=1 \\ n \equiv 1 \pmod{4}}}^{\infty} \frac{q^n + q^{5n}}{1 - q^{8n}} - \sum_{\substack{n=1 \\ n \equiv 3 \pmod{4}}}^{\infty} \frac{q^{3n} + q^{7n}}{1 - q^{8n}} = \frac{\eta^2(32\tau)\eta(16\tau)}{\eta(8\tau)} \left(\frac{1}{G(q^4)} + G(q^4) \right), \quad (24)$$

and

$$\begin{aligned} &\sum_{\substack{n=1 \\ n \equiv 1 \pmod{8}}}^{\infty} \frac{q^n - q^{5n}}{1 - q^{8n}} - \sum_{\substack{n=1 \\ n \equiv 3 \pmod{8}}}^{\infty} \frac{q^{3n} + q^{7n}}{1 - q^{8n}} + \sum_{\substack{n=1 \\ n \equiv 5 \pmod{8}}}^{\infty} \frac{q^n + q^{5n}}{1 - q^{8n}} - \sum_{\substack{n=1 \\ n \equiv 7 \pmod{8}}}^{\infty} \frac{q^{7n} - q^{3n}}{1 - q^{8n}} \\ &= \frac{\eta^2(16z)\eta^2(64z)}{\eta(8z)\eta(32z)} \left(\frac{1}{G(q^8)} - G(q^8) \right). \end{aligned} \quad (25)$$

Proof. Changing n to $-n$ in the second summation, in the left-hand side of (23), we obtain

$$\sum_{\substack{n=1 \\ n \equiv 1 \pmod{2}}}^{\infty} \frac{q^n - q^{3n}}{1 - q^{8n}} + \sum_{\substack{n=-\infty \\ n \equiv 1 \pmod{2}}}^{-1} \frac{q^{-5n} - q^{-7n}}{1 - q^{-8n}} = \sum_{n=-\infty}^{\infty} \frac{q^{2n+1}}{1 - q^{16n+8}} - \sum_{n=-\infty}^{\infty} \frac{q^{6n+3}}{1 - q^{16n+8}}. \quad (26)$$

Using a corollary of Ramanujan's ${}_1\Psi_1$ summation formula with $b = aq$ [1, Entry 17, p. 32]

$$\sum_{n=-\infty}^{\infty} \frac{z^n}{1 - aq^n} = \frac{(az, q/az, q, q; q)_{\infty}}{(a, q/a, z, q/z; q)_{\infty}}, \quad |q| < |z| < 1, \quad (27)$$

in (26), we find that

$$\begin{aligned} & \sum_{\substack{n=1 \\ n \equiv 1 \pmod{2}}}^{\infty} \frac{q^n - q^{3n}}{1 - q^{8n}} + \sum_{\substack{n=-\infty \\ n \equiv 1 \pmod{2}}}^{-1} \frac{q^{-5n} - q^{-7n}}{1 - q^{-8n}} \\ &= \frac{(q^{16}; q^{16})_{\infty}^2}{(q^8; q^{16})_{\infty}^2} \left\{ q \frac{(q^6, q^{10}; q^{16})_{\infty}}{(q^2, q^{14}; q^{16})_{\infty}} - q^3 \frac{(q^2, q^{14}; q^{16})_{\infty}}{(q^6, q^{10}; q^{16})_{\infty}} \right\}. \end{aligned} \quad (28)$$

Using (2) in (28), we obtain (23). Proofs of (24) and (25) are similar to the proof of (23), so we omit them here. $\square$

Now we prove the following remarkable identity:

Lemma 3.2. *We have*

$$\sum_{n=1}^{\infty} \frac{q^n - q^{3n} - q^{5n} + q^{7n}}{1 - q^{8n}} \sin 2nx = -\frac{\theta_1'(0|8z)\theta_1(2\pi z|8z)\theta_1(4\pi z|8z)\theta_1(2x|8z)}{4\theta_1(x + \pi z|8z)\theta_1(x - \pi z|8z)\theta_1(x + 3\pi z|8z)\theta_1(x - 3\pi z|8z)}. \quad (29)$$

Proof. For simplicity, we use $J(x|z)$ to denote the logarithmic derivative of θ_1 with respect to x . Logarithmically differentiating (21) with respect to x , after some manipulation, we have

$$J\left(x + \frac{\pi z}{2}|z\right) = -i + 4 \sum_{n=1}^{\infty} \frac{q^{n/2}}{1 - q^n} \sin 2nx. \quad (30)$$

Replacing z by $8z$ in the above equation, we deduce that

$$J(x + 4\pi z|8z) = -i + 4 \sum_{n=1}^{\infty} \frac{q^{4n}}{1 - q^{8n}} \sin 2nx. \quad (31)$$

Replacing x by $x - 3\pi z$ in the above equation, we obtain

$$J(x + \pi z|8z) = -i + 4 \sum_{n=1}^{\infty} \frac{q^{4n}}{1 - q^{8n}} \sin 2n(x - 3\pi z).$$

Writing x as $-x$ in the above equation, we are led to the identity

$$J(x - \pi z|8z) = i + 4 \sum_{n=1}^{\infty} \frac{q^{4n}}{1 - q^{8n}} \sin 2n(x + 3\pi z).$$

Adding the above two equations together and using the trigonometric identity

$$\sin 2n(x - 3\pi z) + \sin 2n(x + 3\pi z) = 2 \cos 6n\pi z \sin 2nx = (q^{3n} + q^{-3n}) \sin 2nx,$$

in the resulting equation, we immediately deduce that

$$J(x - \pi z|8z) + J(x + \pi z|8z) = 4 \sum_{n=1}^{\infty} \frac{q^n + q^{7n}}{1 - q^{8n}} \sin 2nx.$$

In a similar way, we find that

$$J(x - 3\pi z|8z) + J(x + 3\pi z|8z) = 4 \sum_{n=1}^{\infty} \frac{q^{3n} + q^{5n}}{1 - q^{8n}} \sin 2nx.$$

Combining the above two equations, we find that

$$\begin{aligned} 4 \sum_{n=1}^{\infty} \frac{q^n - q^{3n} - q^{5n} + q^{7n}}{1 - q^{8n}} \sin 2nx \\ = J(x - \pi z|8z) + J(x + \pi z|8z) - J(x - 3\pi z|8z) - J(x + 3\pi z|8z). \end{aligned} \quad (32)$$

Recall the following identity, which can be found in [15, Theorem 5], [17, Corollary 2]:

$$\begin{aligned} J(x_1|z) + J(x_2|z) + J(x_3|z) - J(x_1 + x_2 + x_3|z) \\ = \frac{\theta'_1(0|z)\theta_1(x_1 + x_2|z)\theta_1(x_2 + x_3|z)\theta_1(x_1 + x_3|z)}{\theta_1(x_1|z)\theta_1(x_2|z)\theta_1(x_3|z)\theta_1(x_1 + x_2 + x_3|z)}. \end{aligned} \quad (33)$$

Replacing z by $8z$ in the above equation and then letting x_1 to $x - \pi z$, x_2 to $x + \pi z$, x_3 to $-x + 3\pi z$, we obtain

$$\begin{aligned} J(x - \pi z|8z) + J(x + \pi z|8z) - J(x - 3\pi z|8z) - J(x + 3\pi z|8z) \\ = - \frac{\theta'_1(0|8z)\theta_1(2\pi z|8z)\theta_1(4\pi z|8z)\theta_1(2z|8z)}{\theta_1(x + \pi z|8z)\theta_1(x - \pi z|8z)\theta_1(x + 3\pi z|8z)\theta_1(x - 3\pi z|8z)}. \end{aligned} \quad (34)$$

Combining (34) and (32), we get (29). $\square$

Using identity (29), we can obtain the following Eisenstein series identities:

Theorem 3.3. Let $|q| < 1$. Then, we have the Eisenstein series identities

$$\sum_{n=1}^{\infty} \frac{n(q^n - q^{3n} - q^{5n} + q^{7n})}{1 - q^{8n}} = \frac{\eta^4(8z)\eta^2(4z)}{\eta^2(2z)} \left(\frac{1}{G(q)} + G(q) \right), \quad (35)$$

and

$$\sum_{n=1}^{\infty} \binom{n}{3} \frac{q^n - q^{3n} - q^{5n} + q^{7n}}{1 - q^{8n}} = \frac{\eta(z)\eta^2(2z)\eta(6z)\eta^3(8z)\eta(24z)}{\eta(3z)\eta^5(4z)} \left(\frac{1}{G(q)} - G(q) \right). \quad (36)$$

Proof. Dividing both sides of (29) by z and then letting $z \rightarrow 0$, we get

$$\sum_{n=1}^{\infty} \frac{n(q^n - q^{3n} - q^{5n} + q^{7n})}{1 - q^{8n}} = - \frac{\theta'_1(0|8z)^2\theta_1(2\pi z|8z)\theta_1(4\pi z|8z)}{4\theta_1^2(\pi z|8z)\theta_1^2(3\pi z|8z)}. \quad (37)$$

Using (21), we easily find that

$$\theta_1(\pi z|8z) = iq^{1/2}(q, q^7, q^8; q^8)_{\infty}, \quad \theta_1(2\pi z|8z) = i(q^2, q^6, q^8; q^8)_{\infty}, \quad (38)$$

$$\theta_1(3\pi z|8z) = iq^{-1/2}(q^3, q^5, q^8; q^8)_{\infty}, \quad \theta_1(4\pi z|8z) = iq^{-1}(q^4, q^8; q^8)_{\infty}^2. \quad (39)$$

Employing (38) and (39) in (37), after simplification, we obtain

$$\sum_{n=1}^{\infty} \frac{n(q^n - q^{3n} - q^{5n} + q^{7n})}{1 - q^{8n}} = \frac{q(q^2; q^2)_{\infty}(q^4; q^4)_{\infty}(q^8; q^8)_{\infty}^2}{(q; q^2)_{\infty}^2}. \quad (40)$$

Using Lemma 2.1 and (4) in the right-hand side of the (40), then after some simplifications, we obtain our desire identity (35).

If p is a prime, we use $\left(\frac{\cdot}{p}\right)$ to denote the Legendre symbol modulo p . Setting $x = \frac{\pi}{3}$ in (29) and noting that

$$\sin \frac{2n\pi}{3} = \frac{\sqrt{3}}{2} \left(\frac{n}{3}\right), \quad \theta_1\left(\frac{2\pi}{3}|z\right) = \sqrt{3}q^{1/8}(q^3; q^3)_\infty,$$

we find that

$$\begin{aligned} & \sum_{n=1}^{\infty} \left(\frac{n}{3}\right) \frac{q^n - q^{3n} - q^{5n} + q^{7n}}{1 - q^{8n}} \\ &= - \frac{q\theta_1'(0|8z)\theta_1(2\pi z|8z)\theta_1(4\pi z|8z)(q^{24}; q^{24})_\infty}{2\theta_1(\pi/3 + \pi z|8z)\theta_1(\pi/3 - \pi z|8z)\theta_1(\pi/3 + 3\pi z|8z)\theta_1(\pi/3 - 3\pi z|8z)}. \end{aligned} \quad (41)$$

Recall the beautiful identity [16, Eq. (3. 1)]

$$\theta_1\left(\frac{\pi}{3} - x|z\right)\theta_1\left(\frac{\pi}{3} + x|z\right) = \frac{(q; q)_\infty^3}{(q^3; q^3)_\infty} \frac{\theta_1(3x|3z)}{\theta_1(x|z)}.$$

Using the above identity in (41), after some simplifications, we obtain

$$\sum_{n=1}^{\infty} \left(\frac{n}{3}\right) \frac{q^n - q^{3n} - q^{5n} + q^{7n}}{1 - q^{8n}} = \frac{q(q; q)_\infty (q^4; q^4)_\infty (q^{24}; q^{24})_\infty}{(q^8; q^8)_\infty (q^3; q^6)_\infty}. \quad (42)$$

Using Lemma 2.1 and (3) in the right-hand side of the (42), then after some simplifications, we obtain our desire identity (36). $\square$

4 Combinatorial partition identities

In this section, we give certain inter relationships between Eisenstein series identities and combinatorial partition identities.

Theorem 4.1. Let $|q| < 1$. Then, we have the identities

$$\sum_{n=1 \pmod{2}}^{\infty} \frac{q^n - q^{3n}}{1 - q^{8n}} + \sum_{n=1 \pmod{2}}^{\infty} \frac{q^{5n} - q^{7n}}{1 - q^{8n}} = q^2 R^2(8, 8, 1, 1, 1, 2) \left(\frac{1}{G(q^2)} - G(q^2) \right), \quad (43)$$

$$\sum_{n=1 \pmod{4}}^{\infty} \frac{q^n + q^{5n}}{1 - q^{8n}} - \sum_{n=3 \pmod{4}}^{\infty} \frac{q^{3n} + q^{5n}}{1 - q^{8n}} = q^3 R(8, 8, 1, 1, 1, 2) R(16, 16, 1, 1, 1, 2) \left(\frac{1}{G(q^4)} + G(q^4) \right), \quad (44)$$

and

$$\begin{aligned} & \sum_{n=1 \pmod{8}}^{\infty} \frac{q^n - q^{5n}}{1 - q^{8n}} - \sum_{n=3 \pmod{8}}^{\infty} \frac{q^{3n} + q^{7n}}{1 - q^{8n}} + \sum_{n=5 \pmod{8}}^{\infty} \frac{q^n + q^{5n}}{1 - q^{8n}} - \sum_{n=7 \pmod{8}}^{\infty} \frac{q^{7n} - q^{3n}}{1 - q^{8n}} \\ &= q^5 R(8, 8, 1, 1, 1, 2) R(32, 32, 1, 1, 1, 2) \left(\frac{1}{G(q^8)} - G(q^8) \right), \end{aligned} \quad (45)$$

Proof. Using the identity of (10) with $m = 8$ in (23), we are led to the desire identity (43). Next, using the identity of (10) with $m = 8$ and $m = 16$ in (24), we are led to the desire identity (44). Further, using the identity of (10) with $m = 8$ and $m = 32$ in (25), we are led to the desire identity (45). $\square$

Theorem 4.2. Let $|q| < 1$. Then, we have the identities

$$\sum_{n=1}^{\infty} \frac{n(q^n - q^{3n} - q^{5n} + q^{7n})}{1 - q^{8n}} = q(q^8; q^8)_{\infty}^2 R(2, 2, 1, 1, 2, 2) R^2(1, 1, 1, 1, 1, 2), \quad (46)$$

and

$$\sum_{n=1}^{\infty} \left(\frac{n}{3}\right) \frac{q^n - q^{3n} - q^{5n} + q^{7n}}{1 - q^{8n}} = \frac{q(q; q)_{\infty} (q^8; q^8)_{\infty} (q^{24}; q^{24})_{\infty}}{(q^3; q^6)_{\infty} R(4, 4, 1, 1, 1, 2)}. \quad (47)$$

Proof. Using the identities (9) and (10) with $m = 1$ in (35), we are led to the desire identity (46). Similarly, using the identity of (10) with $m = 4$ in (36), we are led to the desire identity (47). $\square$

Acknowledgements:

The work of the first-named author (M. P. Chaudhary) was funded by the National Board of Higher Mathematics (NBHM) of the Department of Atomic Energy (DAE) of the Government of India by its sanction letter (Ref. No. 02011/12/2020 NBHM (R. P.)/R D II/7867) dated 19 October 2020. The authors are grateful for the anonymous referees for their helpful suggestions and comments for the improvement of this research work.

References

- [1] C. Adiga, B. C. Berndt, S. Bhargava and G. N. Watson, Chapter 16 of Ramanujan's second notebook: Theta functions and q -series, *Mem. Amer. Math. Soc.* 315 (1985), 1-91.
- [2] G. E. Andrews, K. Bringman and K. Mahlburg, Double series representation for Schur's partition function and related identities, *J. Combin. Theory Ser. A* 132 (2015), 102-119.
- [3] B. C. Berndt, *Ramanujan's Notebooks, Part III*, Springer-Verlag, Heidelberg and New York, 1991.
- [4] M. P. Chaudhary, Generalization of Ramanujan's identities in terms of q -products and continued fractions, *Global J. Sci. Frontier Res. Math. Decision Sci.* 12(2) (2012), 53-60.
- [5] M. P. Chaudhary, Some relationships between q -product identities, combinatorial partition identities and continued fractions identities III, *Pacific J. Appl. Math.* 7(2) (2015), 87-95.
- [6] M. P. Chaudhary and J. Choi, Certain identities associated with Eisenstein series, Ramanujan–Göllnitz–Gordon continued fraction and combinatorial partition identities, *Int. J. Math. Anal.* 10 (2016), 237-244.
- [7] M. P. Chaudhary and G. A. S. Salilew, Note on q -product identities and combinatorial partition identities, *Honam Math. J.* 39 (2017), 267-273.
- [8] M. P. Chaudhary, S. Chaudhary and S. Minz, On relationships between q -product identities and combinatorial partition identities, *Mathe. Moravica* 24(1)(2020), 83-91.
- [9] M. P. Chaudhary, A family of theta-function identities based upon R_{α} , R_{β} and R_m - functions related to Jacobi's triple product identity, *Publ. Inst. Math. (Beograd)* 108(122) (2020), 23-32.

- [10] M. P. Chaudhary, S. Guiben and K. Mazhouda, Relations between mock theta functions and combinatorial partition identities, *J. Ramanujan Soc. Math. Sci.* 10(1) (2022), 79-86.
- [11] H. H. Chan and S. -S. Huang, On the Ramanujan–Göllnitz–Gordon continued fraction, *Ramanujan J.* 1 (1997), 75-90.
- [12] H. Göllnitz, Partitionen mit Differenzenbedingungen, *J. Reine Angew. Math.* 225 (1967), 154-190.
- [13] B. Gordon, Some continued fractions of the Rogers-Ramanujan type, *Duke Math. J.* 32(1965), 741-748.
- [14] H. H. Chan, S. H. Chan and Z. -G. Liu, The Rogers–Ramanujan continued fraction and a new Eisenstein series identity, *J. Number Thy.* 129 (2009), 1786-1797.
- [15] Z. -G. Liu, A three-term theta function identity and its applications, *Adv. Math.* 195 (2005), 1-23.
- [16] Z. -G. Liu, A theta function identity and its implications, *Trans. Amer. Math. Soc.* 357 (2005), 825-835.
- [17] S. McCullough and L. -C. Shen, On the Szegő kernel of an annulus, *Proc. Amer. Math. Soc.*, 121 (1994), 1110-1120.
- [18] S. Ramanujan, *Notebooks (2 volumes)*, Tata Inst. Fund. Res., Bombay, 1957.
- [19] H. M. Srivastava and M. P. Chaudhary, Some relationships between q -product identities, combinatorial partition identities and continued fractions identities, *Adv. Stud. Contemporary Math.* 2(3) (2015), 265-272.
- [20] H. M. Srivastava, M. P. Chaudhary, S. Chaudhary and G. A. Salilew, Jacobi's triple product identity and an associated family of theta function identities, *Math. Notes* 112(5) (2022), 755-762.



ISSN: 2820-7114

Moroccan Journal of Algebra and Geometry with Applications

Supported by Sidi Mohamed Ben Abdellah University, Fez, Morocco

Volume 4, Issue 2 (2025), pp 207-238

Title :

Pairs of rings sharing their units

Author(s):

Gabriel Picavet & Martine Picavet-L'Hermitte

Pairs of rings sharing their units

Gabriel Picavet and Martine Picavet-L'Hermitte
Mathématiques 8 Rue du Forez, 63670 - Le Cendre France
e-mail: picavet.gm@wanadoo.fr

Communicated by Ayman Badawi

(Received 12 November 2024, Revised 16 March 2025, Accepted 21 March 2025)

Abstract. We are working in the category of commutative unital rings and denote by $U(R)$ the group of units of a nonzero ring R . An extension of rings $R \subseteq S$, satisfying $U(R) = R \cap U(S)$ is usually called local. This paper is devoted to the study of ring extensions such that $U(R) = U(S)$, that we call strongly local. P. M. Cohn in a paper, entitled Rings with zero divisors, introduced some strongly local extensions. We generalized under the name Cohn's rings his definition and give a comprehensive study of these extensions. As a consequence, we give a constructive proof of his main result. Now Lequain and Doering studied strongly local extensions, where S is semilocal, so that $S/J(S)$, where $J(S)$ is the Jacobson radical of S , is Von Neumann regular. These rings are usually called J -regular. We establish many results on J -regular rings in order to get substantial results on strongly local extensions when S is J -regular. The Picard group of a J -regular ring is trivial, allowing to evaluate the group $U(S)/U(R)$ when R is J -regular. We then are able to give a complete characterization of the Doering-Lequain context. A Section is devoted to examples. In particular, when R is a field, the strongly local and weakly strongly inert properties are equivalent.

Key Words: Group of units, local extension, strongly local extension, J -regular ring, integral extension, FCP extension.

2020 MSC: Primary:13B02; Secondary: 13B25

1 Introduction and Notation

This paper deals with commutative unital rings and their morphisms. Any ring R is supposed nonzero. We denote by $U(R)$ the set of units of a ring R . We will call *strongly local* an extension of rings $R \subseteq S$ such that $U(R) = U(S)$, also termed as an SL extension. The reason why is that a ring extension $R \subseteq S$ is classically called local if $U(R) = U(S) \cap R$. Naturally these notions do not coincide and have a ring morphism version. If $R \rightarrow S$ is a ring morphism and Q is a prime ideal of S lying over P in R , then $R_P \rightarrow S_Q$ is usually called a local morphism of $R \rightarrow S$.

Our work takes its origin in the reading of two papers. One of them was written by P.M. Cohn [6]: for any ring R , he exhibits an SL extension $R \subseteq R'$, such that any non unit of R' is a zerodivisor. To prove his main result, Cohn introduces some special rings in a lemma. We have considered rings of the same vein. The idea is as follows: if I is an ideal of a ring R , we define the ring $R//I := R[X]/XI[X]$ (where X is an indeterminate over R). This notation may seem weird, but it explains that the ring R/I is shifted. When I is a semiprime ideal, we have an SL extension $R \subseteq R//I$ with very nice properties. To have a better understanding, consider a field R and $I = 0$, we recover $R \subseteq R[X]$. We reprove Cohn's result and give a constructive proof, not using a transfinite induction. But Cohn's ring is not necessarily the same as ours, by lack of unicity. All these considerations are developed in Section 6. In Section 7 we consider a ring morphism $R \rightarrow R\{X\}$ used by E. Houston in the context of Noetherian rings and their dimensions. We generalize his results and give a link with the rings $R//M$, where M is a maximal ideal of R .

The other one was written by Doering and Lequain [9]. This paper deals with pair of semilocal rings sharing their group of units. A first observation is that for a semilocal ring R with Jacobson

radical J , the ring R/J is Von Neumann regular-absolutely flat, in which case the ring is called in the literature J -regular. Note that units are closely linked to Jacobson radicals. In order to generalize Lequain-Doering's results in a substantial way, we were lead to study J -regular rings and their behavior with respect to ring morphisms, a subject not treated in the literature. Actually for an extension $R \subseteq S$, there is an exact sequence of Abelian groups $1 \rightarrow U(R) \rightarrow U(S) \rightarrow \mathcal{I}(R, S) \rightarrow \text{Pic}(R)$, where $\mathcal{I}(R, S)$ is the group of R -submodules of S that are invertible. Now if R is J -regular, its Picard group is zero, so that $\mathcal{I}(R, S)$ measures the defect of strong localness of the extension. A first crucial result is that for an SL extension $R \subseteq S$, then S is J -regular if and only if R is J -regular and $R \subseteq S$ is integral seminormal. If these conditions hold, then $J(R) = J(S)$. This material is developed in Section 5. The paper culminates in Section 8 with a substantial result in the Doering-Lequain style: an extension $R \subseteq S$, where S is a semilocal ring, is SL if and only if $R \subseteq S$ is a seminormal integral FIP extension, whose residual extensions are isomorphisms and such that $R/M \cong \mathbb{Z}/2\mathbb{Z}$ for each $M \in \text{MSupp}(S/R)$. Now Section 2 examines the behavior of local and SL extensions and many examples are provided. In Section 3 we give a list of extensions that are local. Section 4 explores the properties of SL extensions. We give in Section 9 a series of examples of SL extensions, for example strongly inert extensions. These examples show that it seems impossible to find a general criterion for the SL property, except in the semilocal case.

As an example, we build at the end of the paper a strongly local ring morphism $f : \mathbb{F}_2[X]/(X^3-1) \rightarrow \mathbb{F}_2[X]/(X^4-X)$.

If $R \subseteq S$ is a (ring) extension, we denote by $[R, S]$ the set of all R -subalgebras of S .

We will mainly consider ring morphisms that are ring extensions. A property (P) of ring morphisms $f : R \rightarrow S$ is called universal if for any base change $R \rightarrow R'$, the ring morphism $R' \rightarrow R' \otimes_R S$ verifies (P) . As usual, $\text{Spec}(R)$ and $\text{Max}(R)$ are the set of prime and maximal ideals of a ring R . We denote by $\kappa_R(P)$ the residual field R_P/PR_P at a prime ideal P of R . If $R \subseteq S$ is a ring extension and $Q \in \text{Spec}(S)$, there exists a residual field extension $\kappa_R(Q \cap R) \rightarrow \kappa_S(Q)$.

A (semi-)local ring is a ring with (finitely many maximal ideals) one maximal ideal. For an extension $R \subseteq S$ and an ideal I of R , we write $V_S(I) := \{P \in \text{Spec}(S) \mid I \subseteq P\}$. The support of an R -module E is $\text{Supp}_R(E) := \{P \in \text{Spec}(R) \mid E_P \neq 0\}$, and $\text{MSupp}_R(E) := \text{Supp}_R(E) \cap \text{Max}(R)$. When $R \subseteq S$ is an extension, we will set $\text{Supp}(T/R) := \text{Supp}_R(T/R)$ and $\text{Supp}(S/T) := \text{Supp}_R(S/T)$ for each $T \in [R, S]$, unless otherwise specified.

For a ring R , we denote by $Z(R)$ the set of all zerodivisors of R , by $\text{Nil}(R)$ the set of nilpotent elements of R and by $J(R)$ its Jacobson radical. The Picard group of a ring R is denoted by $\text{Pic}(R)$.

Now $(R : S)$ is the conductor of $R \subseteq S$. The integral closure of R in S is denoted by $\overline{R}^S$ (or by $\overline{R}$ if no confusion can occur).

A ring extension $R \subseteq S$ is called an i -extension if the natural map $\text{Spec}(S) \rightarrow \text{Spec}(R)$ is injective.

An extension $R \subseteq S$ is said to have FIP (for the "finitely many intermediate algebras property") or is an FIP extension if $[R, S]$ is finite. We also say that the extension $R \subseteq S$ has FCP (or is an FCP extension) if each chain in $[R, S]$ is finite, or equivalently, its lattice is Artinian and Noetherian. An FCP extension is finitely generated, and (module) finite if integral.

In the case of an FCP extension $R \subseteq S$ where S is semilocal, we will show in Theorem [8.10](#) that there is a greatest $T \in [R, S]$ such that $R \subseteq T$ is SL, that is $R \subseteq T$ is a unique MSL-subextension.

Finally, $|X|$ is the cardinality of a set X , $\subset$ denotes proper inclusion and for a positive integer n , we set $\mathbb{N}_n := \{1, \dots, n\}$. If R and S are two isomorphic rings, we will write $R \cong S$. If M and N are R -modules, we write $M \cong_R N$ if M and N are isomorphic as R -modules.

2 First properties of (strongly) local extensions

Generalizing the definition of a local ring morphism between local rings, a ring morphism $f : R \rightarrow S$ is called *local* if $f^{-1}(U(S)) = U(R)$. We recover the case of a local extension of local rings $f : (R, M) \rightarrow (S, N)$ where $f^{-1}(N) = M$. We will mainly be concerned by ring extensions $R \subseteq S$, and in this case the extension is local (reflects units) if $U(R) = U(S) \cap R$.

We call a ring extension $R \subseteq S$ *strongly local (SL)* if $U(R) = U(S)$. A strongly local extension is obviously local and a ring morphism $f : R \rightarrow S$ is called *strongly local (SL)* if $f(U(R)) = U(S)$.

Note that if f is a surjective local morphism then f is SL. Indeed we always have $f(U(R)) \subseteq U(S)$. Assume that f is surjective and local, and let $y \in U(S)$. There exists some $a \in R$ such that $y = f(a) \in U(S)$. It follows that $a \in f^{-1}(U(S)) = U(R)$, so that $y \in f(U(R))$, giving $U(S) \subseteq f(U(R))$, and then $f(U(R)) = U(S)$, that is f is SL.

A first example of local extension is given by an R -module M and its Nagata extension $f : R \rightarrow R \oplus M$, where $f(x) = (x, 0)$. A unit (a, m) of $R \oplus M$ is such that a is a unit of R and (a, m) has an inverse of the form (a', n) , where $a' = a^{-1}$ and $n = -a'^2 m$. But this extension is not SL.

The extension $\mathbb{Z} \subseteq \mathbb{Z}[2i]$ is SL.

If R is a ring then the extension $R[X^2] \subseteq R[X]$ is local but not SL in general. For example, if $a \in R$ is nilpotent, then $1 + aX \in U(R[X])$ but $1 + aX \notin U(R[X^2])$.

Proposition 2.1. *An extension $R \subseteq S$ such that R and S have the same prime ideals is local and is trivial if it is SL.*

Proof. We know that R and S are local rings with the same maximal ideal [4, Proposition 3.3]. Let M be this common maximal ideal. As usual, we have $U(R) \subseteq U(S) \cap R$. Let $x \in U(S) \cap R$. Then, $x \notin P$, for any $P \in \text{Spec}(S) = \text{Spec}(R)$. Since $x \in R$, it follows that $x \in U(R)$, so that $U(R) = U(S) \cap R$ and $R \subseteq S$ is local. If $R \subseteq S$ is SL, that is $U(R) = U(S)$, we have $R = M \cup U(R) = M \cup U(S) = S$. $\square$

See [4] for examples and also PVD and $D + M$ construction.

Proposition 2.2. *Let $f : R \rightarrow S$ and $g : S \rightarrow T$ be two ring morphisms.*

1. *If f and g are (strongly) local, so is $g \circ f$.*
2. *If $g \circ f$ is local, so is f . In case f is surjective, then g is local.*
3. *If $g \circ f$ is SL, so is g . In case g is injective, then f is SL.*

Proof. (1) Assume that f and g are local. Then, $f^{-1}(U(S)) = U(R)$ and $g^{-1}(U(T)) = U(S)$, so that $(g \circ f)^{-1}(U(T)) = f^{-1}[g^{-1}(U(T))] = f^{-1}(U(S)) = U(R)$, so that $g \circ f$ is local.

Assume that f and g are SL. Then, $f(U(R)) = U(S)$ and $g(U(S)) = U(T)$, so that $(g \circ f)(U(R)) = g[f(U(R))] = g(U(S)) = U(T)$, giving that $g \circ f$ is SL.

(2) Assume that $g \circ f$ is local. Then, $(g \circ f)^{-1}(U(T)) = U(R)$, so that $f^{-1}[g^{-1}(U(T))] = U(R)$. Obviously, $U(R) \subseteq f^{-1}(U(S))$. Let $x \in f^{-1}(U(S))$. It follows that $f(x) \in U(S)$, whence $(g \circ f)(x) = g[f(x)] \in g(U(S)) \subseteq U(T)$. To end, $x \in (g \circ f)^{-1}(U(T)) = U(R)$ and $f^{-1}(U(S)) \subseteq U(R)$, giving $f^{-1}(U(S)) = U(R)$ and f is local.

Assume that, moreover, f is surjective. Obviously, $U(S) \subseteq g^{-1}(U(T))$. Let $y \in g^{-1}(U(T))$, so that $g(y) \in U(T)$ (*). But, $y \in S$ and f surjective imply that there exists $x \in R$ such that $y = f(x)$. By (*), we get $(g \circ f)(x) = g[f(x)] = g(y) \in U(T)$, from which it follows that $x \in (g \circ f)^{-1}(U(T)) = U(R)$ and $y = f(x) \in f(U(R)) \subseteq U(S)$. To end, $U(S) = g^{-1}(U(T))$ and g is local.

(3) Assume that $g \circ f$ is SL. Then, $(g \circ f)(U(R)) = U(T)$. Obviously, $g[U(S)] \subseteq U(T)$. Let $y \in U(T)$. There exists $x \in U(R)$ such that $y = (g \circ f)(x) = g[f(x)] \in g[f(U(R))] \subseteq g[U(S)]$, which gives $U(T) \subseteq g[U(S)]$ and $g[U(S)] = U(T)$. Then, g is SL.

Assume that, moreover, g is injective. Obviously, $f[U(R)] \subseteq U(S)$. Let $z \in U(S)$. Then, $g(z) \in U(T) = (g \circ f)(U(R))$, so that there exists $x \in U(R)$ such that $g(z) = (g \circ f)(x) = g[f(x)]$. Since g is injective, it follows that $z = f(x) \in f[U(R)]$ and $U(S) \subseteq f[U(R)]$. To end, $U(S) = f(U(R))$ and f is SL. $\square$

Remark 2.3. Let $f : R \rightarrow S$ be a ring morphism. Since the ring morphism $R/\ker(f) \rightarrow S$ associated to f is injective and the canonical ring morphism $R \rightarrow R/\ker(f)$ is surjective, we may consider the extension $R/\ker(f) \subseteq S$. Then, Proposition 2.2 shows that f is (strongly) local if and only if $R \rightarrow R/\ker(f)$ and $R/\ker(f) \rightarrow S$ are (strongly) local.

Corollary 2.4. Let $R \subseteq S \subseteq T$ be a tower of extensions.

1. $R \subseteq T$ is SL if and only if $R \subseteq S$ and $S \subseteq T$ are SL.
2. If $R \subseteq S$ and $S \subseteq T$ are local, then $R \subseteq T$ is local.
3. If $R \subseteq T$ is local, then $R \subseteq S$ is local.

Proof. Obvious by Proposition 2.2. □

Proposition 2.5. If $\{R_i \subseteq S_i\}_{i \in I}$ is a family of extensions, then $\Pi_{i \in I} R_i \subseteq \Pi_{i \in I} S_i$ is a (strongly) local extension if and only if all the elements of the family are (strongly) local.

Proposition 2.6. Consider a pullback square in the category of commutative rings:

$$\begin{array}{ccc} R & \rightarrow & S \\ \downarrow & & \downarrow \\ R' & \rightarrow & S' \end{array}$$

whose horizontal maps are extensions. Then if $R' \subseteq S'$ is (strongly) local, so is $R \subseteq S$.

Proof. Assume first that $R' \subseteq S'$ is local, so that $U(R') = U(S') \cap R'$. As $U(R) \subseteq U(S) \cap R$, it is enough to show that $U(S) \cap R \subseteq U(R)$. Let $f : S \rightarrow S'$ and $a \in U(S) \cap R$. Then, $b := f(a) \in U(S') \cap R' = U(R')$ is a unit in R' . Let $g : R \rightarrow R'$ and consider $x = (a, b) = (a, f(a)) \in R$ with $b = g(x) = f(a)$. Set $a' := a^{-1} \in U(S)$ and $b' := f(a')$. It follows that $b' \in U(S')$ satisfies $bb' = 1$ in S' and is the (unique) inverse of b , so that $b' \in R'$. Set $x' := (a', b')$, with $b' = g(x') = f(a')$. Then, $xx' = (aa', bb') = 1$, so that $x \in U(R)$. It follows that for any $a \in U(S) \cap R$, there exists a unique $x = (a, f(a)) \in U(R)$, from which we can infer that $U(S) \cap R \subseteq U(R)$ and $R \subseteq S$ is local.

Assume now that $R' \subseteq S'$ is SL, so that $U(R') = U(S')$. The proof is similar, taking $a \in U(S)$ instead of $a \in U(S) \cap R$ and taking in account that $U(S') = U(R')$. Then $R \subseteq S$ is SL. □

Corollary 2.7. Let $R \subseteq S$ be an extension sharing an ideal I such that $R/I \subseteq S/I$ is (strongly) local. Then $R \subseteq S$ is (strongly) local.

Proof. Obvious by Proposition 2.6. □

Proposition 2.8. Let $\{R \subseteq S_i\}_{i \in I}$ be an upward directed family of (strongly) local extensions. Then so is $R \subseteq \cup[S_i \mid i \in I]$.

Proof. Set $\mathcal{F} := \{S_i\}_{i \in I}$ and $T := \cup[S_i \mid i \in I]$. Let $x \in U(T)$. Since $\mathcal{F}$ is an upward directed family of extensions of R , there exists $y \in U(T)$ such that $xy = 1$ (*) and there exists some $i \in I$ such that $x, y \in S_i$, with $xy = 1$ in S_i by (*). This shows that $x \in U(S_i)$ (**).

If $R \subseteq S_i$ is local for each S_i , let $x \in U(T) \cap R$. Then, (**) shows that $x \in U(S_i) \cap R = U(R)$ giving $U(T) \cap R = U(R)$ and $R \subseteq T$ is local.

If $R \subseteq S_i$ is SL for each S_i , let $x \in U(T)$. Then, (**) shows that $x \in U(S_i) = U(R)$ giving $U(T) = U(R)$ and $R \subseteq T$ is SL. □

Proposition 2.9. Let $R \subseteq S$ be a ring extension such that $R_M \subseteq S_M$ is (strongly) local for any $M \in \text{MSupp}(S/R)$, then so is $R \subseteq S$.

Proof. Assume first that $R_M \subseteq S_M$ is local for any $M \in \text{MSupp}(S/R)$. Since we always have $U(R) \subseteq U(S) \cap R$, it is enough to prove that any $x \in U(S) \cap R$ is in $U(R)$. So, let $x \in U(S) \cap R$. There exists $y \in U(S)$ such that $xy = 1$ (*) in S , so that $(x/1)(y/1) = 1$ (**) in S_M for any $M \in \text{MSupp}(S/R)$. Then, $x/1 \in U(S_M) \cap R_M = U(R_M)$ for any $M \in \text{MSupp}(S/R)$. It follows that for any $M \in \text{MSupp}(S/R)$, there exists some $y_M/s_M \in U(R_M)$ such that $(x/1)(y_M/s_M) = 1$ in $R_M \subseteq S_M$. This implies that by (**) we get $y_M/s_M = y/1$ in S_M by the uniqueness of the inverse, so that $y/1 \in R_M$ for any $M \in \text{MSupp}(S/R)$. Moreover, let $M \notin \text{MSupp}(S/R)$. Then, $R_M = S_M$, so that $y/1 \in R_M$ for any $M \in \text{Max}(R)$ and (*) shows that $x \in U(R)$.

Assume that $R_M \subseteq S_M$ is SL for any $M \in \text{MSupp}(S/R)$. Since we always have $U(R) \subseteq U(S)$, it is enough to prove that any $x \in U(S)$ is in $U(R)$. So, let $x \in U(S)$. There exists $y \in U(S)$ such that $xy = 1$ (*) in S which entails that $(x/1)(y/1) = 1$ (**) in S_M for any $M \in \text{MSupp}(S/R)$. For the rest of the proof, it is enough to copy the same part of the proof of the local case. $\square$

Proposition 2.10. *Let $R \subseteq S$ be a ring extension and Σ a saturated multiplicative closed subset of R which is also a saturated multiplicative closed subset of S . If $R_\Sigma \subseteq S_\Sigma$ is (strongly) local, then so is $R \subseteq S$.*

Proof. Assume first that $R_\Sigma \subseteq S_\Sigma$ is local. Since we always have $U(R) \subseteq U(S) \cap R$, it is enough to prove that any $x \in U(S) \cap R$ is in $U(R)$. So, let $x \in U(S) \cap R$. There exists $y \in U(S)$ such that $xy = 1$ (*) in S which implies that $(x/1)(y/1) = 1$ (**) in S_Σ , which is equivalent to $u = uxy$ for some $u \in \Sigma$. In particular, $y \in \Sigma \subseteq R$ because Σ is closed in S . Using (*), we get that $x \in U(R)$ and $R \subseteq S$ is local.

Assume now that $R_\Sigma \subseteq S_\Sigma$ is SL. Since we always have $U(R) \subseteq U(S)$, it is enough to prove that any $x \in U(S)$ is in $U(R)$. So, let $x \in U(S)$. There exists $y \in U(S)$ such that $xy = 1$ (*) in S , whence $(x/1)(y/1) = 1$ (**) in S_Σ . For the rest of the proof, it is enough to copy the same part of the proof of the local case. $\square$

We consider the Nagata idealization $R(+)M$ of an R -module M .

Proposition 2.11. (1) *Let M be an R -module and N an R -submodule of M . Then, $R \subseteq R(+)M$ and $R(+)N \subseteq R(+)M$ are local extensions. But $R \subseteq R(+)M$ is SL if and only if $M = 0$ and $R(+)N \subseteq R(+)M$ is SL if and only if $M = N$.*

(2) *If $R \subseteq S$ is a ring extension and M an S -module, then M is also an R -module and $R \subseteq S$ is SL if and only if $R(+)M \subseteq S(+)M$ is SL.*

Proof. (1) Let $(x, m) \in R(+)M$. Then, $(x, m) \in U(R(+)M)$ if and only if $x \in U(R)$. Under this condition, we have $(x, m)^{-1} = (x^{-1}, -x^{-2}m)$. It follows that $U(R(+)M) \cap R = U(R)$, so that $R \subseteq R(+)M$ is local but $R \subseteq R(+)M$ is SL if and only if $M = 0$.

If N a submodule of M we get that $U(R(+)M) \cap (R(+)N) = U(R(+)N)$, whence $R(+)N \subseteq R(+)M$ is local but $R(+)N \subseteq R(+)M$ is SL if and only if $M = N$.

(2) If M an S -module, then obviously, M is also an R -module. Let $(x, m) \in S(+)M$. By the proof of (1), $(x, m) \in U(S(+)M)$ if and only if $x \in U(S)$. A similar equivalence holds for $U(R(+)M)$ and $U(R)$. Then the equivalence of (2) is obvious. $\square$

We recall in the next section some results of local extensions we get in [36] and add some new results. We will look more precisely at SL extensions in the other sections.

3 Properties of local extensions

An extension $R \subseteq S$ is called *survival* if for each ideal I of R such that $I \neq R$, then $IS \neq S$ (equivalently $PS \neq S$ for each $P \in \text{Spec}(R)$).

Proposition 3.1. *Lying-over or survival extensions are local.*

In case the ideals of a ring R are linearly ordered, an extension $R \subseteq S$ is survival if and only if it is local.

Proof. [36, Definition before Proposition 8.8] gives the result for a survival extension.

Assume that $R \subseteq S$ has lying-over. Since we always have $U(R) \subseteq U(S) \cap R$, it is enough to prove that any $x \in U(S) \cap R$ is in $U(R)$. So, let $x \in U(S) \cap R$ be such that $x \notin U(R)$. There exists some $P \in \text{Spec}(R)$ such that $x \in P$ and there exists some $Q \in \text{Spec}(S)$ lying over P . Then $x \in P \subseteq PS \subseteq Q$, a contradiction with $x \in U(S)$.

Assume that the ideals of a ring R are linearly ordered and that the extension $R \subseteq S$ is local. Let I be an ideal of R such that $I \neq R$ and $IS = S$. There exists some $x_1, \dots, x_n \in I$ and $s_1, \dots, s_n \in S$ such that $\sum_{i=1}^n s_i x_i = 1$ (*). But the Rx_i are linearly ordered. Let x_k be such that $Rx_i \subseteq Rx_k$ for each $i \in \mathbb{N}_n$. Then (*) implies $sx_k = 1$ for some $s \in S$, so that $x_k \in U(S) \cap R = U(R)$, a contradiction. Then, $R \subseteq S$ is survival. $\square$

Proposition 3.2. [36, Proposition 8.8] *An extension $R \subseteq S$ is survival if and only if $R(X) \subseteq S(X)$ is local.*

Recall that an extension $R \subseteq S$ is called *Prüfer* if $R \subseteq T$ is a flat epimorphism for each $T \in [R, S]$ (or equivalently, if $R \subseteq S$ is a normal pair) [18, Theorem 5.2, page 47].

In [31], we defined an extension $R \subseteq S$ to be *quasi-Prüfer* if it can be factored $R \subseteq R' \subseteq S$, where $R \subseteq R'$ is integral and $R' \subseteq S$ is Prüfer. An FCP extension is quasi-Prüfer [31, Corollary 3.4].

Definition 3.3. *A ring extension $R \subseteq S$ has a greatest flat epimorphic subextension $R \subseteq \widehat{R}$ that we call the Morita hull of R in S [22, Corollary 3.4]. We say that the extension is Morita-closed if $\widehat{R} = R$.*

In fact, $\widehat{R}$ coincide with the weakly surjective hull $M(R, S)$ of [18], since weakly surjective morphisms $f : R \rightarrow S$ are characterized by $R/\ker f \rightarrow S$ is a flat epimorphism [23, Proposition p.3]. Our terminology is justified by the fact that the Morita construction is earlier. The Morita hull can be computed by using a (transfinite) induction [22] as follows. Let S' be the set of all $s \in S$, such that there is some ideal I of R , such that $IS = S$ and $Is \subseteq R$, or equivalently, $S' = \{s \in S \mid S = (R :_R s)S\}$. Then $R \subseteq S'$ is a subextension of $R \subseteq S$. We set $S_1 := S'$ and $S_{i+1} := (S_i)' \subseteq S_i$, which defines the transfinite induction.

We introduce the condition ($\star$) on a ring extension $R \subseteq S$: an element $s \in S$ belongs to R if (and only if) $S = (R :_R s)S$. The condition ($\star$) is clearly equivalent to the Morita-closedness of the extension.

An integral extension is Morita-closed because an injective flat epimorphism is trivial as soon as it has LO [19, Lemme 1.2, p.109].

An extension $R \subseteq S$ is Morita-closed if R is zero-dimensional because a prime ideal of R can be lifted up to S , since such a prime ideal is minimal and then it is enough to again apply [19, Lemme 1.2, p.109].

Proposition 3.4. *A Morita-closed extension $R \subseteq S$ is local. Therefore the Morita hull $\widehat{R}$ of an extension $R \subseteq S$ is such that $\widehat{R} \subseteq S$ is local.*

Proof. Use the multiplicatively closed subset $\Sigma_S := \{r \in R \mid r \in U(S)\}$ and the factorization $R \subseteq R_{\Sigma_S} \subseteq S$. $\square$

The condition ($\star$) defined after Definition 3.3 is stronger than the local property. A flat epimorphic extension does not verify the condition ($\star$) because of [39, Exercise 8, p.242]. Actually, a flat epimorphic extension does not need to be local: it is enough to consider a localization $R \rightarrow R_P$, where P is a prime ideal of an integral domain R .

We use the results of Olivier about pure extensions [24]. Recall that an injective ring morphism $f : R \rightarrow S$ is called *pure* if $R' \rightarrow R' \otimes_R S$ is injective for each ring morphism $R \rightarrow R'$, whence purity is an universal property. A faithfully flat morphism is pure.

A pure ring morphism is a strict monomorphism of the category of commutative rings [24, Corollaire 5.2, page 21]. This last condition can be characterized in the category of commutative unital

rings as follows. If $f : R \rightarrow S$ is a ring morphism, the dominion of f is $D(f) := \{s \in S \mid s \otimes 1 = 1 \otimes s \text{ in } S \otimes_R S\}$.

A ring extension $R \subseteq S$ is a *strict monomorphism* if and only if its dominion is R . Now a ring morphism is an epimorphism if and only if its dominion is S [19, Lemme 1.0, page 108]. It follows that a ring extension is strict and an epimorphism if and only if it is trivial.

Denote by D the dominion of an extension $R \subseteq S$ then $D \subseteq S$ is strict, because $S \otimes_D S = S \otimes_R S$.

We will consider minimal (ring) extensions, a concept that was introduced by Ferrand-Olivier [10]. Recall that an extension $R \subseteq S$ is called *minimal* if $[R, S] = \{R, S\}$. A minimal extension is either a flat epimorphism or a strict monomorphism, in which case it is finite. A minimal integral extension is strict [10, Théorème 2.2(ii)].

Lemma 3.5. *A strict monomorphism $f : R \rightarrow S$ is local (e.g. either pure or minimal integral).*

Proof. If $a \in R$ is a unit in S , there is a factorization $R \rightarrow R_a \rightarrow S$. From the natural map $R_a \otimes_R R_a \rightarrow S \otimes_R S$ and $D(R \rightarrow R_a) = R_a$, because $R \rightarrow R_a$ is an epimorphism, we get that $R_a \subseteq D(f) = R$. $\square$

We define the class $\mathcal{TP}$ of rings R such that $\text{Pic}(R) = 0$. It contains semi-local rings and Nagata rings.

Proposition 3.6. *A Prüfer local extension $R \subseteq S$ over a $\mathcal{TP}$ ring is trivial.*

Proof. Assume that $R \neq S$. Since $R \subseteq S$ is Prüfer, it is a flat epimorphism, so that there exists $M \in \text{Max}(R)$ such that $MS = S$ and $1 = \sum_{i=1}^n m_i s_i$, for some positive integer n , $m_i \in M$ and $s_i \in S$ for each $i \in \mathbb{N}_n$. Set $I := \sum_{i=1}^n Rm_i$. Then $IS = S$, so that I is an S -regular R -submodule of S finitely generated. According to [18, Theorem 1.13, p.91], I is S -invertible, and then a projective R -module of rank 1 by [18, Lemma 4.1, p.109]. It follows that I is a free R -module which implies that I is a principal ideal of R .

Set $I := Rx$, with $x \in R$. But $IS = S$ gives $xS = S$, and x is a unit in S . But $x \in R$ implies $x \in U(S) \cap R = U(R)$, a contradiction with $x \in I \subseteq M$. Then, $R = S$. $\square$

This Proposition generalizes [36, Proposition 8.9] which holds for an extension over an arithmetical ring.

4 Generalities about SL extensions

We first give examples of SL extensions.

Example 4.1. (1a) If $R \subseteq S$ is an extension we can consider $L(S) := R[U(S)]$. Then $L(S) \subseteq S$ is SL and $L(S)$ is the smallest element T of $[R, S]$ such that $T \subseteq S$ is SL. Actually $L(S)$ is the intersection of all $T \in [R, S]$ such that $T \subseteq S$ is SL.

(1b) There exist also subextensions $R \subseteq U$ of $[R, S]$, maximal with respect to the property SL. We will call them MSL-subextensions. The proof uses Zorn's Lemma.

If $R \subseteq S$ is a chained extension, then $U := \cup \{V \in [R, S] \mid U(R) = U(V)\}$ is the MSL-subextension.

In Theorem [8, 10], we prove that when $R \subseteq S$ is an FCP extension and S is semilocal, there exists a unique MSL-subextension.

(2) Let $R \subseteq S$ be an extension where S is a Boolean ring, then the extension is SL. This is obvious because the only unit of S and R is 1 since R is also a Boolean ring.

(3) Let R be a reduced ring. Then $R \subseteq R[X]$ is SL because an invertible polynomial of $R[X]$ is of the form $a + Xf(X)$ where a is invertible in R and the coefficients of $f(X)$ are nilpotent, so that $f(X) = 0$.

On the other hand, $R \subseteq R[[X]]$ is never SL because any power series with a unit of R as first coefficient is a unit in $R[[X]]$.

(4) Let Σ be a multiplicative closed subset of a ring R such that $R \subseteq R_\Sigma$ is SL. Then $\Sigma = U(R)$ and $R = R_\Sigma$. Of course, $U(R) \subseteq \Sigma$. Assume $U(R) \neq \Sigma$ and let $x \in \Sigma \setminus U(R)$. Then, $x \in U(R_\Sigma) = U(R)$, a contradiction, so that $\Sigma = U(R)$ and $R = R_\Sigma$.

(5) The ring morphism $j : R \rightarrow R/J(R)$ is SL. Indeed if $\bar{x}$ is the class of an element $x \in R$ that is a unit in $R/J(R)$, there is some $y \in R$, such that $xy - 1 \in J(R)$. Then $1 - (1 - xy)$ is a unit in R ; so that $x \in U(R)$.

(6) Let $R \subseteq S$ be an extension such that $1 \neq -1$ and $U(S)$ is a simple group. Since $U(R)$ is a subgroup of $U(S)$, the only possibilities are either $U(R) = \{1\}$ (*) or $U(R) = U(S)$ (**). But $1 \neq -1$ and $-1 \in U(R)$ show that only case (**) can occur. Then $R \subseteq S$ is SL.

(7) Let $R \subseteq S$ be an extension where $1 \neq -1$ and $U(S)$ has a finite prime order. Then $U(S)$ is a simple group and $R \subseteq S$ is SL by (6).

We will see that in the FCP case, the situation $1 \neq -1$ often occurs through the ring $\mathbb{Z}/2\mathbb{Z}$.

(8) An SL extension $R \subseteq S$ is trivial if (S, M) is a local ring. Indeed since $S = U(S) \cup M = U(R) \cup M$ and any $x \in M$ is such that $1 + x \in U(S) = U(R) \subseteq R$, we get that $M \subseteq R$, giving $R = S$.

Proposition 4.2. *The following holds for an extension $R \subseteq S$ where R is reduced:*

1. If $s \in S$ is not algebraic over R , then $R \subseteq R[s]$ is SL.
2. In case S is also reduced and $V \in [R, S]$ is a MSL-subextension, then $V \subseteq S$ is algebraic.

Proof. (1) Let $s \in S$ which is not algebraic over R and consider the morphism $\varphi : R[X] \rightarrow R[s]$ defined by $\varphi(X) = s$. Then φ is a surjective morphism which is also injective since s is not algebraic over R . Then $R[X] \cong R[s]$ so that $R \subseteq R[s]$ is SL by Example 4.1(3).

(2) Assume, moreover, that S is also reduced. By Example 4.1(1), there exists an MSL-subextension $V \in [R, S]$. Then, V is also reduced. Assume that $S \neq V$ and let $s \in S \setminus V$. If s is not algebraic over V , then $V \subseteq V[s]$ is SL by (1) and so is $R \subseteq V[s]$ because $U(R) = U(V) = U(V[s])$, a contradiction with the maximality of V . Then, any $s \in S \setminus V$ is algebraic over V and then $V \subseteq S$ is algebraic. $\square$

Corollary 4.3. *Let $R \subseteq S$ be an extension where S is reduced. There exists $U \in [R, S]$ such that $R \subseteq U$ is SL and $U \subseteq S$ is quasi-Prüfer.*

Proof. By Example 4.1(1), there exists an MSL-subextension $U \in [R, S]$. Moreover, $U \subseteq S$ is algebraic as $U \subseteq V$ for any $V \in [U, S]$ by Proposition 4.2. This shows that $U \subseteq S$ is a residually algebraic pair, and then is quasi-Prüfer by [31] Theorem 2.3]. $\square$

Proposition 4.4. *Let $R \subseteq S$ be a ring extension. The following conditions are equivalent:*

1. $R \subseteq S$ is SL.
2. $R[X] \subseteq S[X]$ is SL.
3. $R + XS[X] \subseteq S[X]$ is SL.

If these conditions hold, then $\text{Nil}(R) = \text{Nil}(S)$.

Proof. We begin to remark that $1 - x$ is a unit if x is nilpotent for any $x \in R$ (resp. $x \in S$). Then, $U(R) = U(S) \Rightarrow \text{Nil}(R) = \text{Nil}(S)$.

(1) $\Leftrightarrow$ (2) We know that $U(R[X]) = U(R) + X\text{Nil}(R)[X]$ (*) and $U(S[X]) = U(S) + X\text{Nil}(S)[X]$ (**). Then, we get the equivalence applying the previous remark to $R \subseteq S$ and $R[X] \subseteq S[X]$ and using (*) and (**).

(2) $\Rightarrow$ (3) since $R[X] \subseteq S[X]$ SL implies by Corollary 2.4 that $R + XS[X] \subseteq S[X]$ is SL because $R + XS[X] \in [R[X], S[X]]$.

(3) $\Rightarrow$ (1) Let $a \in U(S) \subseteq U(S[X]) = U(R + XS[X])$, which gives $a \in S \cap U(R + XS[X]) \subseteq R + XS[X]$. This shows that $a \in R$. The same property holds for $b := a^{-1} \in S$, so that $a \in U(R)$ and $R \subseteq S$ is SL. $\square$

Corollary 4.5. *Let $R \subseteq S$ be a ring extension such that S is reduced. Then $R \subseteq R + XS[X]$ is SL.*

Proof. Let $a \in U(R + XS[X]) \subset U(S[X]) \cap (R + XS[X])$, so that $a = c + Xf(X)$, where $c \in R$ and $f(X) \in S[X]$. But, as a is an element of $U(S[X])$, we have $f(X) \in \text{Nil}(S)[X] = 0$ because S is reduced. Then, $a = c \in R \cap U(S[X]) \subseteq R \cap U(S)$. The same property holds for $b := a^{-1} \in U(R + XS[X])$, so that $a \in U(R)$ and $R \subseteq R + XS[X]$ is SL. $\square$

Proposition 4.6. *Let $R \subseteq S$ be a ring extension. If $R(X) \subseteq S(X)$ (resp. $R[[X]] \subseteq S[[X]]$) is SL, then $R = S$.*

Proof. Assume that $R(X) \subseteq S(X)$ is SL and let $s \in S$. Then, $P(X) := s + X \in S[X]$ is such that $P(X)/1 \in U(S(X)) = U(R(X))$. This implies that there exist $f(X), g(X) \in R[X]$ with content equal to R such that $P(X)/1 = f(X)/g(X)$. Set $f(X) := \sum_{i=0}^{n+1} a_i X^i$ and $g(X) := \sum_{i=0}^n b_i X^i$, $a_i, b_i \in R$ such that $g(X)P(X) = f(X)$. It follows that $sb_0 = a_0, b_n = a_{n+1}$ and $sb_i + b_{i-1} = a_i$ for any $i \in \mathbb{N}_n$ (*). Since $c(g) = R$, there exist $\lambda_0, \dots, \lambda_n \in R$ such that $\sum_{i=0}^n \lambda_i b_i = 1$. Multiplying each equality of rank i of (*) by λ_i and adding each of these equalities for each $i \in \{0, \dots, n\}$, we get $s(\sum_{i=0}^n \lambda_i b_i) = s = \lambda_0 a_0 + \sum_{i=1}^n \lambda_i (a_i - b_{i-1}) \in R$, so that $S = R$.

Assume now that $R[[X]] \subseteq S[[X]]$ is SL. We know that $U(R[[X]]) = U(R) + XR[[X]]$ and $U(S[[X]]) = U(S) + XS[[X]]$. It follows that $U(R) + XR[[X]] = U(S) + XS[[X]]$. Let $s \in S$. Then $1 + sX \in U(S) + XS[[X]] = U(R) + XR[[X]]$, so that $s \in R$ and $R = S$. $\square$

Definition 4.7. *Let R be a ring.*

1. *A polynomial $p(X) \in R[X]$ is called comonic if $p(0) \in U(R)$.*
2. *A ring extension $R \subseteq S$ is called co-integrally closed if any $x \in S$ which is a zero of a comonic polynomial of $R[X]$ is in R .*

Proposition 4.8. *Let $R \subseteq S$ be a ring extension. The following statements hold:*

1. *If $R \subseteq S$ is SL, then $R \subseteq S$ is co-integrally closed.*
2. *Let $R \subseteq S$ be an integral ring extension. Then $R \subseteq S$ is SL if and only if $R \subseteq S$ is co-integrally closed.*

Proof. (1) Assume that $R \subseteq S$ is SL and let $x \in S$ be a zero of a comonic polynomial $p(X) := \sum_{i=0}^n a_i X^i \in R[X]$. Then, $p(0) = a_0 \in U(R)$ and $\sum_{i=0}^n a_i x^i = 0$, so that $x(\sum_{i=1}^n a_i x^{i-1}) = -a_0 \in U(R) = U(S)$ shows that $x \in U(S) = U(R) \subseteq R$. Then, $R \subseteq S$ is co-integrally closed.

(2) One part of the proof is gotten in (1). So, assume that $R \subseteq S$ is co-integrally closed. Obviously, $U(R) \subseteq U(S)$. Let $x \in U(S)$. Since $R \subseteq S$ is an integral ring extension, there exists a monic polynomial $p(X) := \sum_{i=0}^n a_i X^i \in R[X]$ with $a_n = 1$, such that $p(x) = 0$, giving $x^n + \sum_{i=0}^{n-1} a_i x^i = 0$ (*). Since $x \in U(S)$, multiplying (*) by x^{-n} , we get $1 + \sum_{i=0}^{n-1} a_i x^{i-n} = 1 + \sum_{i=0}^{n-1} a_i (x^{-1})^{n-i} = 0$ which shows that x^{-1} is a zero of the comonic polynomial $q(X) := 1 + \sum_{i=0}^{n-1} a_i X^{n-i} = \sum_{i=1}^n a_{n-i} X^i + 1 \in R[X]$. Then, $x^{-1} \in R$. To sum up, we have shown that any $x \in U(S)$ is such that $x^{-1} \in R$. Setting $y := x^{-1}$, which is also in $U(S)$, the previous proof gives that $y^{-1} = x$ is in R . Moreover, since it also shows that x and x^{-1} are in R , this implies that $x \in U(R)$. To conclude, $U(R) = U(S)$ and $R \subseteq S$ is SL. $\square$

5 J-regular rings

In this section, we look at properties of J-regular rings, which will play an important role in the following study of SL extension. An absolutely flat ring is in this paper called a (Von Neumann) *regular ring*. Actually, many results need only rings R with a Jacobson radical J such that R/J is regular. They are called *J-regular* in the literature.

We recall some results concerning regular rings.

- (1) A ring R is regular if for any $x \in R$, there exists $y \in R$ such that $x^2y = x$. Under these conditions, such an y is unique when satisfying $y^2x = y$ [25, Lemme, p.69]. Moreover, setting $e := xy$ and $u := 1 - e + x$, we get that e is an idempotent, u is a unit with $1 - e + y$ as inverse and $x = eu$.
- (2) A ring is regular if and only if it is reduced and zero-dimensional.
- (3) Let R be a regular ring. For any $P \in \text{Spec}(R)$, there is an isomorphism $R/P \cong R_P$.

Lemma 5.1. *If $f : R \rightarrow S$ is a strict monomorphism and S is regular, then R is regular.*

Proof. See [26, diagram page 40 and Proposition 19]. □

For any ring R there is an (Olivier) ring epimorphism $t : R \rightarrow \mathcal{O}(R)$, whose spectral map is bijective, such that $\mathcal{O}(R)$ is regular and such that any ring morphism $R \rightarrow S$ where S is regular can be factored $R \rightarrow \mathcal{O}(R) \rightarrow S$.

Note that $\ker(t) = \text{Nil}(R)$.

This property is a consequence of the following facts: $V(t^{-1}(I)) = \overline{{}^at(V(I))}$ for any ideal I of $\mathcal{O}(R)$ [13, Proposition 1.2.2.3, p.196] and $\mathcal{O}(R)$ is reduced.

The existence of the ring $\mathcal{O}(R)$, called *the universal regular (absolutely flat) ring associated to R* is due to Olivier [25, Proposition, p.70].

Lemma 5.2. *If $f : R \rightarrow S$ is an epimorphism and $M \in \text{Max}(R)$, there exists $N \in \text{Max}(S)$ such that $M = {}^af(N)$ if and only if $N = f(M)S$.*

If in addition ${}^af$ is bijective, then, for any $M \in \text{Max}(R)$, we have $f(M)S \in \text{Max}(S)$ and $M = {}^af[f(M)S]$.

Proof. Consider the following commutative diagram:

$$\begin{array}{ccc} R & \xrightarrow{f} & S \\ \downarrow & & \downarrow \\ R/M & \xrightarrow{\bar{f}} & S/f(M)S \end{array}$$

where $\bar{f}$ is deduced from f . Since f is an epimorphism, so is $\bar{f}$. Assume that $M := {}^af(N)$ for some $N \in \text{Max}(S)$. Since $f(M)S \subseteq N \subset S$, it follows that $M = {}^af[f(M)S]$, so that $\bar{f}$ is injective. Now, R/M being a field, $\bar{f}$ is surjective, and then an isomorphism. Hence, $S/f(M)S$ is a field and $f(M)S \in \text{Max}(S)$, which infers that $N = f(M)S$.

Conversely, assume that $N = f(M)S$ for some $N \in \text{Max}(S)$. Then, $f(M)S \subset S$. It follows that ${}^af[f(M)S] \in \text{Spec}(R)$ with $M \subseteq {}^af[f(M)S] \subset R$. But $M \in \text{Max}(R)$ implies that $M = {}^af[f(M)S] = {}^af(N)$.

Now if ${}^af$ bijective, for any $M \in \text{Max}(R)$, there exists $N \in \text{Max}(S)$ such that $M = {}^af(N)$. Then the first part of the Lemma gives that $N := f(M)S \in \text{Max}(S)$ and $M = {}^af[f(M)S]$. □

Proposition 5.3. *Let $t : R \rightarrow \mathcal{O}(R)$ be the Olivier ring epimorphism, $\mathcal{T} := \{N \in \text{Spec}(\mathcal{O}(R)) \mid {}^at(N) \in \text{Max}(R)\}$ and $K := \cap[N \in \mathcal{T}]$. Then, ${}^at(\mathcal{T}) = \text{Max}(R)$ and any $N \in \mathcal{T}$ is of the form $t(M)\mathcal{O}(R)$ where $M \in \text{Max}(R)$.*

If R is J-regular, there is an isomorphism $R/J(R) \cong \mathcal{O}(R)/K$.

Proof. Since ${}^at(N) \in \text{Max}(R)$ for any $N \in \mathcal{T}$, we have ${}^at(\mathcal{T}) \subseteq \text{Max}(R)$. Now, let $M \in \text{Max}(R)$. There exists $N \in \text{Spec}(\mathcal{O}(R))$ such that $M = {}^at(N)$ because ${}^at$ is bijective, so that $N \in \mathcal{T}$, giving $M \in {}^at(\mathcal{T})$. To end, ${}^at(\mathcal{T}) = \text{Max}(R)$.

Let $N \in \mathcal{T}$ and set $M := {}^at(N) \in \text{Max}(R)$. By Lemma 5.2, $N = t(M)\mathcal{O}(R)$.

Assume, moreover, that R is J-regular. Then, $R/J(R)$ is regular, that is zero-dimensional. Setting $K := \cap[N \in \mathcal{T}]$, we get $t^{-1}(K) = t^{-1}(\cap[N \in \mathcal{T}]) = \cap[{}^at(N) \mid N \in \mathcal{T}] = \cap[M \in {}^at(\mathcal{T})] = \cap[M \in \text{Max}(R)] =$

$J(R)$. Consider the following commutative diagram:

$$\begin{array}{ccc} R & \xrightarrow{t} & \mathcal{O}(R) \\ \downarrow & & \downarrow \\ R/J(R) & \xrightarrow{\bar{t}} & \mathcal{O}(R)/K \end{array}$$

where $\bar{t}$ is deduced from t . Since t is an epimorphism, so is $\bar{t}$, which is injective because $t^{-1}(K) = J(R)$. Now, $R/J(R)$ being zero-dimensional, $\bar{t}$ is surjective, and then $\bar{t} : R/J(R) \rightarrow \mathcal{O}(R)/K$ is an isomorphism. $\square$

We are now looking at topological characterizations of J-regular rings and add a characterization of J-regular rings given in [18].

Proposition 5.4. *Let R be a ring. The following conditions are equivalent:*

1. R is J-regular.
2. $\text{Max}(R)$ is closed.
3. $\text{Max}(R)$ is proconstructible.
4. $\text{Max}(R)$ is compact for the flat topology.
5. [18 Proposition 6.4, page 60] For every $x \in R$, there exists $y \in R$ such that $xy \in J(R)$ and $x+y \in U(R)$.

Proof. (1) $\Leftrightarrow$ (4) by [41 Theorem 4.5].

(1) $\Rightarrow$ (2) Equality $\overline{\text{Max}(R)} = V(J(R))$ always holds. Then (2) $\Leftrightarrow \overline{\text{Max}(R)} = \text{Max}(R)$. But $\dim(R/J(R)) = 0$ gives that $\text{Max}(R) = V(J(R))$. Moreover, (1) $\Leftrightarrow \dim(R/J(R)) = 0$ and $R/J(R)$ is reduced, this last condition always holding since $J(R)$ is semiprime. It follows that (1) $\Rightarrow \text{Max}(R) = V(J(R)) = \overline{\text{Max}(R)}$, so that $\text{Max}(R)$ is closed.

(2) $\Rightarrow$ (1) If $\text{Max}(R)$ is closed, then $\text{Max}(R) = \overline{\text{Max}(R)} = V(J(R))$, so that $\dim(R/J(R)) = 0$ which implies that R is J-regular.

(2) $\Rightarrow$ (3) because a closed subset is proconstructible.

(3) $\Rightarrow$ (2) According to [13 Corollaire 7.3.2, page 339], a proconstructible subset stable by specialization is closed. $\square$

Corollary 5.5. *Let $R \subseteq S$ be an integral i-extension. Then R is J-regular if and only if S is J-regular.*

Proof. Since $R \subseteq S$ is an integral i-extension, the natural map $\text{Spec}(S) \rightarrow \text{Spec}(R)$ is a homeomorphism. Then it is enough to use the equivalence (1) $\Leftrightarrow$ (2) of Proposition 5.4. $\square$

Corollary 5.6. *A ring R whose spectrum is Noetherian for the flat topology, is J-regular.*

Proof. By [5 Propositions 8 and 9, page 123], $\text{Max}(R)$ is Noetherian, and then compact for the flat topology. Then, use Proposition 5.4. $\square$

Corollary 5.7. *Let $f : R \rightarrow S$ be a ring morphism such that ${}^a f(\text{Max}(S)) = \text{Max}(R)$. If S is J-regular, so is R .*

Proof. By Proposition 5.4, if S is J-regular, $\text{Max}(S)$ is compact for the flat topology. Since ${}^a f$ is continuous for the flat topology, we get that ${}^a f(\text{Max}(S)) = \text{Max}(R)$ is compact, so that R is J-regular. $\square$

Proposition 5.8. *A ring R is J-regular if and only if so is $R(X)$.*

Proof. We know that $\text{Max}(R(X)) = \{MR(X) \mid M \in \text{Max}(R)\}$, so that $J(R(X)) = J(R)(X)$. It follows that $R(X)/J(R(X)) = R(X)/(J(R)(X)) \cong (R/J(R))(X)$. As S is regular if and only if so is $S(X)$, for a ring S , we get that $(R/J(R))(X)$ is regular if and only if so is $R/J(R)$. Then, R is J -regular if and only if so is $R(X)$. $\square$

According to [27, Definitions 1.1, 1.2 and 1.5, Proposition 1.6], [29] and [40], we set $p_r(X) := X^2 - rX \in R[X]$, where $R \subseteq S$ is a ring extension. $R \subseteq S$ is called *s-elementary* (resp.; *t-elementary*, *u-elementary*) if $S = R[b]$, where $p_0(b), bp_0(b) \in R$ (resp.; $p_r(b), bp_r(b) \in R$ for some $r \in R$, $p_1(b), bp_1(b) \in R$). In the following, the letter x denotes s , t or u . $R \subseteq S$ is called *cx-elementary* if $R \subseteq S$ is a tower of finitely many x -elementary extensions, *x-integral* if there exists a directed set $\{S_i\}_{i \in I} \subseteq [R, S]$ such that $R \subseteq S_i$ is cx -elementary and $S = \cup_{i \in I} S_i$. An integral extension $R \subseteq S$ is called *infra-integral* [29], (resp. *subintegral* [40]) if all its residual extensions are isomorphisms (resp.; and is an *i-extension*).

An extension $R \subseteq S$ is called *s-closed* (or *seminormal*) (resp.; *t-closed*, *u-closed* (or *anodal*)) if an element $b \in S$ is in R whenever $p_0(b), bp_0(b) \in R$ (resp.; $p_r(b), bp_r(b) \in R$ for some $r \in R$, $p_1(b), bp_1(b) \in R$) [40, Theorem 2.5]. A ring R is called *seminormal* by Swan if for $x, y \in R$, such that $x^2 = y^3$, there is some $z \in R$ such that $x = z^3$ and $y = z^2$ [40, Definition, page 210]. We say that a ring R is *t-closed* if for $x, y, r \in R$, such that $x^3 + rxy - y^2 = 0$, there is some $z \in R$ such that $x = z^2 - rz$ and $y = z^3 - rz^2$ [28, Définition 1.1]. A t -closed ring is seminormal.

A seminormal ring is reduced. We proved in [28, Proposition 2.1] that a regular ring is t -closed, whence seminormal.

Let $x \in \{s, t, u\}$. The x -closure ${}_x^S R$ of R in S is the smallest element $B \in [R, S]$ such that $B \subseteq S$ is x -closed and the greatest element $B' \in [R, S]$ such that $R \subseteq B'$ is x -integral. It follows that ${}_x^S R \subseteq {}_x^S R$. Note that the s -closure is actually the seminormalization ${}_s^+ R$ of R in S and is the greatest subintegral extension of R in S . Note also that the t -closure ${}_t^S R$ is the greatest infra-integral extension of R in S .

Example 5.9. (1) Let R be a ring and d a positive integer. Set $R_d := \{\sum_{i \in I} \varepsilon_i a_i^d \mid \varepsilon_i \in \{1, -1\}, a_i \in R, |I| < \infty\}$ which is a subring of R such that $f : R_d \subseteq R$ is an integral extension. We claim that f is an i -extension. Let $P, Q \in \text{Spec}(R)$ be such that $P \cap R_d = Q \cap R_d$. Let $x \in Q$, so that $x^d \in Q \cap R_d = P \cap R_d \subseteq P$, which implies $x \in P$, and then $Q \subseteq P$. A similar proof shows that $P \subseteq Q$, so that $P = Q$. Then ${}^a f(\text{Max}(R)) = \text{Max}(R_d)$ and R is J -regular if and only if R_d is J -regular by Corollary 5.5.

(2) Let $R \subseteq S$ be a u -closed FCP integral extension. Then $R \subseteq S$ is an i -extension by [35, Proposition 5.2] and R is J -regular if and only if S is J -regular by Corollary 5.5.

Corollary 5.10. Let $R \subseteq S$ be a subintegral extension, such that S is J -regular. Then R is J -regular and there is a ring isomorphism $R/J(R) \rightarrow S/J(S)$. In case $J(R) = J(S)$, then $R = S$.

Proof. $R/J(R)$ is regular because reduced and zero-dimensional since so is $S/J(S)$, and because the extension is integral. This also implies that $J(R) = R \cap J(S)$, so that the map $j : A := R/J(R) \rightarrow S/J(S) := B$ exists, and its residual extensions are isomorphisms. Such residual extensions are of the form $A_P \rightarrow B_Q$ where Q is a prime ideal of B above P . It follows that $A \rightarrow B$ is a flat epimorphism since $A \rightarrow B$ is an i -extension [31, Scholium A (1)]. Finally, since this extension has the lying-over property for maximal ideals, $A \rightarrow B$ is a faithfully flat epimorphism, whence an isomorphism [19, Lemme 1.2, page 109]. $\square$

We recall that a ring R verifies the primitive condition if for any element $p(X)$ of the polynomial ring $R[X]$, whose content $c(p)$ is R there is some $x \in R$ such that $f(x) \in U(R)$ [21]. The Nagata ring $R(X)$ of a ring R verifies the primitive condition [21, p.457].

Let $R \subseteq S$ be an extension. We denote by $\mathcal{I}(R, S)$ the abelian group of all R -submodules of S that are invertible as in [38, Definition 2.1].

There is an exact sequence [38, Theorem 2.4]:

$$1 \rightarrow U(R) \rightarrow U(S) \rightarrow \mathcal{I}(R, S) \rightarrow \text{Pic}(R) \rightarrow \text{Pic}(S)$$

It follows that there is an injective map $U(S)/U(R) \rightarrow \mathcal{I}(R, S)$.

Proposition 5.11. *Let $R \subseteq S$ be an extension. Then $R \subseteq S$ is an SL extension if and only if $\mathcal{I}(R, S) = \{R\}$.*

Proof. Use the injective map $U(S)/U(R) \rightarrow \mathcal{I}(R, S)$. $\square$

Proposition 5.12. *The Picard group of a ring R is 0 if either R is J-regular or R verifies the primitive condition. Moreover, over such ring, a finitely generated projective module of finite (local) constant rank is free.*

Proof. It is enough to combine [21, Propositions p. 455 and p. 456] and [21, Theorem and Corollary p. 457]. $\square$

Corollary 5.13. [38, Remark 2.5] *Let $R \subseteq S$ be an extension, where $\text{Pic}(R) = 0$ (for example, if either R is a Nagata ring or R is J-regular), then $U(S)/U(R)$ is isomorphic to $\mathcal{I}(R, S)$.*

Proposition 5.14. *Let $R \subseteq S$ be an extension and M an R -submodule of S . Then M belongs to $\mathcal{I}(R, S)$ if and only if M is an R -module of finite type, $MS = S$ and M is projective of rank one. When R is either a Nagata ring or R is J-regular, the last condition can be replaced with M is free of dimension one and then the elements of $\mathcal{I}(R, S)$ are of the form Ru where u is a unit of S .*

Proof. This a consequence of [38, Lemma 2.2 and Lemma 2.3]. $\square$

Remark 5.15. *We now consider an SL extension $R \subseteq S$.*

(1) *Since $x \in R$ belongs to $J(R)$ if and only if $1 - ax$ is a unit for any $a \in R$, let $x \in J(S)$. In particular, $1 - x \in U(S) = U(R)$, which implies $x \in R$. It follows easily that $J(S) \subseteq J(R)$. Therefore $J(S)$ is an ideal shared by R and S . We infer from this fact that if P is a prime ideal of R , that does not contains $J(S)$, we have $R_P = S_P$.*

(2) *If $2 \in U(S)$, we claim that R and S have the same idempotents: Let e be an idempotent of S . Then, $(1 - 2e)^2 = 1 - 4e + 4e^2 = 1$, so that $1 - 2e \in U(S) = U(R)$, which implies $2e \in R$. Since $2 \in U(S) = U(R)$, we get that $e \in R$.*

(3) *If the class of an element $s \in S$ is a unit of $S/J(S)$, there is some $t \in S$, such that $st - 1 \in J(S)$. It follows that s cannot belong to any maximal ideal of S and is therefore a unit of S and then of R . We deduce from these facts that $U(R/J(S)) = U(S/J(S))$ and $R/J(S) \subseteq S/J(S)$ is SL.*

Proposition 5.16. *A ring extension $R \subseteq S$ is SL if and only if $\text{Nil}(R) = \text{Nil}(S)$ and $R/\text{Nil}(R) \subseteq S/\text{Nil}(S)$ is SL.*

Proof. Assume that $R \subseteq S$ is SL. Then $\text{Nil}(R) = \text{Nil}(S)$ by Proposition 4.4. Set $R' := R/\text{Nil}(R)$ and $S' := S/\text{Nil}(S)$. We claim that $R' \subseteq S'$ is SL. Let $\bar{x} \in U(S')$, where $\bar{x}$ is the class of $x \in S$. There exists $y \in S$ such that $\bar{x}\bar{y} = \bar{1}$ (*) in S' , so that $1 - xy \in \text{Nil}(S) = \text{Nil}(R) \subseteq J(S)$. Then $1 - xy \in J(S)$ implies $x, y \in U(S) = U(R) \subseteq R$. As $1 - xy \in \text{Nil}(R)$ with $x, y \in R$, we deduce from (*) that $\bar{x}, \bar{y} \in U(R')$, giving that $U(S') = U(R')$ and $R/\text{Nil}(R) \subseteq S/\text{Nil}(S)$ is SL.

Conversely, assume that $\text{Nil}(R) = \text{Nil}(S)$ and $R/\text{Nil}(R) \subseteq S/\text{Nil}(S)$ is SL. By Corollary 2.7, $R \subseteq S$ is SL. $\square$

Theorem 5.17. *Let $R \subseteq S$ be an SL extension. Then S is J-regular if and only if R is J-regular and $R \subseteq S$ is integral seminormal. If these conditions hold, then $J(R) = J(S)$.*

Proof. (1) According to Remark 5.15(3), $R/J(S) \subseteq S/J(S)$ is SL. Assume that S is J-regular. We want to show that R is J-regular with $R \subseteq S$ integral seminormal. Since $S/J(S)$ is regular, it is enough to suppose that the extension $R \subseteq S$ is SL with S regular and to show that R is regular.

Let r be in R . As an element of S , there is some $r' \in S$ such that $r^2 r' = r$; so that $e = rr'$ is idempotent and $1 - e + r \in U(S) = U(R) \subseteq R$, with $(1 - e + r)^{-1} = 1 - e + r'$ (see (1) at the beginning of Section 5). We have clearly $e \in R$ and, since $1 - e + r' \in U(S) = U(R) \subseteq R$, then $r' \in R$. To conclude, R is regular.

Let $x \in S$. Then, $x = ue$, $u \in U(S) = U(R)$ and e an idempotent of S , that is $e^2 - e = 0$, so that e is integral over R , and so is x . Then, $R \subseteq S$ is integral. According to the absolute flatness of R and S , we deduce that these rings are seminormal. It follows that $R \subseteq S$ is seminormal by [40] Corollary 3.4].

Coming back to the first case, it follows that if S is J-regular, so is R . Since $R/J(S) \subseteq S/J(S)$ is integral seminormal, so is $R \subseteq S$.

(2) We intend to show that $J(R) = J(S)$. Returning to the Jacobson ideals, we see that $J(S)$ is an intersection of maximal ideals of R because $R/J(S)$ is regular and it follows that $J(R) \subseteq J(S)$, the lacking inclusion. By the way, we have shown that a maximal ideal of S contracts to a maximal ideal of R . Actually the natural map $\text{Max}(S) \rightarrow \text{Max}(R)$ is surjective because a minimal prime ideal can be lifted up in the extension $R/J(R) \subseteq S/J(S)$.

(3) Conversely, assume that R is J-regular and $R \subseteq S$ is integral seminormal. By Remark 5.15(1), we know that $J(S) \subseteq J(R)$ and $J(S)$ is an ideal of R , an intersection of the maximal ideals of S . Then, $J(S) = J(S) \cap R$ is also an intersection of maximal ideals of R since $R \subseteq S$ is integral. Hence, $J(R) \subseteq J(S)$ giving $J(R) = J(S)$. Setting $R' := R/J(R)$ and $S' := S/J(S)$, we get that $R' \subseteq S'$ is integral seminormal and SL by Remark 5.15(3). Since R' is regular, it is reduced and we have $\dim(R') = 0 = \dim(S')$ because $R' \subseteq S'$ is integral. We claim that S' is reduced. Assume there exists some $x \in S'$, $x \neq 0$ which is nilpotent, and let n be the least integer > 1 such that $x^n = 0$ with $y := x^{n-1} \neq 0$. We get that $y^2 = x^{n+(n-2)} = 0 = y^3 \in R' (*)$. Since $R' \subseteq S'$ is seminormal, it follows that $y \in R'$. But $(*)$ implies that $y = 0$ since R' is reduced, a contradiction. We have that S' is reduced, and then regular, so that S is J-regular. $\square$

Lequain and Doering have considered in [9] SL extensions $R \subseteq S$ such that S is semilocal. Then Theorem 5.17 implies one of their results, because S is J-regular by the Chinese remainder theorem. We will improve [9, Theorem 1] by using our methods.

Proposition 5.18. *An SL extension $R \subseteq S$, such that S is regular, is u-integral, infra-integral, seminormal, quadratic and R is regular.*

Proof. Since S is regular, any $x \in S$ can be written $x = eu$, where e is an idempotent and $u \in U(S)$. Set $T := \frac{u}{S}R$. Then, $T \subseteq S$ is u-closed. Since $e^2 - e = e^3 - e^2 = 0 \in T$, we get that $e \in T$. Moreover, $U(R) \subseteq U(T) \subseteq U(S) = U(R)$ gives $U(T) = U(S)$, so that $u \in T$, and then $x \in T$, whence $T = S$ and $R \subseteq S$ is u-integral. Since $S = \frac{u}{S}R \subseteq \frac{t}{S}R \subseteq S$, we get $S = \frac{t}{S}R$ and $R \subseteq S$ is infra-integral. Since S is regular, so is $S/J(S)$ and $R \subseteq S$ is seminormal by Theorem 5.17.

Let $x \in S$ and $y \in S$ be such that $x^2 y = x$, since S is regular. Keeping the previous notation and properties of the beginning of the Section, $e := xy$ is the idempotent such that $x = eu$, with $u \in U(S) = U(R)$. It follows that $e = xu^{-1}$, so that $x^2 u^{-1} = xe = x^2 y = x (*)$. Then, $x^2 = xu$ gives that any $x \in S$ is quadratic and $R \subseteq S$ is a quadratic extension. Now, if $x \in R$, $(*)$ is still valid with $u \in U(R)$ as we have just seen. Then, $x^2 u^{-1} = x$ shows that R is regular. $\square$

Corollary 5.19. *Let $R \subseteq S$ be an SL extension such that S is J-regular. Then $R \subseteq S$ is u-integral, infra-integral and quadratic.*

Proof. Since $R \subseteq S$ is SL, so is $R/J(S) \subseteq S/J(S)$ by Remark 5.15(3). Then, we may apply the results of Proposition 5.18 to the extension $R/J(R) \subseteq S/J(S)$ because $J(R) = J(S)$ by Theorem 5.17, which gives that $R/J(R) \subseteq S/J(S)$ is u-integral, infra-integral and quadratic. It follows that $R \subseteq S$ also verifies these properties. $\square$

Recall that a ring extension $R \subseteq S$ is called a Δ_0 -extension if $T \in [R, S]$ for each R -submodule T of S containing R [16].

Corollary 5.20. *Let $R \subseteq S$ be an SL extension such that S is regular. The following properties hold:*

1. *For any $Q \in \text{Spec}(S)$ and $P := Q \cap R$, we have $R_P \cong S_Q$. If, moreover, $R \subseteq S$ is an i -extension, then $R = S$.*
2. *If $R \subseteq S$ is u -closed, then $R = S$.*
3. *If $R \subseteq S$ is simple, then $R \subseteq S$ is a Δ_0 -extension.*
4. *If $2 \in U(S)$, then $R = S$.*

Proof. (1) By Proposition 5.18, $R \subseteq S$ is infra-integral and R is regular. It follows that for any $Q \in \text{Spec}(S)$ and $P := Q \cap R$, we have an isomorphism $R/P \cong S/Q$. But, R and S being regular, they are zero-dimensional, so that $R/P \cong R_P$ and $S/Q \cong S_Q$ giving $R_P \cong S_Q$.

Assume, moreover, that $R \subseteq S$ is an i -extension, then $R \subseteq S$ is a flat epimorphism [31, Scholium A (1)] or [19, Ch. IV]. Then, $R = S$ by [31, Scholium A (2)].

(2) According to Proposition 5.18, $R \subseteq S$ is u -integral. Assume, moreover, that $R \subseteq S$ is u -closed, then $R = {}^u_S R = S$.

(3) According to Proposition 5.18, $R \subseteq S$ is quadratic. Assume, moreover, that $R \subseteq S$ is a simple extension. Set $S := R[y]$, where y is a quadratic element over R . Then, $S = R + Ry$ and it follows from [11, Proposition 4.12] that $R \subset S$ is a Δ_0 -extension.

(4) Since S is regular, according to [3, Theorem 2.10], any $x \in S$ can be written $x = u + v$, where $u, v \in U(S) = U(R)$ which implies $x \in R$ and $R = S$. $\square$

Proposition 5.21. *Let M be an R -module. The following conditions hold:*

1. $J(R(+))M = J(R)(+)M$.
2. $R(+))M$ is J -regular if and only if R is J -regular.

Proof. (1) comes from [2, Theorem 3.2] because any maximal ideal of $R(+))M$ is of the form $P(+))M$ where $P \in \text{Max}(R)$.

(2) $R(+))M$ is J -regular if and only if $(R(+))M/(J(R)(+)M)$ is regular. But $(R(+))M/(J(R)(+)M) \cong (R/J(R))(+))(M/M) \cong R/J(R)$. By [2, Theorem 3.1], we get the result. $\square$

A ring R is called a *Max-ring* if any nonzero R -module has a maximal submodule. An ideal I of R is *T-nilpotent* if for each sequence $\{r_i\}_{i=1}^\infty \subseteq I$, there is some positive integer k with $r_1 \cdots r_k = 0$.

Proposition 5.22. *Let $R \subseteq S$ be an SL extension where S is a Max-ring. Then R is also a Max-ring and R and S are J -regular.*

Proof. S is regular and $J(S)$ is T-nilpotent since S is a Max-ring by [14, Theorem, p.1135]. Then, S is also J -regular, and so is R , with $J(R) = J(S)$ by Theorem 5.17. It follows that $J(R)$ is T-nilpotent. The same reference gives that R is a Max-ring since R is regular by Proposition 5.18. $\square$

6 Cohn's rings

In [6, Theorem 1], P. M. Cohn shows that for each ring R there is an SL extension $R \subseteq R'$ such that $Z(R') = R' \setminus U(R')$. We generalize some results.

Lemma 6.1. *Let I be a semiprime ideal of a ring R and $f(X), g(X) \in R[X]$, $a, b \in U(R)$ such that $af(X) + bg(X) + Xf(X)g(X) \in I[X]$ (*). Then $f(X), g(X) \in I[X]$.*

Proof. We first prove the Lemma for a prime ideal P . We begin to remark that if $f(X) = f_1(X) + f_2(X)$, with $f_2(X) \in P[X]$, then $(*)$ is equivalent to $af_1(X) + bg(X) + Xf_1(X)g(X) \in P[X]$. The same property holds for $g(X)$. Then, the conclusion of the Lemma will result from the fact that $f_1(X), g(X) \in P[X]$. Moreover, once we have proved that $f(X) \in P[X]$, condition $(*)$ shows that $bg(X) \in P[X]$, which gives $g(X) \in P[X]$ because $b \in U(R)$. So, assume that $f(X)$ and $g(X) \notin P[X]$. Hence, we can set $f(X) := \sum_{i=0}^n \alpha_i X^i$ and $g(X) := \sum_{j=0}^p \beta_j X^j$ with α_n and $\beta_p \notin P$, according to the precedent discussion. The only term of highest degree in $(*)$ is $\alpha_n \beta_p X^{n+p+1}$ which is in $P[X]$, so that $\alpha_n \beta_p \in P$, a contradiction with α_n and $\beta_p \notin P$. To conclude, $f(X), g(X) \in P[X]$.

Now, assume that $af(X) + bg(X) + Xf(X)g(X) \in I[X]$ $(*)$ for a semiprime ideal I . Then, $I = \bigcap_{\lambda \in \Lambda} P_\lambda$, for a family of prime ideals $\{P_\lambda\}_{\lambda \in \Lambda}$. Condition $(*)$ shows that $af(X) + bg(X) + Xf(X)g(X) \in P_\lambda[X]$ for each $\lambda \in \Lambda$. By the first part of the proof, it follows that $f(X), g(X) \in P_\lambda[X]$ for each $\lambda \in \Lambda$, which implies that $f(X), g(X) \in \bigcap_{\lambda \in \Lambda} P_\lambda[X] = I[X]$. $\square$

Proposition 6.2. *For any ring R there exists an SL extension $R \subseteq R'$ such that any nonunit of R is a zerodivisor in R' . The extension $R \subseteq R'$ is pure and t -closed and $(R : R') = J(R)$. If R is reduced, so is R' .*

Proof. For each $M \in \text{Max}(R)$, let X_M be an indeterminate attached to M . Set $\mathcal{X} := \{X_M \mid M \in \text{Max}(R)\}$. We consider $R[\mathcal{X}]$ as the ring of polynomials in the indeterminates $X_M \in \mathcal{X}$. At last, define $I := \sum_{M \in \text{Max}(R)} X_M MR[\mathcal{X}]$, which is an ideal of $R[\mathcal{X}]$ and $R' := R[\mathcal{X}]/I$. For each $M \in \text{Max}(R)$, we define x_M as the class of X_M in R' . We prove the Proposition in several steps.

(1) Let $M, N \in \text{Max}(R)$, $M \neq N$. We claim that $x_M x_N = 0$ in R' .

Since $M \neq N$, they are comaximal, and there exist $m \in M$, $n \in N$ such that $m + n = 1$. It follows that $X_M X_N = (m + n)X_M X_N = mX_M X_N + nX_N X_M \in I$, giving $x_M x_N = 0$. Then, the class of a polynomial of $R[\mathcal{X}]$ is written as the class of a finite sum of polynomials in one indeterminate, that is in finitely many X_M .

(2) R is a subring of R' because the composite ring morphism $R \subseteq R[\mathcal{X}] \rightarrow R[\mathcal{X}]/I$ is injective. Indeed, $R \cap I = 0$ since the constant term of any polynomial in I is 0. Then, we can identify the class of the constant term of any polynomial of $R[\mathcal{X}]$ to this constant term.

(3) Any $y \in R'$ can be written in a unique way

$$y = a + \sum_{M \in \Lambda} x_M f_M(x_M)$$

where $a \in R$, f_M is a polynomial of $R[X]$ and the set Λ is a finite subset of $\text{Max}(R)$.

The existence of this writing results from (1) and (2). Assume that there exist $b \in R$, $g_M \in R[X]$ such that $y = b + \sum_{M \in \Lambda} x_M g_M(x_M)$. There is no harm to choose the same Λ for the two writings. Then, $a + \sum_{M \in \Lambda} x_M f_M(x_M) = b + \sum_{M \in \Lambda} x_M g_M(x_M)$ in R' gives that $(a - b) + \sum_{M \in \Lambda} X_M [f_M(X_M) - g_M(X_M)] \in I = \sum_{M \in \text{Max}(R)} X_M MR[\mathcal{X}]$. First, we get $a = b$ by the substitution $X_M \mapsto 0$ for each M . Now, we get that $X_M [f_M(X_M) - g_M(X_M)] \in X_M MR[X_M]$ for each $M \in \Lambda$, so that $x_M f_M(x_M) = x_M g_M(x_M)$ for each $M \in \Lambda$ showing the uniqueness of the writing.

By the way we proved that $R' = R \bigoplus_{M \in \Lambda} x_M R[x_M]$.

(4) We prove that $(R : R') = J(R)$.

Let $t \in R$. Then $t \in (R : R')$ if and only if $tx_M \in R$ for any $M \in \text{Max}(R)$ if and only if $tx_M = 0$ by (3), which is equivalent to $tX_M \in I$ for any $M \in \text{Max}(R)$, that is $t \in \bigcap_{M \in \text{Max}(R)} M = J(R)$. It follows that $(R : R') = J(R)$.

(5) $R \subseteq R'$ is SL.

Let $y \in U(R')$. There exists $z \in U(R')$ such that $yz = 1$ $(*)$. Write $y = a + \sum_{M \in \Lambda} x_M f_M(x_M)$ and $z = b + \sum_{M \in \Lambda} x_M g_M(x_M)$, where $a, b \in R$ and f_M, g_M are polynomials of $R[X]$. We can choose the same Λ for y and z . Then $(*)$ becomes $1 = (a + \sum_{M \in \Lambda} x_M f_M(x_M))(b + \sum_{M \in \Lambda} x_M g_M(x_M)) = ab + \sum_{M \in \Lambda} x_M [ag_M(x_M) + bf_M(x_M) + x_M f_M(x_M)]$

$g_M(x_M)]$ from which it follows that $ab = 1$ (**) and $ag_M(X_M) + bf_M(X_M) + X_M f_M(X_M)g_M(X_M) \in MR[X_M]$ (**). By (**), we get that $a, b \in U(R)$. Then, we may apply Lemma 6.1 to (**), and we get that $f_M(X_M)$ and $g_M(X_M)$ are in $MR[X_M]$, so that $x_M f_M(x_M) = x_M g_M(x_M) = 0$ and $y = a \in U(R)$. Then, $U(R) = U(R')$ and $R \subseteq R'$ is SL.

(6) Any nonunit of R is a zerodivisor in R' .

Obvious: If $y \in R$ is not a unit in R , there exists some $M \in \text{Max}(R)$ such that $y \in M$. Then $X_M y \in X_M MR[X_M]$ giving $x_M y = 0$ in R' with $x_M \neq 0$, so that y is a zerodivisor in R' .

(7) $R \rightarrow R'$ is pure.

Consider the composite ring morphism $R \subseteq R[\mathcal{X}] \rightarrow R[\mathcal{X}]/I$ and let $\varphi : R[\mathcal{X}] \rightarrow R$ be the ring morphism defined by the substitution $X_M \mapsto 0$ for each M . Since I is contained in the kernel of φ , there is a ring morphism $R[\mathcal{X}]/I \rightarrow R$. It follows that $R[\mathcal{X}]/I$ is a retract of R and the extension $R \rightarrow R[\mathcal{X}]/I$ is pure.

(8) $R \subseteq R'$ is t-closed.

Let $y \in R'$ be such that $y^2 - ry, y^3 - ry^2 \in R$ for some $r \in R$. As in the beginning of the proof, set $y = a + \sum_{M \in \Lambda} x_M f_M(x_M)$ where $a \in R$, $f_M(X_M) := \sum_{i=0}^n \alpha_i X_M^i$ is a polynomial of $R[X_M]$, $n := \deg(f_M)$ and the set Λ is a finite subset of $\text{Max}(R)$. Then, $y^2 - ry = (a^2 - ra) + \sum_{M \in \Lambda} [(2a - r)x_M f_M(x_M) + x_M^2 f_M(x_M)^2]$. Assume that $y \notin R$ so that there exists some $M \in \text{Max}(R)$ such that $x_M f_M(x_M) \neq 0$. As in the proof of Lemma 6.1, we may assume that $\alpha_n \notin M$. But $y^2 - ry \in R$ implies that $\alpha_n^2 X_M^{2n+2} \in X_M MR[X_M]$, whence $\alpha_n^2 \in M$ and $\alpha_n \in M$, a contradiction. Then, any $y \in R'$ such that $y^2 - ry, y^3 - ry^2 \in R$ is in R and $R \subseteq R'$ is t-closed, and, in particular, seminormal. This implies that R' is reduced when R is reduced. $\square$

Corollary 6.3. *Let $R \subseteq S$ be a ring extension such that the spectral map $\text{Max}(S) \rightarrow \text{Max}(R)$ is bijective and let R' (resp. S') be the ring associated to R (resp. S) gotten in Proposition 6.2. Then, $R \subseteq S$ is SL if and only if $R' \subseteq S'$ is SL.*

Proof. For each $M \in \text{Max}(R)$, there exists a unique $N \in \text{Max}(S)$ lying above M , and for each $N \in \text{Max}(S)$, then, $N \cap R \in \text{Max}(R)$. We use the notation of Proposition 6.2 and consider for each $M \in \text{Max}(R)$, an indeterminate X_M attached to M . Then, we may say that X_M is also attached to any $N \in \text{Max}(S)$ such that $N \cap R = M \in \text{Max}(R)$. Then, the X_M 's are attached in a unique way to all maximal ideals of S . Set $\mathcal{X} := \{X_M \mid M \in \text{Max}(R)\}$. We consider $R[\mathcal{X}]$ as the ring of polynomials in the indeterminates $X_M \in \mathcal{X}$ over R and $S[\mathcal{X}]$ as the ring of polynomials in the indeterminates $X_M \in \mathcal{X}$ over S . Setting $I := \sum_{M \in \text{Max}(R)} X_M MR[\mathcal{X}]$, we define $J := \sum_{M \in \text{Max}(R)} [X_M NS[\mathcal{X}] \mid M = N \cap R]$ which is an ideal of $S[\mathcal{X}]$. Set $R' := R[\mathcal{X}]/I$ and $S' := S[\mathcal{X}]/J$. We get the following commutative diagram:

$$\begin{array}{ccc} R & \rightarrow & S \\ \downarrow & & \downarrow \\ R[\mathcal{X}] & \rightarrow & S[\mathcal{X}] \\ \downarrow & & \downarrow \\ R' = R[\mathcal{X}]/I & \rightarrow & S' = S[\mathcal{X}]/J \end{array}$$

where all the maps are extensions since $I = J \cap R[\mathcal{X}]$. By Proposition 6.2, $R \subseteq R'$ and $S \subseteq S'$ are both SL extensions. Now, applying Proposition 2.2, if $R \subseteq S$ is SL, so is $R \subseteq S'$ and then also $R' \subseteq S'$. By the same Proposition, if $R' \subseteq S'$ is SL, so is $R \subseteq S'$ and then also $R \subseteq S$ because $S \subseteq S'$ is injective. $\square$

Theorem 6.4. *Let R be a ring. There exists an SL extension $R \subseteq S$ such that any nonunit of S is a zerodivisor in S . The extension $R \subseteq S$ is pure and t-closed. If, moreover, R is reduced, so is S .*

Proof. According to Proposition 6.2, there exists an SL extension $R \subseteq R'$ such that any nonunit of R is a zerodivisor in R' . Set $R_0 := R$ and $R_1 = R'$. We build by induction, with the same Proposition, a chain $\{R_i\}_{i \in I}$ defined by $R_{i+1} := R'_i$ verifying $U(R_{i+1}) = U(R_i)$. The induction shows that $U(R_i) = U(R)$. Now any nonunit of R_i is a zerodivisor in R_{i+1} . Setting $S := \cup_{i \in I} R_i$, we get an extension $R \subseteq S$.

Let $a \in U(S)$ and set $b := a^{-1} \in U(S)$, so that $ab = 1$ (*) in S . There exists some $i \in I$ such that $a, b \in R_i$ (we can take the same i for a and b). Then (*) still holds in R_i , so that $a \in U(R_i) = U(R)$, giving $U(S) = U(R)$ and $R \subseteq S$ is SL.

Let x be a nonunit of S . There exists some $i \in I$ such that $x \in R_i$. Obviously, x is a nonunit of R_i , and then is a zerodivisor in R_{i+1} , and also a zerodivisor in S . So, any nonunit of S is a zerodivisor in S .

Since $R \subseteq R'$ is pure and t -closed by Proposition 6.2, so is $R_i \subseteq R_{i+1}$ for any i . Now, $R \subseteq S$ is pure (resp. t -closed) since $R \subseteq S$ is the union of pure (resp. t -closed) morphisms $R_i \subseteq R_{i+1}$.

If, moreover, R is reduced, so is R' by Proposition 6.2, and so are any R_i , and to end, so is S . $\square$

Remark 6.5. The ring gotten in Theorem 6.4 is not the only one verifying conditions of Theorem 6.4. For example any regular ring R satisfies these conditions as the ring S built from R in Theorem 6.4.

We now build SL extensions from a new type of rings whose construction is close to Cohn's rings. Many proofs are similar. If I is an ideal of a ring R , we set $R//I := R[X]/XI[X]$. Since $XI[X] \cap R = 0$, we can consider that we have an extension $R \subseteq R//I$, with $R \subset R//I$ when $I \neq R$ because $X \in XR[X] \setminus XI[X]$ shows that $X - a \notin XI[X]$ for any $a \in R$.

Lemma 6.6. If P is a prime ideal of a ring R , the extension $R \subseteq R//P$ is SL, pure, t -closed and $R//P$ is reduced if so is R . Moreover, $P = (R : R//P)$, $R//P \cong R \bigoplus (X(R/P)[X])$ and if $P \not\subseteq Q$, then, $\kappa(Q) \otimes_R (R[X]/XP[X]) \cong \kappa(Q)$ and if $P \subseteq Q$, then, $\kappa(Q) \otimes_R (R[X]/XP[X]) \cong \kappa(Q)[X]$ for any $Q \in \text{Spec}(R)$.

Any $a \in R$ is regular in $R//P$ if and only if a is regular in R and $a \notin P$.

Proof. Set $P' := XP[X]$. Any $y \in P'$ can be written $y = \sum_{i=1}^n p_i X^i$, $p_i \in P$ (*). Then, looking at the terms of degrees 0 and 1 in (*), we get $P' \cap R = 0$ and $X \notin P'$.

An element of $R//P = R[X]/XP[X]$ is of the form $y = a + xf(x)$, where x is the class of X in $R//P$ and $a \in R$. As $R \cap XR[X] = 0$, we also have $R \cap xR[x] = 0$, so that $R//P = R \bigoplus (xR[x])$, with $xP = 0$, a direct sum of R -modules. Obviously, $XR[X]/XP[X] \cong X(R/P)[X]$ as R -modules.

Now, $y \in U(R//P)$ if and only if there exists $z \in R//P$ such that $yz = 1$ (**). Set $y = a + xf(x)$ and $z = b + xg(x)$ with $f(X), g(X) \in R[X]$. Then $(**) \Leftrightarrow (a + xf(x))(b + xg(x)) = 1 \Leftrightarrow ab + x[ag(x) + bf(x) + xf(x)g(x)] = 1 \Leftrightarrow ab = 1$ (i) and $ag(X) + bf(X) + Xf(X)g(X) \in P[X]$ (ii). Since (i) $\Leftrightarrow a, b \in U(R)$, then (i) and (ii) implies $f(X), g(X) \in P[X]$, according to Lemma 6.1, so that $y = a$, $z = b \in U(R)$ which give $U(R//P) = U(R)$ and $R \subseteq R//P$ is SL.

We now prove the second statement. Let $\varphi : R[X] \rightarrow R$ be the ring morphism defined by $X \mapsto 0$. Since $P' \subseteq \ker(\varphi)$, there is a ring morphism $R//P \rightarrow R$. It follows that $R//P$ is a retract of R and the extension $R \rightarrow R//P$ is pure.

We claim that $R \subseteq R//P$ is t -closed. Let $y \in R//P$ be such that $y^2 - ry, y^3 - ry^2 \in R$ for some $r \in R$. Assume that $y \notin R$. According to the beginning of the proof, we can write $y = a + xf(x)$ where $a \in R$, $f(X) := \sum_{i=0}^n \alpha_i X^i$ is a polynomial of $R[X]$, $n := \deg(f)$ and either $\alpha_i = 0$ or $\alpha_i \notin P$, with in particular, $\alpha_n \notin P$. Then, $y^2 - ry = (a^2 - ra) + (2a - r)xf(x) + x^2 f(x)^2$. But $y^2 - ry \in R$ implies that $\alpha_n^2 X^{2n+2} \in XPR[X]$, so that $\alpha_n^2 \in P$ and $\alpha_n \in P$, a contradiction. Then, any $y \in R//P$ such that $y^2 - ry, y^3 - ry^2 \in R$ is in R and $R \subseteq R//P$ is t -closed, and, in particular, is seminormal, whence $R//P$ is reduced when R is reduced.

Now, let $a \in R$. Then, $a \in (R : R//P) \Leftrightarrow aX^k \in R + XP[X]$ for each integer $k \geq 1 \Leftrightarrow a \in P$, so that $P = (R : R//P)$ since $P(R : R//P) \subseteq R$.

Set $S := R[X]$, so that $R//P = S/P'$. Let $Q \in \text{Spec}(R)$. Then, $\kappa(Q) \otimes_R S/P' = (S_Q/P'_Q)/Q(S_Q/P'_Q) \cong (S_Q/P'_Q)/((QS_Q + P'_Q)/P'_Q) \cong S_Q/(QS_Q + P'_Q) \cong R_Q[X]/(QR_Q[X] + XPR_Q[X])$.

If $P \not\subseteq Q$, then, $XPR_Q[X] = XR_Q[X]$ and $\kappa(Q) \otimes_R S/P' \cong R_Q[X]/(QR_Q[X] + XR_Q[X]) \cong R_Q/QR_Q = \kappa(Q)$.

If $P \subseteq Q$, then, $QR_Q[X] + XPR_Q[X] = QR_Q[X]$, so that $\kappa(Q) \otimes_R S/P' \cong R_Q[X]/QR_Q[X] \cong \kappa(Q)[X]$.

Let $a \in R$. If a is a regular element of $R//P$, it is regular in R . If $a \in P$, then $aX \in P'$, so that $ax = 0$, with $x \neq 0$, a contradiction. Conversely, if a is regular in R and $a \notin P$, a is a regular element of $R//P$. Otherwise, there exists $y \in R//P$, $y \neq 0$ such that $ay = 0$. We may assume that $y \notin R$ since a is a regular element of R . As in the beginning of the proof, we can write $y = b + xf(x)$ where $b \in R$, $f(X) := \sum_{i=0}^n \alpha_i X^i$ is a polynomial of $R[X]$, $n := \deg(f)$ and either $\alpha_i = 0$ or $\alpha_i \notin P$, with $\alpha_n \notin P$. Then $ay = 0 = a(b + xf(x)) = ab + axf(x)$ implies $ab + aXf(X) \in P' = XPR[X]$, so that $ab = 0$ (iii) and $af(X) \in PR[X]$ (iv). Since a is a regular element of R , it follows that $b = 0$ by (iii) and (iv) gives $f(X) \in PR[X]$ because $a \notin P$. Then, $y = 0$, a contradiction, and a is a regular element of $R//P$. $\square$

Proposition 6.7. *If I is a semiprime ideal of a ring R , the extension $R \subseteq R//I$ is SL, pure and t-closed. Moreover, $I = (R : R//I)$ and is also semiprime in $R//I$. If R is reduced, then $R//I$ is reduced.*

Proof. Since I is semiprime, set $I := \bigcap_{\lambda \in \Lambda} P_\lambda$. Let $P \in \text{Spec}(R)$ be such that $I \subseteq P$, so that $XI[X] \subseteq XP[X]$, and there is a surjective morphism $f : R[X]/XI[X] \rightarrow R[X]/XP[X]$ giving the following commutative diagram:

$$\begin{array}{ccc} R & \xrightarrow{i} & R[X]/XI[X] = R//I \\ j \searrow & & \downarrow f \\ & & R[X]/XP[X] = R//P \end{array}$$

with two injective morphisms i and j . This holds for any P_λ . According to Lemma 6.6, j is SL, which implies that f is SL by Proposition 2.2. It follows that $j(U(R)) = U(R//P_\lambda) = f(U(R//I))$ (*). Let $y \in U(R//I)$. Then, we may write $y = i(a_0) + \sum_{k=1}^r \overline{a_k} \overline{X}^k$, where $\overline{a_k}$ and $\overline{X}$ are respectively the classes of $a_k \in R$ and X in $R//I$. It follows that $f(y) = j(a_0) + \sum_{k=1}^r \tilde{a}_k \tilde{X}^k$, where $\tilde{a}_k$ and $\tilde{X}$ are respectively the classes of $a_k \in R$ and X in $R//P_\lambda$. We deduce from (*) that $\sum_{k=1}^r \tilde{a}_k \tilde{X}^k = \tilde{0}$, giving $\sum_{k=1}^r a_k X^k \in XP_\lambda R[X]$, and then $a_k \in P_\lambda$ (**) for each $k \geq 1$ and for each $\lambda \in \Lambda$. Moreover, $a_0 \in U(R)$. Because (**) holds for each P_λ , we get $a_k \in I$ for each $k \geq 1$ and then $\overline{a_k} \overline{X}^k = \tilde{0}$ for each $k \geq 1$. To conclude, $y = i(a_0) \in i(U(R))$ and $i(U(R)) = U(R//I)$, that is $R \subseteq R//I$ is SL.

It is enough to mimic the proofs of Lemma 6.6 for each P_λ to get that $R \subseteq R//I$ is pure and t-closed. Moreover, $I = (R : R//I)$. Since $R \subseteq R//I$ is t-closed, it is also seminormal, so that $I = (R : R//I)$ is semiprime in $R//I$ by [7] Lemma 4.8].

If R is reduced, then $R//I$ is reduced as in Lemma 6.6. $\square$

Corollary 6.8. *Let $R \subseteq S$ be an extension with I an ideal of R and K a semiprime ideal of S such that $I = R \cap K$. Then, $R \subseteq S$ is SL if and only if $R//I \subseteq S//K$ is SL.*

Proof. Since $I = R \cap K$, we get that I a semiprime ideal of R and $I[X] = R[X] \cap K[X]$, so that the following commutative diagram holds:

$$\begin{array}{ccc} R & \subseteq & S \\ \downarrow & & \downarrow \\ R//I & \subseteq & S//K \end{array}$$

where the vertical maps are injective and SL morphisms by Proposition 6.7. If either $R \subseteq S$ (1) or $R//I \subseteq S//K$ (2) is SL, so is $R \rightarrow S//K$ by Proposition 2.2 (1). If (1) holds, then (2) holds by Proposition 2.2 (3). If (2) holds, then (1) holds by the same Proposition because $S \rightarrow S//K$ is injective. $\square$

Theorem 6.9. Let R be a ring and $N \in \text{Max}(R[X])$. The following conditions are equivalent:

1. $N \cap R \in \text{Max}(R)$.

2. $M[X] \subseteq N$ for some $M \in \text{Max}(R)$.
3. There exists a monic polynomial $f(X) \in N$.

If these conditions hold, then $N = M[X] + f(X)R[X]$ and $M = N \cap R$.

Proof. (1) $\Rightarrow$ (2) Assume that $M := N \cap R \in \text{Max}(R)$. It follows that $M \subseteq N$ which implies $M[X] \subseteq N$ for some $M \in \text{Max}(R)$.

(2) $\Rightarrow$ (3) Let $M \in \text{Max}(R)$ be such that $M[X] \subseteq N$. Of course, $M[X] + R[X]f(X) \subseteq N$ for any $f(X) \in N$. Consider the following commutative diagram:

$$\begin{array}{ccc} R & \rightarrow & R[X] \\ \downarrow & & \downarrow \\ R/M & \rightarrow & R[X]/M[X] = (R/M)[X] \end{array}$$

Since $M \in \text{Max}(R)$, it follows that R/M is a field and $(R/M)[X]$ is a PID. Then, there exists a monic polynomial $f(X) \in N$ such that $N/M[X] = \overline{f(X)}(R[X]/M[X])$, where $\overline{f(X)}$ is the class of $f(X)$ in $R[X]/M[X]$.

Then any element of N can be written $f(X)g(X) + h(X)$, where $g(X) \in R[X]$ and $h(X) \in M[X]$, giving $N = M[X] + R[X]f(X)$.

(3) $\Rightarrow$ (1) Assume that there exists a monic polynomial $f(X) \in N$ and set $f(X) := X^n + \sum_{i=0}^{n-1} a_i X^i \in N$. Consider the following commutative diagram:

$$\begin{array}{ccc} R & \rightarrow & R[X] \\ \downarrow & & \downarrow \\ R/(N \cap R) & \rightarrow & R[X]/N = [R/(N \cap R)][x] \end{array}$$

where x is the class of X in $R[X]/N$. Since $N \in \text{Max}(R[X])$, it follows that $[R/(N \cap R)][x]$ is a field. Moreover, $R/(N \cap R) \rightarrow R[X]/N$ is injective and $x^n + \sum_{i=0}^{n-1} \overline{a_i} x^i = 0$, where $\overline{a_i}$ is the class of a_i in $R/(N \cap R)$. This implies that $R[X]/N$ is integral over $R/(N \cap R)$, which gives that $R/(N \cap R)$ is a field by [17, Theorem 16] because $R/(N \cap R)$ is an integral domain. To conclude, $N \cap R \in \text{Max}(R)$. If the equivalent conditions (1), (2) and (3) hold then $N = M[X] + f(X)R[X]$ by (2) and $M = N \cap R$. $\square$

Proposition 6.10. *Let R be a ring. Then, $R \subseteq R/J(R)$ is SL, $J(R) = (R : R/J(R)) = J(R/J(R))$ and $R/J(R)$ is not J-regular.*

Proof. The two first assertions come from Proposition 6.7 since $J(R)$ is semiprime.

Let $Q \in \text{Max}(R/J(R))$. Then, there exists $N \in \text{Max}(R[X])$ such that $XJ(R)[X] \subseteq N$, with $Q = N/(XJ(R)[X])$. It follows that either $X \in N$ (*) or $J(R)R[X] \subseteq N$ (**).

In case (*), Theorem 6.9 shows that $M := N \cap R \in \text{Max}(R)$ and $N = M[X] + XR[X]$. But $J(R) \subseteq M$ implies that $J(R)[X] \subseteq N$. Since $J(R)[X] \subseteq N$ in case (**), we get that $J(R)[X] \subseteq N$ in both cases. It follows that $N/J(R)[X] \in \text{Max}(R[X]/J(R)[X])$.

Conversely, if N is a maximal ideal of $R[X]$ containing $J(R)[X]$, it follows that $N/(J(R)[X]) \in \text{Max}(R[X]/(J(R)[X]))$ and $N/(XJ(R)[X]) \in \text{Max}(R[X]/(XJ(R)[X]))$.

Recall that for a ring T , we have $J(T[X]) = \text{Nil}(T[X])$. Moreover, $R[X]/J(R)[X] \cong (R/J(R))[X]$ which is reduced. It follows that $\cap[N/J(R)[X] \mid J(R)[X] \subseteq N \text{ and } N \in \text{Max}(R[X])] = J(R[X]/J(R)[X]) = J((R/J(R))[X]) = \overline{0}$ (*) where $\overline{0}$ the class of 0 in $R[X]/J(R)[X]$.

To make the reading easier, we set $I := J(R)[X]$, $K := \cap[N \in \text{Max}(R[X]) \mid I \subseteq N]$ and $S := R[X]$. Of course, $I \subseteq K$. We have proved that $\cap[N/I \mid I \subseteq N \text{ and } N \in \text{Max}(S)] = \overline{0}$. Assume that $I \subset K$, so that there exists some $y \in K \setminus I$. This means that y is in any $N \in \text{Max}(S)$ which contains I with $y \notin I$. If $\overline{y}$ the class of y in S/I , we get that $\overline{y} \in \cap[N/I \mid I \subseteq N \text{ and } N \in \text{Max}(S)] = \overline{0}$ by (*), giving $y \in I$, a

contradiction. Therefore, $\cap[N \in \text{Max}(S) \mid XI \subseteq N] = I$ which gives $J(R/J(R)) = \cap[Q \in \text{Max}(R/J(R))] = \cap[N/XI \in \text{Max}(R/J(R))] = I/IX = J(R)[X]/XJ(R)[X] = J(R)$.

At last, $(R/J(R))/J(R) = (R[X]/XJ(R)[X])/(J(R)[X]/XJ(R)[X]) \cong R[X]/J(R)[X] \cong (R/J(R))[X]$, which is not zero-dimensional, giving that $R/J(R)$ is not J -regular. $\square$

7 The ring $R\{X\}$

We now consider a ring used by Houston and some other authors for results concerning the dimension of rings [15]. When R is a semilocal (Noetherian) domain, he introduces the ring $R\langle X \rangle$.

This notation is in conflict with the notation of the ring used to solve the Serre conjecture. Therefore, we will denote it by $R\{X\}$. Let Σ be the multiplicatively closed subset of $R[X]$ defined as follows: let T_1 be the set of all maximal ideals N of $R[X]$ such that $N \cap R \in \text{Max}(R)$, then Σ is the complementary set in $R[X]$ of $\cup[N \mid N \in T_1]$ and $R\{X\} := R[X]_\Sigma$. As we consider arbitrary rings, a more precise characterization of T_1 is given in Theorem 6.9, completing [15] Lemma 1.2].

Proposition 7.1. *For any ring R , there is a factorization $R \rightarrow R\{X\} \rightarrow R(X)$, where $R(X)$ is the Nagata ring of R .*

Proof. Let $p(X) \in \Sigma$. We claim that $c(p) = R$. Otherwise, there exists $M \in \text{Max}(R)$ such that $c(p) \subseteq M$. Then $p(X) \in M[X] \subseteq N$ for some $N \in \text{Max}(R[X])$. It follows that $M = N \cap R$, so that $N \in T_1$ by Theorem 6.9 and $p(X) \in N$, a contradiction with $p(X) \in \Sigma$. Since $c(p) = R$, we get that $p(X)/1 \in U(R(X))$ giving the factorization $R \rightarrow R\{X\} \rightarrow R(X)$. $\square$

We recall that R is a *Jacobson ring* if and only if maximal ideals of $R[X]$ contract to maximal ideals of R . Then we have the following:

Proposition 7.2. *Let R be a Jacobson ring. Then $R\{X\} = R[X]$.*

Proof. Since R is a Jacobson ring, it follows that $T_1 = \text{Max}(R[X])$ where $T_1 = \{N \in \text{Max}(R[X]) \mid N \cap R \in \text{Max}(R)\}$. This implies that $\Sigma = R[X] \setminus \cup[N \mid N \in T_1] = R[X] \setminus \cup[N \mid N \in \text{Max}(R[X])] = U(R[X])$ and $R\{X\} := R[X]_\Sigma = R[X]$. $\square$

Mimicking [15] and using also [12] Lemma 3], the following proposition characterizes in a more general setting, and when R is J -regular, the maximal ideals of $R\{X\}$.

Proposition 7.3. *If R is J -regular, $\text{Max}(R\{X\}) = \{NR\{X\} \mid N \in T_1\}$.*

Proof. Since R is J -regular, we get that $V(J(R)) = \text{Max}(R)$. Let $N \in \text{Max}(R[X])$. Then, $N \in T_1$ if and only if $N \cap R \in \text{Max}(R)$ if and only if $J(R) \subseteq N$ if and only if $J(R)[X] \subseteq N$. Then, $T_1 = \text{Max}(R[X]) \cap V(J(R)[X])$. According to [12] Lemma 3], and since $R\{X\} = R[X]_\Sigma$, it follows that $\text{Max}(R\{X\}) = \{NR\{X\} \mid N \in T_1\}$. $\square$

Proposition 7.4. *If M is a maximal ideal of R , then there is a factorization $R \rightarrow R\{X\} \rightarrow R/M$ and $R \rightarrow R\{X\}$ is faithfully flat.*

Proof. Since $R\{X\} = R[X]_\Sigma$, we have $U(R\{X\}) = \{p(X)/q(X) \mid p(X), q(X) \in \Sigma\}$. Let $p(X) \in \Sigma$, so that $p(X) \notin Q$ for any $Q \in T_1$. Let $M \in \text{Max}(R)$. We claim that $p(X)R[X] + XM[X] = R[X]$. Otherwise, there exists some $N \in \text{Max}(R[X])$ such that $p(X) \in N$ and $XM[X] \subseteq N$ (*). But (*) holds if and only if either $X \in N$ (1) or $M[X] \subseteq N$ (2). In case (1), N contains the monic polynomial X , so that $N \in T_1$ by Theorem 6.9, and in case (2), the same reference shows that $N \in T_1$. In both cases, we infer that we get a contradiction with $N \in T_1$ and $p(X) \in N$ since $p(X) \notin Q$ for any $Q \in T_1$, so that $p(X)R[X] + XM[X] = R[X]$ holds. This implies that there exist $f(X) \in R[X]$ and $g(X) \in M[X]$ such that $p(X)f(X) + Xg(X) = 1$.

Working in $R//M = R[X]/XM[X]$, this gives $\overline{p(X)} \overline{f(X)} = \overline{1}$, so that $\overline{p(X)} \in U(R//M)$. Then, we have the wanted factorization thanks to the following commutative diagram:

$$\begin{array}{ccccc} R & \rightarrow & R[X] & \rightarrow & R//M = R[X]/XM[X] \\ & \searrow & \downarrow & \nearrow & \\ & & R\{X\} = R[X]_{\Sigma} & & \end{array}$$

Consider now the following factorization $R \rightarrow R[X] \rightarrow R\{X\} \rightarrow R//M$. By Lemma 6.6, the extension $R \subseteq R//M$ is pure. Then, so is $R \subseteq R\{X\}$ by [24] Lemme 2.3, p.19]. Moreover, $R \subseteq R[X]$ is flat as well as $R[X] \subseteq R\{X\}$. Then, so is $R \subseteq R\{X\}$. Since the maximal ideals of R can be lifted on in $R\{X\}$, then $R \rightarrow R\{X\}$ is faithfully flat. $\square$

Proposition 7.5. *Let $R \subseteq S$ be an integral ring extension. Then, there is an integral ring extension $R\{X\} \subseteq S\{X\}$. In case S is J-regular, then $R\{X\} \subseteq S\{X\}$ is SL if and only if $R = S$.*

Proof. Set $T_1 := \{N \in \text{Max}(R[X]) \mid N \cap R \in \text{Max}(R)\}$, $T'_1 := \{N' \in \text{Max}(S[X]) \mid N' \cap S \in \text{Max}(S)\}$, $\Sigma := R[X] \setminus \cup\{N \mid N \in T_1\}$ and $\Sigma' := S[X] \setminus \cup\{N' \mid N' \in T'_1\}$. We have the following diagram:

$$\begin{array}{ccccc} R & \rightarrow & R[X] & \rightarrow & R\{X\} \\ \downarrow & & \downarrow & & \\ S & \rightarrow & S[X] & \rightarrow & S\{X\} \end{array}$$

Since $R \subseteq S$ is integral, so is $f : R[X] \subseteq S[X]$. Let $N \in T_1$, so that $M := N \cap R \in \text{Max}(R)$, and there exists $N' \in \text{Max}(S[X])$ lying above N . Set $M' := N' \cap S \in \text{Spec}(S)$. Then, $M' \cap R = N' \cap S \cap R = N' \cap R[X] \cap S \cap R = N \cap R = M \in \text{Max}(R)$. It follows that $M' \in \text{Max}(S)$ since it is a prime ideal of S lying above a maximal ideal of R . Then, $N' \in T'_1$. Conversely, let $N' \in T'_1$ and set $N := N' \cap R[X]$. Then, $M' := N' \cap S \in \text{Max}(S)$ and $N \cap R = N' \cap R[X] \cap R = N' \cap S \cap R[X] \cap R = M' \cap R \in \text{Max}(R)$ since $M' \in \text{Max}(S)$. It follows that there is a surjective map $T'_1 \rightarrow T_1$ which is the restriction of ${}^a f : \text{Spec}(S[X]) \rightarrow \text{Spec}(R[X])$.

Now, let $p(X) \in \Sigma$, so that $p(X) \notin N$ for any $N \in T_1$. We claim that $p(X) \in \Sigma'$. Otherwise, there exists $N' \in T'_1$ such that $p(X) \in N'$. But $p(X) \in R[X]$, so that $p(X) \in N' \cap R[X] \in T_1$ by the beginning of the proof, a contradiction. Then, $\Sigma \subseteq \Sigma'$ and $U(R\{X\}) \subseteq U(S\{X\})$.

We show that f defines an injective morphism $R\{X\} \rightarrow S\{X\}$. Let $p(X)/q(X) \in R\{X\}$, $p(X), q(X) \in R[X]$, $q(X) \in \Sigma$ be such that $p(X)/q(X) = 0$ in $S\{X\}$. There exist $g(X) \in \Sigma'$ such that $p(X)g(X) = 0$ (*) in $S[X]$. Then, $g(X) \notin N'$, for any $N' \in T'_1$. We claim that $c(g) = S$. Otherwise, there exists $N \in \text{Max}(S)$ such that $c(g) \subseteq N$. Then $g(X) \in N[X] \subseteq N'$ for some $N' \in \text{Max}(S[X])$. It follows that $N' \in T'_1$ by Theorem 6.9 and $g(X) \in N'$, a contradiction with $g(X) \notin N'$, for any $N' \in T'_1$. Since, $c(g) = S$, we obtain that g is a regular element of $S[X]$ and it results from (*) that $p(X) = 0$. Then there is an integral ring extension $R\{X\} \subseteq S\{X\}$.

If $R = S$, obviously $R\{X\} \subseteq S\{X\}$ is SL.

Conversely, assume that S is J-regular and $R\{X\} \subseteq S\{X\}$ is SL. We mimic the proof of Proposition 4.6. Let $s \in S$ and set $p(X) := s + X \in S\{X\}$. Since S is J-regular, then $\text{Max}(S\{X\}) = \{NS\{X\} \mid N \in T'_1\}$ by Proposition 7.3, so that $p(X) \in U(S\{X\}) = U(R\{X\})$. It follows that there exists $h(X), k(X) \in \Sigma$ such that $p(X)/1 = h(X)/k(X)$ in $S\{X\}$, and then there exists $q(X) \in \Sigma'$ such that $q(X)p(X)k(X) = q(X)h(X)$. Because $q(X) \in \Sigma'$, we get that $c(q) = S$ (see the proof we give in the previous paragraph), which implies that $q(X)$ is a regular element of $S[X]$. Then $p(X)k(X) = h(X) = (s + X)k(X)$. As $Xk(X)$ and $h(X)$ are in $R[X]$, it follows that $sk(X) \in R[X]$. Now, R is also J-regular by Corollary 5.7. The same proof as for $q(X) \in S[X]$ before shows that $c(k) = R$. Set $k(X) := \sum_{i=0}^n a_i X^i$, $a_i \in R$ and $b_i := sa_i \in R$ (*) for each $i \in \{0, \dots, n\}$. There exist $\lambda_0, \dots, \lambda_n \in R$ such that $\sum_{i=0}^n \lambda_i a_i = 1$. Multiplying each equality of (*) by λ_i and adding each of these equalities for each $i \in \{0, \dots, n\}$, we get $s(\sum_{i=0}^n \lambda_i a_i) = s = \sum_{i=0}^n \lambda_i b_i \in R$, so that $S = R$. $\square$

Corollary 7.6. *Let $R \subseteq S$ be an integral ring extension. If $R\{X\} \subseteq S\{X\}$ is SL, so is $R \subseteq S$.*

Proof. Let $s \in U(S)$. In particular, $s/1 \in U(S\{X\}) = U(R\{X\})$. Then $s/1 = f(X)/g(X)$ in $S\{X\}$ for some $f(X)/g(X) \in U(R\{X\})$, that is $f(X), g(X) \in \Sigma$. The same proof as in Proposition 7.5 shows that $sg(X) = f(X) (*)$ in $S[X]$ and $c(f) = c(g) = R$. Set $f(X) := \sum_{i=0}^n a_i X^i, a_i \in R$ and $g(X) := \sum_{i=0}^n b_i X^i, b_i \in R$, so that $sb_i = a_i$ for each $i \in \{0, \dots, n\}$ (**). There exist $\lambda_0, \dots, \lambda_n \in R$ such that $\sum_{i=0}^n \lambda_i b_i = 1$. Multiplying each equality of (**) by λ_i and adding each of these equalities for each $i \in \{0, \dots, n\}$, we get $s(\sum_{i=0}^n \lambda_i b_i) = s = \sum_{i=0}^n \lambda_i a_i \in R$, so that $s \in R$. Then, (*) shows that $sc(g) = c(f) = R$ and gives that $Rs = R$, that is $s \in U(R)$ and $U(R) = U(S)$. To conclude, $R \subseteq S$ is SL. $\square$

Corollary 7.7. *Let R be a J-regular ring. Then there is a factorization $R \rightarrow R\{X\} \rightarrow R//J(R)$.*

Proof. We use the beginning of the proof of Proposition 7.4. Let $p(X) \in \Sigma$, so that $p(X) \notin Q$ for any $Q \in T_1$. We claim that $\overline{p(X)} \in U(R//J(R))$. Otherwise, there exists some $N \in \text{Max}(R[X])$ with $XJ(R)[X] \subseteq N$ such that $p(X) \in N$. As in the quoted proof, $X \notin N$ because $N \notin T_1$. It follows that $J(R)[X] \subseteq N$. But R being J-regular, any prime ideal of R containing $J(R)$ is maximal. As $J(R)[X] \subseteq N$, we get $J(R) \subseteq N \cap R$, so that $N \cap R \in \text{Max}(R)$, giving $N \in T_1$, a contradiction. Then, $\overline{p(X)} \in U(R//J(R))$, and we get the wanted factorization thanks to the following commutative diagram:

$$\begin{array}{ccccc} R & \rightarrow & R[X] & \rightarrow & R//J(R) \\ & \searrow & \downarrow & \nearrow & \\ & & R\{X\} = R[X]_{\Sigma} & & \end{array}$$

$\square$

Corollary 7.8. *Let R be a ring and I an ideal intersection of finitely many maximal ideals M_i . Then, $R \rightarrow R//I$ is SL and there is a factorization $R \rightarrow R\{X\} \rightarrow R//I \rightarrow R//M_i$ for any M_i .*

If, moreover, R is J-regular, there is a factorization $R \rightarrow R\{X\} \rightarrow R//J(R) \rightarrow R//I \rightarrow R//M_i$ for any M_i .

Proof. By Proposition 6.7, $R \rightarrow R//I$ is SL. For the other assertions, as we have the inclusions $J(R) \subseteq I \subseteq M_i$ for any M_i , we get the wanted factorization, mimicking the proof of Corollary 7.7 and using the fact that R/I is regular as a product of finitely many fields. $\square$

8 FCP SL extensions

Proposition 8.1. *Let $R \subseteq S$ be an SL extension where S is a semilocal ring. Then R is semilocal, $J(R) = J(S)$ and $R \subseteq S$ is an FIP seminormal and infra-integral extension.*

Proof. Since S is semilocal, S is J-regular. According to Remark 5.15 (3), Theorem 5.17 and Proposition 5.18, we have $J(R) = J(S)$ and we can assume that $R \subseteq S$ is seminormal and infra-integral, R and S are regular and semi-local and that S is a finite product of fields each of them being a residual field of R . Finally the extension can be viewed as a product of extensions $R/M \rightarrow (R/M)^n$ where $M \in \text{Max}(R)$. By using suitable localizations and [8, Proposition 4.15], we get that $R \subseteq S$ is an FIP seminormal and infra-integral extension. $\square$

Corollary 8.2. *Let $R \subseteq S$ be an SL extension where S is a semilocal ring. If $R \subseteq S$ is a flat epimorphism, then $R = S$.*

Proof. By Proposition 8.1, $R \subseteq S$ is integral and a flat epimorphism, then $R = S$. $\square$

Theorem 8.3. *An extension $R \subseteq S$, where S is a semilocal ring, is SL if and only if $R \subseteq S$ is a seminormal infra-integral FIP extension such that $R/M \cong \mathbb{Z}/2\mathbb{Z}$ for each $M \in \text{MSupp}(S/R)$.*

Proof. Assume that $R \subseteq S$ is SL. According to Proposition 8.1, we get that $J(R) = J(S)$ and $R \subseteq S$ is an FIP seminormal and infra-integral extension. Set $I := J(S) = J(R) = \bigcap_{i=1}^n M_i = \bigcap [M_{i,j} \mid M_{i,j} \in \text{Max}(S)]$, where $\text{Max}(R) = \{M_i\}_{i=1}^n$ and $\text{Max}(S) = \{M_{i,j} \mid i = 1, \dots, n, M_i = M_{i,j} \cap R \text{ for each } j \in \mathbb{N}_{n_i}\}$. By Remark 5.15 (3), $R/I \subseteq S/I$ is SL. But $R/I \cong \prod_{i=1}^n R/M_i$ and $S/I \cong \prod [S/M_{i,j} \mid M_{i,j} \in \text{Max}(S)]$. Set $X_1 := \text{MSupp}(S/R)$, $X_2 := \text{Max}(R) \setminus X_1$, $I_1 := \bigcap_{M \in X_1} M$, $I_2 := \bigcap_{M \in X_2} M$, $R_1 := R/I_1 = \prod_{M \in X_1} R/M$ and $R_2 := R/I_2 = \prod_{M \in X_2} R/M$. Then, $R/I = R_1 \times R_2$ because I_1 and I_2 are comaximal. It follows that $U(R/I) = U(R_1) \times U(R_2)$. For $M_i \in X_2$, there is a unique $M_{i,j}$ lying above M_i and we have $R/M_i \cong S/M_{i,j}$, so that $R_2 \cong S_2 := \prod_{M_i \in X_2} S/M_{i,j}$ and $U(R_2) \cong U(S_2)$ (*). Set $S_1 := \prod_{M_i \in X_1} S/M_{i,j} = \prod_{M_i \in X_1} [\prod_{j \in \mathbb{N}_{n_i}} S/M_{i,j}]$. Since $R \subseteq S$ is infra-integral and $M_i = M_{i,j} \cap R$ for each $j \in \mathbb{N}_{n_i}$, we get that $R/M_i \cong S/M_{i,j}$, so that $S_1 \cong \prod_{M_i \in X_1} (R/M_i)^{n_i}$. Whence $U(S_1) \cong \prod_{M_i \in X_1} [U(R/M_i)]^{n_i}$ (**). Since $R \subseteq S$ is SL and because of (*), we get that $U(R_1) \cong U(S_1) \cong \prod_{M_i \in X_1} [U(R/M_i)]^{n_i}$. But, for any $M_i \in X_1$, we have $R_{M_i} \subseteq S_{M_i}$ seminormal and infra-integral, which gives that $n_i > 1$ for any $M_i \in X_1$. Then, $U(R_1) \cong U(S_1)$ if and only if $|U(R/M_i)| = 1$ for any $M_i \in X_1$. Since R/M_i is a field for any $M_i \in X_1$, it follows that $R/M_i \cong \mathbb{Z}/2\mathbb{Z}$ for each $M_i \in \text{MSupp}(S/R)$.

Conversely, assume that S is a semilocal ring and $R \subseteq S$ is a seminormal infra-integral FIP extension such that $R/M \cong \mathbb{Z}/2\mathbb{Z}$ for each $M \in \text{MSupp}(S/R)$. We can use the results and notation of the first part of the proof related to the sets I_1, I_2, R_1, R_2 and S_1, S_2 . Since $R \subseteq S$ is seminormal FIP with S semilocal, we get that $(R : S) = \bigcap_{M_i \in X_1} M_i = \bigcap_{M_i \in X_1} M_{i,j}$ by [34, Proposition 2.4]. In addition, $J(S) = \bigcap_{i=1}^n M_{i,j} = (R : S) \cap_{M_i \in X_2} M_{i,j} = (R : S) \cap_{M_i \in X_2} M_i = J(R)$. Set $I := J(S) = J(R)$. We still have $U(R/I) = U(R_1) \times U(R_2)$, $U(R_2) \cong U(S_2)$, $U(S/I) = U(S_1) \times U(S_2)$ and $U(S_1) \cong \prod_{M_i \in X_1} [U(R/M_i)]^{n_i}$. Since $R/M_i \cong \mathbb{Z}/2\mathbb{Z}$ and $R/M_i \cong S/M_{i,j}$ for any $M_i \in X_1$ and $M_{i,j}$ lying over M_i , it follows that $|U(R/M_i)| = 1 = |U(S/M_{i,j})|$ for any $M_i \in X_1$, so that $U(R_1) \cong U(S_1)$, which yields that $R/I \subseteq S/I$ is SL and $R \subseteq S$ is SL by Corollary 2.7. $\square$

Corollary 8.4. *A seminormal infra-integral FCP extension $R \subseteq S$ is SL if $R/M \cong \mathbb{Z}/2\mathbb{Z}$ for each $M \in \text{MSupp}(S/R)$.*

Proof. Since $R \subseteq S$ is an FCP extension, it follows that $\text{MSupp}(S/R)$ has finitely many elements. Set $I := (R : S)$. Moreover, $R \subseteq S$ being seminormal infra-integral, I is an intersection of finitely many maximal ideals of S by [34, Proposition 2.4]. It follows that the extension $R/I \subseteq S/I$ satisfies the assumptions of Theorem 8.3 because $R/I \subseteq S/I$ has FIP by [8, Proposition 4.15], and is then SL. Now, it is enough to use Corollary 2.7 to get that $R \subseteq S$ is SL. $\square$

The following result did not seem to appear in earlier papers: we show that there is a seminormal infra-integral closure for FCP extensions. This will be useful to build a closure for SL extensions in an FCP extension.

Lemma 8.5. *Let $R \subseteq S$ be an FCP extension and $T, V \in [R, S]$ be such that $R \subseteq T$ and $R \subseteq V$ are both seminormal infra-integral. Then, $R \subseteq TV$ is seminormal infra-integral.*

Proof. Since $R \subseteq T$ and $R \subseteq V$ are both infra-integral, we have $T, V \in [R, {}^t_S R]$, giving $TV \in [R, {}^t_S R]$, so that $R \subseteq TV$ is infra-integral.

We claim that $R \subseteq TV$ is seminormal. Let $M \in \text{MSupp}(TV/R)$, so that $(TV)_M = T_M V_M \neq R_M$. In particular, either $T_M \neq R_M$ or $V_M \neq R_M$. In both cases, $R_M \subseteq T_M$ and $R_M \subseteq V_M$ are either seminormal or equality. Set $R' := R_M$, $T' := T_M$, $V' := V_M$ and $M' := MR_M$. According to [34, Proposition 2.4], we get that $M' \subseteq (R' : T')$ and $M' \subseteq (R' : V')$, giving $M'T' = M'V' = M' \subseteq R'$, so that $M'T'V' = M' \subseteq R'$. It follows that $M' = (R' : T'V')$. Set $M' = \bigcap_{i=1}^n M'_i = \bigcap_{j=1}^m N'_j$ (*), where the M'_i are in $\text{Max}(T')$ (resp. N'_j are in $\text{Max}(V')$) because $R' \subseteq T'$ and $R' \subseteq V'$ are either seminormal or equality. It follows that $T'/M'_i \cong R'/M' \cong V'/N'_j$ for each i and j since $R' \subseteq T'$ and $R' \subseteq V'$ are both infra-integral. In addition, $T'/M' \cong (R'/M')^n$ and $V'/M' \cong (R'/M')^m$ by (*). This implies that $(T'V')/M' \cong (T'/M')(V'/M') \cong (R'/M')^{n+m}$ where R'/M' is a field. According to [8, Proposition 4.15], we get that $R'/M' \subseteq (T'V')/M'$ is seminormal

infra-integral as $R' = R_M \subseteq T'V' = T_M V_M = (TV)_M$. Since this holds for any $M \in \text{MSupp}(TV/R)$, we get that $R \subseteq TV$ is seminormal infra-integral. $\square$

Proposition 8.6. *Let $R \subseteq S$ be an FCP extension. There exists a greatest $T \in [R, S]$ such that $R \subseteq T$ is seminormal infra-integral. It satisfies the following properties:*

1. $T = \Pi[V \in [R, S] \mid R \subseteq V \text{ seminormal infra-integral}]$.
2. $T = \sup[V \in [R, S] \mid R \subseteq V \text{ seminormal infra-integral}]$.
3. $T = \cup[V \in [R, S] \mid R \subseteq V \text{ seminormal infra-integral}]$.

Proof. Set $\mathcal{F} := \{V \in [R, S] \mid R \subseteq V \text{ seminormal infra-integral}\}$. The result is obvious if $\mathcal{F} = \{R\}$. So, assume that $\mathcal{F} \neq \{R\}$. Since $R \subseteq V$ is infra-integral for any $V \in \mathcal{F}$, it follows that $\mathcal{F} \subseteq [R, {}^t_S R]$. In particular, any $V \in \mathcal{F}$ is integral over R . Then, we may assume that $R \subseteq S$ is infra-integral. Since $R \subseteq S$ has FCP, $\mathcal{F}$ has maximal elements. We claim that $\mathcal{F}$ has only one maximal element. Otherwise, there exist $V, V', V \neq V'$ which are maximal elements of $\mathcal{F}$. Then, $VV' \notin \mathcal{F}$. According to Lemma 8.5, we get that $R \subseteq VV'$ is seminormal infra-integral, a contradiction. Then, $\mathcal{F}$ has only one maximal element. Let T be this maximal element. Equalities (1), (2) and (3) follow obviously because $V \subseteq T$ for any $V \in \mathcal{F}$ and $T \in \mathcal{F}$. $\square$

There are four types of minimal extensions, but only two types are used in the paper, characterized in [7 Theorems 2.1 and 2.2] and [32 Proposition 4.5]. We recall some results about minimal extensions:

Proposition 8.7. (1) [7 Theorem 2.1] *Let $R \subseteq T$ be a minimal integral extension. Then, $M := (R : T) \in \text{Max}(R)$ and there is a bijection $\text{Spec}(T) \setminus V_T(M) \rightarrow \text{Spec}(R) \setminus \{M\}$, with at most two maximal ideals of T lying above M .*

(2) *Let $R \subseteq S$ be an FCP extension. Then, any maximal chain of $[R, S]$ results from juxtaposing finitely many minimal extensions.*

Proof. Obvious. $\square$

Definition 8.8. (1) *Let $R \subset T$ be an extension and $M := (R : T)$. Then $R \subset T$ is minimal decomposed if and only if $M \in \text{Max}(R)$ and there exist $M_1, M_2 \in \text{Max}(T)$ such that $M = M_1 \cap M_2$ and the natural maps $R/M \rightarrow T/M_i$ for $i \in \{1, 2\}$ are both isomorphisms. A minimal decomposed extension is seminormal infra-integral.*

(2) *A minimal extension $R \subset T$ is minimal Prüfer if and only if $R \subset T$ is a flat epimorphism and there exists $M \in \text{Max}(R)$ such that $MT = T$ with $R_P \cong T_P$ for any $P \in \text{Spec}(R)$, $P \neq M$ [10 Theorem 2.2]. In particular, there is a bijection $\text{Spec}(T) \rightarrow \text{Spec}(R) \setminus \{M\}$.*

Lemma 8.9. *Let $R \subseteq S$ be an FCP integral extension where S is semilocal.*

1. *Let $T \in]R, S]$ be such that $R \subset T$ is minimal. Then, $R \subset T$ is SL if and only if $R \subset T$ is minimal decomposed such that $M := (R : T)$ satisfies $R/M \cong \mathbb{Z}/2\mathbb{Z}$.*
2. *Let $T \in]R, S]$. Then $R \subset T$ is SL if and only if $T \in [R, {}^u_S R]$ and $T/(R : T) \cong (\mathbb{Z}/2\mathbb{Z})^m$ for some positive integer m .*
3. *Let $T, V \in [R, S]$ be such that $R \subset T$ and $R \subset V$ are SL. Then, $R \subset TV$ is SL.*

Proof. Since $R \subseteq S$ is an FCP integral extension such that S is semilocal, any element of $[R, S]$ is semilocal.

(1) Let $T \in [R, S]$ be such that $R \subset T$ is minimal SL. Then, T is semilocal and $R \subset T$ satisfies conditions of Theorem 8.3 that $R \subset T$ is a seminormal infra-integral extension such that $R/M \cong \mathbb{Z}/2\mathbb{Z}$ for $M = (R : T)$ since $\text{MSupp}(T/R) = \{M\}$. It follows that $R \subset T$ is minimal decomposed by [32, Proposition 4.5].

Conversely, if $R \subset T$ is minimal decomposed such that $M := (R : T)$ satisfies $R/M \cong \mathbb{Z}/2\mathbb{Z}$, then $R \subset T$ is seminormal infra-integral with $R/M \cong \mathbb{Z}/2\mathbb{Z}$ for $M \in \text{MSupp}(T/R)$ by the previous reference. Then Theorem 8.3 shows that $R \subset T$ is SL.

(2) According to Theorem 8.3, $R \subseteq T$ is SL if and only if (i) and (ii) hold where :

(i) $R \subseteq T$ is a seminormal infra-integral FIP extension.

(ii) $R/M \cong \mathbb{Z}/2\mathbb{Z}$ for each $M \in \text{MSupp}(T/R)$.

Assume first that $R \subseteq T$ is SL. By (i) and [35, Theorem 5.9], we get that $R \subseteq T$ is u-integral, so that $T \in [R, {}^u_S R]$. Moreover, since $R \subseteq T$ is seminormal, it follows that $(R : T) = \cap [N_{i,j} \mid N_{i,j} \in \text{Max}(T), N_{i,j} \cap R = M_i]$, where $\text{MSupp}(T/R) := \{M_i\}_{i=1}^n$. Then, $T/(R : T) \cong T/(\cap N_{i,j}) \cong \prod (T/N_{i,j}) \cong \prod (R/M_i)^{n_i}$, where $n_i := |\{N_{i,j} \in \text{Max}(T) \mid N_{i,j} \cap R = M_i\}|$ and because of (i). Then, (ii) gives that $T/(R : T) \cong (\mathbb{Z}/2\mathbb{Z})^m$ for some positive integer m .

Conversely, assume that $T \in [R, {}^u_S R]$ and $T/(R : T) \cong (\mathbb{Z}/2\mathbb{Z})^m$ for some positive integer m . Since $T \in [R, {}^u_S R]$, we get that $R \subset T$ is u-integral, and in particular infra-integral. Moreover, since $T/(R : T) \cong (\mathbb{Z}/2\mathbb{Z})^m$, a product of finitely many finite fields, $T/(R : T)$ is reduced, so that $(R : T)$ is an intersection of finitely many maximal ideals of T (and R), and $R \subset T$ is seminormal by [34, Proposition 2.4]. Then, (i) holds because $T/(R : T)$ has finitely many elements, giving that $R \subseteq T$ has FIP. At last, $(R : T)$ is semi-prime, it is an intersection of the maximal ideals $N_{i,j}$ of T lying above the maximal ideals M_i of R of $\text{MSupp}(T/R)$. It follows that $R/M \cong \mathbb{Z}/2\mathbb{Z}$ for each $M \in \text{MSupp}(T/R)$ and (ii) holds. To conclude, $R \subseteq T$ is SL (we also can use Corollary 8.4).

(3) Let $T, V \in [R, S]$ be such that $R \subset T$ and $R \subset V$ are SL. Then $R \subset T$ and $R \subset V$ are both seminormal infra-integral, and so is $R \subset TV$ by Lemma 8.5. Moreover, $\text{MSupp}(TV/R) = \text{MSupp}(T/R) \cup \text{MSupp}(V/R)$, so that any $M \in \text{MSupp}(TV/R)$ is either in $\text{MSupp}(T/R)$ or in $\text{MSupp}(V/R)$, which implies that $R/M \cong \mathbb{Z}/2\mathbb{Z}$, whence $R \subseteq TV$ is SL by Corollary 8.4. $\square$

Theorem 8.10. Let $R \subseteq S$ be an FCP extension where S is semilocal. There exists a greatest $T \in [R, S]$ such that $R \subseteq T$ is SL. It satisfies the following properties:

1. $T = \Pi[V \in [R, S] \mid R \subseteq V \text{ seminormal infra-integral, } R/M \cong \mathbb{Z}/2\mathbb{Z} \text{ for any } M \in \text{MSupp}(V/R)]$.
2. $T = \Pi[V \in [R, S] \mid R \subseteq V \text{ SL}]$.
3. $T = \sup[V \in [R, S] \mid R \subseteq V \text{ SL}]$.
4. $T = \cup[V \in [R, S] \mid R \subseteq V \text{ SL}]$.

Proof. Let $V \in [R, S]$ be such that $R \subseteq V$ is SL. According to Lemma 8.9, we have $V \in [R, {}^u_S R]$ and $R \subset V$ is u-integral, and in particular $V \in [R, \bar{R}]$, where $\bar{R}$ is the integral closure of $R \subseteq S$. As $\bar{R} \subseteq S$ has FCP, any element of $[\bar{R}, S]$ is semilocal. It follows that we can assume that $R \subseteq S$ is an FCP integral extension such that S is semilocal.

Setting $\mathcal{F}' := \{V \in [R, S] \mid R \subseteq V \text{ seminormal infra-integral, } R/M \cong \mathbb{Z}/2\mathbb{Z} \text{ for any } M \in \text{MSupp}(V/R)\}$ and using notation of Proposition 8.6, we get that $\mathcal{F}' \subseteq \mathcal{F}$ and $V \in \mathcal{F}'$ if and only if $R \subseteq V$ is SL by Theorem 8.3, because $R \subseteq V$ has FIP (see the proof of Lemma 8.9(2)). Since $R \subseteq S$ has FCP, $\mathcal{F}'$ has maximal elements. Applying Lemmas 8.5 and 8.9, we get that $\mathcal{F}'$ has only one maximal element T which is the greatest $V \in [R, S]$ such that $R \subseteq V$ is SL. Equations (1), (2), (3) and (4) follow obviously because $V \subseteq T$ for any $V \in \mathcal{F}'$ and since $T \in \mathcal{F}'$. $\square$

9 Some special cases of SL extensions

In this last section, we characterize SL extensions satisfying another property at the same time. We recall that an extension $R \subseteq S$ is called *Boolean* if $[R, S]$ is a Boolean lattice, that is a distributive lattice such that each $T \in [R, S]$ has a complement T' in $[R, S]$ (such that $T \cap T' = R$ and $TT' = S$) [33].

Corollary 9.1. *Let $R \subseteq S$ be an FCP SL extension such that S is semilocal and $|V_S(MS)| = 2$ for each $M \in \text{MSupp}(S/R)$. Then $R \subseteq S$ is a Boolean extension.*

Proof. Since $R \subseteq S$ is an SL extension such that S is semilocal, Proposition 8.1 gives that $R \subseteq S$ is a seminormal infra-integral FIP extension, and so is $R_M \subseteq S_M$ for each $M \in \text{MSupp}(S/R)$. But $|V_S(MS)| = 2$ for each $M \in \text{MSupp}(S/R)$ implies that $R_M \subseteq S_M$ is minimal decomposed by [7] Lemma 5.4] and then Boolean by [33] Lemma 3.27], from which we can infer that $R \subseteq S$ is a Boolean extension by [33] Proposition 3.5]. $\square$

Remark 9.2. *The SL criteria of Theorem 8.3 (resp. Corollary 8.4) may hold even if S (resp. $S/(R : S)$) is not a semilocal ring.*

A weaker condition is gotten with the following example. Take for instance $R := \prod_{i \in \mathbb{N}} R_i$ where $R_i \cong \mathbb{Z}/2\mathbb{Z}$ for each $i \in \mathbb{N}$ and set $S := R^2$. According to [30] Proposition 1.4], $R \subseteq S$ is seminormal infra-integral but not FCP with $(R : S) = 0$, so that $S/(R : S)$ is not semilocal. But since $|U(R)| = |U(S)| = 1$, $R \subseteq S$ is SL.

Example 9.3. (1) *In Number Theory, we can find a lot of SL extensions $R \subseteq S$ that are not FCP and S is neither semilocal nor regular. Let $K := \mathbb{Q}(\sqrt{-d})$, where d is a square-free positive integer such that $d \neq 1, 3$. By [37] 10.2, D, p.169], $U(A) = \{1, -1\}$, where A is the ring of integers of K . As $U(\mathbb{Z}) = \{1, -1\}$, we get that $U(\mathbb{Z}) = U(R) = U(A)$, for any $R \in [\mathbb{Z}, A]$, so that $\mathbb{Z} \subseteq R$ and $R \subseteq A$ are SL for any $R \in [\mathbb{Z}, A]$. Of course, $\mathbb{Z} \subseteq A$ is an integral extension which has not FCP since $(\mathbb{Z} : A) = 0$ [7] Theorem 4.2] and A is neither semilocal nor regular. This also holds for a ring of integers R with integral closure A . By Dirichlet's Theorem [37] Theorem 1, page 179], these are the only cases where the ring of algebraic integers A of an algebraic number field is such that $\mathbb{Z} \subseteq A$ is SL.*

(2) *We can say more considering a particular situation of (1). Let $d := 5$. Then, $A = \mathbb{Z} + \mathbb{Z}\sqrt{-5}$ by [37] 5.4, V, p.97] and 5 is ramified in K [37] 11.2, K, p.199]. This means that $5A = M^2$, where $M \in \text{Max}(A)$. Set $P := 5A$ and $R := \mathbb{Z} + 5A$. Then, $R \in [\mathbb{Z}, A]$ with $R \subseteq A$ SL by (1). We have $P = (R : A) \in \text{Max}(R)$ because $R/P = (\mathbb{Z} + 5A)/5A \cong \mathbb{Z}/(\mathbb{Z} \cap 5A) = \mathbb{Z}/5\mathbb{Z}$ which is a field. Since $P = M^2$, it follows that M is the only maximal ideal of A lying above P . Then, A_P is a local ring. Assume that $R_P \subseteq A_P$ is SL. Then, Example 4.1(8) says that $R_P = A_P$, a contradiction with $P = (R : A) \in \text{MSupp}(A/R)$.*

This example shows that Proposition 2.9 has no converse: an extension $R \subseteq S$ may be SL with $R_M \subseteq S_M$ not SL for some $M \in \text{MSupp}(S/R)$.

Let R be a ring and F its prime subring, that is $F := \mathbb{Z}/\ker(c)$, where $c : \mathbb{Z} \rightarrow R$ is the ring morphism defined by $c(x) := x1_R$. Then, either $F = \mathbb{Z}$ or $F = \mathbb{Z}/n\mathbb{Z}$ where n is the least positive integer such that $n1_R = 0_R$.

Proposition 9.4. *Let R be a ring with F its prime subring. Then $F[U(R)] \rightarrow R$ is SL.*

Proof. Use Example 4.1(1a). $\square$

Corollary 9.5. *If R is a local ring with prime subring F , then $F[U(R)] = R$. If, in addition, $U(R)$ is a finitely generated group, R is Noetherian.*

Proof. By Proposition 9.4 and Example 4.1(8) $F[U(R)] = R$.

Now, assume that $U(R)$ is a finitely generated group. Let $\{x_1, \dots, x_n\}$ be a system of generators of $U(R)$, so that any $x \in U(R)$ is of the form $x = \prod_{i=1}^n x_i^{n_i}$, with $n_i \in \mathbb{Z}$ for each $i \in \mathbb{N}_n$. Then, $R = F[U(R)]$ is an F -algebra generated by $\{x_i, x_i^{-1} \mid i \in \mathbb{N}_n\}$, where either $F = \mathbb{Z}$ or $F = \mathbb{Z}/m\mathbb{Z}$, and so is Noetherian. $\square$

Proposition 9.6. *Let S be a ring with prime subring F .*

1. *Let Σ be a saturated multiplicatively closed subset of S and set $R := F[\Sigma]$. Then, $R_\Sigma \subseteq S_\Sigma$ is SL and so is $R \subseteq S$.*

If, in addition, S_Σ is regular, then $R_\Sigma \subseteq S_\Sigma$ is u-integral, infra-integral, seminormal, quadratic and R_Σ is regular.

2. *Assume that Σ is the set of regular elements of S .*

(a) *Then $R_\Sigma \subseteq \text{Tot}(S)$ is SL.*

(b) *If, in addition, $\text{Tot}(S)$ is regular, so is R_Σ .*

(c) *If S has few zerodivisors, then $\text{Tot}(S)$ is semilocal as R_Σ .*

Proof. (1) Let $x = a/s \in S_\Sigma$, with $a \in S$ and $s \in \Sigma$. Then, $x \in U(S_\Sigma) \Leftrightarrow$ there exists $y = b/t \in S_\Sigma$, with $b \in S$ and $t \in \Sigma$ such that $xy = 1$ (*). Now, (*) $\Leftrightarrow ab/st = 1 \Leftrightarrow$ there exists $u \in \Sigma$ such that $uab = ust \in \Sigma$. It follows that $a \in \Sigma$ and $U(S_\Sigma) = \{a/s \in S_\Sigma \mid a, s \in \Sigma\}$. Then, $U(S_\Sigma) \subseteq R_\Sigma$, with obviously $U(S_\Sigma) \subseteq U(R_\Sigma) \subseteq U(S_\Sigma)$ giving $U(R_\Sigma) = U(S_\Sigma)$. Then $R_\Sigma \subseteq S_\Sigma$ is SL, and so is $R \subseteq S$ by Proposition 2.10.

Assume, in addition, that S_Σ is regular. Then, according to Proposition 5.18, $R_\Sigma \subseteq S_\Sigma$ is u-integral, infra-integral, seminormal, quadratic and R_Σ is regular.

(2) Now, Σ is the set of regular elements of S . Then $\text{Tot}(S) = S_\Sigma$.

(a) and (b) follow from (1).

(c) If S has few zerodivisors, then $Z(S) = \bigcup_{i=1}^n P_i$ is a finite union of prime ideals of S and $\Sigma = S \setminus Z(R)$ gives that $S_\Sigma = \text{Tot}(S)$ has finitely many maximal ideals, so that $\text{Tot}(S)$ is semilocal as R_Σ since $R_\Sigma \subseteq S_\Sigma$ is integral. $\square$

In [1], D. D. Anderson and S. Chun introduced strongly inert extensions and related extensions in the following way: a ring extension $R \subseteq S$ is *strongly inert* (resp. *weakly strongly inert*) if for nonzero $a, b \in S$, then $ab \in R$ (resp. $ab \in R \setminus \{0\}$) implies $a, b \in R$.

The link between strongly inert and SL extensions has been noticed by Anderson and Chun and gives many examples of SL extensions.

Proposition 9.7. *Let $R \subseteq S$ be a strongly inert extension. The following properties hold:*

1. [1 Proposition 3.1 (2) and Theorem 3.2] $R \subseteq S$ is SL and either $R = S$ or R and S are integral domains.
2. If $R \neq S$, then 0 is the only proper ideal shared by R and S .
3. If S is J-regular, then $R = S$.

Proof. (2) Assume that $R \neq S$, so that R and S are integral domains. Let I be a proper ideal shared by R and S . We claim that $I = 0$. Otherwise, there exists some $a \in I$, $a \neq 0$. Since $R \subseteq S$ is SL and $R \neq S$, there exists some $x \in S \setminus R$ with $x \neq 0$. Then, $ax \in I \subseteq R$. It follows that ax is in R . Since $R \subseteq S$ is strongly inert, this implies $x \in R$, a contradiction. Then, 0 is the only proper ideal shared by R and S .

(3) Since $R \subseteq S$ is strongly inert, $R \subseteq S$ is SL. If, moreover, S is J-regular, then, by Theorem 5.17, $J(R) = J(S)$ and $R \subseteq S$ is integral. But, [1 Theorem 3.5 (7)] says that any element of $S \setminus R$ is transcendental over R . It follows that $R = S$. $\square$

Remark 9.8. *The strongly local property is weaker than the strongly inert property in the following way: Let $R \subseteq S$ be SL and $a, b \in S$ be such that $ab \in U(R)$. Then $ab \in U(S)$ which implies that $a, b \in U(S) = U(R)$, so that $a, b \in R$.*

But, in case R is a field, the following Corollary shows that the notions of SL extension and of weakly strongly inert extension are equivalent.

Corollary 9.9. *Let $K \subseteq S$ be an extension where K is a field. The following properties holds:*

1. $K \subseteq S$ is weakly strongly inert if and only if $K \subseteq S$ is SL.
2. If, in addition, S is an integral domain, then $K \subseteq S$ is strongly inert if and only if $K \subseteq S$ is SL. In this case, $K \subseteq S$ is algebraically closed.
3. If $K \subseteq S$ is SL, then $K \subseteq S$ is an FCP extension if and only if either $K = S$ or $K \cong \mathbb{Z}/2\mathbb{Z}$ and $S \cong K^n$ for some integer n .

Proof. Since $U(K) = K \setminus \{0\}$, we get that $K \subseteq S$ is SL if and only if $U(S) = K \setminus \{0\}$.

(1) Assume that $K \subseteq S$ is SL and let $a, b \in S \setminus \{0\}$ be such that $ab \in K \setminus \{0\}$. Then, $ab \in U(S)$, so that $a, b \in U(S) = K \setminus \{0\} \subseteq K$ and $K \subseteq S$ is weakly strongly inert. Conversely, if $K \subseteq S$ is weakly strongly inert, then $K \subseteq S$ is SL according to [1, Theorem 4.1].

(2) Assume that $K \subseteq S$ is SL and, in addition, that S is an integral domain. It follows that $K \subseteq S$ is weakly strongly inert by (1) and $Z(S) = Z(K) = \{0\}$, so that $K \subseteq S$ is strongly inert by [1, Proposition 3.1] and algebraically closed by [1, Theorem 3.5]. Conversely, if $K \subseteq S$ is strongly inert, then $K \subseteq S$ is SL according to [1, Proposition 3.1].

(3) Assume that $K \subseteq S$ is SL.

If $K = S$, then $K \subseteq S$ has FCP.

If $K \cong \mathbb{Z}/2\mathbb{Z}$ and $S \cong K^n$ for some integer n , then $K \subseteq S$ has FCP by [30, Proposition 1.4] or because S has finitely many elements.

Conversely, assume that $K \subseteq S$ has FCP. Then S is semilocal by Proposition [8.7] and Definition [8.8]. It follows from Theorem [8.3] that $K \cong \mathbb{Z}/2\mathbb{Z}$ because $\text{MSupp}(S/K) = \{0\}$ and $S \cong K^n$ for some integer n by Lemma [8.9] since $K \subseteq S$ is infra-integral, and then integral. $\square$

We say that an extension $R \subseteq S$ is *semi-inert* if for nonzero $a, b \in S$, $ab \in R$ implies either $a \in R$ or $b \in R$. Such an extension exists by [10, Proposition 3.1], for example a minimal Prüfer extension.

More generally, if $R \subseteq S$ is semi-inert and $S \subseteq T$ is strongly inert, then $R \subseteq T$ is semi-inert.

Proposition 9.10. *Let $R \subseteq S$ be a semi-inert extension. Then $R \subseteq S$ is integrally closed. If, in addition, $R \subseteq S$ is local, then $R \subseteq S$ is SL.*

Proof. Let $s \in S \setminus R$ and assume that s is integral over R . Then $s^n + \sum_{i=0}^{n-1} a_i s^i = 0$ (*) for some positive integer n and $a_i \in R$ for any $i \in \{0, \dots, n-1\}$. We may assume that n is the least integer such that (*) is satisfied. Then, $n > 1$ since $s \notin R$. It follows that (*) implies $s(s^{n-1} + \sum_{i=0}^{n-2} a_{i+1} s^i) = -a_0 \in R$. Since $s \neq 0$ because $s \in S \setminus R$ and $s^{n-1} + \sum_{i=0}^{n-2} a_{i+1} s^i \neq 0$ by the choice of n , it follows that either $s \in R$ or $s^{n-1} + \sum_{i=0}^{n-2} a_{i+1} s^i \in R$ because $R \subseteq S$ is semi-inert. In both cases, we get a contradiction, giving that s is not integral over R . Then, $R \subseteq S$ is integrally closed.

Obviously, $U(R) \subseteq U(S)$. Assume, in addition, that $R \subseteq S$ is local. Then, $U(S) \cap R = U(R)$. Let $s \in U(S)$. There exists $t \in U(S)$ such that $st = 1 \in R$ (**), that is $s = t^{-1}$. Since $R \subseteq S$ is semi-inert, it follows that either s or $t \in R$. Assume first that $s \in R$. Then, $s \in U(S) \cap R = U(R)$. Assume now that $s \notin R$. We get that $t \in R \cap U(S) = U(R)$. Then, t has an inverse in R , which is unique and is also its inverse in S , so that $s \in U(R)$, a contradiction since $s \notin R$. Hence, $U(S) = U(R)$ and $R \subseteq S$ is SL. $\square$

We can also build SL extensions with cyclotomic extensions.

Proposition 9.11. *Let p be a prime integer different from 2 and such that 2 is a primitive root in $\mathbb{Z}/p\mathbb{Z}$.*

Set $K := \mathbb{Z}/2\mathbb{Z}$, $L := K[X]/(X^{p-1} + \dots + 1)$, $R := K[X]/(X^p - 1)$ and $S := K[X]/(X^{p+1} - X)$. The following properties hold:

1. $X^{p-1} + \dots + 1$ is irreducible over K .

2. There exists an injective ring morphism $f : R \rightarrow S$.

3. f is SL.

Proof. (1) comes from [20, Theorem 2.47] because 2 is a primitive root in $\mathbb{Z}/p\mathbb{Z}$.

(2) Since $X^p - 1 = (X - 1)(X^{p-1} + \dots + 1)$, the Chinese Remainder Theorem shows that $R \cong [K[X]/(X - 1)] \times [K[X]/(X^{p-1} + \dots + 1)] \cong K \times L$ with $K \subseteq L$ a field extension of degree $p - 1$. Similarly, $S \cong [K[X]/(X)] \times [K[X]/(X - 1)] \times [K[X]/(X^{p-1} + \dots + 1)] \cong K^2 \times L$. There is an injective ring morphism $g : K \times L \rightarrow K^2 \times L$, given by $(x, y) \mapsto (x, x, y)$. Then, the following commutative diagram

$$\begin{array}{ccc} K \times L & \xrightarrow{g} & K^2 \times L \\ \uparrow & & \downarrow \\ R & \xrightarrow{f} & S \end{array}$$

implies an injective ring morphism $f : R \rightarrow S$ gotten by

$$f : R \rightarrow K \times L \rightarrow K^2 \times L \rightarrow S$$

In fact, g is defined as $g := (g_1, g_2)$ where $g_1 : K \rightarrow K^2$ is the diagonal map and g_2 is the identity on L . From now, we may identify R with $K \times L$, S with $K^2 \times L$ and f with g .

Let x be the class of X in L , so that $L = K[x]$. Setting $y := (0, x) \in R$, we get that $y^p = (0, 1_L)$ and any element of R is of the form (a, b) , where $a \in K = \{0, 1_K\}$ and $b = \sum_{i=0}^{p-2} \alpha_i x^i \in L$ with $\alpha_i \in K$ for each i . Then, $(a, b) = (a, 0) + (0, \sum_{i=0}^{p-2} \alpha_i x^i) = (a, a) - (0, a) + (0, \sum_{i=0}^{p-2} \alpha_i x^i)$ can be written as $a \cdot 1_R + \sum_{i=0}^{p-2} \beta_i y^i$, with a and $\beta_i \in K$ for each i . It follows that $R = K[y]$.

Setting $z := (0, 0, x)$, we get that $z = f(y)$, so that we have the injective ring morphism $f : R \rightarrow S$ defined by $f(y) = z$. We may remark that $S \neq K[z]$ because $(0, 1, 0) \in S \setminus K[z]$.

(3) Since $|U(K)| = 1$, we get that $|U(R)| = |U(K \times L)| = |U(L)| = |U(K^2 \times L)| = |U(S)|$. It follows that $f(U(R)) = U(S)$ since $f(U(R)) \subseteq U(S)$ and f is SL. $\square$

In the previous proposition the injective ring morphism $f : R \rightarrow S$ we built may not be unique as it is shown in the following example:

Example 9.12. Set $K := \mathbb{Z}/2\mathbb{Z}$, $R := K[X]/(X^3 - 1)$ and $S := K[X]/(X^4 - X)$. We will build two injective ring morphisms $f : R \rightarrow S$ which are SL.

Let y be the class of X in R and t the class of X in S , so that $R = K[y]$ and $S = K[t]$. We may use the proof of Proposition 9.11 with $p = 3$ since 2 is a primitive root in $\mathbb{Z}/3\mathbb{Z}$. Then, we get that $|U(R)| = 3$ giving $U(R) = \{1, y, y^2\}$. Since there exists an injective ring morphism $f : R \rightarrow S$ which is SL, we also have $|U(S)| = 3$. As f is also a linear morphism over the K -vector space R , we may define f by the image of the basis $\{1, y, y^2\}$ of R over K . An easy calculation of $(a + bt + ct^2 + dt^3)^3 = 1$, with $a, b, c, d \in K$ shows that $U(S) = \{1, t^3 + t + 1, t^3 + t^2 + 1\}$. Since we must have $f(1) = 1$ and $f(y) \neq f(y^2)$ both in $U(S)$, we get that $f(y)$ and $f(y^2)$ are the two different elements of $\{t^3 + t + 1, t^3 + t^2 + 1\}$. Whatever the value we give to y , we get that $f(y^2) = f(y)^2$.

So, such an f is a ring morphism, which is obviously injective. At last, $f(U(R)) = U(S)$ shows that $f : R \rightarrow S$ is SL. There are two such morphisms: f_1 and f_2 defined by $f_1(y) = t^3 + t + 1$ and $f_2(y) = t^3 + t^2 + 1$.

Proposition 9.13. Let R be a ring. Set $K := \mathbb{Z}/2\mathbb{Z}$, $T := K^n \times R$ and $S = K^m \times R$, where $n < m$ are two positive integers. There is an injective ring morphism $f : T \rightarrow S$ given by $f(x, y) := (\varphi(x), y)$ where $\varphi : K^n \rightarrow K^m$ is an injective ring morphism. Then, f is SL.

Proof. Since $n < m$, we can build an injective ring morphism $\varphi : K^n \rightarrow K^m$ given, for instance, by $\varphi(x_1, \dots, x_n) = (x_1, \dots, x_n, x_n, \dots, x_n)$ where the $m - n$ last terms are all equal to x_n . Then, the map $f : T \rightarrow S$ given by $f(x, y) := (\varphi(x), y)$ is an injective ring morphism. Since $K = \mathbb{Z}/2\mathbb{Z}$, it follows that $|U(K)| = 1 = |U(K^n)| = |U(K^m)|$. But, $|U(T)| = |U(K^n)||U(R)|$ and $|U(S)| = |U(K^m)||U(R)|$, giving $|U(T)| = |U(S)| = |U(R)|$, so that f is SL. $\square$

References

- [1] D. D. Anderson and S. Chun, Inert type extensions and related factorization properties, *J. Algebra Appl.*, **21**, (2022), 27 pages.
- [2] D. D. Anderson and M. Winders, Idealization of modules, *Journal of Commutative Algebra*, **1**, (2009), 3–56.
- [3] D. F. Anderson and A. Badawi, Von Neumann regular and related elements in Commutative Rings, *Algebra Colloquium*, **19** (Spec 1), (2012), 1017–1040.
- [4] D. F. Anderson and D. E. Dobbs, Pairs of rings with the same prime ideals, *Can. J. Math.*, **32** (2) (1980), 362–384.
- [5] N. Bourbaki, *Algèbre Commutative*, Chs. 1–2, Hermann, Paris, 1961.
- [6] P.M. Cohn, Rings of zero divisors, *Proc. Amer. Math. Soc.*, **9** (6) (1958), 909–914.
- [7] D. E. Dobbs, G. Picavet and M. Picavet-L’Hermitte, Characterizing the ring extensions that satisfy FIP or FCP, *J. Algebra*, **371** (2012), 391–429.
- [8] D. E. Dobbs, G. Picavet and M. Picavet-L’Hermitte, Transfer results for the FIP and FCP properties of ring extensions, *Comm. Algebra*, **43** (2015), 1279–1316.
- [9] A. M. Doering and Y. Lequain, Extensions of semi-local rings sharing the same group of units, *J. Pure Appl. Algebra*, **173** (2002), 281–291.
- [10] D. Ferrand and J.-P. Olivier, Homomorphismes minimaux d’anneaux, *J. Algebra*, **16** (1970), 461–471.
- [11] M. S. Gilbert, Extensions of commutative rings with linearly ordered intermediate rings, Ph. D. dissertation, University of Tennessee, Knoxville, (1996).
- [12] R. Gilmer and W. Heinzer, On the number of generators of an invertible ideal, *J. Algebra*, **14** (1970), 139–151.
- [13] A. Grothendieck and J. Dieudonné, *Eléments de Géométrie Algébrique I*, Springer Verlag, Berlin, 1971.
- [14] R. M. Hamsher, Commutative rings over which every module has a maximal submodule, *Proc. Amer. Math. Soc.*, **9** (18) (1967), 1133–1137.
- [15] E. G. Houston, Chains of primes in $R < X >$, *Michigan Math. J.*, **24** (1977), 353–364.
- [16] J. A. Huckaba and I. J. Papick, A note on a class of extensions, *Rend. Circ. Mat. Palermo*, **Serie II, Tomo XXXVIII**, (1989), 430–436.
- [17] I. Kaplansky, *Commutative Rings*, rev. ed., Univ. Chicago Press, Chicago, 1974.
- [18] M. Knebusch and D. Zhang, *Manis Valuations and Prüfer Extensions I*, Springer, Berlin, 2002.
- [19] D. Lazard, Autour de la platitude, *Bull. Soc. Math. France*, **97**, (1969), 81–128.
- [20] R. Lidl and H. Niederreiter, *Finite Fields, Encyclopedia of Mathematics and its Applications*, **20**, Cambridge University Press, Cambridge, (1997).

- [21] B. R. McDonald and W. C. Waterhouse, Projective modules over rings with many units, *Proc. Amer. Math. Soc.*, **83** (1981), 455–458.
- [22] K. Morita, Flat modules, Injective modules and quotient rings, *Math. Z.*, **120** (1971), 25–40.
- [23] J.P. Olivier, Morphismes immergeants de Ann. U.E.R. de Mathématiques, Secrétariat des Mathématiques, Université des Sciences et Techniques du Languedoc, Publication No. 106, Montpellier, (1971), 15 pp.
- [24] J.P. Olivier, Descente de quelques propriétés élémentaires par morphismes purs, *An Acad. Brasil Ci.*, **45**, (1973), 17–33.
- [25] J.P. Olivier, L'anneau absolument plat universel, les épimorphismes et les parties constructibles, *Boletín de la Sociedad Matemática Mexicana*, **23** No 2, (1978), 68–74.
- [26] G. Picavet, Factorisations de morphismes d'anneaux commutatifs, *Ann. Sci. Univ. Clermont-Ferrand II Math.* No. 24 (1987), 33–59.
- [27] G. Picavet, Anodality, *Comm. Algebra*, **26** (1998), 345–393.
- [28] G. Picavet and M. Picavet-L'Hermitte, Anneaux t-clos, *Comm. Algebra*, **23** (1995), 2643–2677.
- [29] G. Picavet and M. Picavet-L'Hermitte, T-Closedness, pp. 369–386, in: *Non-Noetherian Commutative Ring Theory*, *Math. Appl.* 520, Kluwer, Dordrecht, 2000.
- [30] G. Picavet and M. Picavet-L'Hermitte, FIP and FCP products of ring morphisms, *Palestine J. of Maths*, **5** (Special Issue) (2016), 63–80.
- [31] G. Picavet and M. Picavet-L'Hermitte, Quasi-Prüfer extensions of rings, pp. 307–336, in: *Rings, Polynomials and Modules*, Springer, 2017.
- [32] G. Picavet and M. Picavet-L'Hermitte, Rings extensions of length two, *J. Algebra Appl.*, **18** (2019 no 8), 1950174, 34pp..
- [33] G. Picavet and M. Picavet-L'Hermitte, Boolean FIP ring extensions, *Comm. Algebra*, **48** (2020), 1821–1852.
- [34] G. Picavet and M. Picavet-L'Hermitte, Splitting ring extensions, *Beitr. Algebra Geom.*, **64** (2023), 627–668.
- [35] G. Picavet and M. Picavet-L'Hermitte, Closures and co-closures attached to FCP ring extensions, *Palestine J. of Maths*, **11** (2022), 33–67.
- [36] G. Picavet and M. Picavet-L'Hermitte, Flat epimorphisms and Nagata rings, to appear in *Bull. Belg. Math. Soc. Simon Stevin*.
- [37] P. Ribenboim, *Classical Theory of Algebraic Numbers*, Springer, Berlin, 1972.
- [38] L. G. Roberts and B. Singh, Subintegrality, invertible modules and the Picard group, *Compositio Mathematica*, **85** (1993), 249–279.
- [39] B. Stenström, *Rings and modules of quotients*, Lecture Notes in Mathematics, 237, Springer, New York, 1971.
- [40] R. G. Swan, On seminormality, *J. Algebra*, **67** (1980), 210–229.
- [41] A. Tarizadeh, Zariski compactness of minimal spectrum and flat compactness of maximal spectrum, *J. Algebra Appl.*, **18** (2019), 1950202, 8 pp..



ISSN: 2820-7114

Moroccan Journal of Algebra and Geometry with Applications

Supported by Sidi Mohamed Ben Abdellah University, Fez, Morocco

Volume 4, Issue 2 (2025), pp 239-247

Title :

On rings over which every flat module is finitely projective

Author(s):

Abdelhaq El Khalfi, Oussama Aymane Es-Safi & Moutu Abdou Salam Moutui

On rings over which every flat module is finitely projective

Abdelhaq El Khalfi¹, Oussama Aymane Es-Safi² and Moutu Abdou Salam Moutui³

¹ Fundamental and Applied Mathematics Laboratory

Faculty of Sciences Ain Chock, Hassan II University of Casablanca, Morocco.

e-mail: abdelhaqelkhalfi@gmail.com

² Laboratory of Modeling and Mathematical Structures

Faculty of Science and Technology, Sidi Mohamed ben Abdellah University of Fez, Morocco.

e-mail: essafi.oussamaaymane@gmail.com

³ Department of Mathematics and Statistics St. Francis Xavier University Antigonish,

Nova Scotia, Canada B2G 2W5.

e-mail: amoutu@stfx.ca

Communicated by Najib Mahdou

(Received 14 August 2024, Revised 20 March 2025, Accepted 28 March 2025)

Abstract. The main goal of this paper is to investigate the class of rings for which every flat module is finitely projective (called *FMF*-ring, for short). We examine the stability of this property in several distinguished contexts of commutative ring extensions such as direct product, polynomial ring, power series ring, localization, homomorphic image, trivial ring extensions and amalgamation rings. Our results enrich the current literature with various new and original families of non-coherent, non-perfect, non-arithmetical and non-Noetherian rings that satisfying this property.

Key Words: FMF-ring, direct product, localization, homomorphic image, amalgamation of rings, trivial ring extension.

2020 MSC: Primary 13D05, 13D02.

Dedicated to the memory of Oussama Aymane Es-Safi,
our esteemed co-author, who has recently passed away

1 Introduction

All rings considered in this paper are assumed to be commutative with identity elements and all modules are unitary. For a ring R , we denote by $Q(R)$, the total ring of quotients of R , that is, the localization of R by the set of all its regular elements, $Z(R)$ denotes the set of all zero-divisors of R , and $\text{gldim}(R)$ (resp. $\text{wdim}(R)$) denotes the classical global (resp. weak) dimension of R . If R is an integral domain, we will usually denote its quotient field by $\text{qf}(R)$.

Recall that an R -module M is called finitely projective if, for any finitely generated submodule N , the inclusion map $N \rightarrow M$ factors through a free module F . The notion of finitely projective module is due to Jones [25]. An interesting study of finitely projective modules is also done by Azumaya in [2]. Note that Jones [25] uses the term f -projective, Mao [31] and Simson [39] use the term $\aleph_{-1}$ -projective. It is well known that every projective module is finitely projective and any finitely generated finitely projective module is projective and also every finitely projective module is flat. The following diagram of implications summarizes the relations between them:

$$M \text{ is projective} \implies M \text{ is finitely projective} \implies M \text{ is flat.}$$

But these are not generally reversible, for example the rationals are finitely projective as $\mathbb{Z}$ -module, though not projective. Let F be any field, $R := \prod_{n \in \mathbb{N}} F$ and $K := \bigoplus_{n \in \mathbb{N}} F$. R/K is R -flat since R is regular. But R/K is not finitely projective (see [25, page 1611]).

Let A and B be two rings, J an ideal of B and let $f : A \rightarrow B$ be a ring homomorphism. In this setting, we can consider the following subring of $A \times B$: called the amalgamation of A and B along J with respect to f is the subring of $A \times B$ defined by:

$$A \bowtie^f J := \{(a, f(a) + j) ; a \in A, j \in J\}.$$

This construction is a generalization of the amalgamated duplication of a ring along an ideal (introduced and studied by D'Anna, Finacchiaro, and Fontana in [12, 13, 14, 15, 16, 18]). Amalgamation rings are a class of rings quite recently introduced and widely studied; the motivation is that this construction is a sort of generalization of many classical constructions and it allows to build rings with prescribed properties, so being a good source of examples.

Let A be a ring and E an A -module. The trivial ring extension of A by E (also called the idealization of E over A) is the ring $R := A \ltimes E$ whose underlying group is $A \times E$ with multiplication given by $(a, e)(a', e') := (aa', ae' + a'e)$. For the reader's convenience, recall that if I is an ideal of A and E' is a submodule of E such that $IE \subseteq E'$, then $J := I \ltimes E'$ is an ideal of R . Recall that, prime (resp., maximal) ideals of R have the form $p \ltimes E$, where p is a prime (resp., maximal) ideal of A [1, Theorem 3.2]. Suitable background on commutative trivial ring extensions is [1, 17, 22, 26, 27, 28, 29, 30].

The aim of this paper is to investigate the class of rings for which every flat module is finitely projective (called *FMF-ring*, for short). We examine the transfer of this property in several distinguished contexts of commutative ring extensions such as direct product, localization, homomorphic image, trivial ring extensions and amalgamation rings. Our results enrich the current literature with new and original families of non-coherent, non-perfect, non-arithmetical and non-Noetherian rings satisfying this property. Examples of *FMF-rings* are perfect rings, Noetherian rings and Prüfer domains (see for instance [2, 6, 8, 25, 38], for more details).

2 Main Results

Recall that a ring R is called semihereditary if every finitely generated ideal of R is projective and is said to have weak global dimension ≤ 1 (denoted by $\text{wdim}(R) \leq 1$) if every finitely generated ideal of R is flat. It is well known that a semi-hereditary ring R have $\text{wdim}(R) \leq 1$. In the domain context, all these conditions coincide with the definition of a Prüfer domain. Glaz [21, Example 3.2.1] provides example of non-semihereditary ring of $\text{wdim} \leq 1$. See for instance [3, 4, 21].

We start with examples of non-*FMF-rings*.

Proposition 2.1. 1. Any non-semihereditary ring of $\text{wdim} \leq 1$ is a non-*FMF-ring*.

2. A non-Noetherian von Neumann regular ring is a non-*FMF-ring*.

Proof. (1) Let R be a non-semihereditary ring with $\text{wdim} R \leq 1$. Then there exists a finitely generated ideal I of R which is not projective. So, I is not finitely projective. On the other hand, I is flat since $\text{wdim} R \leq 1$. Hence, R is a non-*FMF-ring*.

(2) Let R be a non-Noetherian von Neumann regular ring and I be a non finitely generated ideal of R . Assume that R is a *FMF-ring*. Since R is a von Neumann regular ring, we get R/I is a flat

R -module which is finitely generated. Hence, R/I is a projective R -module which implies that I is finitely generated, a contradiction. Finally, R is a non- FMF -ring. $\square$

Remark 2.2. In [2 Proposition 18], Azumaya proved that a Prüfer domain is a FMF -ring. However, [2 Proposition 18] can not be extended beyond the context of integral domains, since a non-semihereditary ring of $\text{wdim} \leq 1$ is a Prüfer ring which is not a FMF -ring by Proposition 2.1(1).

Recall that it is well known that a ring is semisimple if and only if it is von Neumann regular Noetherian. In the next proposition, we give a similar characterization of semisimple rings by replacing the concept “Noetherian” with “ FMF -ring”.

Proposition 2.3. *A ring R is von Neumann regular FMF -ring if and only if R is semisimple.*

Proof. Assume that R is von Neumann regular FMF -ring and let I be an ideal of R . Clearly, R/I is a finitely projective module of R and so R/I is projective since it is finitely generated. Then $\text{gldim}(R) = 0$. Therefore, R is semisimple. The converse is straightforward via the well known fact that a commutative semisimple ring is Von Neumann regular Noetherian and so is Von Neumann regular FMF -ring. $\square$

The next proposition establishes some facts of FMF -rings. Recall that a ring R is called S -ring if every finitely generated flat module is projective (see [38]).

Proposition 2.4. 1. *Let R be a ring such that every finitely generated submodule of a flat R -module is finitely presented. Then R is an FMF -ring.*

2. *Any FMF -ring is an S -ring.*

3. *Assume that R is an FMF -ring. Then R is a perfect ring if and only if every finitely projective R -module is projective.*

Proof. (1) Let M be a flat R -module and N be a finitely generated submodule of M . From assumption, N is finitely presented. Hence, by [7 Theorem 1], we have the desired result.

(2) Assume that R is an FMF -ring and let M be a finitely generated flat R -module. Then, M is finitely projective and so M is projective since it is finitely generated.

(3) Trivial. $\square$

The FMF -property descends into an injective (respectively finitely generated flat, faithfully flat) ring homomorphism.

Proposition 2.5. *Let $f: R \rightarrow S$ be a ring homomorphism.*

1. *Assume that f is injective. Then if S is an FMF -ring, then so is R .*

2. *Assume that f is flat epimorphism. If R is an FMF -ring, then so is S .*

3. *Assume that S is finitely generated flat R -module. Then if R is an FMF -ring, then so is S .*

4. *Assume that S is a finitely generated faithfully flat R -module. Then R is an FMF -ring if and only if so is S .*

Before proving this proposition, we establish the following Lemmas.

Lemma 2.6. [8 Lemma 5] *Let R be a subring of a ring S and let M be a flat left R -module. Assume that $S \otimes_R M$ is finitely projective over S . Then M is finitely projective.*

Lemma 2.7. Let $R \rightarrow S$ be a ring homomorphism making S a finitely generated faithfully flat R -module. If an S -module M is finitely projective as an R -module, then M is a finitely projective as an S -module.

Proof. Let N be a finitely generated S -submodule of M . Then N is a finitely generated R -submodule of M since S is finitely generated R -module. So, there exist a free R -module F , a morphism $\varphi : N \rightarrow F$ and a morphism $\psi : F \rightarrow M$ such that $\psi \circ \varphi := id_N$. Consider the following morphisms: g, φ_1 and ψ_1 defined by: $g : F \rightarrow F \otimes_R S$, $\varphi_1 : N \rightarrow F \otimes_R S$, where $\varphi_1 := g \circ \varphi$ and $\psi_1 : F \otimes_R S \rightarrow M$, where $\psi := \psi_1 \circ g$. Then $\psi_1 \circ \varphi_1 = id_N$. Therefore, M is finitely projective S -module, which completes the proof. $\square$

Proof of Proposition 2.5

(1) Assume that S is a FMF-ring and let M be a flat R -module. Then $M \otimes_R S$ is a flat S -module and so $M \otimes_R S$ is a finitely projective S -module (since S is an FMF-ring). Hence, M is a finitely projective R -module by Lemma 2.6. It follows that R is an FMF-ring.

(2) Assume that R is an FMF-ring and let M be a flat S -module. Then M is a flat R -module (as S is R -flat) and so M is a finitely projective R -module (since R is an FMF-ring). Hence, M is a finitely projective S -module by [5] Proposition 3.2. It follows that S is an FMF-ring.

(3) Assume that R is an FMF-ring and let M be a flat S -module. Then M is a flat R -module (since S is R -flat) and so M is a finitely projective R -module (since R is an FMF-ring). Hence, M is a finitely projective S -module by Lemma 2.7. It follows that S is an FMF-ring.

(4) f is injective since S is faithfully flat R -module. We do a similar proof as in assertion (2) above. $\square$

Now, we study the transfer of FMF property to polynomial and power series rings.

Corollary 2.8. Let R be a ring and let X be an indeterminate over R . The following statements are equivalent:

1. R is an FMF-ring.
2. $R[X]$ is an FMF-ring.
3. $R[[X]]$ is an FMF-ring.

Proof. This follows from assertion (4) of Proposition 2.5, as $R[X]$ (resp. $R[[X]]$) is a faithfully flat R -module. $\square$

The next result establishes the transfer of the FMF-property to localization.

Theorem 2.9. Let R be a commutative ring and let S be a multiplicative subset of R . Then:

1. If R is an FMF-ring, then so is $S^{-1}(R)$.
2. If S contains no zero-divisors then, $S^{-1}(R)$ is an FMF-ring if and only if so is R . (In particular $Q(R)$ is an FMF-ring if and only if so is R).

Before proving this theorem, we need the following Lemma.

Lemma 2.10. [8] Proposition 6.] Let R be a ring and let S be a multiplicative subset of R . Then:

1. For each finitely projective R -module M , $S^{-1}M$ is finitely projective over $S^{-1}R$.
2. Let M be a finitely projective $S^{-1}R$ -module. If S contains no zero-divisors, then M is finitely projective over R .

Proof of Theorem 2.9.

(1) We assume that R is an FMF -ring. Let M be a flat $S^{-1}(R)$ -module. Then M is flat over R , so it is finitely projective over R , since R is an FMF -ring. It follows that $M = S^{-1}M$ is finitely projective over $S^{-1}R$ by Lemma 2.10. We get that $S^{-1}R$ is an FMF -ring.

(2) Notice that if S contains no zero-divisors, then R is a subring of $S^{-1}R$. We conclude by Proposition 2.5 and (1). $\square$

Remark 2.11. Notice that in Theorem 2.9(2), the assumption that S contains no zero-divisors is essential. For example, let R be a non-Noetherian von Neumann regular ring. Then R_M is an FMF -ring for a maximal ideal M of R , since R_M is a field. But, by Proposition 2.1(2) R is a non- FMF -ring. Furthermore, $S = R \setminus M$ contains zero-divisors elements since R is not local and $M \subsetneq Z(R)$.

Corollary 2.12. *Every domain is an FMF -ring.*

The following proposition studies the FMF -ring property into a particular homomorphic image.

Proposition 2.13. *Let R be a ring and let I be a pure ideal of R . If R is an FMF -ring, then so is R/I .*

Proof. R/I is a finitely generated flat R -module since I is a pure ideal of R . Then R/I is an FMF -ring by Proposition 2.5. $\square$

The converse of Proposition 2.13 is not true in general, as shown by the following example.

Example 2.14. Let R be any non- FMF -ring and let p be a prime ideal of R . Then R/p is always an FMF -ring.

Next, we study the transfer of the FMF -property to direct products.

Theorem 2.15. Let $(R_i)_{i=1,\dots,n}$ be a family of commutative rings. Then $R = \prod_{i=1}^n R_i$ is an FMF -ring if and only if so is R_i for each $i = 1, \dots, n$.

Proof. We do as in the proof of [9] Theorem 2.10]. $\square$

As an application of Proposition 2.5 we have the following result that examines the transfer of FMF -property between a ring A and the trivial ring extension of A by E , where E be an A -module.

Proposition 2.16. *Let A be a ring, let E be an A -module and let $R := A \ltimes E$ be a trivial ring extension of A by E . Then:*

1. *If R is an FMF -ring, then so is A .*
2. *Assume that E is a flat A -module. Then R is an FMF -ring if and only if so is A .*

Proof. (1) By Proposition 2.5(1) since A is a subring of R .

(2) Notice that, if E is a flat A -module. Then $R := A \ltimes E$ is faithfully flat over A . Hence, Proposition 2.5(3) completes the proof of (2). $\square$

Corollary 2.17. *Let A be a ring. Then $A \ltimes A$ is an FMF -ring if and only if so is A .*

The aforementioned result enriches the current literature with new examples of FMF -rings with zero-divisors which are neither coherent nor arithmetical.

Example 2.18. Let A be a domain which is not Prüfer, $K =: qf(A)$, and let $R := A \rtimes K$ be the trivial ring extension of A by K . Then:

1. R is an FMF-ring by Proposition 2.16(2).
2. R is not coherent by [26, Theorem 2.8(1)].
3. R is not an arithmetical ring by [3, Corollary 2.4.].

Example 2.19. Let K be a field and E be a K -vector space with $\dim_K(E) \geq 2$. Then $R = K \rtimes E$ is a non-arithmetical FMF-ring by Proposition 2.16(2) and [3, Theorem 3.1].

We combine Theorem 2.15 with Proposition 2.5 to get the transfer of the FMF-property to the amalgamation $A \rtimes^f J$.

Proposition 2.20. Let A and B be two rings, $f : A \rightarrow B$ be a ring homomorphism and let J be an ideal of B . Then the following assertions hold:

1. Assume that $f^{-1}(J)$ is a pure ideal of A . Then the following assertions are equivalent:
 - (a) $A \rtimes^f J$ is an FMF-ring.
 - (b) $A \times f(A) + J$ is an FMF-ring.
 - (c) A and $f(A) + J$ are FMF-rings.
2. Assume that J and $f^{-1}(J)$ are regular ideals of B and A , respectively. Then $A \rtimes^f J$ is an FMF-ring if and only if so are A and B .

Proof. (a) $\Rightarrow$ (c) Assume that $A \rtimes^f J$ is an FMF-ring. By Proposition 2.5(1), it follows that A is an FMF-ring. Next, by [15, Proposition 5.1(3)], $f(A) + J \simeq \frac{A \rtimes^f J}{f^{-1}(J) \times \{0\}}$. Using the fact that $f^{-1}(J)$ is a pure ideal of A , it follows that $f^{-1}(J) \times \{0\}$ is a pure ideal of $A \rtimes^f J$. By Proposition 2.13, $f(A) + J$ is an FMF-ring.

(c) $\Leftrightarrow$ (b) This follows from Theorem 2.15.

(b) $\Rightarrow$ (a) Assume that $A \times f(A) + J$ is an FMF-ring. Since $A \rtimes^f J$ is a subring of $A \times (f(A) + J)$. Then by Proposition 2.5(1), it follows that $A \rtimes^f J$ is an FMF-ring.

(2) By [16, Proposition 3.1], we have $Q(A \rtimes^f J) := Q(A) \times Q(B)$. Then $A \rtimes^f J$ is an FMF-ring if and only if $Q(A \rtimes^f J)$ is an FMF-ring if and only if so are $Q(A)$ and $Q(B)$ if and only if so are A and B , by Theorem 2.15 and Theorem 2.9. $\square$

Let I be a proper ideal of A . The (amalgamated) duplication of A along I is a special amalgamation given by

$$A \bowtie I := A \rtimes^{id_A} I = \{(a, a + i) \mid a \in A, i \in I\}.$$

The following corollaries are consequences of Theorem 2.20 on the transfer of FMF-ring property to duplications.

Corollary 2.21. Let A be a ring and I be an ideal of A . Then the following assertions hold:

1. Assume that I is a pure ideal of A . Then $A \bowtie I$ is an FMF-ring if and only if so is A .
2. Assume that I is a regular ideal of A . Then $A \bowtie I$ is an FMF-ring if and only if so is A .

Corollary 2.22. Let A and B be two integral domains, and let J be an ideal of B . Then $A \rtimes^f J$ is an FMF-ring.

In particular, if I is a nonzero ideal of an integral domain A , then $R := A \bowtie I$ is an FMF-ring.

Corollary 2.22 allows us to construct a new original class of *FMF*-rings which are not perfect.

Example 2.23. Let R be an integral domain which is not a field and I be an ideal of R . Then:

1. $R \bowtie I$ is an *FMF*-ring by Corollary 2.22
2. $R \bowtie I$ is not perfect by [10, Theorem 2.6].

Now, we provide a new example of an *FMF*-ring which is not arithmetical.

Example 2.24. Let R be a domain which is not a Prüfer domain and I be a nonzero ideal of R . Then:

1. $R \bowtie I$ is an *FMF*-ring by Corollary 2.22
2. $R \bowtie I$ is not arithmetical by [11, Corollary 3.8].

Now, we show how one may use Theorem 2.20 to construct new examples of *FMF*-rings which are not Noetherian.

Example 2.25. Let $A := \mathbb{Z}_6$ be an *FMF*-ring, $K := \mathbb{Z}_6/3\mathbb{Z}_6$, $E := K^\infty$ be a K -vector space and $B := A \ltimes E$ be the trivial ring extension of A by E . Consider the injective ring homomorphism $f : A \hookrightarrow B$ defined by $f(a) = (a, 0)$. Let $J := 3\mathbb{Z}_6 \ltimes E$ be an ideal of B . Clearly $f^{-1}(J) = 3\mathbb{Z}_6$. Then:

1. $A \bowtie^f J$ is an *FMF*-ring.
2. $A \bowtie^f J$ is not Noetherian.

Proof. (1) Since $f^{-1}(J) = (3)$ is an idempotent ideal of A , then $f^{-1}(J)$ is a pure ideal of A . By Theorem 2.20(1), $A \bowtie^f J$ is an *FMF*-ring.

(2) We claim that $A \bowtie^f J$ is not Noetherian. Indeed, $f(A) + J = B$ is not Noetherian since E is not finitely generated. Therefore, by [15, Proposition 5.6], $A \bowtie^f J$ is not Noetherian. $\square$

Example 2.26. Let A be an integral domain with quotient field K , E be nonzero K -vector space such that $\dim_K(E) \geq 2$ and $B := A \ltimes E$ be the trivial ring extension of A by E . Consider the ring injective homomorphism $f : A \hookrightarrow B$ defined by $f(a) = (a, 0)$ and let $J := I \ltimes E$ be a regular ideal of B with I a nonzero regular ideal of A . Then:

1. $A \bowtie^f J$ is an *FMF*-ring.
2. $A \bowtie^f J$ is not Noetherian.

Proof. (1) Since A is an integral domain, then A is an *FMF*-ring and by Theorem 2.16(2), it follows that $f(A) + J = A \ltimes 0 + I \ltimes E = A \ltimes E = B$ is an *FMF*-ring. Using the fact that $f^{-1}(J)$ (resp., J) is a regular ideal of A (resp., of B), by Theorem 2.20(2), it follows that $A \bowtie^f J$ is an *FMF*-ring.

(2) Using similar arguments as [26, Theorem 3.1(1)], we show that $A \ltimes E$ is not coherent. Indeed, let $0 \neq f \in E$ and $L = (A \ltimes E)(0, f)$. Then one can easily check that the principal ideal L is not finitely presented; and therefore $A \ltimes E$ is not coherent and so $A \ltimes E$ is not Noetherian. Moreover $f(A) + J = (A \ltimes 0) + (I \ltimes E) = ((A + I) \ltimes E) = A \ltimes E$ is not Noetherian. Hence, by [15, Proposition 5.6], $A \bowtie^f J$ is not Noetherian since $f(A) + J$ is not Noetherian. $\square$

References

- [1] D. D. Anderson and M. Winders, *Idealization of a module*, J. Commut. Algebra, 1(1) (2009) 3-56.
- [2] G. Azumaya, *Finite splitness and finite projectivity*, J. Algebra, 106 (1987) 114-134.
- [3] C. Bakkari, S. Kabbaj and N. Mahdou, *Trivial extensions defined by Prüfer conditions*, J. Pure and Appl. Algebra 214 (2010) 53-60.
- [4] S. Bazzoni and S. Glaz, *Gaussian properties of total rings of quotients*, J. Algebra 310 (2007) 180-193.
- [5] M. Behboodi, F. Couchot and S. H. Shojaei, Σ -semi-compact rings and modules*, J. Algebra Appl., Vol. 13, No. 8 (2014) 1450069 (19 pages).
- [6] S. Bouchiba, M. El-Arabi and Y. Najem, *On rings whose finitely generated flat submodules of free modules are finitely presented*, Moroccan J. Algebra Geom. Appl., 1(1) (2022), 122-131.
- [7] N. Bourbaki, *Algèbre commutative, Chapitre 10*, Masson, Paris, 1989.
- [8] F. Couchot, *Flat modules over valuation rings*, J. Pure and Appl. Algebra 211 (2007) 235-247.
- [9] F. Cheniour and N. Mahdou, *When every flat ideal is finitely projective*, Arab J Math (2013) 2:255-261.
- [10] M. Chhiti and N. Mahdou, *Some homological properties of an amalgamated duplication of a ring along an ideal*, Bull.Iranian. Math. Soc, Vol. 38 No. 2 (2012), pp 507-515.
- [11] M. Chhiti, M. Jarrar, S. Kabbaj and N. Mahdou, *Prüfer conditions in an amalgamated duplication of a ring along an ideal*, Comm. Algebra, 43 (2015) 249-261.
- [12] M. D'Anna, *A construction of Gorenstein rings*, J. Algebra 306 (2006) 507-519.
- [13] M. D'Anna and M. Fontana, *An amalgamated duplication of a ring along an ideal: the basic properties*, J. Algebra Appl. 6 (2007) 443-459.
- [14] M. D'Anna and M. Fontana, *An amalgamated duplication of a ring along a multiplicative-canonical ideal*, Arkiv Mat. 6 (2007) 241-252.
- [15] M. D'Anna, C.A. Finacchiaro and M. Fontana, *Amalgamated algebra along an ideal*, Comm Algebra and Applications, Walter De Gruyter (2009), 241-252.
- [16] M. D'Anna, C. A. Finacchiaro, and M. Fontana, *Properties of chains of prime ideals in amalgamated algebra along an ideal*, J. Pure and Appl. Algebra 214 (2010) 1633-1641.
- [17] S. El Baghdadi, A. Jhilal, and N. Mahdou, *On FF-rings*, J. Pure and Appl. Algebra 216 (2012) 71-76.
- [18] Y. El Haddaoui, *On ϕ -Prüfer and ϕ -Bézout rings in amalgamation algebra along an ideal*, Moroccan J. Algebra Geom. Appl., 3(1) (2024), 178-186.
- [19] A. El Khalfi, H. Kim and N. Mahdou, *Amalgamation extension in commutative ring theory, a survey*, Moroccan Journal of algebra and Geometry with applications, 1(1) (2022), 139-182.
- [20] C. M. Fadden, M. Greferath and J. Zumbärgel, *Characteristics of Invariant Weights Related to Code Equivalence over Rings*, inria-00607730, version 1 - 11 Jul 2011

- [21] S. Glaz, *Prüfer conditions in rings with zero-divisors*, CRC Press Ser. Lect. Pure Appl. Math. 241 (2005) 272-282.
- [22] S. Glaz, *Commutative coherent rings*, Springer-Verlag, Lecture Notes in Mathematics, 1371 (1989).
- [23] S. Glaz, *Controlling the zero divisors of a Commutative Rings*, Marcel Dekker Lecture Notes in Pure and Applied Mathematics 231 (2002) 191-212
- [24] J. A. Huckaba, *Commutative Rings with Zero Divisors*, Marcel Dekker, New York Basel, (1988).
- [25] M. F. Jones, *f-projectivity and flat epimorphisms*, Comm. Algebra, 9(16), 1603-1616 (1981).
- [26] S. Kabbaj and N. Mahdou, *Trivial extensions defined by coherent-like conditions*, Comm. Algebra 32 (10) (2004) 3937-3953.
- [27] S. Kabbaj, *Matlis's semi-regularity and semi-coherence in trivial ring extensions: a survey*, Moroccan J. Algebra Geom. Appl., 1(1) (2022), 1-17.
- [28] N. Mahdou, *On Costa-conjecture*, Comm. Algebra, 29 (2001), 2775-2785.
- [29] N. Mahdou, *On 2-Von Neumann regular rings*, Comm. Algebra 33 (2005) 3489-3496.
- [30] M. A. Majid, *Idealization and Theorems of D. D. Anderson II*, Comm. Algebra, 35 (2007), 2767-2792.
- [31] L. Mao and N. Ding, *Relative flatness, Mittag-leffler modules, and endocoherence*, Comm. Algebra 34 (2006) 3281-3299.
- [32] N. Mahdou and H. Mouanis, *Some homological properties of subrings retract and applications to fixed rings*, Comm. Algebra, 32, No. 5 (2004) 1823-1834.
- [33] M. Nagata, *Local Rings*, Interscience, New York, (1962).
- [34] G. Puninski and P. Rothmaler, *when every finitely generated flat module is projective*, J. Algebra 277(2004), 542-558.
- [35] Y. Quentel, *Sur La Compacité Du Spectre Minimal D'un Anneau*, Bull. Soc. Math. France 99 (1971), 265 - 272
- [36] J.J. Rotman, *An introduction to homological algebra*, Academic Press, New York (1979).
- [37] J. D. Sally and W. V. Vasconcelos, *Flat ideal I*, Comm. Algebra 3 (1975) 531-543.
- [38] Z. Shenglin, *On rings over which every flat left module is finitely projective*, J. Algebra 139 (1991) 311-321.
- [39] D. Simson, *$\aleph$ -flat and $\aleph$ -projective modules*, Bull. Acad. Polom. Sci. Ser. Sci. Math. Astron. Phys., 20 (1972) 109-114.



ISSN: 2820-7114

Moroccan Journal of Algebra and Geometry with Applications

Supported by Sidi Mohamed Ben Abdellah University, Fez, Morocco

Volume 4, Issue 2 (2025), pp 248-258

Title :

Weakly J -filters property in lattices

Author(s):

Shahabaddin Ebrahimi Atani

Weakly J -filters property in lattices

Shahabaddin Ebrahimi Atani

Department of Pure Mathematics, Guilan university, Rasht, Iran.
e-mail: ebrahimi@guilan.ac.ir

Communicated by Mohammed Tamekkante

(Received 17 September 2024, Revised 13 May 2025, Accepted 17 May 2025)

Abstract. Let $\mathcal{L}$ be a bounded distributive lattice. Similar to the definition of weakly J -ideals of commutative rings, we introduce and study weakly J -filters of lattices. The main purpose of this paper is devoted to extend the notion of weakly J -ideal property in commutative rings to weakly J -filter property in lattices.

Key Words: lattice; J -filter; weakly J -filter.

2020 MSC: Primary: 05C69, 06B99; Secondary: 05C15, 05C25. 47B47.

1 Introduction

All lattices considered in this paper are assumed to have a least element denoted by 0 and a greatest element denoted by 1, in other words they are bounded. As algebraic structures, lattices are undoubtedly a natural choice of generalizations of rings. Recently, the study of algebraic structures, using the properties of lattices, has become a research topic, leading to many interesting results. There are growing interest in developing the algebraic theory of lattices can be found in several papers and books (see for instance, [5, 7, 8, 9]).

Over the years, several types of ideals have been developed in order to let us fully understand the structures of rings in general. The notion of prime ideals has a significant place in the theory of rings, and it is used to characterize certain classes of rings. Recall from Atiyah and MacDonald in [1], a prime ideal P of R is a proper ideal having the property that $ab \in P$ implies either $a \in P$ or $b \in P$ for each $a, b \in R$ (also see [2, 4]). In [17], Mohamadian defined a proper ideal I of R as an r -ideal if whenever $a, b \in R$ with $ab \in I$ and $\text{ann}(a) = 0$ imply that $b \in I$, where $\text{ann}(a) = \{r \in R : ra = 0\}$. He investigated the behavior of r -ideals and compare them with other classical ideals such as prime and maximal ideals. In [18], Tekir et al., defined and studied some subclass of r -ideals, namely, the class of n -ideals. A proper ideal I of a ring R is called an n -ideal if whenever $a, b \in R$ with $ab \in I$ and $a \notin \sqrt{0}$, then $b \in I$. For any ring R , By $J(R)$, we denote the Jacobson radical of R . Khashan and Bani-Ata generalized the concept of n -ideals in [15]. A proper ideal I of a ring R is called a J -ideal if whenever $a, b \in R$ with $ab \in I$ and $a \notin J(R)$, then $b \in I$. Khashan and Celikel [16] introduced the notion of a weakly J -ideals, i.e. a proper ideal I of a ring R is called a weakly J -ideal if whenever $a, b \in R$ with $0 \neq ab \in I$ and $a \notin J(R)$, then $b \in I$. Let $\mathcal{L}$ be a bounded distributive lattice and $J(\mathcal{L})$ denote the Jacobson radical of $\mathcal{L}$ (i.e. to be the intersection of all the maximal filters of $\mathcal{L}$). In [13], the present author, introduced the concept of J -filters. A proper filter F of $\mathcal{L}$ is called a J -filter if whenever $x \vee y \in F$ with $x \notin J(\mathcal{L})$, then $y \in F$ for every $x, y \in \mathcal{L}$. Our objective in this paper is to extend the notion of weakly J -ideal property in commutative rings to weakly J -filter property in the lattices. Among many other results in this paper, the first, Preliminaries section contains elementary observations needed later on.

Section 3 is devoted to the investigate the basic properties of weakly J -filters as a new generalization of J -filters. A proper filter F of $\mathcal{L}$ is called a weakly J -filter if whenever $1 \neq x \vee y \in F$ with $x \notin J(\mathcal{L})$, then $y \in F$ for every $x, y \in \mathcal{L}$. At first, we provide an example of lattices for which their J -filters and weakly J -filters are the same (Theorem 3.3). Many equivalent characterizations of weakly J -filters for any bounded distributive lattice are presented in Proposition 3.4 and Theorem 3.8. In 2003, Anderson and Smith in [1] defined weakly prime ideals which is a generalization of prime ideals. A proper ideal P of a ring R is said to be a weakly prime if $0 \neq xy \in P$ for each $x, y \in R$ implies either $x \in P$ or $y \in P$. A proper filter P of a lattice $\mathcal{L}$ is said to be a weakly prime if $1 \neq x \vee y \in P$ for each $x, y \in \mathcal{L}$ implies either $x \in P$ or $y \in P$. In the Example 3.10, it is shown that, in general, the class of weakly J -filters is not comparable with the classes of weakly prime filters. Then we justify the relationships between these two concepts in Proposition 3.11 and Proposition 3.12. Further, for two weakly J -filters F_1 and F_2 of a lattice $\mathcal{L}$, we show that $F_1 \cap F_2$ is a weakly J -filter (see Proposition 3.13), but the converse is not true (see Example 3.14). Here, we provide some condition under which the converse of Proposition 3.13 is true (see Theorem 3.15).

We continue in this Section by investigation the stability of weakly J -filters in various lattice-theoretic constructions. In particular, we investigate the behavior of weakly J -filters under homomorphism, in factor lattices and in cartesian products of lattices (see Theorem 3.16, Corollary 3.17, Proposition 3.18, Proposition 3.19 and Theorem 3.31). Further, for two weakly J -filters F and G of a lattice $\mathcal{L}$, we show that $F \wedge G$ is a weakly J -filter of $\mathcal{L}$ (see Theorem 3.21). An element x of $\mathcal{L}$ is called *identity join* of a lattice $\mathcal{L}$, if there exists $1 \neq y \in \mathcal{L}$ such that $x \vee y = 1$. The set of all identity joins of a lattice $\mathcal{L}$ is denoted by $I(\mathcal{L})$. Similar to the definition of *presimplifiable* ring from Bouvier in [6], a lattice $\mathcal{L}$ is called *presimplifiable* if $I(\mathcal{L}) \subseteq J(\mathcal{L})$. It is well known from Anderson and Axtell in [3] that *presimplifiable* property does not pass in general to homomorphic images. However, we show that this holds under a certain condition: If F is a weakly J -filter of a *presimplifiable* lattice $\mathcal{L}$, then $\mathcal{L}/F$ is a *presimplifiable* lattice (see Proposition 3.23, Theorem 3.24 and Theorem 3.27). Similar to the idealization of a module over a ring (Huckaba in [14]), the remaining part of this section mainly devoted to investigation the stability of weakly J -filters in the *filterlization* of a lattice and a filter. Let $\mathcal{M}$ be a filter of lattice $\mathcal{L}$. The filterlization $\mathcal{L}(+)\mathcal{M} = \{(a, m) : a \in \mathcal{L}, m \in \mathcal{M}\}$ of $\mathcal{M}$ in $\mathcal{L}$ is a lattice with respect to the following definitions: (1) $(a, m) = (a', m')$ if $a = a'$ and $m = m'$, (2) $(a, m_1) \wedge_F (b, m_2) = (a \wedge b, m_1 \wedge m_2)$ and (3) $(a, m_1) \vee_F (b, m_2) = (a \vee b, (a \vee m_2) \wedge (b \vee m_1))$. Here we clarify the relationships between weakly J -filters in a lattice $\mathcal{L}$ and in a filterlization lattice $\mathcal{L}(+)\mathcal{M}$ in Theorem 3.33.

2 Preliminaries

A poset $(\mathcal{L}, \leq)$ is a lattice if $\sup\{a, b\} = a \vee b$ and $\inf\{a, b\} = a \wedge b$ exist for all $a, b \in \mathcal{L}$ (and call $\wedge$ the *meet* and $\vee$ the *join*).

Definition 2.1. (1) A lattice $\mathcal{L}$ is called a *distributive lattice* if $(a \vee b) \wedge c = (a \wedge c) \vee (b \wedge c)$ for all a, b, c in $\mathcal{L}$ (equivalently, $\mathcal{L}$ is distributive if $(a \wedge b) \vee c = (a \vee c) \wedge (b \vee c)$ for all a, b, c in $\mathcal{L}$).

(2) A non-empty subset F of a lattice $\mathcal{L}$ is called a *filter*, if for $a \in F$, $b \in \mathcal{L}$, $a \leq b$ implies $b \in F$, and $x \wedge y \in F$ for all $x, y \in F$ (so if $\mathcal{L}$ is a lattice with 0 and 1, then $1 \in F$, $\{1\}$ is a filter of $\mathcal{L}$ and $0 \in F$ if and only if $F = \mathcal{L}$).

(3) A proper filter F of $\mathcal{L}$ is called *prime* if $x \vee y \in F$, then $x \in F$ or $y \in F$.

(4) A proper filter F of $\mathcal{L}$ is said to be *maximal* if G is a filter in $\mathcal{L}$ with $F \subsetneq G$, then $G = \mathcal{L}$. We define the *Jacobson radical* of $\mathcal{L}$, denoted by $J(\mathcal{L})$, to be the intersection of all the maximal filters of $\mathcal{L}$. The set of all maximal filters of $\mathcal{L}$ is denoted $\text{Max}(\mathcal{L})$.

(5) Let D be subset of a lattice $\mathcal{L}$. Then the filter generated by D , denoted by $T(D)$, is the intersection of all filters that is containing D . A filter F is called *finitely generated* if there is a finite subset D of F such that $F = T(D)$.

(6) A lattice $\mathcal{L}$ with 1 is called $\mathcal{L}$ -domain if $a \vee b = 1$ ($a, b \in \mathcal{L}$), then $a = 1$ or $b = 1$ (so $\mathcal{L}$ is $\mathcal{L}$ -domain if and only if $\{1\}$ is a prime filter of $\mathcal{L}$).

(7) A lattice $\mathcal{L}$ is called *local* if it has exactly one maximal filter that contains all proper filters.

(8) If $x \in \mathcal{L}$, then a *complement* of x in $\mathcal{L}$ is an element $y \in \mathcal{L}$ such that $x \vee y = 1$ and $x \wedge y = 0$. The lattice $\mathcal{L}$ is *complemented* if every element of $\mathcal{L}$ has a complement in $\mathcal{L}$.

(9) If $\mathcal{L}$ and $\mathcal{L}'$ are lattices, then a *lattice homomorphism* $f : \mathcal{L} \rightarrow \mathcal{L}'$ is a map from $\mathcal{L}$ to $\mathcal{L}'$ satisfying $f(x \vee y) = f(x) \vee f(y)$ and $f(x \wedge y) = f(x) \wedge f(y)$ for $x, y \in \mathcal{L}$.

(10) A filter G of $\mathcal{L}$ is called *small* in $\mathcal{L}$, written $G \ll \mathcal{L}$, if for every filter H of $\mathcal{L}$, the equality $G \wedge H = \mathcal{L}$ implies $H = \mathcal{L}$.

For undefined notations or terminologies in lattice theory, we refer the reader to [5, 7]. First we need the following easy observation proved in [5, 7, 9, 11].

Lemma 2.2. Let $\mathcal{L}$ be a lattice.

(1) A non-empty subset F of $\mathcal{L}$ is a filter of $\mathcal{L}$ if and only if $x \vee z \in F$ and $x \wedge y \in F$ for all $x, y \in F, z \in \mathcal{L}$. Moreover, since $x = x \vee (x \wedge y)$, $y = y \vee (x \wedge y)$ and F is a filter, $x \wedge y \in F$ gives $x, y \in F$ for all $x, y \in \mathcal{L}$.

(2) If F_1, F_2 are filters of $\mathcal{L}$ and $a \in \mathcal{L}$, then $F_1 \vee F_2 = \{a_1 \vee a_2 : a_1 \in F_1, a_2 \in F_2\}$ and $a \vee F_1 = \{a \vee a_1 : a_1 \in F_1\}$ are filters of $\mathcal{L}$ and $F_1 \vee F_2 = F_1 \cap F_2$.

(3) Let A be an arbitrary non-empty subset of $\mathcal{L}$. Then

$$T(A) = \{x \in \mathcal{L} : a_1 \wedge a_2 \wedge \cdots \wedge a_n \leq x \text{ for some } a_i \in A (1 \leq i \leq n)\}.$$

Moreover, if F is a filter and A is a subset of $\mathcal{L}$ with $A \subseteq F$, then $T(A) \subseteq F$, $T(F) = F$ and $T(T(A)) = T(A)$.

(4) If $\mathcal{L}$ is distributive, F, G are filters of $\mathcal{L}$ and $y \in \mathcal{L}$, then $(G :_{\mathcal{L}} F) = \{x \in \mathcal{L} : x \vee F \subseteq G\}$, $(F :_{\mathcal{L}} T(\{y\})) = (F :_{\mathcal{L}} y) = \{a \in \mathcal{L} : a \vee y \in F\}$ and $(1 :_{\mathcal{L}} y) = \{x \in \mathcal{L} : x \vee y = 1\}$ are filters of $\mathcal{L}$.

(5) If $\mathcal{L}$ is distributive and F_1, F_2 are filters of $\mathcal{L}$, then $F_1 \wedge F_2 = \{a_1 \wedge a_2 : a_1 \in F_1, a_2 \in F_2\}$ is a filter of $\mathcal{L}$ and $F_1, F_2 \subseteq F_1 \wedge F_2$.

Lemma 2.3. [12, Lemma 3.13] Let $\mathcal{E}_1$ and $\mathcal{E}_2$ be lattices and $f : \mathcal{E}_1 \rightarrow \mathcal{E}_2$ be a lattice homomorphism such that $f(1) = 1$. The following hold:

(1) $\text{Ker}(f) = \{x \in \mathcal{E}_1 : f(x) = 1\}$ is a filter of $\mathcal{E}_1$;

(2) If f is injective, then $\text{Ker}(f) = \{1\}$;

(3) If $\mathcal{E}_1$ is a complemented lattice, then f is injective if and only if $\text{Ker}(f) = \{1\}$.

3 Characterization of weakly J -filters

In this section, we collect some basic properties concerning weakly J -filters and remind the reader with the following definition.

Definition 3.1. A proper filter F of a lattice $\mathcal{L}$ is called a weakly J -filter if whenever $x, y \in \mathcal{L}$ with $1 \neq x \vee y \in F$ and $x \notin J(\mathcal{L})$, then $y \in F$.

Example 3.2. (1) It is easy to see that every J -filter is a weakly J -filter.

(2) Let $A = \{1, 2, 3\}$. Then $\mathcal{L} = \{X : X \subseteq A\}$ forms a distributive lattice under set inclusion with greatest element A and least element $\emptyset$ (note that if $x, y \in \mathcal{L}$, then $x \vee y = x \cup y$ and $x \wedge y = x \cap y$). It can be easily seen that the set of all proper filters $\mathcal{L}$ is $\{\{A\}, F_1, F_2, F_3, F_4, F_5, F_6\}$, where $F_1 = \{A, \{1, 2\}\}$, $F_2 = \{A, \{1, 3\}\}$, $F_3 = \{A, \{2, 3\}\}$,

$$F_4 = \{A, \{1, 3\}, \{1, 2\}, \{1\}\},$$

$F_5 = \{A, \{2, 3\}, \{1, 2\}, \{2\}\}$ and $F_6 = \{A, \{1, 3\}, \{3, 2\}, \{3\}\}$ with $J(\mathcal{L}) = F_4 \cap F_5 \cap F_6 = \{A\}$. Set $F = \{A\}$. Then F is not a J -filter. For example, $\{1, 2\}, \{3\} \in \mathcal{L}$ with $\{1, 2\} \vee \{3\} \in F$ and $\{3\} \notin J(\mathcal{L})$ but $\{1, 2\} \notin F$. However, since F is always weakly J -filter (by definition), a weakly J -filter need not be J -filter.

The next result determines the class of lattices for which their J -filters and weakly J -filters are the same. Compare the next theorem with Theorem 2.3 in [16].

Theorem 3.3. If $\mathcal{L}$ is a lattice, then the following statements are equivalent:

- (1) $\mathcal{L}$ is a local lattice;
- (2) Every proper filter of $\mathcal{L}$ is a J -filter;
- (3) Every proper filter of $\mathcal{L}$ is a weakly J -filter;
- (4) Every proper principal filter of $\mathcal{L}$ is a weakly J -filter.

Proof. (1) $\Rightarrow$ (2) Let G be a proper filter of a local lattice $\mathcal{L}$ with unique maximal filter M and let $a, b \in \mathcal{L}$ with $a \vee b \in G$ and $a \notin J(\mathcal{L}) = M$. Then $M \wedge T(\{a\}) = \mathcal{L}$ by maximality of M which implies that $T(\{a\}) = \mathcal{L}$, as M is small in $\mathcal{L}$ by [9, Lemma 3.1]. So $0 = a \vee c$ for some $c \in \mathcal{L}$. Then $a = 0$ gives $b \in G$. Thus, G is a J -filter.

The implication (2) $\Rightarrow$ (3) $\Rightarrow$ (4) Clear.

(4) $\Rightarrow$ (1) Let M be a maximal filter of $\mathcal{L}$. If $M = \{1\}$ and $1 \neq a \in \mathcal{L}$, then $\{1\} \subsetneq T(\{a\}) \subseteq \mathcal{L}$ gives $T(\{a\}) = \mathcal{L}$; hence $a \leq a \vee b = 0$ for some $b \in \mathcal{L}$. Therefore, $\mathcal{L} = \{0, 1\}$ and so the result follows clearly. Otherwise, let $1 \neq x \in M$. Now, $T(\{x\})$ is a weakly J -filter by (4) and $1 \neq x \vee 0 \in T(\{x\})$. If $x \notin J(\mathcal{L})$, then $0 \in T(\{x\})$ which is impossible. Hence, $x \in J(\mathcal{L})$ and $J(\mathcal{L}) = M$, i.e. (1) holds. $\square$

For a filter F of a lattice $\mathcal{L}$, the Jacobson radical of F , denoted by $J(F)$, is defined as the intersection of all maximal filters of $\mathcal{L}$ containing F . The following properties can be easily verified for any filters F and G of $\mathcal{L}$:

- (1) $F \subseteq J(F)$.
- (2) If $F \subseteq G$, then $J(F) \subseteq J(G)$.
- (3) $J(\mathcal{L}) \subseteq J(F)$.
- (4) $J(J(F)) = J(F)$.

Proposition 3.4. If F is a proper filter of a lattice $\mathcal{L}$, then the following statements are equivalent:

- (1) F is a weakly J -filter of $\mathcal{L}$;
- (2) $F \subseteq J(\mathcal{L})$ and whenever $x, y \in \mathcal{L}$ with $1 \neq x \vee y \in F$, then $x \in J(F)$ or $y \in F$.

Proof. (1) $\Rightarrow$ (2) Let $1 \neq f \in F$. Since $1 \neq f \vee 0 \in F$ and $0 \notin F$, we conclude that $f \in J(\mathcal{L})$. Therefore, $F \subseteq J(\mathcal{L})$. Now, let $1 \neq x \vee y \in F$ with $x \notin J(F)$. Since $J(\mathcal{L}) \subseteq J(F)$ and F is weakly J -filter, we infer that $y \in F$.

(2) $\Rightarrow$ (1) Let $x, y \in \mathcal{L}$ such that $1 \neq x \vee y \in F$ and $x \notin J(\mathcal{L})$. As $F \subseteq J(\mathcal{L})$, we conclude that $J(F) \subseteq J(J(\mathcal{L})) = J(\mathcal{L})$ and so we have $x \notin J(F)$. Thus, $y \in F$ and F is a weakly J -filter. $\square$

The following example shows that we can find a filter F of a lattice $\mathcal{L}$ with $\{1\} \neq F \subseteq J(\mathcal{L})$ which is not a weakly J -filter.

Example 3.5. Assume that $\mathcal{L} = \{0, a, b, c, 1\}$ is a lattice with the relations $0 \leq a \leq c \leq 1$, $0 \leq b \leq c \leq 1$, $a \vee b = c$ and $a \wedge b = 0$. An inspection will show that the nontrivial filters of $\mathcal{L}$ are $F_1 = \{1, a, c\}$, $F_2 = \{1, b, c\}$ and $F_3 = \{1, c\}$ with $F_3 \subseteq J(\mathcal{L}) = F_1 \cap F_2 = F_3$. But F_3 is not a weakly J -filter since $1 \neq a \vee b = c \in F_3$ with $a \notin J(\mathcal{L})$ and $b \notin F_3$.

A lattice $\mathcal{L}$ is called *semiprimitive* if $J(\mathcal{L}) = \{1\}$.

Corollary 3.6. If $\mathcal{L}$ is a semiprimitive lattice, then $\{1\}$ is the only weakly J -filter of $\mathcal{L}$.

Proof. This is a direct consequence of Proposition 3.4 (2). $\square$

Compare the next theorem with Theorem 2.5 in [16].

Theorem 3.7. Let F be a weakly J -filter of $\mathcal{L}$. If F is not J -filter, then $F = \{1\}$.

Proof. On the contrary, assume that $F \neq \{1\}$. We show that F is a J -filter. Let $a, b \in \mathcal{L}$ such that $a \vee b \in F$ and $a \notin J(\mathcal{L})$. If $1 \neq a \vee b \in F$, then F is a weakly J -filter gives $b \in F$. Now, suppose that $a \vee b = 1$. Since $F \neq \{1\}$, there exists $f \in F$ such that $f \neq 1$. Clearly, $a \wedge f \notin J(\mathcal{L})$ (otherwise, $a \in J(\mathcal{L})$ by Lemma 2.2 (1)). Then $1 \neq (a \wedge f) \vee (b \wedge f) = f \in F$ gives $f \wedge b \in F$. Therefore, $b \in F$ by Lemma 2.2 (1). This shows that F is a J -filter, as required. $\square$

We next give four other characterizations of weakly J -filters. Compare the next theorem with Theorem 2.7 in [16].

Theorem 3.8. Let P be a proper filter of a lattice $\mathcal{L}$. Then the following statements are equivalent:

- (1) P is a weakly J -filter of $\mathcal{L}$;
- (2) $(P :_{\mathcal{L}} x) = P \cup (1 :_{\mathcal{L}} x)$ for every $x \notin J(\mathcal{L})$;
- (3) $(P :_{\mathcal{L}} x) \subseteq J(\mathcal{L}) \cup (1 :_{\mathcal{L}} x)$ for every $x \notin P$;
- (4) If $x \in \mathcal{L}$ and F is a filter of $\mathcal{L}$ with $\{1\} \neq x \vee F \subseteq P$, then $F \subseteq J(\mathcal{L})$ or $x \in P$;
- (5) If F and G are filters of $\mathcal{L}$ with $\{1\} \neq F \vee G \subseteq P$, then $F \subseteq J(\mathcal{L})$ or $G \subseteq P$.

Proof. (1) $\Rightarrow$ (2) Let $x \notin J(\mathcal{L})$. Since the inclusion $P \cup (1 :_{\mathcal{L}} x) \subseteq (P :_{\mathcal{L}} x)$ is clear, we will prove the reverse inclusion. Let $y \in (P :_{\mathcal{L}} x)$. If $x \vee y \neq 1$, then by (1), $y \in P$. If $x \vee y = 1$, then $y \in (1 :_{\mathcal{L}} x)$. Therefore, $(P :_{\mathcal{L}} x) \subseteq P \cup (1 :_{\mathcal{L}} x)$ and so we have equality.

(2) $\Rightarrow$ (1) Let $x, y \in \mathcal{L}$ such that $1 \neq x \vee y \in P$ and $x \notin J(\mathcal{L})$. Since $y \notin (1 :_{\mathcal{L}} x)$ and $y \in (P :_{\mathcal{L}} x)$, we conclude that $y \in P$ by (2).

(1) $\Rightarrow$ (3) Let $x \notin P$ and $y \in (P :_{\mathcal{L}} x)$. If $x \vee y \neq 1$, then by (1), $y \in J(\mathcal{L})$. If $x \vee y = 1$, then $y \in (1 :_{\mathcal{L}} x)$. Therefore, $(P :_{\mathcal{L}} x) \subseteq J(\mathcal{L}) \cup (1 :_{\mathcal{L}} x)$.

(3) $\Rightarrow$ (4) Let $\{1\} \neq x \vee F \subseteq P$ and $x \notin P$. Then $(1 :_{\mathcal{L}} x) \subsetneq (P :_{\mathcal{L}} x)$ and so $F \subseteq (P :_{\mathcal{L}} x) \subseteq J(\mathcal{L})$ by [8, Remark 2.3 (i)], as required.

(4) $\Rightarrow$ (5) On the contrary, assume that there exist filters F and G of $\mathcal{L}$ such that $\{1\} \neq F \vee G \subseteq P$ but $F \not\subseteq J(\mathcal{L})$ and $G \not\subseteq P$. Since $F \vee G \neq \{1\}$, we conclude that there exists $g \in G$ such that $\{1\} \neq g \vee F \subseteq P$ which implies that $g \in P$ by (4), as $F \not\subseteq J(\mathcal{L})$. Consider $g' \in G \setminus P$. If $g' \vee F \neq \{1\}$, then $g' \in P$ by (4), a contradiction. Thus, $g' \vee F = \{1\}$. Since $g \wedge g' \in G$ and $g \vee F \neq \{1\}$, we infer that $\{1\} \neq (g \wedge g') \vee F \subseteq P$ and $F \not\subseteq J(\mathcal{L})$ implies that $g \wedge g' \in P$; so $g' \in P$ by Lemma 2.1 (1) which is a contradiction.

(5) $\Rightarrow$ (1) Let $x, y \in \mathcal{L}$ such that $1 \neq x \vee y \in P$ and $x \notin J(\mathcal{L})$. Set $F = T(\{x\})$ and $G = T(\{y\})$. Then $\{1\} \neq F \vee G \subseteq P$ and $F \not\subseteq J(\mathcal{L})$. Now the assertion follows from (5). $\square$

Proposition 3.9. Let S be a non-empty subset of $\mathcal{L}$. If F and $(1 :_{\mathcal{L}} S)$ are weakly J -filters with $S \not\subseteq F$, then $(F :_{\mathcal{L}} S)$ is a weakly J -filter.

Proof. If $(F :_{\mathcal{L}} S) = \mathcal{L}$, then $0 \in (F :_{\mathcal{L}} S)$ and so $S \subseteq F$, a contradiction. Thus, $(F :_{\mathcal{L}} S)$ is a proper filter. Let $x, y \in \mathcal{L}$ such that $1 \neq x \vee y \in (F :_{\mathcal{L}} S)$ with $x \notin J(\mathcal{L})$. If $1 \neq x \vee y \vee s \in F$ for every $s \in S$, then F is a J -filter gives $y \vee s \in F$ and so $y \in (F :_{\mathcal{L}} S)$. If $x \vee y \vee S = \{1\}$, then $1 \neq x \vee y \in (1 :_{\mathcal{L}} S)$ gives $y \in (1 :_{\mathcal{L}} S) \subseteq (F :_{\mathcal{L}} S)$, as $(1 :_{\mathcal{L}} S)$ is a J -filter, as needed. $\square$

In the following example, it is shown that, in general, the class of weakly J -filters is not comparable with the classes of weakly prime filters.

Example 3.10. (1) Let $\mathcal{L}$ be the lattice as in Example 3.2 (2). Then the filter F_5 is a prime filter (so a weakly prime filter). On the other hand, F_5 is not a weakly J -filter of $\mathcal{L}$, as $F_5 \not\subseteq J(\mathcal{L})$.

(2) The collection of ideals of $\mathbb{Z}$, the ring of integers, form a lattice under set inclusion which we shall denote by $\mathcal{L}$ with respect to the following definitions: $m\mathbb{Z} \vee n\mathbb{Z} = (m, n)\mathbb{Z}$ and $m\mathbb{Z} \wedge n\mathbb{Z} = [m, n]\mathbb{Z}$ for all ideals $m\mathbb{Z}$ and $n\mathbb{Z}$ of $\mathbb{Z}$, where (m, n) and $[m, n]$ are greatest common divisor and least common multiple of m, n , respectively. Note that $\mathcal{L}$ is a distributive complete lattice with least element the

zero ideal and the greatest element $\mathbb{Z}$. By [8, Theorem 2.9 (ii)], $\mathcal{L} \setminus \{0\}$ is the only maximal filter of $\mathcal{L}$ and so $\mathcal{L}$ is a local lattice. It follows from Theorem 3.3 that every proper filter of $\mathcal{L}$ is a weakly J -filter. Consider the filter $P = \{\mathbb{Z}, 2\mathbb{Z}\}$. Since $1 \neq 14\mathbb{Z} \vee 18\mathbb{Z} = 2\mathbb{Z} \in P$ with $14\mathbb{Z}, 18\mathbb{Z} \notin P$, we infer that P is not a weakly prime filter.

Proposition 3.11. *Let P be a weakly prime filter such that $P \subseteq J(\mathcal{L})$. Then P is a weakly J -filter of $\mathcal{L}$.*

Proof. The proof is straightforward. $\square$

The following proposition provides some condition under which a weakly J -filter is a weakly prime filter.

Proposition 3.12. *Let P be a filter of $\mathcal{L}$. Assume P is maximal with respect to property: P and $(1 :_{\mathcal{L}} x)$ are weakly J -filters for all $x \notin P$. Then P is a weakly prime filter in $\mathcal{L}$.*

Proof. Let $x, y \in \mathcal{L}$ such that $1 \neq x \vee y \in P$ and $x \notin P$. Set $S = \{x\}$. Then $(P :_{\mathcal{L}} x)$ is a weakly J -filter by Proposition 3.9. Since $P \subseteq (P :_{\mathcal{L}} x)$, we conclude that $z \notin P$ for all $z \notin (P :_{\mathcal{L}} x)$ and so $(1 :_{\mathcal{L}} z)$ is a weakly J -filter. Therefore, we have $y \in (P :_{\mathcal{L}} x) = P$ by maximality of P , as needed. $\square$

Proposition 3.13. *Let $\mathcal{L}$ be a lattice. If $\{F_i\}_{i \in \Lambda}$ is a nonempty family of weakly J -filters of $\mathcal{L}$, then $\cap_{i \in \Lambda} F_i$ is a weakly J -filter.*

Proof. (1) Let $a, b \in \mathcal{L}$ such that $1 \neq a \vee b \in \cap_{i \in \Lambda} F_i$ and $a \notin J(\mathcal{L})$. By the hypothesis, $1 \neq a \vee b \in F_i$ for all $i \in \Lambda$ gives $b \in F_i$ for all $i \in \Lambda$ and so $b \in \cap_{i \in \Lambda} F_i$, as needed. $\square$

Example 3.14. In general, the converse Proposition 3.13 is not true. For example, while $F_4 \cap F_5 = \{1\}$ is a weakly J -filter of the lattice as in 3.2 (2), none of the filters F_4 and F_5 are (weakly) J -filters.

The following theorem provides some condition under which the converse Proposition 3.13 is true.

Theorem 3.15. *Let $F_1, \dots, F_n$ be weakly prime filters of $\mathcal{L}$ which are not comparable and $(\mathcal{L} \setminus F_i) \cap I(\mathcal{L}) = \emptyset$ for all $1 \leq i \leq n$. Then $\cap_{i=1}^n F_i$ is a weakly J -filter if and only if F_i is a weakly J -filter for $i \in \{1, \dots, n\}$.*

Proof. One side is clear by Proposition 3.13. To see the other side, let $1 \neq a \vee b \in F_i$ with $a \notin J(\mathcal{L})$ and take $c \in (\bigvee_{i \neq j} F_j) \setminus F_i$. Therefore, $a \vee b \vee c \in \bigvee_{i=1}^n F_i = \cap_{i=1}^n F_i$. If $a \vee b \vee c = 1$, then $c \in (\mathcal{L} \setminus F_i) \cap I(\mathcal{L})$ which is a contradiction. So we may assume that $a \vee b \vee c \neq 1$. Since $\cap_{i=1}^n F_i$ is a weakly J -filter and $a \notin J(\mathcal{L})$, we conclude that $b \vee c \in \cap_{i=1}^n F_i$ and so $b \vee c \in F_i$. This implies that $b \in F_i$, i.e. F_i is a weakly J -filter of $\mathcal{L}$. $\square$

We continue this section with the investigation of the stability of weakly J -filters in various lattice-theoretic constructions.

Theorem 3.16. *Let $\mathcal{L}$ be a complemented lattice. If $f : \mathcal{L} \rightarrow \mathcal{L}'$ is a lattice homomorphism such that $f(0) = 0$ and $f(1) = 1$, then the following hold:*

- (1) *If f is a monomorphism and K is a weakly J -filter of $\mathcal{L}'$, then $f^{-1}(K)$ is a weakly J -filter of $\mathcal{L}$.*
- (2) *If f is an epimorphism and G is a weakly J -filter of $\mathcal{L}$ with $\ker(f) \subseteq G$, then $f(G)$ is a weakly J -filter of $\mathcal{L}'$.*

Proof. (1) Let $a, b \in \mathcal{L}$ with $1 \neq a \vee b \in f^{-1}(K)$ and $a \notin J(\mathcal{L})$. Then $f(a) \vee f(b) = f(a \vee b) \in K$. We show that $f(a) \notin J(\mathcal{L}')$. On the contrary, assume that $f(a) \in J(\mathcal{L}')$. Let M be a maximal filter of $\mathcal{L}$. Then $f(M) \neq \{1\}$, as f is a monomorphism. Let $f(M) \subsetneq F \subseteq \mathcal{L}'$ for some filter F of $\mathcal{L}'$. Then there exists $c \in \mathcal{L} \setminus M$ such that $f(c) \in F \setminus f(M)$. Since $M \subsetneq M \wedge T(\{c\})$, we conclude that $M \wedge T(\{c\}) = \mathcal{L}$ and so $0 = m \wedge (c \vee b) = (m \wedge c) \vee (m \wedge b)$ for some $m \in M$ and $b \in \mathcal{L}$; hence $m \wedge c = 0$. It follows that

$f(m \wedge c) = f(m) \wedge f(c) = f(0) = 0 \in F$ which implies that $F = \mathcal{L}'$. Thus, $f(M)$ is a maximal filter of $\mathcal{L}'$ which implies that $f(a) \in f(M)$ and so $a \in M$. Hence $a \in J(\mathcal{L})$ which is impossible. Therefore, $f(a) \notin J(\mathcal{L}')$. Since by Lemma 2.3, $\text{Ker}(f) = \{1\}$, we conclude that $\{1\} \neq f(a \vee b) = f(a) \vee f(b) \in K$; hence $f(b) \in K$, as K is a weakly J -filter and so $b \in f^{-1}(K)$. Thus, $f^{-1}(K)$ is a J -filter of $\mathcal{L}$.

(2) Let $x, y \in \mathcal{L}'$ such that $1 \neq x \vee y \in f(G)$ and $x \notin J(\mathcal{L}')$. Since f is an epimorphism, there exist $a, b \in \mathcal{L}$ such that $x = f(a)$ and $y = f(b)$. Then $x \vee y = f(a \vee b) \in f(G)$ (so $a \vee b \neq 1$) and then $f(a \vee b) = f(g)$ for some $g \in G$. By the hypothesis, $g \vee g' = 1$ and $g \wedge g' = 0$ for some $g' \in \mathcal{L}$. Since $f(a \vee b \vee g') = f(a \vee b) \vee f(g') = 1$, we conclude that $a \vee b \vee g' \in \text{ker}(f) \subseteq G$; hence $a \vee b = (a \vee b) \vee (g \wedge g') = (a \vee b \vee g) \wedge (a \vee b \vee g') \in G$, as G is a filter. Also, note that $a \notin J(\mathcal{L})$ since otherwise if $a \in J(\mathcal{L})$, then $x = f(a) \in J(\mathcal{L}')$, as $f(J(\mathcal{L})) = f(\bigcap_{M \in \text{Max}(\mathcal{L})} M) \subseteq \bigcap_{M \in \text{Max}(\mathcal{L})} f(M) \subseteq J(\mathcal{L}')$ which is impossible. Since G is a J -filter, we infer that $b \in G$ and so $y = f(b) \in f(G)$, as needed. $\square$

If F is a filter of a lattice $(\mathcal{L}, \leq)$, we define a relation on $\mathcal{L}$, given by $x \sim y$ if and only if there exist $a, b \in F$ satisfying $x \wedge a = y \wedge b$. Then $\sim$ is an equivalence relation on $\mathcal{L}$, and we denote the equivalence class of a by $a \wedge F$ and these collection of all equivalence classes by $\mathcal{L}/F$. We set up a partial order $\leq_Q$ on $\mathcal{L}/F$ as follows: for each $a \wedge F, b \wedge F \in \mathcal{L}/F$, we write $a \wedge F \leq_Q b \wedge F$ if and only if $a \leq b$. The following notation below will be used in this paper: It is straightforward to check that $(\mathcal{L}/F, \leq_Q)$ is a lattice with $(a \wedge F) \vee_Q (b \wedge F) = (a \vee b) \wedge F$ and $(a \wedge F) \wedge_Q (b \wedge F) = (a \wedge b) \wedge F$ for all elements $a \wedge F, b \wedge F \in \mathcal{L}/F$. Note that $f \wedge F = F$ if and only if $f \in F$ (see [10, Remark 4.2 and Lemma 4.3]).

Corollary 3.17. Suppose $\mathcal{L}$ is a complemented lattice and let F, G be two proper filters of $\mathcal{L}$ with $F \subseteq G$. If G is a weakly J -filter of $\mathcal{L}$, then G/F is a weakly J -filter of $\mathcal{L}/F$.

Proof. Let $v : \mathcal{L} \rightarrow \mathcal{L}/F$ be the natural epimorphism defined by $v(x) = x \wedge F$. Then $\text{ker}(v) = \{x \in \mathcal{L} : x \wedge F = 1 \wedge F\} = F \subseteq G$ by [10, Lemma 4.3] and so by Theorem 3.16 (2) and [10, Lemma 4.3] that $v(G) = \{x \wedge F : x \in G\} = G/F$ is a weakly J -filter of $\mathcal{L}/F$. $\square$

Proposition 3.18. Suppose $\mathcal{L}$ is a lattice and let F, G be two proper filters of $\mathcal{L}$ with $F \subseteq G$. Then the followings hold:

- (1) If F is a J -filter of $\mathcal{L}$ and G/F is a weakly J -filter of $\mathcal{L}/F$, then G is a J -filter of $\mathcal{L}$.
- (2) If F is a weakly J -filter of $\mathcal{L}$ and G/F is a weakly J -filter of $\mathcal{L}/F$, then G is a weakly J -filter of $\mathcal{L}$.

Proof. (1) Let $x, y \in \mathcal{L}$ such that $x \vee y \in G$ and $x \notin J(\mathcal{L})$. If $x \vee y \in F$, then $y \in F \subseteq G$. So we may assume that $x \vee y \notin F$ (so $(x \vee y) \wedge F \neq F = 1 \wedge F$). By [10, Lemma 4.3], $M/F \in \text{Max}(\mathcal{L}/F)$ if and only if $M \in \text{Max}(\mathcal{L})$ with $F \subseteq M$. Since F is a J -filter, we infer that $F \subseteq J(\mathcal{L})$ and so clearly $x \wedge F \notin J(\mathcal{L}/F)$. Since $F = 1 \wedge F \neq (x \wedge F) \vee_Q (y \wedge F) = (x \vee y) \wedge F \in G/F$ by Lemma [10, Lemma 4.3] and G/F is a weakly J -filter, we include that $y \wedge F \in G/F$; hence $y \in G$, as required.

- (2) The proof is similar to that in case (1) and we omit it. $\square$

One can easily show that if G is a filter of a complemented lattice $\mathcal{L}$, then $\mathcal{L}/G$ is a complemented lattice.

Proposition 3.19. Let F and G be two filters of a complemented lattice $\mathcal{L}$. Then there is a lattice isomorphism $\phi : F/(F \cap G) \rightarrow (F \wedge G)/G$ that sends each residue class $x \wedge (F \cap G)$ to $x \wedge G$.

Proof. At first, note that since $(a \wedge b) \wedge b = a \wedge b$ for some $b \in G$ and $a \in \mathcal{L}$, we conclude that $(a \wedge b) \wedge G = a \wedge G$. If $x \wedge (F \cap G) = y \wedge (F \cap G)$, then $x \wedge a = y \wedge b$ for some $a, b \in F \cap G \subseteq G$; so $x \wedge G = y \wedge G$. This shows that ϕ is well defined. Clearly, ϕ is surjective. If $A = x \wedge (F \cap G)$ and $B = y \wedge (F \cap G)$ are elements of $F/(F \cap G)$, then $\phi(A \vee_Q B) = \phi((x \vee y) \wedge F \cap G) = (x \vee y) \wedge G = (x \wedge G) \vee_Q (y \wedge G) = \phi(A) \vee_Q \phi(B)$. Similarly, $\phi(A \wedge_Q B) = \phi(A) \wedge_Q \phi(B)$. Since $\text{Ker}(\phi) = \{x \wedge (F \cap G) \in F/(F \cap G) : x \wedge G = 1 \wedge G\} = (F \wedge G)/(F \wedge G) = \{\bar{1}\}$, we infer that ϕ is injective by Lemma 2.3, as required. $\square$

Lemma 3.20. If G is a weakly J -filter of $\mathcal{L}$, then it is small in $\mathcal{L}$.

Proof. Let K be a filter of $\mathcal{L}$ such that $G \wedge K = \mathcal{L}$. Assume on the contrary, that $K \neq \mathcal{L}$. Since $K \neq \{1\}$, we conclude that $K \subseteq M$ for some maximal filter M of $\mathcal{L}$ by [10, Lemma 2.1]. It follows from Proposition 3.4 that $G \subseteq J(\mathcal{L}) \subseteq M$ and so $\mathcal{L} = K \wedge G \subseteq M$ which is a contradiction. Therefore, $K = \mathcal{L}$. $\square$

Compare the next theorem with Proposition 2.26 in [16].

Theorem 3.21. If G and F are weakly J -filters of a complemented lattice $\mathcal{L}$, then $F \wedge G$ is a weakly J -filter of $\mathcal{L}$.

Proof. Let F and G be weakly J -filters of $\mathcal{L}$. By Lemma 3.20, $F \wedge G \neq \mathcal{L}$. Since $F \cap G$ is a weakly J -filter by Proposition 3.13, then $F/(F \cap G)$ is a weakly J -filter of $\mathcal{L}/(F \cap G)$ by Corollary 3.17. Now, Proposition 3.19 gives $(F \wedge G)/G$ is a weakly J -filter of $\mathcal{L}/G$. Hence, $F \wedge G$ is a weakly J -filter of $\mathcal{L}$ by Proposition 3.18 (2). $\square$

Proposition 3.22. Let $\mathcal{L}$ be a presimplifiable lattice. Then every weakly J -filter of $\mathcal{L}$ is a J -filter.

Proof. At first, we show that $F = \{1\}$ is a J -filter of $\mathcal{L}$. Let $a, b \in \mathcal{L}$ such that $a \vee b \in F$ and $a \notin J(\mathcal{L})$. By the hypothesis, $a \notin I(\mathcal{L})$ and so $b = 1 \in F$. Suppose that G is a weakly J -filter of $\mathcal{L}$. We show that G is a J -filter. Let $x, y \in \mathcal{L}$ such that $x \vee y \in G$ and $x \notin J(\mathcal{L})$. If $x \vee y \neq 1$, then G is a weakly J -filter gives $y \in G$. If $x \vee y = 1$, then $\{1\}$ is a J -filter implies that $y = 1 \in G$. This shows that G is a J -filter. $\square$

Proposition 3.23. Let F be a proper filter of $\mathcal{L}$. Then F is a J -filter if and only if $F \subseteq J(\mathcal{L})$ and $\mathcal{L}/F$ is a presimplifiable lattice.

Proof. Suppose F is a J -filter of $\mathcal{L}$. Then $F \subseteq J(\mathcal{L})$ by Proposition 3.4. Now, let $x \wedge F \in I(\mathcal{L}/F)$. Then there exists $F = 1 \wedge F \neq y \wedge F \in \mathcal{L}/F$ (so $y \notin F$) such that $(x \wedge F) \vee_Q (y \wedge F) = (x \vee y) \wedge F = 1 \wedge F$. So there are elements $p, q \in F$ such that $(x \wedge p) \vee (y \wedge p) = (x \vee y) \wedge p = 1 \wedge p = q \in F$. Since F is a filter and $y \notin F$, we conclude that $y \wedge p \notin F$ by Lemma 2.2 (1). As F is a J -filter and $p \wedge y \notin F$, we infer that $p \wedge x \in J(\mathcal{L})$; so $x \in J(\mathcal{L})$. This shows that $x \wedge F \in J(\mathcal{L})/F = J(\mathcal{L}/F)$ which gives $I(\mathcal{L}/F) \subseteq J(\mathcal{L}/F)$. Conversely, let $a, b \in \mathcal{L}$ such that $a \vee b \in F$ and $a \notin J(\mathcal{L})$. Then $a \wedge F \notin J(\mathcal{L})/F = J(\mathcal{L}/F)$ and by assumption $a \wedge F \notin I(\mathcal{L}/F)$. Since $(a \wedge F) \vee_Q (b \wedge F) = (a \vee b) \wedge F = 1 \wedge F$ by [10, Lemma 4.3], we infer that $b \wedge F = 1 \wedge F$. So there exists $c, d \in F$ such that $b \wedge c = 1 \wedge d = d \in F$. This shows that $b \in F$. Thus, F is a J -filter. $\square$

Compare the next theorem with Proposition 2.20 in [16].

Theorem 3.24. If $\mathcal{L}$ is a presimplifiable lattice and F is a weakly J -filter of $\mathcal{L}$, then $\mathcal{L}/F$ is presimplifiable.

Proof. By Proposition 3.22, F is a J -filter. Now the assertion follows from Proposition 3.23. $\square$

Definition 3.25. Let $F \neq \{1\}$ be a filter of $\mathcal{L}$. An element $x \wedge F \in \mathcal{L}/F$ is called *strongly identity join* in $\mathcal{L}/F$ if there exists $1 \wedge F \neq y \wedge F \in \mathcal{L}/F$ such that $(x \wedge F) \vee_Q (y \wedge F) = 1 \wedge F$ and $x \vee y \neq 1$.

Example 3.26. One can easily show that any strongly identity join in $\mathcal{L}/F$ is a identity join. We provide an example of lattices for which The converse is not true. Let $\mathcal{L} = \{0, a, b, c, d, 1\}$ be a lattice with the relations $0 \leq a \leq d \leq 1$, $0 \leq b \leq d \leq 1$, $0 \leq c \leq 1$ and $a \wedge b = a \wedge c = d \wedge c = c \wedge b = 0$. Set $P = \{1, a, d\}$. Since $(b \wedge P) \vee_Q (c \wedge P) = (b \vee c) \wedge P = 1 \wedge P$, we conclude that $b \wedge P$ is an identity join in $\mathcal{L}/P$ which is not a strongly identity join.

Let $F \neq \{1\}$ be a filter of $\mathcal{L}$. The set of all strongly identity joins of a lattice $\mathcal{L}/F$ is denoted by $SI(\mathcal{L}/F)$. A lattice $\mathcal{L}/F$ is called *S-presimplifiable* if $SI(\mathcal{L}/F) \subseteq J(\mathcal{L}/F)$. The next theorem gives a more explicit description of weakly J -filters $F \neq \{1\}$ in terms of S-presimplifiable quotient lattices.

Compare the next theorem with Theorem 2.23 in [16].

Theorem 3.27. Let $F \neq \{1\}$ be a filter of $\mathcal{L}$. Then the following statements are equivalent:

- (1) F is a weakly J -filter of $\mathcal{L}$;
- (2) $F \subseteq J(\mathcal{L})$ and $\mathcal{L}/F$ is S -presimplifiable.

Proof. (1) $\Rightarrow$ (2) Assume F is a weakly J -filter of $\mathcal{L}$ (so $F \subseteq J(\mathcal{L})$ by Proposition 3.4). Let $x \wedge F \in \text{SI}(\mathcal{L}/F)$. Then there exists $1 \wedge F \neq y \wedge F \in \mathcal{L}/F$ (so $y \notin F$) such that $(x \wedge F) \vee_Q (y \wedge F) = (x \vee y) \wedge F = 1 \wedge F$ and $x \vee y \neq 1$ which implies that $(x \vee y) \wedge f = 1 \wedge e = e \in F$ for some $e, f \in F$. This shows that $1 \neq x \vee y \in F$ by Lemma 2.2 (1). Hence, $x \in J(\mathcal{L})$, as F is a weakly J -filter. Therefore, $x \wedge F \in J(\mathcal{L})/F = J(\mathcal{L}/F)$, i.e. (2) holds.

(2) $\Rightarrow$ (1) Let $a, b \in \mathcal{L}$ such that $1 \neq a \vee b \in F$ and $b \notin F$. One can easily show that $a \wedge F$ is a strongly identity join in $\mathcal{L}/F$ and so $a \wedge F \in J(\mathcal{L}/F) = J(\mathcal{L}/F)$ by (2) which gives $a \in J(\mathcal{L})$, i.e. (1) holds. $\square$

Definition 3.28. If S is a nonempty subset of a lattice $\mathcal{L}$ such that $\mathcal{L} \setminus J(\mathcal{L}) \subseteq S$, then S is called a *weakly J -join-subset* of $\mathcal{L}$ if $x \vee y \in S$ or $x \vee y = 1$ for all $x \in \mathcal{L} \setminus J(\mathcal{L})$ and all $y \in S$.

In the following proposition, we describe the relation between weakly J -filters and weakly J -join-subsets of $\mathcal{L}$.

Proposition 3.29. A filter F is a weakly J -filter of a lattice $\mathcal{L}$ if and only if $\mathcal{L} \setminus F$ is a weakly J -join-subset of $\mathcal{L}$.

Proof. Let F be a weakly J -filter of $\mathcal{L}$. Since $F \subseteq J(\mathcal{L})$ by Proposition 3.4, we conclude that $\mathcal{L} \setminus J(\mathcal{L}) \subseteq \mathcal{L} \setminus F$. Let $a \in \mathcal{L} \setminus J(\mathcal{L})$ and $b \in \mathcal{L} \setminus F$. If $a \vee b = 1$, then we are done. So we may assume that $a \vee b \neq 1$. Now, we show that $a \vee b \in \mathcal{L} \setminus F$. On the contrary, assume that $a \vee b \in F$. Then F is a weakly J -filter and $x \notin J(\mathcal{L})$ implies that $y \in F$ which is a contradiction. Thus, $x \vee y \in \mathcal{L} \setminus F$ and so $\mathcal{L} \setminus F$ is a weakly J -join-subset of $\mathcal{L}$.

Conversely, let $a, b \in \mathcal{L}$ and $1 \neq a \vee b \in F$ with $a \notin J(\mathcal{L})$. Then we have $b \in F$ since otherwise we would have $a \vee b \in \mathcal{L} \setminus F$ which is impossible. Therefore, F is a weakly J -filter of $\mathcal{L}$. $\square$

Proposition 3.30. Suppose S is a weakly J -join-subset of a lattice $\mathcal{L}$ with $S \cap \bigcup_{y \notin J(\mathcal{L})} (1 :_{\mathcal{L}} y) = \emptyset$. If a filter F of $\mathcal{L}$ is maximal with respect to the property $F \cap S = \emptyset$, then F is a weakly J -filter of $\mathcal{L}$.

Proof. On the contrary, assume that F is not a weakly J -filter of $\mathcal{L}$. Then there are elements $x \notin J(\mathcal{L})$ and $y \notin F$ such that $1 \neq x \vee y \in F$. Since $F \subsetneq (F :_{\mathcal{L}} x)$, we infer that $(F :_{\mathcal{L}} x) \cap S \neq \emptyset$. Consider $s \in (F :_{\mathcal{L}} x) \cap S$. Then $x \vee s \in F$ and S is a weakly J -join-subset gives either $x \vee s \in S$ or $x \vee s = 1$. If $x \vee s \in S$, then $x \vee s \in F \cap S$ which is a contradiction. If $x \vee s = 1$, then $s \in S \cap \bigcup_{y \notin J(\mathcal{L})} (1 :_{\mathcal{L}} y)$, a contradiction. Thus, F is a weakly J -filter of $\mathcal{L}$. $\square$

Assume that $(\mathcal{L})_1, \leq_1), (\mathcal{L})_2, \leq_2)$ are lattices and let $\mathcal{L} = \mathcal{L}_1 \times \mathcal{L}_2$. We set up a partial order $\leq_c$ on $\mathcal{L}$ as follows: for each $x = (x_1, x_2), y = (y_1, y_2) \in \mathcal{L}$, we write $x \leq_c y$ if and only if $x_i \leq_i y_i$ for each $i \in \{1, 2\}$. The following notation below will be used in this paper: It is straightforward to check that $(\mathcal{L}, \leq_c)$ is a lattice with $x \vee_c y = (x_1 \vee y_1, x_2 \vee y_2)$ and $x \wedge_c y = (x_1 \wedge y_1, x_2 \wedge y_2)$. In this case, we say that $\mathcal{L}$ is a *decomposable lattice*.

In the next theorem, we characterize weakly J -filters of a decomposable lattice.

Theorem 3.31. Suppose $\mathcal{L} = \mathcal{L}_1 \times \mathcal{L}_2$ is a decomposable lattice and let $F \neq \{(1, 1)\}$ be a filter of $\mathcal{L}$. Then the following statements are equivalent:

- (1) F is a weakly J -filter of $\mathcal{L}$;
- (2) $F = F_1 \times \mathcal{L}_2$ where F_1 is a J -filter of $\mathcal{L}_1$ or $F = \mathcal{L}_1 \times F_2$ where F_2 is a J -filter of $\mathcal{L}_2$;
- (3) F is a J -filter of $\mathcal{L}$.

Proof. (1) $\Rightarrow$ (2) At first, note that if P is a maximal filter of $\mathcal{L}_1$ and Q is a maximal filter of $\mathcal{L}_2$, then $M = P \times \mathcal{L}_2$ and $M' = \mathcal{L}_1 \times Q$ are maximal filters of $\mathcal{L}$ and $(a, 0), (0, b) \notin J(\mathcal{L})$ for all $a \in \mathcal{L}_1$ and $b \in \mathcal{L}_2$. Let $F = F_1 \times F_2 \neq \{(1, 1)\}$ be a weakly J -filter of $\mathcal{L}$. Suppose $F_1 \neq \mathcal{L}_1$, $F_2 \neq \mathcal{L}_2$ and consider $(1, 1) \neq (x, y) \in F$. Since $(1, 1) \neq (x, 0) \vee_Q (0, y) = (x, y) \in F$ and $(x, 0), (0, y) \notin J(\mathcal{L})$, we conclude that $F = \mathcal{L}$ which is impossible. So we may assume with no loss of generality that $F_1 \neq \mathcal{L}_1$ and $F_2 = \mathcal{L}_2$. Since $F \neq (1, 1)$, we infer that F is a J -filter by Theorem 3.7. It remains to show that F_1 is a J -filter of $\mathcal{L}_1$. Let $a, b \in \mathcal{L}_1$ such that $a \vee b \in F_1$ and $a \notin J(\mathcal{L}_1)$. Then $(a, 0) \vee_Q (b, 0) \in F = F_1 \times \mathcal{L}_2$ and $(a, 0) \notin J(\mathcal{L})$ gives $(b, 0) \in F$ and so $b \in F_1$, as needed.

(2) $\Rightarrow$ (3) We can assume that $F = F_1 \times \mathcal{L}_2$, where F_1 is a J -filter of $\mathcal{L}_1$. Let $(a, b), (c, d) \in \mathcal{L}$ such that $(a, b) \vee_q (c, d) = (a \vee c, b \vee d) \in F$ and $(a, b) \notin J(\mathcal{L})$. Then $a \notin J(\mathcal{L}_1)$ and $a \vee c \in F_1$ which gives $c \in F_1$. Therefore, $(c, d) \in F$ and so F is a J -filter of $\mathcal{L}$. The implication (3) $\Rightarrow$ (1) is clear. $\square$

Suppose $\mathcal{M}$ is a filter of a lattice $\mathcal{L}$ and let $\mathcal{L}(+)\mathcal{M}$ be the filterlization lattice. Let M be a module over a commutative ring R . Anderson and Smith in [2] determine when $P(+)M$ is a weakly prime ideal in $R(+)M$. Now, we will give a similar result for weakly J -filters.

Lemma 3.32. *Let $\mathcal{L}$ and $\mathcal{M}$ be as above. The following hold:*

- (1) *If H is a filter of $\mathcal{L}(+)\mathcal{M}$, then $H = G(+)K$, where G is a filter of $\mathcal{L}$ and K is a subfilter of $\mathcal{M}$;*
- (2) *If G is a filter of $\mathcal{L}$ and K is a subfilter of $\mathcal{M}$, then $G(+)K$ is a filter of $\mathcal{L}(+)\mathcal{M}$ if and only if $G \vee \mathcal{M} \subseteq K$.*
- (3) *$J(\mathcal{L}(+) \mathcal{M}) = J(\mathcal{L})(+) \mathcal{M}$.*

Proof. (1) Set $G = \{x \in \mathcal{L} : (x, m) \in H \text{ for some } m \in \mathcal{M}\}$ and $K = \{m \in \mathcal{M} : (x, m) \in H \text{ for some } x \in \mathcal{L}\}$. Let $x, y \in G$ and $z \in \mathcal{L}$. Then $(x, m), (y, m') \in H$ for some $m, m' \in \mathcal{M}$ implies that $(x \wedge y, m \wedge m') = (x, m) \wedge_F (y, m') \in H$ and $(x \vee z, m \vee z) = (x, m) \vee_F (z, 1) \in H$, as H is a filter; hence $x \wedge y, x \vee z \in G$. Thus G is a filter of $\mathcal{L}$. Similarly, K is a filter of $\mathcal{M}$. Finally, it is easy to see that $H = G(+)K$.

(2) Suppose $H = G(+)K$ is a filter of $\mathcal{L}(+)\mathcal{M}$ and let $g \vee m \in G \vee \mathcal{M}$ for some $g \in G$ and $m \in \mathcal{M}$. Then $(g, 1) \in H$ gives $(g, 1) \vee_F (g, m) = (g, g \vee m) \in H$; so $g \vee m \in K$. Thus, $G \vee \mathcal{M} \subseteq K$. Conversely, assume that $G \vee \mathcal{M} \subseteq K$ and let $(a, n), (b, m) \in H$ and $(c, x) \in \mathcal{L}$. Then $(a, n) \wedge_F (b, m) = (a \wedge b, n \wedge m) \in H$ and $(a, n) \vee_F (c, x) = (a \vee c, (a \vee x) \wedge (n \vee c)) \in H$ since $a \vee x \in G \vee \mathcal{M} \subseteq K$ and $n \vee c \in K$, i.e. H is a filter of $\mathcal{L}(+)\mathcal{M}$.

(3) One can easily show that $G(+)K$ is a maximal filter of $\mathcal{L}(+)\mathcal{M}$ if and only if G is a maximal filter of $\mathcal{L}$, i.e. (3) holds. $\square$

Compare the next theorem with Theorem 2.30 in [16].

Theorem 3.33. *Let $\mathcal{L}$ and $\mathcal{M}$ be as above. If G is a filter of $\mathcal{L}$ and K is a filter of $\mathcal{M}$, then the following hold:*

- (1) *If $G(+)K$ is a weakly J -filter of $\mathcal{L}(+)\mathcal{M}$, then G is a weakly J -filter of $\mathcal{L}$.*
- (2) *$G(+)\mathcal{M}$ is a weakly J -filter of $\mathcal{L}(+)\mathcal{M}$ if and only if G is a weakly J -filter of $\mathcal{L}$ and for $a, b \in \mathcal{L}$ with $a \vee b = 1$ but $a \notin J(\mathcal{L})$ and $b \notin G$, $a, b \in (1 :_{\mathcal{L}} \mathcal{M})$.*

Proof. (1) Clearly, $G \neq \mathcal{L}$. Let $x, y \in \mathcal{L}$ such that $1 \neq x \vee y \in G$ and $x \notin J(\mathcal{L})$. Then $(1, 1) \neq (x, 1) \vee_F (y, 1) = (x \vee y, 1) \in G(+)K$ and $(x, 1) \notin J(\mathcal{L})(+)\mathcal{M} = J(\mathcal{L}(+)\mathcal{M})$ gives $(y, 1) \in G(+)K$, as $G(+)K$ is a weakly J -filter; hence $y \in G$.

(2) Let $G(+)\mathcal{M}$ be a weakly J -filter of $\mathcal{L}(+)\mathcal{M}$. Then G is a weakly J -filter of $\mathcal{L}$ by (1). Now, for $a, b \in \mathcal{L}$, assume that $a \vee b = 1$ but $a \notin J(\mathcal{L})$ and $b \notin G$. On the contrary, suppose that $a \notin (1 :_{\mathcal{L}} \mathcal{M})$. Then $a \vee m \neq 1$ for some $m \in \mathcal{M}$. It follows that $(1, 1) \neq (a, 1) \vee_F (b, m) = (1, a \vee m) \in G(+)\mathcal{M}$ but $(a, 1) \notin J(\mathcal{L})(+)\mathcal{M}$ and so $(b, m) \in G(+)\mathcal{M}$ which is a contradiction. Therefore, $a \in (1 :_{\mathcal{L}} \mathcal{M})$. Similarly, $b \in (1 :_{\mathcal{L}} \mathcal{M})$. Conversely, let $(a, n), (b, m) \in \mathcal{L}(+)\mathcal{M}$ such that $(1, 1) \neq (a, n) \vee_F (b, m) \in G(+)\mathcal{M}$ and $(a, n) \notin J(\mathcal{L}(+)\mathcal{M})$. So $a \vee b \in G$ and $a \notin J(\mathcal{L})$. If $a \vee b \neq 1$, then G is a weakly J -filter gives $b \in G$ and so $(b, m) \in G(+)\mathcal{M}$. So we may assume that $a \vee b = 1$ but $a \notin J(\mathcal{L})$ and $b \notin G$. By the hypothesis, $a, b \in (1 :_{\mathcal{L}} \mathcal{M})$ and then $(a, n) \vee_F (b, m) = (1, 1)$ which is impossible. Therefore, $a \vee b \neq 1$ and clearly $G(+)\mathcal{M}$ is a weakly J -filter of $\mathcal{L}(+)\mathcal{M}$, as required. $\square$

References

- [1] M. F. Atiyah and I. G. MacDonald, *Introduction to Commutative Algebra*, Addison-Wesley, Reading, MA, 1969.
- [2] D. D. Anderson and E. Smith, *Weakly prime ideals*, Houston J. Math., 29 (4): 831-840, 2003.
- [3] D. D. Anderson and M. Axtell, *When are associates unit multiples*, Rocky Mountain J. Math., 34 (3): 811-828, 2004.
- [4] F. A. A. Almahdi, E. M. Bouba and M. Tamekkante, *On weakly S -prime ideals of commutative rings*, An. St. Univ. Ovidius Constanta, 29 (2): 173-186, 2021.
- [5] G. Birkhoff, *Lattice theory*, Amer. Math. Soc., 197).
- [6] A. Bouvier, *Anneaux presimplifiables et anneaux atomiques*, C.R. Acad. Sci. Paris S´er. A-B 272: 992-994, 1971.
- [7] G. Călugăreanu, *Lattice Concepts of Module Theory*, Kluwer Academic Publishers, 2000.
- [8] S. Ebrahimi Atani and M. sedghi Shanbeh Bazari, *On 2-absorbing filters of lattices*, Discuss. Math. Gen. Algebra Appl., 36: 157-168, 2016.
- [9] S. Ebrahimi Atani, M. Khoramdel and M. Chenari, *The small intersection graph of filters of a bounded distributive lattice*, Journal of Mahani Mathematical Research, 12 (1): 311-326, 2023.
- [10] S. Ebrahimi Atani, *G-Supplemented property in the lattices*, Mathematica Bohemica, 147 (4): 525-545, 2022.
- [11] S. Ebrahimi Atani, *On Baer filters of bounded distributive lattices*, Quasigroups and Related Systems, 32: 1-20, 2024.
- [12] S. Ebrahimi Atani, *S-prime property in lattices*, Mathematica, 66 (89): 168-187, 2024.
- [13] S. Ebrahimi Atani, *J-filters of bounded lattices*, Eur. J. Math. Appl. (2024) 4:12. DOI: 10.28919/ejma.2024.4.12.
- [14] J. A. Huckaba, *Commutative Rings with Zero divisors*, New York, Marcel Dekker, 1988.
- [15] H. A. Khashan and A. B. Bani-Ata, *J-ideals of commutative rings*, Int. Electron. J. Algebra, 29: 148-164, 2021.
- [16] H. A. Khashan and E. Y. Celikel, *weakly J-ideals of commutative rings*, Filomat, 36 (2): 485-495, (2022).
- [17] R. Mohamadian, *r-Ideals in commutative rings*, Turkish J. Math., 39: 733-749, (2015).
- [18] Ü. Tekir, S. Koc and K. H. Oral, *n-Ideals of commutative rings*, Filomat, 31 (10): 2933-2941, 2017.



ISSN: 2820-7114

Moroccan Journal of Algebra and Geometry with Applications

Supported by Sidi Mohamed Ben Abdellah University, Fez, Morocco

Volume 4, Issue 2 (2025), pp 259-267

Title :

On quasi n -absorbing submodules

Author(s):

Malik Tusif Ahmed, Mohammed Issoual & Mohammed Tamekkante

On quasi n -absorbing submodules

Malik Tusif Ahmed¹, Mohammed Issoual² and Mohammed Tamekkante³

¹ Department of Mathematics and Statistics, Hazara University Mansehra, KPK, Pakistan.

e-mail: tusifahmed@hu.edu.pk

² CRMEF Fès-Meknès, Morocco.

e-mail: issoual2@yahoo.fr

³ Department of Mathematics, Faculty of Science, Box 11201 Zitoune, University Moulay Ismail Meknes, Morocco.

e-mail: tamekkante@yahoo.fr

Communicated by Moutu Abdou Salam Moutui

(Received 20 September 2024, Revised 15 May 2025, Accepted 27 May 2025)

Abstract. Let R be a commutative ring with $1 \neq 0$, M be an R -module, and n be a positive integer. The purpose of this article is to investigate quasi n -absorbing (resp., weakly quasi n -absorbing) submodules generalizing quasi n -absorbing ideals of rings. We will say a proper submodule N of M is quasi n -absorbing (resp., weakly quasi n -absorbing) submodule of M if whenever $a \in R$ and $x \in M$ with $a^n x \in N$, (resp., $0 \neq a^n x \in N$) then, either $a^n \in (N :_R M)$ or $a^{n-1}x \in N$.

Key Words: n -absorbing ideals, n -absorbing submodules, quasi n -absorbing ideals, quasi n -absorbing submodules.

2010 MSC: 13C13, 13A15.

Dedicated to our Professor David E. Dobbs for his 80th Birthday

1 Introduction

In this paper, all rings are commutative with non-zero identity and all modules are unital. Let R be a ring, M an R -module and N a submodule of M . We will denote by $(N :_R M)$ the residual of N by M , that is, the set of all $r \in R$ such that $rM \subseteq N$. The $\text{ann}_R(M)$ is $(0 :_R M)$. An R -module M is called a multiplication module if every submodule N of M has the form IM for some ideal I of R . In this case, since $I \subseteq (N :_R M)$ then $N = IM \subseteq (N :_R M)M \subseteq N$. So that $N = (N :_R M)M$ [15].

A submodule N of M is called idempotent if $N = (N :_R M)N$, [3]. It is shown [4 Theorem 3] that if M is a multiplication module and $(N :_R M)$ is idempotent ideal of R then N is idempotent in M . The converse is true if we assume further that M is finitely generated and faithful. A submodule N of the R -module M is called a nilpotent submodule if $(N :_R M)^p N = 0$ for some positive integer p , and $m \in M$ is said to be nilpotent if Rm is a nilpotent submodule of M , [3]. Set $\text{Nil}(M)$ the set of all nilpotent elements of M . Then, $\text{Nil}(M)$ is a submodule of M provided that M is faithful module, and in addition M is multiplication, then $\text{Nil}(M) = \text{Nil}(R)M = \bigcap P$, where the intersection runs over all prime submodules of M , [3 Theorem 6]. A submodule N of M is prime (resp., primary) if whenever $ax \in N$ for some $a \in R$ and $x \in M$, then either $a \in (N :_R M)$ or $x \in N$ (resp., $a^p \in (N :_R M)$ for some positive integers p). If N is prime (resp., primary) submodule of M , then $P := (N :_R M)$ (resp., $P := \sqrt{(N :_R M)}$) is a prime ideal of R . In this case, we say that N is a P -prime (resp., P -primary) submodule of M . We say that M is *secondary* precisely when, for each $a \in R$, either $aM = M$ or there exists $p \in \mathbb{N}$ such that $a^p M = 0$. When this is the case, $P := \sqrt{(0 :_R M)}$ is a prime ideal of R : we say that M is P -secondary R -module.

In [7] Badawi introduced a new generalization of prime ideals in a commutative ring R . He defined a nonzero proper ideal I of R to be a 2-absorbing ideal if whenever $a, b, c \in R$ and $abc \in I$, then $ab \in I$ or

$ac \in I$ or $bc \in I$. This concept has a generalization, called weakly 2-absorbing ideals, which has been studied in [8]. A proper ideal I of R to be weakly 2-absorbing ideal of R if whenever $a, b, c \in R$ and $0 \neq abc \in I$, then $ab \in I$ or $ac \in I$ or $bc \in I$. Later Anderson and Badawi in [5], introduced the concept of n -absorbing ideals of R for a positive integer n . A proper ideal I of R is called n -absorbing (resp., strongly n -absorbing) ideal if whenever $a_1 \dots a_{n+1} \in I$ for $a_1, \dots, a_{n+1} \in R$ (resp., $I_1 \dots I_{n+1} \subseteq I$ for ideals $I_1, \dots, I_{n+1}$ of R), then there are n of the a_i 's (resp., n of the I_i 's) whose product is in I . Inspired by the study of absorbing ideals, in [14] Mukhtar et al. and later in [1] Ahmed et al. introduced and studied, respectively, the 2-absorbing factorization and n -absorbing factorization in commutative rings. In [13] H. Mostafanasab and A.Y. Darani introduced the notion of quasi- n -absorbing and semi n -absorbing ideals of a commutative ring. A proper ideal I of a commutative ring is said to be a quasi- n -absorbing (resp., semi n -absorbing) if whenever $a^n b \in I$ for $a, b \in R$, then either $a^n \in I$ or $a^{n-1} b \in I$ (resp., $a^{n+1} \in I$ for $a \in R$, then $a^n \in I$).

The concept of 2-absorbing (resp., weakly 2-absorbing) submodules was introduced and investigated in [10]. Let M be an R -module and N a proper submodule of M . N is said to be a 2-absorbing submodule (resp., weakly 2-absorbing submodule) of M if whenever $a, b \in R$ and $x \in M$ such that $abx \in N$ (resp., $0 \neq abx \in N$), then $ab \in (N :_R M)$ or $ax \in N$ or $bx \in N$. This concept has a generalization, called n -absorbing submodule introduced and investigated in [11]. Let n be a positive integer. A proper submodule N of an R -module M is called n -absorbing submodule if whenever $a_1 \dots a_n x \in N$ for $a_1, \dots, a_n \in R$ and $x \in M$ (resp., $I_1 \dots I_n L \subseteq N$ for ideals $I_1, \dots, I_n$ of R and submodule L of M), then either $a_1 \dots a_n \in (N :_R M)$ (resp., $I_1 \dots I_n \subseteq (N :_R M)$) or there are $n-1$ of a_i 's (resp., I_i 's) whose product with x (resp., with L) is in N . A proper submodule N of M is called an quasi n -absorbing (resp., weakly quasi n -absorbing) submodule of M if whenever $a^n x \in N$ for $a \in R$ and $x \in M$ (resp., $0 \neq a^n x \in N$) then either $a^n \in (N :_R M)$ or $a^{n-1} x \in N$. It is clear that if N is an n -absorbing submodule it is also a quasi n -absorbing submodule of M . But the converse is not true in general case, take for example $N = 30\mathbb{Z}$ as submodule of the $\mathbb{Z}$ -module $\mathbb{Z}$, we have N is not 2-absorbing submodule, but is quasi 2-absorbing submodule of $\mathbb{Z}$ (Proposition 2.14) and $N = 0$ is weakly quasi 2-absorbing submodule of the $\mathbb{Z}$ -module $\mathbb{Z}$ which is not quasi 2-absorbing submodule.

Thus, if N is a submodule of the R -module M , then " N is a prime submodule of M " implies " N is an n -absorbing submodule of M " implies " N is a quasi n -absorbing submodule of M ".

In this paper, we study the concept of quasi n -absorbing submodule and weakly quasi n -absorbing submodule, for a positive integer n .

2 Properties of quasi n -absorbing submodules

In this section we study some basic properties of quasi n -absorbing submodules of the R -module M . Let n be a positive integer. We recall that a proper submodule N of M is called quasi n -absorbing submodule of M , if whenever $a \in R$ and $x \in M$ with $a^n x \in N$, then $a^n \in (N :_R M)$ or $a^{n-1} x \in N$.

Let R be a ring, M be an R -module, N be a submodule of M , and I be an ideal of R . We set $(N :_M I) = \{x \in M \mid xI \subseteq N\}$.

Theorem 2.1. Let R be a ring, M an R -module and N be a submodule of M . Then the following statements are equivalent:

- (1) N is a quasi n -absorbing submodule of M .
- (2) For each $a \in R$ with $a^n \notin (N :_R M)$, we have $(N :_M a^n) = (N :_M a^{n-1})$.
- (3) For each $a \in R$ and every submodule L of M with $a^n L \subseteq N$, either $a^n \in (N :_R M)$ or $a^{n-1} L \subseteq N$.

Proof. (1) $\Rightarrow$ (2) It is clear that $(N :_R a^{n-1}) \subseteq (N :_R a^n)$ for every $a \in R$. Let $a \in R$ such that $a^n \notin (N :_R M)$ and $x \in (N :_M a^n)$. Since N is a quasi n -absorbing submodule, $a^{n-1} x \in N$. Hence $x \in (N :_M a^{n-1})$.

(2) $\Rightarrow$ (3) Let $a \in R$ and L be a submodule of M such that $a^n L \subseteq N$. Suppose that $a^n \notin (N :_R M)$. By (2), for each $x \in L$, we have $a^{n-1}x \in N$. Thus, $a^{n-1}L \subseteq N$.

(3) $\Rightarrow$ (1) Assume that $a^n x \in N$ for some $a \in R$ and $x \in M$. By leading $L = Rx$, we obtain the desired result. $\square$

Corollary 2.2. *Let R be a ring and M be an R -module. Then 0 is a quasi n -absorbing submodule of M if and only if for each $a \in R$, either $a^n \notin \text{ann}_R(M)$ or $\text{ann}_M(a^n) = \text{ann}_M(a^{n-1})$.*

Corollary 2.3. *Let M be an R -module and N be a quasi n -absorbing submodule of M . Then $(N :_R M)$ is a quasi n -absorbing ideal of R .*

Proof. Let $a, b \in R$ such that $a^n b \in (N :_R M)$. If $a^n \notin (N :_R M)$, by Theorem 2.1, we have $b \in (N :_R a^{n-1}) = (N :_R a^n)$. So $a^{n-1}b \in N$, and hence $(N :_R M)$ is a quasi n -absorbing ideal of R . $\square$

Corollary 2.4. *Let R be a ring and I be a proper ideal of R . Then the following statements hold:*

- (1) I is a quasi n -absorbing ideal of R .
- (2) For each $a \in R$ with $a^n \notin I$, we have $(I :_R a^n) = (I :_R a^{n-1})$.
- (3) For each $a \in R$ and every ideal J of R with $a^n J \subseteq I$, either $a^n \in I$ or $a^{n-1}J \subseteq I$.

Example 2.5. The converse of the corollary 2.3 is not true in general. For example, consider $N = 8\mathbb{Z}$ as a submodule of $\mathbb{Z}$ -module $\mathbb{Z}$. While $(N :_{\mathbb{Z}} \mathbb{Z}) = 8\mathbb{Z}$ is clearly a quasi 2-absorbing ideal of $\mathbb{Z}$, N is not quasi 2-absorbing. In fact $2^2 \cdot 2 \in N$, but $2^2 \notin N$ and $2 \cdot 2 \notin (N :_{\mathbb{Z}} \mathbb{Z})$.

Theorem 2.6. *Let M be a cyclic R -module. Then for every submodule N of M the following statements are equivalent:*

- (1) N is a quasi n -absorbing submodule of M .
- (2) $(N :_R M)$ is a quasi n -absorbing ideal of R .

Proof. Following Corollary 2.3 it suffices to prove (2) $\Rightarrow$ (1). Set $M = Rm$. Assume that $(N :_R M)$ is a quasi n -absorbing ideal of R . Let $a \in R$ and $x \in M$ such that $a^n x \in N$. There exists $b \in R$ such that $x = bm$. Thus $a^n bm \in N$. So $a^n b \in (N :_R m) = (N :_R M)$. Since $(N :_R M)$ is a quasi n -absorbing ideal of R , we conclude that $a^n \in (N :_R M)$ or $a^{n-1}b \in (N :_R M)$. Hence $a^n \in (N :_R M)$ or $a^{n-1}bm = a^{n-1}x \in N$, that is, N is quasi n -absorbing submodule of M . $\square$

Corollary 2.7. *Let R be a Von Neumann regular ring, M be a cyclic R -module and n be a positive integer. Then every submodule of M is quasi n -absorbing.*

Proof. Since every ideal of R is radical, it is clear that every ideal of R is quasi n -absorbing. Hence, the result follows from the theorem 2.6. $\square$

Theorem 2.8. *Let R be a ring and M be a multiplication non-torsion R -module. If every submodule of M is quasi n -absorbing, then $\dim(M) = 0$.*

Proof. Suppose that $\dim(M) \geq 1$. There exists a prime submodule N of M and a submodule L of M such that $N \subset L$. Since M is a multiplication non torsion module, then $(N :_R M)$ is a prime ideal of R and $(N :_R M) \subset (L :_R M)$. Let $a \in (L :_R M) \setminus (N :_R M)$. Since M is multiplication non-torsion R module, there exists a submodule K of M such that $J := (K :_R M) = a^{n+1}R$. Then $a^{n+1}R$ is quasi n -absorbing ideal of R , and $a^n \cdot a \in J$ so $a^n \in J$ and there exists $b \in R$ with $a^n = a^{n+1}b$. Hence $a^n(1 - ab) = 0 \in (N :_R M)$ and $a^n \notin (N :_R M)$, thus $1 - ab \in (N :_R M) \subset (L :_R M)$ and $a \in (L :_R M)$ we conclude that $1 \in (L :_R M)$ a contradiction. Thus $\dim(M) = 0$. $\square$

Corollary 2.9. Let R be a ring. If every ideal of R is n -absorbing, then $\dim R = 0$.

Definition 2.10. Let $m > n$ be positive integers. A proper submodule N of a R -module M is called quasi (m, n) -absorbing if whenever $a^{m-1}x \in N$ for $a \in R$ and $x \in M$, then $a^n \in (N :_R M)$ or $a^{n-1}x \in N$.

Theorem 2.11. Let N be a proper submodule of a R -module M and $m > n$ positive integers. Then N is quasi (m, n) -absorbing if and only if it is quasi n -absorbing.

Proof. Assume that N is quasi (m, n) -absorbing. Let $a^n x \in N$ for some $a \in R$ and $x \in M$. Since $n \leq m-1$, then $a^{m-1}x \in N$. Therefore $a^n \in (N :_R M)$ or $a^{n-1}x \in N$. Hence N is quasi n -absorbing submodule. Conversely, assume that N is quasi n -absorbing. Let $a^{m-1}x \in N$ for some $a \in R$ and $x \in M$. Therefore $a^n(a^{m-1-n}x) \in N$. Hence $a^n \in (N :_R M)$ or $a^{n-1}(a^{m-1-n}x) = a^{m-2}x \in N$. Repeating the same argument we conclude that $a^n \in (N :_R M)$ or $a^{n-1}x \in N$. Thus N is a quasi (m, n) -absorbing submodule of M . $\square$

Corollary 2.12. [13 Proposition 3.8]. Let I be a proper ideal of a ring R and $m > n$ be positive integers. Then, I is a quasi (m, n) -absorbing ideal if and only if I is a quasi n -absorbing ideal of R .

Proposition 2.13. Let N be proper submodule of an R -module M .

- (1) N is a prime submodule if and only if it is a quasi 1-absorbing submodule of M .
- (2) If N is a quasi n -absorbing submodule then it is an i -absorbing submodule for all $i \geq n$.
- (3) If N is a prime submodule then it is a quasi n -absorbing for all $n \geq 1$.
- (4) If N is an n -absorbing submodule then it is a quasi n -absorbing.

Proof. Clear. $\square$

Proposition 2.14. Let R be a ring and M be an R -module. Let $\{N_\lambda\}_{\lambda \in \Lambda}$ be a family of prime submodules of M . Then $\cap_{\lambda \in \Lambda} N_\lambda$ is a quasi i -absorbing submodule for every $i \geq 2$.

Proof. Let $N = \cap_{\lambda \in \Lambda} N_\lambda$. By Proposition 2.13, it is sufficient to show that N is a quasi 2-absorbing submodule of M . Indeed, let $a \in R$ and $x \in M$ with $a^2x = a(ax) \in N = \cap_{\lambda \in \Lambda} N_\lambda$. Since N_λ is prime submodule of M and $a^2x = a(ax) \in N_\lambda$, then either $a \in (N_\lambda :_R M)$ or $ax \in N_\lambda$. In either case $ax \in N$. Hence N is a quasi 2-absorbing submodule of M . $\square$

Remark 2.15. Let $p_1, \dots, p_{n+1}$ distinct prime numbers. Set $N_i = p_i \mathbb{Z}$ for $1 \leq i \leq n+1$. It is clear that N_i is a prime submodule of the $\mathbb{Z}$ -module $\mathbb{Z}$. By Proposition 2.14, we have $N = \cap_{i=1}^{n+1} N_i$ is a quasi i -absorbing submodule for every positive integers $i \geq 2$. But N is not a n -absorbing submodule of M by Corollary 2.3 since $(N :_{\mathbb{Z}} \mathbb{Z}) = \cap_{i=1}^{n+1} p_i \mathbb{Z}$ is a $n+1$ -absorbing ideal but not a n -absorbing ideal of $\mathbb{Z}$, cf. [5, corollary 2.15].

Corollary 2.16. Let R be a ring, M be a faithful and multiplication R -module. Then $\text{Nil}(M)$ is a quasi i -absorbing submodule of M for every positive integer $i \geq 2$.

Proof. By [3 Theorem 6], we have $\text{Nil}(M) = \cap_{P \text{ prime}} P$. Now the results follows from Proposition 2.14. $\square$

Theorem 2.17. Let $N_1, \dots, N_t$ be submodules of an R -module M .

- (1) If N_1 is quasi n -absorbing and N_2 is quasi m -absorbing for $m < n$, then $N_1 \cap N_2$ is quasi $n+1$ -absorbing.
- (2) If $N_1, \dots, N_t$ are quasi n -absorbing, then $N_1 \cap N_2 \cdots \cap N_t$ is quasi $n+t$ -absorbing.

- (3) If $N_1, \dots, N_t$ are quasi n_i -absorbing, for every $1 \leq i \leq t$ with $n_1 < n_2 < \dots < n_t$ and $t > 2$, then $N_1 \cap N_2 \cap \dots \cap N_t$ is quasi $n_t + 2$ -absorbing.

Proof. 1. Let $a \in R$ and $x \in M$ such that $a^{n+1}x \in N_1 \cap N_2$. We will show that either $a^{n+1} \in (N_1 \cap N_2 :_R M)$ or $a^n x \in N_1 \cap N_2$. Since N_1 is a quasi n -absorbing submodule of M , then by Theorem 2.11 it is quasi $(n+2, n)$ -absorbing. Therefore either $a^n \in N_1$ or $a^{n-1}x \in N_1$. On the other hand N_2 is a quasi m -absorbing submodule of M and by Theorem 2.11 either $a^m \in (N_2 :_R M)$ or $a^{m-1}x \in N_2$. There are four cases:

Case 1. Assume that $a^n \in (N_1 :_R M)$ and $a^m \in (N_2 :_R M)$. Then $a^n \in (N_1 \cap N_2 :_R M)$.

Case 2. Assume that $a^n \in (N_1 :_R M)$ and $a^{m-1}x \in N_2$. Then $a^n x \in N_1 \cap N_2$.

Case 3. Assume that $a^{n-1}x \in N_1$ and $a^m \in (N_2 :_R M)$. Then $a^{n-1}x \in N_1 \cap N_2$.

Case 4. Assume that $a^{n-1}x \in N_1$ and $a^{m-1}x \in N_2$. Then $a^{n-1}x \in N_1 \cap N_2$.

In any case, we conclude that $a^n x \in N_1 \cap N_2$ and therefore $N_1 \cap N_2$ is a quasi $n+1$ -absorbing submodule of M .

2. By induction on t : For $t = 1$ there is nothing to prove. Let $t > 1$ and suppose the claim holds for $t-1$. Then $N_1 \cap \dots \cap N_{t-1}$ is a quasi $n+t-1$ -absorbing submodule of M . Since N_t is a quasi n -absorbing submodule and $n+t-2 \geq n$, then N_t is a quasi $n+t-2$ -absorbing submodule. Now the result follows from (1).

3. By induction on $t \geq 3$. The case of $t = 3$ is deduced from (1) and (2). Let $t > 3$ and suppose that for $t-1$ the claim holds. Then $N_1 \cap N_2 \cap \dots \cap N_{t-1}$ is a quasi $n_{t-1} + 2$ -absorbing submodule. There are three cases:

Case 1. Assume that $n_{t-1} + 2 < n_t$. Then $N_1 \cap N_2 \cap \dots \cap N_t$ is quasi $n_t + 1$ -absorbing submodule from (1). Therefore $N_1 \cap N_2 \cap \dots \cap N_t$ is a quasi $n_t + 2$ -absorbing submodule of M .

Case 2. Assume that $n_{t-1} + 2 = n_t$. Then $N_1 \cap N_2 \cap \dots \cap N_t$ is a quasi $n_t + 2$ -absorbing submodule of M .

Case 3. Assume that $n_{t-1} + 2 > n_t$, in this case $n_{t-1} + 1 = n_t$ because $n_{t-1} < n_t$. Then $N_1 \cap N_2 \cap \dots \cap N_t$ is a quasi $n_{t-1} + 3 = n_t + 2$ -absorbing submodule of M .

□

Proposition 2.18. Let $M = M_1 \oplus M_2$ where M_1 and M_2 are R -modules. Let N_1 a proper submodule of M_1 and N_2 a proper submodule of M_2 . Then N_1 (resp. N_2) is a quasi n -absorbing submodule of M_1 (resp. M_2) if and only if $N_1 \oplus M_2$ (resp. $M_1 \oplus N_2$) is a quasi n -absorbing submodule of M .

Proof. ($\Rightarrow$) Suppose that N_1 is a quasi n -absorbing submodule of M_1 . Let $a^n(x, y) \in N_1 \oplus M_2$ for some $a \in R$ and $(x, y) \in M$. Therefore $a^n x \in N_1$, and so either $a^n \in (N_1 :_R M_1)$ or $a^{n-1}x \in N_1$. Consequently, either $a^n \in [N_1 \oplus M_2 :_R M]$ or $a^{n-1}(x, y) \in N_1 \oplus M_2$. Hence $N_1 \oplus M_2$ is a quasi n -absorbing submodule of M .

($\Leftarrow$) Assume that $N_1 \oplus M_2$ is a quasi n -absorbing submodule of M . Let $a^n x \in N_1$ for some $a \in R$ and $x \in M_1$. Then $a^n(x, 0) \in N_1 \oplus M_2$. Hence $a^n \in [N_1 \oplus M_2 :_R M] = [N_1 :_R M_1]$ or $a^{n-1}(x, 0) \in N_1 \oplus M_2$. Therefore $a^n \in [N_1 :_R M_1]$ or $a^{n-1}x \in N_1$. That is N_1 is quasi n -absorbing submodule of M_1 . □

Theorem 2.19. Let $N_1, \dots, N_t$ be submodules of R -modules $M_1, M_2, \dots, M_t$ respectively.

- (1) If N_1 is a quasi n -absorbing submodule of M_1 and N_2 is a quasi m -absorbing submodule of M_2 for $m < n$, then $N_1 \oplus N_2$ is a quasi $n+1$ -absorbing submodule of $M_1 \oplus M_2$.
- (2) If $N_1, \dots, N_t$ are quasi n -absorbing submodules of $M_1, M_2, \dots, M_t$ respectively, then $N_1 \oplus N_2 \oplus \dots \oplus N_t$ is a quasi $n+t$ -absorbing submodule of $M_1 \oplus M_2 \oplus \dots \oplus M_t$.

- (3) If N_i is a quasi n_i -absorbing submodule of M_i for every $1 \leq i \leq t$ with $n_1 < n_2 < \dots < n_t$ and $t > 2$, then $N_1 \oplus N_2 \oplus \dots \oplus N_t$ is a quasi $n_t + t$ -absorbing submodule of $M_1 \oplus M_2 \oplus \dots \oplus M_t$.

Proof. 1. Let $a \in R$ and $(x, y) \in M_1 \oplus M_2$ such that $a^{n+1}(x, y) \in N_1 \oplus N_2$. Therefore $a^{n+1}x = a^n(ax) \in N_1$ and $a^{n+1}y \in N_2$. Since N_1 is a quasi n -absorbing submodule of M_1 , then $a^n \in (N_1 :_R M_1)$ or $a^n x \in N_1$. Also, N_2 is a quasi m -absorbing submodule of M_2 and $a^{n+1}y = a^m(a^{n+1-m}y) \in N_2$, so $a^m \in (N_2 :_R M_2)$ or $a^{m-1}(a^{n+1-m}y) = a^n y \in N_2$.

Consider the following cases.

Case 1. Assume that $a^n \in (N_1 :_R M_1)$ and $a^m \in (N_2 :_R M_2)$. Then $a^n \in (N_1 \oplus N_2 :_R M_1 \oplus M_2)$.

Case 2. Assume that $a^n \in (N_1 :_R M_1)$ and $a^n y \in N_2$. Then $a^n(x, y) \in N_1 \oplus N_2$.

Case 3. Assume that $a^n x \in N_1$ and $a^m \in (N_2 :_R M_2)$. Then $a^n(x, y) \in N_1 \oplus N_2$.

Case 4. Assume that $a^n x \in N_1$ and $a^n y \in N_2$. Then $a^n(x, y) \in N_1 \oplus N_2$.

We conclude that $N_1 \oplus N_2$ is a quasi $n + 1$ -absorbing submodule of M .

2. We use induction on t . For $t = 1$ the claim is follows from (1). Let $t > 1$ and assume that for $t - 1$ the claim holds. That is $N_1 \oplus N_2 \oplus \dots \oplus N_{t-1}$ is a quasi $n + t - 1$ -absorbing submodule of $M_1 \oplus M_2 \oplus \dots \oplus M_{t-1}$. As N_t is a quasi n -absorbing submodule of M_t , so it is a quasi $(n + t - 2)$ -absorbing submodule of M_t . Therefore $N_1 \oplus N_2 \oplus \dots \oplus N_{t-1} \oplus N_t$ is a quasi $n + t$ -absorbing submodule of $M_1 \oplus M_2 \oplus \dots \oplus M_{t-1} \oplus M_t$.

3. We use induction on t . The results for $t = 3$ follows from (1) and (2). Let $t > 3$ and suppose that for $t - 1$ the claim holds. Then $N_1 \oplus N_2 \oplus \dots \oplus N_{t-1}$ is a quasi $n_{t-1} + 2$ -absorbing submodule of $M_1 \oplus M_2 \oplus \dots \oplus M_{t-1}$. We consider the following cases:

Case 1. If $n_{t-1} + 2 < n_t$. In this case $N_1 \oplus \dots \oplus N_t$ is a quasi $n_t + 1$ -absorbing submodule of $M_1 \oplus \dots \oplus M_t$ by (1). Hence $N_1 \oplus \dots \oplus N_t$ is a quasi $n_t + 2$ -absorbing submodule of $M_1 \oplus \dots \oplus M_t$.

Case 2. If $n_{t-1} + 2 = n_t$. Then $N_1 \oplus \dots \oplus N_t$ is a quasi $n_t + 2$ -absorbing submodule of $M_1 \oplus M_2 \oplus \dots \oplus M_t$ by (2).

Case 3. If $n_{t-1} + 2 > n_t$. Then $N_1 \oplus \dots \oplus N_t$ is a quasi $n_{t-1} + 3$ -absorbing submodule of $M_1 \oplus M_2 \oplus \dots \oplus M_t$ by (1). Since $n_{t-1} + 1 = n_t$, because $n_{t-1} < n_t$. We conclude that $N_1 \oplus \dots \oplus N_t$ is a quasi $n_t + 2$ -absorbing submodule of $M_1 \oplus M_2 \oplus \dots \oplus M_t$. □

Theorem 2.20. Let M be an R -module and N a P -primary submodule of M such that $P^n M \subseteq N$. Then N is a quasi n -absorbing submodule of M . In particular, if M is a multiplication module and $P^n M$ is a P -primary submodule of M , then $P^n M$ is a quasi n -absorbing submodule of M .

Proof. Let $a \in R$ and $x \in M$ such that $a^n x = a \cdot a^{n-1} x \in N$ and $a^{n-1} x \notin N$. Since N is a P -primary submodule, we conclude that $a \in P = \sqrt{(N :_R M)}$. Hence $a^n \in P^n \subseteq (N :_R M)$. Thus N is a quasi n -absorbing submodule of M . The in particular is clear. □

Theorem 2.21. If N is a secondary submodule of an R -module M and L is a quasi n -absorbing submodule of M . Then $N \cap L$ is also a secondary submodule of M .

Proof. Assume that N is P -secondary where $P := \sqrt{(0 :_R N)}$, and let $a \in R$. If $a \in P$ and since $(0 :_R N) \subseteq (0 :_R N \cap L)$ we conclude that $a \in \sqrt{(0 :_R N \cap L)}$. If $a \notin P$, then $aN = N$, so $a^n N = N$. Let $x \in N \cap L$, there exists $y \in N$ with $x = a^n y$. Thus $a^n y \in L$, but L is quasi n -absorbing submodule we get either $a^n \in (L :_R M)$ or $a^{n-1} y \in L$. If $a^n \in (L :_R M)$ then $a^n M \subseteq L$, on the other hand $N = a^n N \subseteq a^n M \subseteq L$ so $a(N \cap L) = aN = N = N \cap L$. If $a^{n-1} y \in L$, then $x = a^n y \in aL$, and $x \in a(N \cap L)$ hence $a(N \cap L) = N \cap L$. Which is the desired conclusion. □

Proposition 2.22. Let $f : M \rightarrow M'$ be a homomorphism of R -modules. Then we have the following

- (1) If N' is a quasi n -absorbing submodule of M' , then $f^{-1}(N')$ is a quasi n -absorbing submodule of M .
- (2) If f is an epimorphism and N is a quasi n -absorbing submodule of M containing $\ker(f)$, then $f(N)$ is quasi n -absorbing submodule of M' .

Proof. 1. Let N' be a quasi n -absorbing submodule of M' and $a^n x \in f^{-1}(N')$ for some $a \in R$ and $x \in M$. Then $f(a^n x) = a^n f(x) \in N'$, and therefore, either $a^n \in (N' :_R M')$ or $a^{n-1} f(x) = f(a^{n-1} x) \in N'$. Thus $a^n \in (f^{-1}(N') :_R M)$ or $a^{n-1} x \in f^{-1}(N')$, as desired.

2. Let $a \in R$ and $x' \in M'$ such that $a^n x' \in f(N)$. Since f is an epimorphism, so there exists $x \in M$ such that $x' = f(x)$ and $a^n x' = a^n f(x) = f(a^n x) \in f(N)$. Also $\ker(f) \subseteq N$ implies that $a^n x \in N$. As N is a quasi n -absorbing submodule of M , either $a^n \in (N :_R M)$ or $a^{n-1} x \in N$. Therefore either $a^n \in (f(N) :_R M')$, as f is an epimorphism, or $a^{n-1} x' \in f(N)$. Thus $f(N)$ is a quasi n -absorbing submodule of M' . □

Let R be a ring and M an R -module. Then $R(M) := R \propto M = \{(a, x)/a \in R, x \in M\}$, with multiplication $(a, x)(b, y) = (ab, ay + bx)$ and with point wise addition, is a commutative ring with identity, called the idealization of an R -module M . Let I be an ideal of R and N be a submodule of M , then $I \propto N$ is an ideal of $R(M)$ if and only if $IM \subseteq N$, i.e. $I \subseteq (N :_R M)$.

Theorem 2.23. Let R be a ring, M an R -module and $n > 1$ a positive integer.

- (1) For an ideal I of R and a submodule N of M . If $I \propto N$ is a quasi n -absorbing ideal of $R(M)$, then I is a quasi n -absorbing ideal of R and N is a quasi n -absorbing submodule of M . In particular I is quasi n -absorbing ideal of R if and only if $I \propto M$ is a quasi n -absorbing ideal of $R(M)$.
- (2) Assume that $\mathbb{Q} \subseteq R$. If N is a quasi $n-1$ -absorbing submodule of M and I is a quasi n -absorbing ideal of R , then $I \propto N$ is a quasi $n+1$ -absorbing ideal of $R(M)$.
- (3) Assume that R is an integral domain, then $0 \propto N$ is a quasi n -absorbing ideal of $R(M) := R \propto M$ if and only if N is a quasi n -absorbing submodule of M and $(N :_R M)$ is a semi $n-1$ -absorbing ideal of R .
- (4) Assume that R is an integral domain and M is a K -vector space where K is the quotient field of R . Then $0 \propto N$ is a quasi n -absorbing ideal of $R(M)$ if and only if N is a K -subspace of M . Furthermore, the quasi n -absorbing ideals of $R(M)$ are either of the form $I \propto M$, where I is a quasi n -absorbing ideal of R , or $0 \propto N$, where N is a K -subspace of M .

Proof. 1. Assume that $I \propto N$ is an quasi n -absorbing ideal of $R(M)$. Let $a, b \in R$ such that $a^n b \in I$, then $(a, 0)^n(b, 0) \in I \propto N$. Since $I \propto N$ is a quasi n -absorbing ideal, therefore $(a, 0)^n \in I \propto N$ or $(a, 0)^{n-1}(b, 0) \in I \propto N$. Hence $a^n \in I$ or $a^{n-1}b \in I$, that is, I is quasi n -absorbing ideal of R . Now let $a \in R$ and $x \in M$ such that $a^n x \in N$, then $(a, 0)^n(0, x) \in I \propto N$. As $I \propto N$ is quasi n -absorbing ideal of $R(M)$, so $(a, 0)^n \in I \propto N$ or $(a, 0)^{n-1}(0, x) \in I \propto N$. Consequently, $a^n \in I \subseteq (N :_R M)$ or $a^{n-1}x \in N$, that is N is a quasi n -absorbing submodule of M .

2. Let $(a, e), (b, f) \in R(M)$ such that $(a, e)^{n+1}(b, f) = (a^{n+1}b, (n+1)a^n be + a^{n+1}f) \in I \propto N$. Then $a^{n+1}b \in I$ and $(n+1)a^n be + a^{n+1}f \in N$. Therefore, since I is a quasi n -absorbing ideal of R , $a^n \in I$ or $a^{n-1}b \in I$. If $a^n \in I$, then $(a, e)^{n+1} = (a^{n+1}, (n+1)a^n e) \in I \propto N$ because $IM \subseteq N$. If $a^{n-1}b \in I$, then $a^{n+1}f = a^{n-1}(a^2 f) \in N$. Consequently, as N is quasi $n-1$ -absorbing submodule of M , $a^n f \in N$. In the mean time, $(n+1)a^n be \in N$ and $\mathbb{Q} \subseteq R$, and the fact that $[N :_R \{e\}]$ is quasi $(n-1)$ -absorbing ideal of R , we conclude that $a^{n-1}be \in N$. Finally $(a, e)^n(b, f) = (a^n b + na^{n-1}be + a^n f) \in I \propto N$. That is $I \propto N$ is a quasi $n-1$ -absorbing ideal of $R(M)$.

3. Assume that $0 \propto N$ is a quasi n -absorbing ideal of $R(M)$. Then from (1) we conclude that N is a quasi n -absorbing submodule of M . Now, let $0 \neq a \in R$ such that $a^n \in (N :_R M)$. Then $(a, 0)^n(0, x) \in 0 \propto N$ for every $x \in M$. Since $0 \propto N$ is quasi n -absorbing ideal and $(a, 0)^n \notin 0 \propto N$, we conclude that $(a, 0)^{n-1}(0, x) = (0, a^{n-1}x) \in 0 \propto N$. Then $a^{n-1}x \in N$ for each $x \in M$. Hence $a^{n-1} \in (N :_R M)$, that is $(N :_R M)$ is a semi $n-1$ -absorbing ideal of R .

Conversely assume that $(N :_R M)$ is a semi $n-1$ -absorbing ideal of R and N is a quasi n -absorbing submodule of M . Let $(a, x), (b, y) \in R(M)$ such that $(a, x)^n(b, y) \in 0 \propto N$. Then $a^n b = 0$ and $a^n y + nba^{n-1}x \in N$. So, since R is an integral domain, $a = 0$ or $b = 0$. If $a = 0$, then $(0, x)^n = (0, 0) \in I \propto N$. If $b = 0$, then $a^n y \in N$. Consequently, since N is a quasi n -absorbing submodule of M , $a^n \in (N :_R M)$ or $a^{n-1}y \in N$. Suppose that $a^n \in (N :_R M)$, the fact that $(N :_R M)$ is semi $(n-1)$ -absorbing ideal of R , implies $a^{n-1} \in [N :_R M]$. Hence $(a, x)^{n-1}(0, y) = (0, a^{n-1}y) \in 0 \propto N$. Now suppose that $a^{n-1}y \in N$, then $(a, x)^{n-1}(0, y) = (0, a^{n-1}y) \in 0 \propto N$. Thus, $0 \propto N$ is quasi n -absorbing ideal of $R(M)$, as desired.

4. Assume that N is a K -subspace of M , then by [9 Theorem 3.2] $0 \propto N$ is n -absorbing ideal of $R(M)$ henceforth quasi n -absorbing ideal of $R(M)$. Now assume that $0 \propto N$ is a quasi n -absorbing ideal of $R(M)$. Let a be a nonzero element of R , we show that $\frac{1}{a}f \in N$ for every $f \in N$.

For this purpose, consider $f \in N$ and assume that $x = (a, 0), y = (0, \frac{f}{a^n})$, then $x^n y = (0, f) \in 0 \propto N$.

Since $a \neq 0$ and $0 \propto N$ is a quasi n -absorbing ideal of $R(M)$, we conclude that $x^{n-1}y = (0, \frac{f}{a}) \in$

$0 \propto N$. Thus $\frac{f}{a} \in N$. Now, if $f \in N$ and $b \in K$. Then $b = \frac{c}{a}$ for some $c, a \in R$ with $a \neq 0$. Therefore,

since $\frac{1}{a}f \in N$ and N is a R submodule of M , we conclude that $bf \in N$. Hence N is a K -subspace of M . Furthermore, every ideal of $R(M)$ has either of the form $I \propto M$ or $0 \propto N$, where I is an ideal of R and N is a submodule of M , since M is R -module divisible. Now the result follows from (3) and (1). □

Acknowledgement. The authors thank the anonymous referee for helpful comments and suggestions, which improved the content and presentation of the paper.

References

- [1] M. T. Ahmed, T. Dumitrescu, and M. A. Khadam, *Commutative rings with absorbing factorization*, Comm. Algebra 48 (2020), 5067-5075.
- [2] M. M. Ali, *Invertibility of multiplication modules*, New Zealand J. Math 35 (2006). 17-29.
- [3] M. M. Ali, *Idempotent and nilpotent submodules of multiplication modules*, Comm. Algebra 36 (2008), 4620-4642.
- [4] M. M. Ali, *Invertibility of multiplication modules III*, New Zealand J. Math . 39 (2009), 193-213.
- [5] D. F. Anderson, A. Badawi, *On the n -absorbing ideals of commutative rings*, Comm. Algebra 39 (2011), 1646-1672.
- [6] D.D. Anderson and M. Winderes, *Idealisation of a module*, J. Comm. Algebra 1 (2009), 3-56.
- [7] A. Badawi, *On the 2-absorbing ideals of commutative rings*, Bull. Austral. Math. Soc. 75 (2007), 417-429.

- [8] A. Badawi, A.Y. Darani, *On weakly 2-absorbing ideals of commutative rings*, Houston J. Math.
- [9] A. Badawi, M. Issoual and N. Mahdou, *On n -absorbing ideals and (m, n) -closed ideals in trivial extension rings*, J. Algebra Appl. 18(7), 2019.
- [10] A.Y.Darani and F. Soheilnia, *2-absorbing and weakly 2-absorbing submodules*, Thai J. Math. 9 (2011), 577-584.
- [11] A.Y.Darani and F. Soheilnia, *On n -absorbing submodules*, Math, commune.17 (2012), 547-557
- [12] S. Kabbaj, *Matlis' semi-regularity and semi-coherence in trivial ring extensions: a survey*, Moroccan J. Algebra, Geom. Appl. 1(1) (2022), 1-17
- [13] H. Mostafanasab, A. Y. Darani, *On n -absorbing ideals and two generalizations of semiprime ideals*, Thai J. Math 15 (2017) 387-408.
- [14] M. Mukhtar, M.T. Ahmed and T. Dumitrescu, *Commutative rings with two-absorbing factorization*, Comm. Algebra 46 (2018), 970-978.
- [15] P. F. Smith, Z. EL-Bast, *Multiplication modules*, Comm. Algebra 16 (1988), 755-799.
- [16] E. A. Ugurlu, *On 1-absorbing prime submodules*, Moroccan J. Algebra, Geom. Appl. 2(1) (2023), 162-173



ISSN: 2820-7114

Moroccan Journal of Algebra and Geometry with Applications

Supported by Sidi Mohamed Ben Abdellah University, Fez, Morocco

Volume 4, Issue 2 (2025), pp 268-274

Title :

On the lattice of basic z° -ideals

Author(s):

Ali Taherifar

On the lattice of basic z° -ideals

Ali Taherifar

Department of Mathematics, Yasouj University, Yasouj, Iran
e-mail: ataherifar@yu.ac.ir, ataherifar54@gmail.com

Communicated by Najib Mahdou

(Received 02 February 2025, Revised 19 May 2025, Accepted 21 May 2025)

Abstract. It has been shown that for a reduced f -ring R with bounded inversion property, the lattice of basic z° -ideals is a complemented lattice if and only if the space of minimal prime ideals, $\text{Min}(R)$, is compact and R satisfies the annihilator condition. Examples are provided to illustrate and delineate these results.

Key Words: Commutative ring, z -ideal, ring of continuous functions, reduced ring.

2020 MSC: 13A15, 16G30, 54C40

1 Introduction

In this paper, R is assumed to be an f -ring with *bounded inversion property*. In [12], it was prove that for such a ring, the set

$$BZ(R) = \{M_f : f \in R\},$$

partially ordred by inclusion forms a distributive lattice with operations:

$$M_a \vee M_b = M_{a^2+b^2} \quad \text{and} \quad M_a \wedge M_b = M_{ab}.$$

Moreover, it was also shown that the set

$$BZ^\circ(R) = \{P_f : f \in R\},$$

partially ordred by inclusion, forms a distributive lattice with the operations:

$$P_a \vee P_b = P_{a^2+b^2} \quad \text{and} \quad P_a \wedge P_b = P_{ab}.$$

In [12 Theorem 2], it was proved that for an f -ring R with bounded inversion property, the lattice $BZ(R)$ is a complemented lattice and R is a semiprimitive ring if and only if the lattice $BZ^\circ(R)$ is a complemented lattice and R is a reduced ring if and only if the base elements for closed sets in the space of $\text{Max}(R)$ are open and R is semiprimitive if and only if the base elements for closed sets in the space $\text{Min}(R)$ are open and R is reduced. We observe that this theorem holds for basic z -ideals. Therefore, Theorem 3.5 is essentially a restatement (or translation) of the original proof from [12], adapted to the language of the basic z -ideals. However, we will demonstrate that [12 Theorem 2] does not hold when extended to the context of basic z° -ideals. This highlights a fundamental distinction between the behavior of these two classes of ideals. It is proved that for a reduced f -ring R with bounded inversion property, the lattice of basic z° -ideals is a complemented lattice if and only if the space of minimal prime ideals, $\text{Min}(R)$, is compact and R satisfies the annihilator condition (Theorem 3.6). Finally, we prove that for a reduced f -ring R with bounded inversion property, two lattices $\{\text{Ann}(f) : f \in R\}$ and $BZ^\circ(R)$ are isomorphic (Theorem 3.8).

2 Preliminaries

An f -ring is a lattice ordered ring which satisfies the condition that, for any $a, b \in R$ and any $c \geq 0$ in R , $(a \wedge b)c = (ac) \wedge (bc)$. By a positive element of an f -ring R we mean an element $a \geq 0$, and we set $R^+ = \{a \in R : a \geq 0\}$. An f -ring has bounded inversion if every element $a \geq 1$ is invertible. We write $J(R)$ for the Jacobson radical of R , which is the intersection of all maximal ideals of R and we say R is *semiprimitive* if $J(R) = 0$. A ring R is *semiprime* (*reduced*) if it has no nonzero nilpotent element.

As usual, we write $\text{Max}(R)$ for the set of maximal ideals of R . We shall view $\text{Max}(R)$ as a topological space with the Zariski topology. To recall, for $a \in R$ and $A \subseteq R$, we set

$$\mathcal{M}(a) = \{M \in \text{Max}(R) : a \in M\} \quad \text{and} \quad \mathcal{M}(A) = \{M \in \text{Max}(R) : A \subseteq M\},$$

and also

$$\mathcal{D}(a) = \{M \in \text{Max}(R) : a \notin M\} \quad \text{and} \quad \mathcal{D}(A) = \{M \in \text{Max}(R) : A \not\subseteq M\},$$

so that

$$\mathcal{D}(a) = \text{Max}(R) \setminus \mathcal{M}(a) \quad \text{and} \quad \mathcal{D}(A) = \text{Max}(R) \setminus \mathcal{M}(A).$$

The family $\{\mathcal{M}(a) : a \in R\}$ is a base for the closed sets in Zariski topology on $\text{Max}(R)$.

Similarly, we write $\text{Min}(R)$ for the set of minimal prime ideals of R . We shall also endow $\text{Min}(R)$ with the Zariski topology, and for $a \in R$ and $A \subseteq R$, we set

$$\mathcal{P}(a) = \{P \in \text{Min}(R) : a \in P\} \quad \text{and} \quad \mathcal{P}(A) = \{P \in \text{Min}(R) : A \subseteq P\},$$

The family $\{\mathcal{P}(a) : a \in R\}$ is a base for the closed sets in Zariski topology on $\text{Min}(R)$. There will be no confusion since at no stage are we going to consider $\text{Max}(R)$ and $\text{Min}(R)$ simultaneously.

An ideal I of a ring R is a z -ideal (resp., z^0 -ideal) if for each $a, b \in R$ and $\mathcal{M}(a) = \mathcal{M}(b)$ (resp., $\mathcal{P}(a) = \mathcal{P}(b)$), $a \in I$, imply $b \in I$, or equivalently, $M_a \subseteq I$ (resp., $P_a \subseteq I$) for each $a \in I$, where M_a (resp., P_a) is the intersection of all maximal ideals (resp., all minimal prime ideals) of R containing a . Trivially, we have $M_a \subseteq M_b$ (resp., $P_a \subseteq P_b$) if and only if $\mathcal{M}(b) \subseteq \mathcal{M}(a)$ (resp., $\mathcal{P}(b) \subseteq \mathcal{P}(a)$). See [9], for a detailed study of z -ideals in rings.

Recall that an ideal I of an f -ring R is an ℓ -ideal, if for any $a, b \in R$, $|a| \leq |b|$ and $b \in I$ imply $a \in I$. As showed in [10], if R is an f -ring with bounded inversion, then every z -ideal in R is an ℓ -ideal. In fact, an f -ring R has bounded inversion precisely when every z -ideal in R is an ℓ -ideal. Thus in this case of R every maximal ideal is an ℓ -ideal which is known to be equivalent to having the bounded inversion property. Whenever $J(R) = 0$, then every minimal prime ideal of R is a z -ideal and hence is an ℓ -ideal.

In this paper, $C(X)$ ($C^*(X)$) is the ring of all (bounded) real-valued continuous functions on a completely regular Hausdorff space X . In fact, for every topological space X there exists a completely regular Hausdorff space Y such that $C(X)$ and $C(Y)$ are isomorphic as two rings. So, whenever we speak about $C(X)$, X is a completely regular and Hasdorff space.

In studying relations between topological properties of a space X and algebraic properties of $C(X)$, it is natural to look at the subsets of X of the form $f^{-1}\{0\}$, for each $f \in C(X)$. The set $f^{-1}\{0\}$ is called the zero-set of f and denoted by $Z(f)$. Any set that is a zero-set of some function in $C(X)$ is called a zero-set in X . Thus, Z is a mapping from the ring $C(X)$ onto the set of all zero-sets in X . A $\text{coz}f$ is the set $X \setminus Z(f)$ which is called the cozero-set of f . The set of all zero-sets in X is denoted by $Z[X]$ and for each ideal I in $C(X)$, $Z[I]$ is the set of all zero-sets of the form $Z(f)$, where $f \in I$.

Lemma 2.1. *Let R be an f -ring with bounded inversion.*

1. $BZ(R) = \{M_a : a \in R\}$ is a distributive bounded lattice with inclusion order.
2. If R is reduced ring, then $BZ^0(R) = \{P_a : a \in R\}$ is a distributive bounded lattice with inclusion order.

Proof. (1) It suffices to show that for each $a, b \in R$, $M_a \vee M_b$ and $M_a \wedge M_b$ exist in $BZ(R)$. We first claim that $M_a \vee M_b = M_{a^2+b^2}$. To see this, note that since $0 \leq a^2 \leq a^2 + b^2$, and since every maximal ideal is assumed to be an ℓ -ideal (by the comment preceding the lemma), we have $M_a = M_{a^2} \subseteq M_{a^2+b^2}$ and similarly $M_b = M_{b^2} \subseteq M_{a^2+b^2}$. Thus, $M_{a^2+b^2}$ is an upper bounded for $\{M_a, M_b\}$. Now suppose $M_a \subseteq M_c$ and $M_b \subseteq M_c$. Then we have $\mathcal{M}(c) \subseteq \mathcal{M}(a)$ and $\mathcal{M}(c) \subseteq \mathcal{M}(b)$, which implies $\mathcal{M}(c) \subseteq \mathcal{M}(a) \cap \mathcal{M}(b)$. By the hypothesis that every maximal ideal is an ℓ -ideal, it follows that $\mathcal{M}(a) \cap \mathcal{M}(b) = \mathcal{M}(a^2 + b^2)$, and hence $\mathcal{M}(c) \subseteq \mathcal{M}(a^2 + b^2)$, which implies $M_{a^2+b^2} \subseteq M_c$. Therefore, $M_{a^2+b^2}$ is the least upper bound (join) of M_a and M_b . Next, it is straightforward to show that:

$$M_a \wedge M_b = M_a \cap M_b = M_{ab},$$

as also noted in Lemma 3.1, Part (1) of [4]. To verify the distributivity of the lattice $BZ(R)$, consider $a, b, c \in R$. Then we have

$$M_a \vee (M_b \wedge M_c) = M_a \vee M_{bc} = M_{a^2+(bc)^2},$$

and

$$(M_a \vee M_b) \wedge (M_a \vee M_c) = M_{a^2+b^2} \wedge M_{a^2+c^2} = M_{(a^2+b^2)(a^2+c^2)}.$$

On the other hand, it is easy to see that both expressions coincide. So we are done. Finally, the least and greatest elements of $BZ(R)$ are $M_0 = J(R)$ and $M_1 = R$, respectively.

(2) Similarly, by hypothesis and the earlier comments preceding the lemma, we see that for each $a, b \in R$, $P_a \vee P_b = P_{a^2+b^2}$ and $P_a \wedge P_b = P_{ab}$. Analogous to the proof of Part (1) and using the hypothesis, for each $a, b, c \in R$ we have,

$$P_a \vee (P_b \wedge P_c) = (P_a \vee P_b) \wedge (P_a \vee P_c).$$

This shows $BZ^o(R)$ is a distributive lattice. Moreover, the elements $P_0 = N(R)$ and $P_1 = R$ serve as the least and greatest elements of $BZ^o(R)$. $\square$

3 Some properties of the lattice of basic z° -ideals

In this section, we begin by presenting some preliminary results, followed by the main result of the paper.

Lemma 3.1. *For a ring R the following statements are equivalent:*

1. *For each $a \in R$, $P_a = \text{Ann}(\text{Ann}(a))$;*
2. *The ring R is reduced;*
3. *Every annihilator ideal of R is a z° -ideal.*

Proof. (1) $\Rightarrow$ (2) We have $P_0 = \text{Ann}(\text{Ann}(0)) = 0$. This says that the intersection of all minimal prime ideals of R is zero, i.e., R is a reduced ring.

(2) $\Rightarrow$ (3) Let I be an annihilator ideal in R , $a \in I$ and $x \in P_a$. Then $\text{Ann}(I) \subseteq \text{Ann}(a) \subseteq \text{Ann}(x)$, by [1, Proposition 1.5]. Thus $x \in I$, i.e., $P_a \subseteq I$. That is I is a z° -ideal.

(3) $\Rightarrow$ (1) $\text{Ann}(\text{Ann}(a))$ is an annihilator ideal and hence it is a z° -ideal. Thus, $a \in \text{Ann}(\text{Ann}(a))$, implies $P_a \subseteq \text{Ann}(\text{Ann}(a))$. On the other hand, $b \in \text{Ann}(\text{Ann}(a))$ implies $\text{Ann}(a) \subseteq \text{Ann}(b)$. By [1, Proposition 1.5], $b \in P_a$. So we are done. $\square$

Similar to the above result, we can prove the following result.

Lemma 3.2. *For a ring R the following statements are equivalent:*

1. For each $a \in R$, $M_a \subseteq \text{Ann}(\text{Ann}(a))$;
2. The ring R is semiprimitive;
3. Every annihilator ideal of R is a z -ideal.

Corollary 3.3. Let R be a reduced ring. A principal ideal Ra is an annihilator ideal if and only if it is a z° -ideal.

Theorem 3.4. Let R be an f -ring with bounded inversion property. The following statements are equivalent:

1. $BZ(R)$ is a complemented lattice and R is a semiprimitive ring;
2. R is a regular ring;
3. The base elements for closed sets in $\text{Max}(R)$ are open and R is semiprime.

Proof. (1) $\Rightarrow$ (2) Let $a \in R$. By hypothesis, there exists $b \in R$ such that

$$M_a \vee M_b = M_1 = R \quad \text{and} \quad M_a \wedge M_b = M_{ab} = M_0 = 0.$$

Thus $M_{a^2+b^2} = R$ and $M_{ab} = 0$. This shows $ab = 0$ and hence $a^2 + b^2$ is unit in R . It follows there exists $c \in R$ such that;

$$c(a^2 + b^2) = 1 \Rightarrow a = a^3c + ab^2c = a^2(ac).$$

This shows that R is a regular ring.

(2) $\Rightarrow$ (1) Trivially, the regularity of R implies $J(R) = 0$. Now, let $a \in R$. By hypothesis, there exists $b \in R$ such that $a = a^2b$. Hence, $a(1 - ab) = 0$. This implies that

$$M_a \wedge M_{1-ab} = M_{a(1-ab)} = M_0 = 0. \quad (1)$$

Since R has the bounded inversion property, every maximal ideal is an l -ideal. Therefore, no maximal ideal contains $a^2 + (1 - ab)^2$. In fact, a maximal ideal contains $a^2 + (1 - ab)^2$ if and only if it is containing a and $(1 - ab)$. Hence we have,

$$M_a \vee M_{1-ab} = M_{a^2+(1-ab)^2} = M_1. \quad (2)$$

The equalities (1) and (2) show that for each $a \in R$, M_a has complement. Thus, $BZ(R)$ is a complemented lattice.

(2) $\Rightarrow$ (3) Since R is regular, it follows that $J(R) = 0$ and hence R is a reduced ring. By hypothesis, for each $a \in R$, there exists a $b \in R$ such that $a = a^2b$. This implies that $a(1 - ab) = 0$. Therefore, every maximal ideal must contain either a or $1 - ab$, which yields

$$M(a) \cup M(1 - ab) = \text{Max}(R) \quad \text{and} \quad M(a) \cap M(1 - ab) = \emptyset.$$

Thus $M(a) = \text{Max}(R) \setminus M(1 - ab)$ is open in the Zariski topology.

(3) $\Rightarrow$ (2) Let $a \in R$ such that $M(a)$ is clopen in $\text{Max}(R)$. Since $J(R) = 0$, there exists an idempotent $e \in R$ such that $M(a) = \text{Max}(R) \setminus M(e)$. Thus we have,

$$M(ae) = M(a) \cup M(e) = \text{Max}(R) \Rightarrow ae \in J(R) = 0.$$

On the other hand, we compute:

$$M(a^2 + e^2) = M(a) \cap M(e) = D(e) \cap M(e) = \emptyset.$$

Which implies that $a^2 + e^2 = a^2 + e$ is not contained in any maximal ideal, and therefore is a unit in R . So there exists $c \in R$ such that

$$c(a^2 + e) = 1 \Rightarrow ca^2 + ce = 1.$$

Multiplying both sides by a , we get $a = ca^3 + cea$. But since $ae = 0$, we have $a = a^2(ca)$. Thus, R is a regular ring. $\square$

It is well-known that $C(X)$ is a regular ring if and only if X is a P -space (i.e., every zero-set, see [5, 4]). This fact together with the above result imply the following.

Corollary 3.5. $BZ(C(X))$ is a complemented lattice if and only if X is a P -space.

A space X is *cozero complemented* if, given any cozero set U , there is a disjoint cozero set V such that $U \cup V$ is dense in X . There are many equivalent algebraic or topological conditions for cozero complemented spaces, see [6] and [8].

Remark 3.6. Let X be a cozero complemented space. Then we claim that $BZ^\circ(C(X))$ is a complemented lattice and hence this shows that the results of Theorem 2 in [12] for basic z° -ideals is not true. In fact, it is enough to consider the space $\mathbb{R}$ with standard topology. Then $BZ^\circ(C(\mathbb{R}))$ is a complemented lattice, while $C(\mathbb{R})$ is not a regular ring. To see our claim, let $P_f \in BZ^\circ(C(X))$. Since X is a cozero complemented space, there exists $g \in C(X)$ such that

$$\text{cl}_X(X \setminus Z(f)) \cup \text{cl}_X(X \setminus Z(g)) = X \quad \text{and} \quad (X \setminus Z(f)) \cap (X \setminus Z(g)) = \emptyset.$$

$$\text{Thus } \text{int}_X Z(f^2 + g^2) = \text{int}_X Z(f) \cap \text{int}_X Z(g) = \emptyset,$$

$$\text{and } \text{int}_X Z(fg) = \text{int}_X (Z(f) \cup Z(g)) = X.$$

This implies

$$P_f \wedge P_g = P_{fg} = P_{\text{int}_X Z(fg)} = P_X = 0, \quad \text{and}$$

$$P_f \vee P_g = P_{f^2+g^2} = P_{\text{int}_X Z(f^2+g^2)} = P_\emptyset = R.$$

See also [11] Proposition 3.8].

We recall that for a, b in a reduced f -ring R , $\text{Ann}(a^2 + b^2) = \text{Ann}(a) \cap \text{Ann}(b)$. For, we have $\text{Ann}(a) \cap \text{Ann}(b) \subseteq \text{Ann}(a^2 + b^2)$. Now, let $r \in \text{Ann}(a^2 + b^2)$. Then $(ra)^2 + (rb)^2 = 0$. As $0 \leq (ra)^2 \leq (ra)^2 + (rb)^2 = 0$. Thus $(ra)^2 = 0$ and hence $ra = 0$ and similarly $rb = 0$. These imply $r \in \text{Ann}(a) \cap \text{Ann}(b)$. In the next result we give a correct form of Theorem 2 in [12] for basic z° -ideals.

Theorem 3.7. For a reduced f -ring R with bounded inversion property, the following statements are equivalent:

1. $\text{Min}(R)$ is compact, and R satisfies the annihilator condition;
2. For each $x \in R$ there exists $y \in R$ such that $\text{Ann}(\text{Ann}(y)) = \text{Ann}(x)$;
3. For each $x \in R$ there exists $y \in R$ such that $\text{Ann}(x) = P_y$;
4. $BZ^\circ(R)$ is a complemented lattice.

Proof. (1) $\Leftrightarrow$ (2) See Theorem 3.4 in [7].

(2) $\Leftrightarrow$ (3) This follows from Lemma 3.1.

(3) $\Rightarrow$ (4) It is enough to show that every element of $BZ^\circ(R)$ has a complement. Consider $P_r \in BZ^\circ(R)$. By Lemma 3.1, $P_r = \text{Ann}(\text{Ann}(r))$. Since R is a reduced ring, $\text{Ann}(\text{Ann}(r)) \cap \text{Ann}(r) = 0 = P_0$. By hypothesis, there exists $y \in R$ such that $\text{Ann}(r) = P_y$. Hence $P_r \wedge P_y = P_r \cap P_y = 0$. On the other hand,

$$P_r \vee P_y = P_{r^2+y^2} = \text{Ann}(\text{Ann}(r^2 + y^2)) = \text{Ann}(\text{Ann}(r) \cap \text{Ann}(y))$$

$$= \text{Ann}(P_y \cap \text{Ann}(y)) = \text{Ann}(\text{Ann}(\text{Ann}(y)) \cap \text{Ann}(y)) = \text{Ann}(0) = R.$$

Thus P_y is a complement of P_r .

(4) $\Rightarrow$ (3) Let $x \in R$. Then there exists $y \in R$ such that $P_y \cap P_x = 0$ and $\text{Ann}(\text{Ann}(x^2 + y^2)) = P_{x^2+y^2} = P_x \vee P_y = R$. The first equality shows that $\text{Ann}(\text{Ann}(x)) \cap P_y = 0$ and hence $P_y \subseteq \text{Ann}(\text{Ann}(\text{Ann}(x))) = \text{Ann}(x)$. The second equality shows that $\text{Ann}(x) \cap \text{Ann}(y) = \text{Ann}(x^2 + y^2) = 0$ and hence $\text{Ann}(x) \subseteq \text{Ann}(\text{Ann}(y)) = P_y$. Thus $\text{Ann}(x) = P_y$. $\square$

It is also easy to see that for a reduced f -ring R , the set $\{\text{Ann}(f) : f \in R\}$, partially ordered with inclusion, forms a lattice with the following operations;

$$\text{Ann}(f) \vee \text{Ann}(g) = \text{Ann}(fg), \quad \text{Ann}(f) \wedge \text{Ann}(g) = \text{Ann}(f^2 + g^2).$$

We need the following well-known result in the sequel, see [2 Lemma 4.2] and [1 Proposition 1.5]. We note that for a subset A of $\text{Min}(R)$, $\text{int } A = \text{int}_{\text{Min}(R)} A$.

Lemma 3.8. *For a reduced ring R the following statements hold.*

1. *If $a \in R$, then $P_a = \{x \in R : \text{int } V(a) \subseteq \text{int } V(x)\}$.*
2. *For ideals I, J of R , $\text{Ann}(I) \subseteq \text{Ann}(J)$ if and only if $\text{int } V(I) \subseteq \text{int } V(J)$.*

Theorem 3.9. *Let R be a reduced f -ring with bounded inversion property. Then two lattices $(\{\text{Ann}(f) : f \in R\}, \subseteq)$ and $(BZ^\circ(R), \supseteq)$ are isomorphic.*

Proof. Define $\phi : \{\text{Ann}(f) : f \in R\} \rightarrow BZ^\circ(R)$, by $\phi(\text{Ann}(f)) = P_f$, where $f \in R$. Let $\text{Ann}(f) = \text{Ann}(g)$. Then, $\text{int } V(f) = \text{int } V(g)$, by Lemma 3.8. This implies $P_f = P_g$, i.e., $\phi(\text{Ann}(f)) = \phi(\text{Ann}(g))$. If $\phi(\text{Ann}(f)) = \phi(\text{Ann}(g))$ for some $f, g \in R$, then $P_f = P_g$. This implies $f \in P_f = P_g$ and hence $\text{int } V(g) \subseteq \text{int } V(f)$. Also, $g \in P_g = P_f$ implies $\text{int } V(f) \subseteq \text{int } V(g)$. Thus, $\text{int } V(f) = \text{int } V(g)$. By Lemma 3.8, $\text{Ann}(f) = \text{Ann}(g)$. This says, ϕ is a one-one map. Clearly, ϕ is onto. It is enough to show that ϕ preserves $\vee$ and $\wedge$. Assume $f, g \in R$. Then, we have

$$\phi(\text{Ann}(f) \vee \text{Ann}(g)) = \phi(\text{Ann}(fg)) = P_{fg} = P_f \vee P_g = \phi(\text{Ann}(f)) \vee \phi(\text{Ann}(g)),$$

and

$$\phi(\text{Ann}(f) \wedge \text{Ann}(g)) = \phi(\text{Ann}(f^2 + g^2)) = P_{f^2+g^2} = P_f \wedge P_g = \phi(\text{Ann}(f)) \wedge \phi(\text{Ann}(g)).$$

$\square$

Theorems 3.7 and 3.9 imply the next result, see also [11 Proposition 3.4].

Corollary 3.10. *The following statements are equivalent:*

1. *The lattice $\{\text{Ann}(f) : f \in C(X)\}$ is a complemented lattice;*
2. *The lattice $BZ^\circ(C(X))$ is a complemented lattice;*
3. *The space X is a cozero complemented space.*

Acknowledgments.

The author is grateful to Professor Najib Mahdou for his comments and suggestions that helped improve the presentation of the paper.

References

- [1] F. Azarpanah, O.A. S. Karamzadeh and A.R. Aliabad, *On ideals consisting entirely of zero-divisors*, Commun. Algebra 28(2) (2000), 1061-1073.
- [2] G. F. Birkenmeier, M. Ghirati and A. Taherifar, *When is a sum of annihilator ideals an annihilator ideal?*, Commun. Algebra 43 (2015), 2690-2702.
- [3] M. Ahmadi and A. Taherifar, *On the lattice of z° -ideals (resp., z -ideals) and its applications*, Filomat 38(22) (2024), 7811-7822.
- [4] T. Dube, *A note on lattice of z -ideals of f -rings*, New York J. Math. 22 (2016), 351-361.
- [5] L. Gillman and M. Jerison, *Rings of Continuous Functions*. Springer (1976).
- [6] F. Golrikhatami and A. Taherifar, *Some class of topological spaces related to zero-sets*, Applied general topology, 23(1) (2022), 1-16.
- [7] M. Henriksen and M. Jerison, *The space of minimal prime ideals of a commutative ring*, Trans. Amer. Math. Soc. 115 (1965), 110-130.
- [8] M. Henriksen and G. Woods, *Cozero complemented spaces; when the space of minimal prime ideals of a $C(X)$ is compact*, Topo. Appl. 141 (2004), 147-170.
- [9] G. Mason, *z -ideals and prime ideals*, J. Algebra 26 (1973), 280-297.
- [10] L. Suzanne, *A characterization of f -rings in which the sum of semiprime ideals is semiprime and its consequences*, Comm. Algebra 23(14) (1995), 5461-5481.
- [11] A. Taherifar and M. R. Ahmadi Zand, *Topological Representation of some lattices of ideals and their applications*, Math. Slovaca 74(2) (2024), 281-292.
- [12] A. Taherifar, *On lattice of basic z -ideals*, Mathematical researches 7(1) (2021), 127-132.



ISSN: 2820-7114

Moroccan Journal of Algebra and Geometry with Applications

Supported by Sidi Mohamed Ben Abdellah University, Fez, Morocco

Volume 4, Issue 2 (2025), pp 275-291

Title :

Evolution algebras satisfying a train identity of degree 2 and exponent $m > 3$

Author(s):

Savadoغو Souleymane, Tenkodogo Joseph & Conseibo André

Evolution algebras satisfying a train identity of degree 2 and exponent $m > 3$

Savadogo Souleymane¹, Tenkodogo Joseph² and Conseibo André³

Département de Mathématiques, Université Norbert ZONGO, Burkina Faso.

¹ e-mail: sara01souley@yahoo.fr

² e-mail: josephntenkodogo603@gmail.com

³ e-mail: andreconseibo@gmail.com

Communicated by Abdenacer Makhlouf

(Received 06 January 2025, Revised 22 May 2025, Accepted 29 May 2025)

Abstract. The present paper is devoted to the study of evolution algebras that satisfy the identity $x^m x^m = \omega(x)^m x^m$, where the integer $m > 3$. This polynomial identity is known as the train identity of degree 2 and exponent m . We determine the Peirce decomposition, the set of nonzero idempotents and characterise the derivations and automorphisms of the algebras of this class. In passing, we show that they strictly contain the class of finite-dimensional baric evolution algebras that are power-associative. Finally, we provide the classification of evolution algebras of dimension at most 5 that satisfy strictly the train identity of degree 2 and exponent m , for some integer $m > 3$.

Key Words: Bernstein algebra, Evolution algebra, Train identity of degree 2 and exponent m , Peirce decomposition, Derivation, Idempotent.

2010 MSC: Primary 17A30, 17D92 ; Secondary 17A60, 17D99.

1 Introduction

In 1939, Etherington established the first link between the concept of algebra and that of population genetics. Bernstein algebras [6] are an efficient algebraic tool for studying populations reaching a steady state after the first generation. However, the notion of Bernstein algebra does not appear explicitly in the work of S. Bernstein, nor that of Lyubich [11, 12]. They were introduced by Ph. Holgate in 1975 [9]. Since then, work on this class of non-associative algebras has expanded considerably. In [1], Abraham gives the mathematical formulation of a genetic population that reaches its equilibrium state at the $(k+1)$ th generation: Bernstein algebras of order k thus make their appearance in the literature.

Given a commutative field F , a commutative F -algebra A is a:

- *Jordan algebra* if $(xy)x^2 = x(yx^2)$, $\forall x \in A$;
- *baric algebra* if there is a non-zero morphism of algebras $\omega : A \longrightarrow F$.

Let (A, ω) be a baric F -algebra. The algebra A is a:

- *Bernstein algebra* of order $k \geq 1$, if $x^{[k+2]} = \omega(x)^{2k} x^{[k+1]}$ for any $x \in A$;
- *train algebra* of rank $n \geq 2$ if there are scalars $\gamma_1, \dots, \gamma_{n-1}$ such that $x^n + \gamma_1 \omega(x) x^{n-1} + \dots + \gamma_{n-1} \omega(x)^{n-1} x = 0$, for all $x \in A$.

The plenary power $x^{[k]}$ and principal power x^k of $x \in A$, are defined by:

$$x^{[1]} = x^1 = x \text{ and } x^{[r+1]} = x^{[r]}x^{[r]}; \quad x^{r+1} = x^r x \text{ with } r \in \mathbb{N}^*,$$

and those of algebra A are given by:

$$A^{[1]} = A^1 = A \text{ and } A^{[r+1]} = (A^{[r]})^2; \quad A^{r+1} = A^r A \text{ with } r \in \mathbb{N}^*.$$

Bernstein algebras appear as Bernstein algebras of order 1. In [18], the author shows that in Bernstein algebra, the identity

$$2x^i x^j = \omega(x)^i x^j + \omega(x)^j x^i \quad (1)$$

is hold for all integers $i, j \geq 2$ and the structure of this identity has been studied for $2 \leq i, j \leq 3$; for $i = 2, j = 4$ and for $i = j = 4$ in [19, 3, 5, 10, 18]. In [7, 16], the authors study respectively evolution algebras that are Bernstein algebras and evolution algebras satisfying the train identity of degree 2 and exponent 3, i.e. the identity

$$x^3 x^3 = \omega(x)^3 x^3. \quad (2)$$

They give the general form of the idempotents and a classification in dimension ≤ 4 , of algebras of this class. They also show that evolution algebras satisfying the identity (2) are subclass of Bernstein algebras of order 2. Thus, in the present paper, we study evolution algebras that satisfy the identity

$$x^m x^m = \omega(x)^m x^m, \quad (3)$$

for some integer $m > 3$. This identity is known as *the train identity of degree 2 and exponent m*. An evolution algebra is not defined by an identity like the Bernstein algebras of order k . A F -algebra of dimension n is said to be an evolution algebra if it has a basis $B = \{e_1, \dots, e_n\}$ such that

$$e_i e_j = 0 \text{ for } 1 \leq i \neq j \leq n \text{ and } e_i^2 = \sum_{k=1}^n a_{ik} e_k \quad (4)$$

Such a basis is called a natural basis of the evolution algebra A and the matrix $M = (a_{ik})_{1 \leq i, k \leq n}$ is the matrix of the structural constants of A relative to the natural basis B . Evolution algebras are commutative but they are not associative in general [17]. In Section 2, we give the Peirce decomposition of baric evolution algebra satisfying a train identity of degree 2 and exponent $m > 3$. The general form of nonzero idempotents, a characterisation of automorphisms groups and the connection with Bernstein algebras are given. We also show that the class of finite-dimensional baric evolution algebras that are power-associative is strictly included in the class of evolution algebras satisfying the identity (3) for some $m > 3$. Section 3 is devoted to the study of the classification in dimension ≤ 5 , of the algebras strictly satisfying the train identity of degree 2 and exponent $m > 3$. In Section 4, we study the Lie algebra of derivations of finite-dimensional evolution algebras satisfying our identity and we show that this Lie algebra is abelian for an evolution algebra of dimension 5 strictly satisfying the identity (3) for some $m > 3$.

2 Structure of evolution algebras satisfying the identity (3)

In this paper, assume that F is a commutative field of $\text{Char}(F) \neq 2$. In [13] Proof of Corollary 3.4], the authors show that any baric evolution algebra of dimension n has a natural basis $B = \{e_1, \dots, e_n\}$ whose multiplication table is given by:

$$e_1^2 = e_1 + \sum_{k=2}^n a_{1k} e_k \text{ and } e_j^2 = \sum_{k=2}^n a_{jk} e_k \text{ with } \omega(e_1) = 1 \text{ and } \omega(e_j) = 0 \text{ for all } 2 \leq j \leq n.$$

In the following, a baric evolution algebra of dimension n will be provided with such a natural basis.

2.1 About Peirce Decomposition

We give here the Peirce decomposition of evolution algebra satisfying the identity (3) for some $m > 3$.

Lemma 2.1. *Let (A, ω) be a baric evolution F -algebra of dimension n satisfying the identity (3) for some $m > 3$. For all $2 \leq j, k \leq n$, the following assertions are satisfied:*

- (i) $e_1^2 e_1^2 = e_1^2$;
- (ii) $2e_1^2(e_1^2 e_j) = e_1^2 e_j$;
- (iii) $2e_1^2 e_j^3 = e_j^3$;
- (iv) $(e_1^2 e_j)(e_1^2 e_k) = 0$;
- (v) $2e_1^2((e_1^2 e_j)e_k) = (e_1^2 e_j)e_k$.

Proof. The equality $e_1^3 = e_1^2$ leads to $e_1^m = e_1^2$ for $m > 3$ and the identity (3) tells us that $e_1^2 = e_1^m \omega(e_1)^m = e_1^m e_1^m = e_1^2 e_1^2$: we obtain the assertion (i). Let $x = \alpha e_1 + y$ with $y \in \ker \omega$ and $\alpha \in F$. We have $x^2 = \alpha^2 e_1^2 + y^2$ and we show by induction that for any integer $t \geq 3$, $x^t = \alpha^t e_1^2 + \sum_{k=1}^{t-2} \alpha^{t-k} R_y^k(e_1^2) + y^t$ where R_y is the right multiplication of A determined by y . It follows that

$$x^m = \alpha^m e_1^2 + \sum_{k=1}^{m-2} \alpha^{m-k} R_y^k(e_1^2) + y^m$$

and

$$\begin{aligned} x^m x^m &= \alpha^{2m} e_1^2 e_1^2 + 2\alpha^m e_1^2 y^m + \sum_{k,j=1}^{m-2} \alpha^{2m-(k+j)} R_y^k(e_1^2) R_y^j(e_1^2) \\ &\quad + 2 \sum_{k=1}^{m-2} \alpha^{2m-k} e_1^2 R_y^k(e_1^2) + 2 \sum_{k=1}^{m-2} \alpha^{m-k} y^m R_y^k(e_1^2) \end{aligned}$$

By identifying the coefficients of α^{2m-1} , α^{2m-2} and α^m in the equality $x^m x^m = \omega(x)^m x^m$, we obtain respectively identities (5), (6) and (7) below:

$$R_y(e_1^2) = 2e_1^2 R_y(e_1^2) \quad (5)$$

$$R_y^2(e_1^2) = (R_y(e_1^2))^2 + 2e_1^2 R_y^2(e_1^2) \quad (6)$$

$$y^m = 2e_1^2 y^m + \sum_{k=2}^{m-2} R_y^{m-k}(e_1^2) R_y^k(e_1^2) \quad (7)$$

For $2 \leq j \leq n$, replacing y by e_j in the identity (5), we obtain the assertion (ii) and replacing y by e_j in the identity (6), we get

$$(e_1^2 e_j)^2 = e_j(e_1^2 e_j) - 2e_1^2(e_j(e_1^2 e_j)) = a_{1j} a_{jj}(e_j^2 - 2e_1^2 e_j^2).$$

If $a_{1j} = 0$, then $(e_1^2 e_j)^2 = 0$. Otherwise, the assertion (ii) tells us that $2e_1^2 e_j^2 = e_j^2$ and it follows that $(e_1^2 e_j)^2 = 0$. We deduce that

$$(e_1^2 e_j)^2 = 0, \text{ for all } 2 \leq j \leq n. \quad (8)$$

Replacing y by e_j with $2 \leq j \leq n$ in the identity (7), we obtain

$$e_j^m = 2e_1^2 e_j^m + \sum_{k=2}^{m-2} R_{e_j}^{m-k}(e_1^2) R_{e_j}^k(e_1^2) = 2e_1^2 e_j^m + a_{jj}^{m-2} \sum_{k=2}^{m-2} (e_1^2 e_j)^2 = 2e_1^2 e_j^m.$$

Since $e_j^m = a_{jj}^{m-2} e_j^2$ and $m > 3$, the relation $e_j^m = 2e_1^2 e_j^m$ gives $a_{jj} e_j^2 = 2a_{jj} e_1^2 e_j^2$, i.e. $e_j^3 = 2e_1^2 e_j^3$. So, we have the assertion (iii).

For $2 \leq j \neq k \leq n$, by setting in the identity (6), $y = e_j + e_k$, we obtain

$$(e_1^2 e_j) e_k + (e_1^2 e_k) e_j = 2(e_1^2 e_k)(e_1^2 e_j) + 2e_1^2((e_1^2 e_j) e_k + (e_1^2 e_k) e_j) \quad (9)$$

It follows that

$$2(e_1^2 e_j)(e_1^2 e_k) = a_{1k} a_{kj} (e_j^2 - 2e_1^2 e_j^2) + a_{1j} a_{jk} (e_k^2 - 2e_1^2 e_k^2).$$

If $a_{1j} a_{1k} = 0$, then $(e_1^2 e_j)(e_1^2 e_k) = 0$. Otherwise, the assertion (ii) tells us that $0 = e_j^2 - 2e_1^2 e_j^2 = e_k^2 - 2e_1^2 e_k^2$ and it follows that

$$(e_1^2 e_j)(e_1^2 e_k) = 0, \text{ for all } 2 \leq j \neq k \leq n. \quad (10)$$

The assertion (iv) results from the identities (8) and (10). Since $(e_1^2 e_j)(e_1^2 e_k) = 0$, for $2 \leq j \neq k \leq n$, the identity (9), leads to

$$(e_1^2 e_j) e_k + (e_1^2 e_k) e_j = 2e_1^2((e_1^2 e_j) e_k + (e_1^2 e_k) e_j). \quad (11)$$

If $a_{1k} = 0$ then the identity (11) becomes $2e_1^2((e_1^2 e_j) e_k) = (e_1^2 e_j) e_k$. Otherwise, the assertion (ii) tells us that $2e_1^2 e_k^2 = e_k^2$ and we have $(e_1^2 e_j) e_k = a_{1j} a_{jk} e_k^2 = 2a_{1j} a_{jk} e_1^2 e_k^2 = 2e_1^2(a_{1j} a_{jk} e_k^2) = 2e_1^2((e_1^2 e_j) e_k)$. This gives us the assertion (v). $\square$

An evolution F -algebra satisfying the five assertions of Lemma 2.1 does not necessarily satisfy a train identity of degree 2 and exponent 3. This is illustrated by the following example.

Example 2.2. Let (A, ω) be a five-dimensional evolution algebra with the natural basis $B = \{e_1, \dots, e_5\}$ whose multiplication table is given by:

$$e_1^2 = e_1 + e_2 + e_3, \quad e_2^2 = \frac{1}{4}(e_2 - e_3), \quad e_3^2 = -e_2^2, \quad e_4^2 = e_2 + e_3, \quad e_5^2 = e_4.$$

Since $e_5^2 e_5^2 \neq 0$, this algebra is not a Bernstein algebra. Moreover, it does not satisfy the identity (2). Indeed, for $y = e_1 + e_4 + e_5$, we have $y^2 = e_1^2 + e_4^2 + e_5^2$, $y^3 = e_1^2 + e_4^2 = e_1 + 2(e_2 + e_3)$ and $y^3 y^3 = e_1^2 \neq \omega(y)^3 y^3$. It satisfies the assertions of Lemma 2.1 because it satisfies the train identity of degree 2 and exponent 4.

Definition 2.3. Let A be an evolution algebra of dimension n in the natural basis $B = \{e_1, \dots, e_n\}$ and $x = \sum_{i=1}^n x_i e_i$ an element of A . The support of x relative to B , denoted $\text{Support}(x)$ is defined as the set $\text{Support}(x) := \{i \in \{1, \dots, n\} \mid x_i \neq 0\}$.

Notation. Let (A, ω) be a finite-dimensional baric evolution algebra. Let $\Lambda_B := \text{Support}(e_1^2) \setminus \{1\} = \{j \in \{2, \dots, n\} \mid a_{1j} \neq 0\}$ and denote its cardinal by $\text{Card}(\Lambda_B)$.

Theorem 2.4. Let (A, ω) be a baric evolution F -algebra of dimension n satisfying the identity (3) for some $m > 3$. Then, the algebra A admits the following Peirce decomposition:

$$A = Fe_1^2 \oplus A_0(e_1^2) \oplus A_{\frac{1}{2}}(e_1^2) \text{ where } A_\lambda(e_1^2) = \{x \in \ker(\omega) \mid e_1^2 x = \lambda x\} \text{ with } \lambda \in \left\{0, \frac{1}{2}\right\}.$$

Furthermore,

$$A_{\frac{1}{2}}(e_1^2) = \langle e_j^2 \mid j \in \Lambda_B \rangle \text{ and } A_0(e_1^2) = \langle e_j - 2e_1^2 e_j \mid 2 \leq j \leq n \rangle.$$

Proof. A partial linearisation of identity (3) gives us

$$2x^m \left(\sum_{k=0}^{m-3} R_x^k(yx^{m-1-k}) + 2R_x^{m-1}(y) \right) = \omega(x)^m \left(\sum_{k=0}^{m-3} R_x^k(yx^{m-1-k}) + 2R_x^{m-1}(y) \right) \quad (12)$$

for all $x \in A$ and $y \in \ker(\omega)$. By replacing x by e_1 in the identity (12) and taking into account the equalities $e_1 \ker(\omega) = 0$ and $e_1^2 \ker(\omega) \subset \ker(\omega)$, we obtain

$$0 = 2e_1^2(e_1^2y) - e_1^2y = R_{e_1^2}(2R_{e_1^2} - Id_{\ker(\omega)})(y).$$

It follows that $P = X(2X - 1)$ is the annihilating polynomial of $R_{e_1^2}|_{\ker(\omega)} : \ker(\omega) \rightarrow \ker(\omega), x \mapsto e_1^2x$. From kernel lemma we deduce that $\ker(\omega) = A_{\frac{1}{2}}(e_1^2) \oplus A_0(e_1^2)$ with $A_{\frac{1}{2}}(e_1^2) = \ker(2R_{e_1^2} - Id_{\ker(\omega)}) = \{y \in \ker(\omega) \mid 2e_1^2y = y\}$ and $A_0(e_1^2) = \ker(R_{e_1^2}) = \{y \in \ker(\omega) \mid e_1^2y = 0\}$. Thus, we obtain the Peirce decomposition of the algebra A given by $A = Fe_1^2 \oplus A_{\frac{1}{2}}(e_1^2) \oplus A_0(e_1^2)$. Let $x = x_2e_2 + \dots + x_ne_n \in \ker(\omega)$; we have $e_1^2x = x_2e_1^2e_2 + \dots + x_ne_1^2e_n = \sum_{k \in \Lambda_B} x_k e_1^2 e_k$.

- Assume that $x \in A_{\frac{1}{2}}(e_1^2)$. Then $x = 2e_1^2x = \sum_{k \in \Lambda_B} 2x_k e_1^2 e_k \in \langle e_1^2 e_j \mid j \in \Lambda_B \rangle$. Reciprocally, the assertion (ii) of Lemma 2.1 tells us that $e_1^2 e_j \in A_{\frac{1}{2}}(e_1^2)$ for all $j \in \Lambda_B$. It follows that $A_{\frac{1}{2}}(e_1^2) = \langle e_1^2 e_j \mid a_{1j} \neq 0 \text{ for all } 2 \leq j \leq n \rangle = \langle e_j^2 \mid j \in \Lambda_B \rangle$.
- It is assumed that $x \in A_0(e_1^2)$. Then, $0 = e_1^2x = x_2e_1^2e_2 + \dots + x_ne_1^2e_n$ and $x = x_2(e_2 - 2e_1^2e_2) + \dots + x_n(e_n - 2e_1^2e_n) \in \langle e_j - 2e_1^2e_j \mid 2 \leq j \leq n \rangle$. Conversely, according to the assertion (ii) of Lemma 2.1, we have $e_1^2(e_j - 2e_1^2e_j) = 0$ for all $2 \leq j \leq n$, i.e. $e_j - 2e_1^2e_j \in A_0(e_1^2)$ for all $2 \leq j \leq n$. We deduce that $A_0(e_1^2) = \langle e_j - 2e_1^2e_j \mid 2 \leq j \leq n \rangle$.

□

Corollary 2.5. Let $A = Fe_1^2 \oplus A_{\frac{1}{2}}(e_1^2) \oplus A_0(e_1^2)$ be a Peirce decomposition of a finite-dimensional baric evolution algebra satisfying the identity (3) for some $m > 3$. Then,

$$A_{\frac{1}{2}}(e_1^2)^2 = 0 \text{ and } A_{\frac{1}{2}}(e_1^2)\ker(\omega) \subset A_{\frac{1}{2}}(e_1^2).$$

In particular $A_{\frac{1}{2}}(e_1^2)A_0(e_1^2) \subset A_{\frac{1}{2}}(e_1^2)$.

Proof. This corollary is a consequence of the assertions (iv) and (v) of Lemma 2.1 and Theorem 2.4.

□

Proposition 2.6. Let $A = Fe_1^2 \oplus A_{\frac{1}{2}}(e_1^2) \oplus A_0(e_1^2)$ be a Peirce decomposition of a finite-dimensional baric evolution algebra satisfying the identity (3) for some $m > 3$. Then, the Peirce subspace $A_0(e_1^2)$ is nonzero.

Proof. It is assumed that $A_0(e_1^2) = 0$ and let $x = \alpha e_1^2 + x_{\frac{1}{2}} \in A$. We have $x^2 = \alpha^2 e_1^2 + \alpha x_{\frac{1}{2}} = \alpha(\alpha e_1^2 + x_{\frac{1}{2}}) = \omega(x)x$. It follows that A is train algebra of rank 2. This is absurd by [13, Proposition 3.7] and the result follows.

□

Lemma 2.7. Let $A = Fe_1^2 \oplus A_{\frac{1}{2}}(e_1^2) \oplus A_0(e_1^2)$ be a Peirce decomposition of a finite-dimensional baric evolution algebra satisfying the identity (3) for some $m > 3$. Then

$$y^m \in A_{\frac{1}{2}}(e_1^2) \text{ for all } y \in \ker(\omega).$$

Proof. Since $A_{\frac{1}{2}}(e_1^2)\ker(\omega) \subset A_{\frac{1}{2}}(e_1^2)$, the lemma follows from the identity (7). Indeed, for all $2 \leq k \leq m - 2$ and $y \in \ker(\omega)$, we have $R_y^{m-k}(e_1^2), R_y^k(e_1^2) \in A_{\frac{1}{2}}(e_1^2)$ which leads to $R_y^{m-k}(e_1^2)R_y^k(e_1^2) = 0$, hence the desired result.

□

Proposition 2.8. Let $A = Fe_1^2 \oplus A_{\frac{1}{2}}(e_1^2) \oplus A_0(e_1^2)$ be a Peirce decomposition of a finite-dimensional baric evolution algebra satisfying the identity (3) for some $m > 3$. If the Peirce subspace $A_{\frac{1}{2}}(e_1^2)$ is zero, then algebra A is a train algebra of rank at most $m + 1$.

Proof. Assume that $A_{\frac{1}{2}}(e_1^2) = 0$ and let $y \in \ker \omega = A_0(e_1^2)$. Lemma 2.7 tells us that $y^m = 0$. It follows that $\ker \omega$ is a nilalgebra of nilindex at most m . The result follows by [13, Theorem 3.8]. $\square$

Theorem 2.9. [Characterisation] Let (A, ω) be a baric evolution F -algebra of dimension n . Then, the algebra A satisfies the identity (3) if, and only if, the following assertions hold:

- (i) $e_1^2 e_1^2 = e_1^2$;
- (ii) $A = Fe_1^2 \oplus A_{\frac{1}{2}}(e_1^2) \oplus A_0(e_1^2)$;
- (iii) $(A_{\frac{1}{2}}(e_1^2))^2 = 0$; $A_{\frac{1}{2}}(e_1^2) \ker(\omega) \subseteq A_{\frac{1}{2}}(e_1^2)$;
- (iv) $y^m \in A_{\frac{1}{2}}(e_1^2)$ for all $y \in \ker(\omega)$.

Proof. It is assumed that the algebra A satisfies the identity (3). Then assertions (i) to (iv) follow from Lemma 2.1, Theorem 2.4, Corollary 2.5 and Lemma 2.7. Reciprocally, we assume that the assertions (i) to (iv) are satisfied. Let $x = \alpha e_1^2 + x_{\frac{1}{2}} + x_0 \in A$ with $x_{\frac{1}{2}} \in A_{\frac{1}{2}}(e_1^2)$ and $x_0 \in A_0(e_1^2)$. We have $x^2 = \alpha^2 e_1^2 + \alpha x_{\frac{1}{2}} + 2x_{\frac{1}{2}} x_0 + x_0^2$ and we show that for any integer $k \geq 3$, $x^k = \alpha^k e_1^2 + z_k + x_0^k$ where (z_j) is a sequence of elements in $A_{\frac{1}{2}}(e_1^2)$. It follows that $x^m = \alpha^m e_1^2 + z_m + x_0^m$ with $z_m \in A_{\frac{1}{2}}(e_1^2)$. Since $A_{\frac{1}{2}}(e_1^2)^2 = 0$ and $y^m \in A_{\frac{1}{2}}(e_1^2)$ for all $y \in \ker(\omega)$, we have $x^m x^m = \alpha^{2m} e_1^2 + \alpha^m (z_m + x_0^m) = \alpha^m (\alpha^m e_1^2 + z_m + x_0^m) = \omega(x)^m x^m$. Thus algebra A satisfies the identity (3) and the proposition is thus established. $\square$

Corollary 2.10. Let (A, ω) be a finite-dimensional baric evolution algebra satisfying the identity (3) for an integer $m_0 > 3$. Then, the algebra A satisfies the identity (3) for all integer $m_1 > m_0$.

Proof. It is assumed that the algebra A satisfies the identity (3) for $m = m_0$ and let $y \in \ker \omega$. The relations $A_{\frac{1}{2}}(e_1^2) \ker(\omega) \subseteq A_{\frac{1}{2}}(e_1^2)$ and $y^{m_0} \in A_{\frac{1}{2}}(e_1^2)$ tell us that for all integer $m_1 > m_0$, $y^{m_1} \in A_{\frac{1}{2}}(e_1^2)$. We deduce from Theorem 2.9 that the algebra A satisfies the identity (3) for $m = m_1$. $\square$

Proposition 2.11. Let $A = Fe_1^2 \oplus A_{\frac{1}{2}}(e_1^2) \oplus A_0(e_1^2)$ be a Peirce decomposition of finite-dimension baric evolution algebra of dimension n satisfying the identity (3) for some $m > 3$. If $\ker(\omega)^m \subseteq A_{\frac{1}{2}}(e_1^2)$, then the algebra A is a Bernstein algebra of order $m - 1$.

Proof. Let $x = \alpha e_1^2 + x_0 + x_{\frac{1}{2}} \in A$ with $\alpha \in F$, $x_{\frac{1}{2}} \in A_{\frac{1}{2}}(e_1^2)$ and $x_0 \in A_0(e_1^2)$. We show that for any integer $k \geq 2$, $x^{[k]} = \alpha^{2^{k-1}} e_1^2 + z_k + x_0^{[k]}$ where (z_j) is a sequence of elements in $A_{\frac{1}{2}}(e_1^2)$. We deduce that $x^{[m]} = \alpha^{2^{m-1}} e_1^2 + z_m + x_0^{[m]}$ with $x_0^{[m]} \in \ker(\omega)^{[m]} \subseteq \ker(\omega)^m \subseteq A_{\frac{1}{2}}(e_1^2)$. It follows that $x^{[m+1]} = (x^{[m]})^2 = \alpha^{2^m} e_1^2 + \alpha^{2^{m-1}} (z_m + x_0^{[m]}) = \alpha^{2^{m-1}} (\alpha^{2^{m-1}} e_1^2 + z_m + x_0^{[m]}) = \omega(x)^{2^{m-1}} x^{[m]}$. We deduce that the algebra A is a Bernstein of order $m - 1$. $\square$

2.2 About the idempotents

Proposition 2.12. Let $A = Fe_1^2 \oplus A_{\frac{1}{2}}(e_1^2) \oplus A_0(e_1^2)$ be a Peirce decomposition of a finite-dimensional baric evolution algebra satisfying the identity (3) for some $m > 3$. Then, the set $\mathcal{I}(A)$ of nonzero idempotents of A is given by:

$$\mathcal{I}(A) = \{e_1^2 + u \mid u \in A_{\frac{1}{2}}(e_1^2)\}.$$

Furthermore, for any idempotent $f = e_1^2 + u$ with $u \in A_{\frac{1}{2}}(e_1^2)$, we have

$$A_{\frac{1}{2}}(f) = A_{\frac{1}{2}}(e_1^2) \text{ and } A_0(f) = \{x_0 - 2ux_0 \mid x_0 \in A_0(e_1^2)\}.$$

Proof. Let $f = e_1^2 + f_{\frac{1}{2}} + f_0$ with $f_{\frac{1}{2}} \in A_{\frac{1}{2}}(e_1^2)$ and $f_0 \in A_0(e_1^2)$, a nonzero idempotent of A . The equality $f = f^2 = e_1^2 + f_{\frac{1}{2}} + f_0^2 + 2f_{\frac{1}{2}}f_0$ gives

$$f_0 = f_0^2 + 2f_{\frac{1}{2}}f_0.$$

Multiplying this last equality by f_0 , we get $f_0^2 = f_0^3 + 2R_{f_0}^2(f_{\frac{1}{2}})$ and we deduce that

$$f_0 = f_0^3 + 2 \sum_{k=1}^2 R_{f_0}^k(f_{\frac{1}{2}}).$$

We show by induction that for any $j \geq 2$, $f_0 = f_0^j + 2 \sum_{k=1}^{j-1} R_{f_0}^k(f_{\frac{1}{2}})$. Thus,

$$f_0 = f_0^m + 2 \sum_{k=1}^{m-1} R_{f_0}^k(f_{\frac{1}{2}}).$$

Since $1 \leq k \leq m-1$ and $f_{\frac{1}{2}} \in A_{\frac{1}{2}}(e_1^2)$, we have $R_{f_0}^k(f_{\frac{1}{2}}) \in A_{\frac{1}{2}}(e_1^2)$. Also $f_0^m \in A_{\frac{1}{2}}(e_1^2)$ according to Lemma 2.7. It follows that $f_0 \in A_{\frac{1}{2}}(e_1^2) \cap A_0(e_1^2) = \{0\}$ and $f = e_1^2 + f_{\frac{1}{2}} \in \mathcal{I}(A)$. Conversely, for any $f_{\frac{1}{2}} \in A_{\frac{1}{2}}(e_1^2)$, the vector $e_1^2 + f_{\frac{1}{2}}$ is a nonzero idempotent of the algebra A .

Let $f = e_1^2 + f_{\frac{1}{2}}$ be a nonzero idempotent of A and $x = x_{\frac{1}{2}} + x_0$ an element of $\ker(\omega)$ with $f_{\frac{1}{2}}, x_{\frac{1}{2}} \in A_{\frac{1}{2}}(e_1^2)$ and $x_0 \in A_0(e_1^2)$. We have $fx = \frac{1}{2}(x_{\frac{1}{2}} + 2f_{\frac{1}{2}}x_0)$

- Assume that $x \in A_{\frac{1}{2}}(f)$. The equality $fx = \frac{1}{2}x$ leads to $x_0 = 2f_{\frac{1}{2}}x_0 \in A_{\frac{1}{2}}(e_1^2)$. It follows that $x_0 = 0$ and $x = x_{\frac{1}{2}} \in A_{\frac{1}{2}}(e_1^2)$. Reciprocally, for any $y \in A_{\frac{1}{2}}(e_1^2)$, we have $fy = (e_1^2 + f_{\frac{1}{2}})y = \frac{1}{2}y$ and, consequently, $y \in A_{\frac{1}{2}}(f)$. Thus, $A_{\frac{1}{2}}(f) = A_{\frac{1}{2}}(e_1^2)$.
- Assume that $x \in A_0(f)$. The equality $fx = 0$ gives $x_{\frac{1}{2}} = -2f_{\frac{1}{2}}x_0$. So $x = -2f_{\frac{1}{2}}x_0 + x_0 \in \{y_0 - 2f_{\frac{1}{2}}y_0 \mid y_0 \in A_0(e_1^2)\}$. Conversely, for all $x_0 \in A_0(e_1^2)$, we have $f(-2f_{\frac{1}{2}}x_0 + x_0) = (e_1^2 + f_{\frac{1}{2}})(-2f_{\frac{1}{2}}x_0 + x_0) = -f_{\frac{1}{2}}x_0 + f_{\frac{1}{2}}x_0 = 0$. We deduce that $A_0(f) = \{y_0 - 2f_{\frac{1}{2}}y_0 \mid y_0 \in A_0(e_1^2)\}$. □

In [16], the authors give a characterisation of the automorphisms of an evolution algebra satisfying the identity (2). However, in the relation (6) of their Theorem 5.6, the term " $-2u_{\sigma}g_{\sigma}((x_0y_0)_0)$ " is too much, as shown by the proposition below:

Proposition 2.13. *Let $A = Fe_1^2 \oplus A_{\frac{1}{2}}(e_1^2) \oplus A_0(e_1^2)$ be a Peirce decomposition of a finite-dimensional baric evolution algebra satisfying the identity (3) for some $m > 3$. A bijective linear map σ is an algebra automorphism of the algebra A if, and only if, there exists an element $u_{\sigma} \in A_{\frac{1}{2}}(e_1^2)$ and two morphisms $f_{\sigma} \in \text{GL}_F(A_{\frac{1}{2}}(e_1^2))$ and $g_{\sigma} \in \text{GL}_F(A_0(e_1^2))$ such that for all $x_{\frac{1}{2}} \in A_{\frac{1}{2}}(e_1^2)$ and $x_0 \in A_0(e_1^2)$ the following conditions hold:*

- (i) $\sigma(e_1^2) = e_1^2 + u_{\sigma}$;
- (ii) $\sigma(x_{\frac{1}{2}}) = f_{\sigma}(x_{\frac{1}{2}})$;
- (iii) $\sigma(x_0) = g_{\sigma}(x_0) - 2u_{\sigma}g_{\sigma}(x_0)$;
- (iv) $f_{\sigma}(x_{\frac{1}{2}}x_0) = f_{\sigma}(x_{\frac{1}{2}})g_{\sigma}(x_0)$;
- (v) $g_{\sigma}((x_0y_0)_0) = (g_{\sigma}(x_0)g_{\sigma}(y_0))_0$;
- (vi) $f_{\sigma}((x_0y_0)_{\frac{1}{2}}) = (g_{\sigma}(x_0)g_{\sigma}(y_0))_{\frac{1}{2}} - 2g_{\sigma}(x_0)(u_{\sigma}g_{\sigma}(y_0)) - 2g_{\sigma}(y_0)(u_{\sigma}g_{\sigma}(x_0))$.

Proof. Assume that σ is an algebras automorphism. The assertions (i), (ii) and (iii) follow from Proposition 2.12. The relation $f_{\sigma}(x_0x_{\frac{1}{2}}) = \sigma(x_0x_{\frac{1}{2}}) = \sigma(x_0)\sigma(x_{\frac{1}{2}}) = f_{\sigma}(x_0)g_{\sigma}(x_{\frac{1}{2}})$ gives the assertion (iv). The

assertions (v) and (vi) follow from the relation

$$\begin{aligned}
 f_{\sigma}((x_0 y_0)_{\frac{1}{2}}) + g_{\sigma}((x_0 y_0)_0) &= \sigma(x_0 y_0) \\
 &= \sigma(x_0) \sigma(y_0) \\
 &= (g_{\sigma}(x_0) - 2u_{\sigma} g_{\sigma}(x_0))(g_{\sigma}(y_0) - 2u_{\sigma} g_{\sigma}(y_0)) \\
 &= (g_{\sigma}(x_0) g_{\sigma}(y_0))_{\frac{1}{2}} + (g_{\sigma}(x_0) g_{\sigma}(y_0))_0 - 2(g_{\sigma}(x_0)(u_{\sigma} g_{\sigma}(y_0)) - \\
 &\quad 2(g_{\sigma}(y_0)(u_{\sigma} g_{\sigma}(x_0))).
 \end{aligned}$$

By identifying traces on $A_{\frac{1}{2}}(e_1^2)$ and on $A_0(e_1^2)$, we obtain the desired statements. Conversely, It is assumed that the assertions (i) to (vi) are satisfied and let $x = \alpha e_1^2 + x_{\frac{1}{2}} + x_0$, $y = \beta e_1^2 + y_{\frac{1}{2}} + y_0 \in A$ with $\alpha, \beta \in F$, $x_{\frac{1}{2}}, y_{\frac{1}{2}} \in A_{\frac{1}{2}}(e_1^2)$, $x_0, y_0 \in A_0(e_1^2)$. We have

$$\begin{aligned}
 xy &= \alpha \beta e_1^2 + \frac{1}{2}(\alpha y_{\frac{1}{2}} + \beta x_{\frac{1}{2}}) + x_{\frac{1}{2}} y_0 + x_0 y_{\frac{1}{2}} + x_0 y_0 \\
 \sigma(xy) &= \alpha \beta (e_1^2 + u_{\sigma}) + \frac{1}{2}(\alpha f_{\sigma}(y_{\frac{1}{2}}) + \beta f_{\sigma}(x_{\frac{1}{2}})) + f_{\sigma}(x_{\frac{1}{2}} y_0) + f_{\sigma}(x_0 y_{\frac{1}{2}}) \\
 &\quad + f_{\sigma}((x_0 y_0)_{\frac{1}{2}}) + g_{\sigma}((x_0 y_0)_0) \\
 &= \alpha \beta (e_1^2 + u_{\sigma}) + \frac{1}{2}(\alpha f_{\sigma}(y_{\frac{1}{2}}) + \beta f_{\sigma}(x_{\frac{1}{2}})) + f_{\sigma}(x_{\frac{1}{2}}) g_{\sigma}(y_0) + f_{\sigma}(y_{\frac{1}{2}}) g_{\sigma}(x_0) \\
 &\quad + g_{\sigma}(x_0) g_{\sigma}(y_0) - 2g_{\sigma}(x_0)(u_{\sigma} g_{\sigma}(y_0)) - 2g_{\sigma}(y_0)(u_{\sigma} g_{\sigma}(x_0)) \\
 &= (\alpha (e_1^2 + u_{\sigma}) + f_{\sigma}(x_{\frac{1}{2}}) + g_{\sigma}(x_0) - 2u_{\sigma} g_{\sigma}(x_0)) \\
 &\quad (\beta (e_1^2 + u_{\sigma}) + f_{\sigma}(y_{\frac{1}{2}}) + g_{\sigma}(y_0) - 2u_{\sigma} g_{\sigma}(y_0)) = \sigma(x) \sigma(y).
 \end{aligned}$$

We get the proposition. $\square$

Proposition 2.12 and Proposition 2.13 show that the form of the idempotents and the characterisation of an algebras automorphisms of the algebra satisfying the identity (3) for some $m > 3$ do not depend on the integer m .

2.3 Link with Bernstein algebras

Let (A, ω) be a Bernstein algebra over a commutative field F of $\text{Char}(F) \neq 2$. In [18], the author shows that the algebra A admits nonzero idempotents and for any nonzero idempotent e , the algebra A admits the following Peirce decomposition $A = Ke \oplus U_e \oplus V_e$ where $U_e = \{x \in A \mid ex = \frac{1}{2}x\}$ and $V_e = \{x \in A \mid ex = 0\}$. Furthermore, the Peirce subspaces U_e and V_e satisfy the following relations:

$$U_e V_e \subseteq U_e, V_e^2 \subseteq U_e, U_e^2 \subseteq V_e \text{ and } U_e V_e^2 = 0.$$

Theorem 2.14. Let $A = Fe_1^2 \oplus A_{\frac{1}{2}}(e_1^2) \oplus A_0(e_1^2)$ be a Peirce decomposition of finite-dimensional baric evolution algebra satisfying the identity (3) for some $m > 3$. Then A is a Bernstein algebra if, and only if, $(A_0(e_1^2))^2 \subset A_{\frac{1}{2}}(e_1^2)$.

Proof. It is assumed that A is a Bernstein algebra. Then $(A_0(e_1^2))^2 \subset A_{\frac{1}{2}}(e_1^2)$. Reciprocally, if $(A_0(e_1^2))^2 \subset A_{\frac{1}{2}}(e_1^2)$ then, for any $x = \alpha e_1^2 + x_0 + x_{\frac{1}{2}} \in A$, we have $x^2 = \alpha^2 e_1^2 + \alpha x_{\frac{1}{2}} + x_0^2 + 2x_0 x_{\frac{1}{2}}$ and $x^2 x^2 = \alpha^4 e_1^2 + \alpha^3 x_{\frac{1}{2}} + \alpha^2 (x_0^2 + 2x_0 x_{\frac{1}{2}}) = \alpha^2 x^2$. We deduce that A is a Bernstein algebra. $\square$

Proposition 2.15. Let $A = Fe_1^2 \oplus A_{\frac{1}{2}}(e_1^2) \oplus A_0(e_1^2)$ be a Peirce decomposition of finite-dimensional baric evolution algebra satisfying the identity (3) for some $m > 3$ such that $(\ker \omega)^2 = A_{\frac{1}{2}}(e_1^2)$. Then, A is a Bernstein algebra.

Proof. This proposition follows from Proposition 2.11. It is sufficient to take $m = 2$ in Proposition 2.11. $\square$

The following results given for a finite-dimensional baric evolution algebra satisfying a train identity of degree 2 and exponent 3, remain true for a finite-dimensional baric evolution algebra satisfying the identity (3) for some $m > 3$. We give proofs based on Proposition 2.15.

Corollary 2.16. *Let $A = Fe_1^2 \oplus A_{\frac{1}{2}}(e_1^2) \oplus A_0(e_1^2)$ be a Peirce decomposition of a finite-dimensional baric evolution algebra satisfying the identity (3) for some $m > 3$ such that $A_{\frac{1}{2}}(e_1^2) \neq 0$ and $\dim(\ker \omega)^2 = 1$. Then, A is a Bernstein algebra.*

Proof. We have $0 \neq A_{\frac{1}{2}}(e_1^2) \subset (\ker \omega)^2$. Since $\dim(\ker \omega)^2 = 1$, it follows that $A_{\frac{1}{2}}(e_1^2) = (\ker \omega)^2$. Proposition 2.15 tells us that A is a Bernstein algebra. $\square$

Corollary 2.17. *Let $A = Fe_1^2 \oplus A_{\frac{1}{2}}(e_1^2) \oplus A_0(e_1^2)$ be a Peirce decomposition of a finite-dimensional baric evolution algebra satisfying the identity (3) for some $m > 3$ such that $\text{Card}(\text{Support}(e_1^2)) = \dim(A)$. Then, A is a Bernstein algebra.*

Proof. The equality $\text{Card}(\text{Support}(e_1^2)) = \dim(A)$ leads to $(\ker \omega)^2 = A_{\frac{1}{2}}(e_1^2)$ because the annihilator of A is $\langle e_i \in B \mid e_i^2 = 0 \rangle$ [8, Lemma 2.7]. Thus, we obtain the corollary. $\square$

2.4 Link with power-associative algebras

Definition 2.18. A commutative F -algebra A is power-associative if for any $x \in A$, $x^i x^j = x^{i+j}$ for all $i, j \geq 1$ integers.

Theorem 2.19. [2] Let F be a commutative field of $\text{Char}(F) \neq 2, 3, 5$. A commutative F -algebra A is power-associative if, and only if, $x^2 x^2 = x^4$ for all $x \in A$.

The proposition below shows that the class of power-associative baric evolution algebra is included in the class of the algebras satisfying the identity (3) for some $m > 3$.

Proposition 2.20. *Let (A, ω) be a finite-dimensional power-associative baric evolution algebra. Then, the algebra A satisfies the identity (3) with $m = 4$.*

Proof. It is assumed that A is a power-associative algebra. [13, Remark 3.20] tells us that the Peirce decomposition of the algebra A is given by the direct sum of algebras $A = Fe_1^2 \oplus A_0(e_1^2)$ where e_1^2 is the unique nonzero idempotent of the algebra A and $\ker(\omega) = A_0(e_1^2)$. Since $A_{\frac{1}{2}}(e_1^2) = 0$, Lemma 2.7 tells us that $A_0(e_1^2)$ is a nilalgebra. Furthermore, following [14, Theorem 5 and Corollary 2] we deduce that $A_0(e_1^2)$ is a nil power-associative evolution algebra of nilindex at most 4. It follows that for all $y \in \ker(\omega)$ we have $y^4 = 0 \in A_{\frac{1}{2}}(e_1^2)$. Theorem 2.9 shows that the algebra A satisfies the identity (3) for $m = 4$. $\square$

The class of power-associative baric evolution algebras is strictly included in that of algebras satisfying the identity (3) for some $m > 3$. Indeed, the algebra defined in Example 2.2 is not a power-associative algebra because $e_5^2 e_5^2 \neq 0 = e_5^4$.

Corollary 2.21. *Let (A, ω) be a finite-dimensional power-associative baric evolution algebra. Then, the algebra A is Jordan algebra and train algebra with train equation $x^4 - \omega(x)x^3 = 0$.*

Proof. This result follows from Proposition 2.20 and from [4, Corollary 4.5 and Proposition 5.2]. $\square$

3 Classification

In [16, 7], the authors give the classification of evolution algebra satisfying strictly the identities $x^2x^2 = \omega(x)^2x^2$ and $x^3x^3 = \omega(x)^3x^3$ in dimension ≤ 4 . We continue this classification in dimension ≤ 5 for the evolution algebras verifying the identity (3) with $m > 3$.

Definition 3.1. We say that a baric evolution algebra (A, ω) satisfies strictly the identity (3) for some $m > 3$ if (3) holds for m but it does not hold for any integer strictly less than m .

Proposition 3.2. There is no two-dimensional baric evolution algebra satisfying the identity (3) for some $m > 3$.

Proof. Assume that A is 2-dimensional baric evolution algebra satisfying the identity (3) for some $m > 3$. Since $A_0(e_1^2) \neq 0$ and $\dim(\ker \omega) = 1$, we have $A_0(e_1^2) = \ker \omega = Ke_2$ and $A_{\frac{1}{2}}(e_1^2) = 0$. Let $e_2^2 = \alpha e_2$ with $\alpha \in F$. According to the assertion (iii) of Lemma 2.1, we have $e_2^3 = 2e_1^2e_2^3$, this leads to $0 = e_2^3 = \alpha^2e_2$, i.e. $\alpha = 0$ and $e_2^2 = 0$. Let $x = ae_1^2 + x_2e_2 \in A$, we have $x^2 = a^2e_1^2$ and $x^2x^2 = \omega(x)^2x^2$. It follows that A is a Bernstein algebra and since $A_{\frac{1}{2}}(e_1^2) = 0$, it is also a train algebra. [18, Lemma 9.11] tells us that the algebra A is a train evolution algebra of rank 2: this is impossible. Thus, there is no evolution algebra of 2-dimensional satisfying the identity (3) for some $m > 3$. $\square$

Lemma 3.3. Let (A, ω) be a baric evolution algebra of dimension $n \geq 3$ satisfying the identity (3) for some $m > 3$. If $\text{Card}(\text{Support}(e_1^2)) = 1$ or 2, then A is a train algebra of rank at most $m + 1$.

Proof. • If $\text{Card}(\text{Support}(e_1^2)) = 1$, then $e_1^2 = e_1$ and $A_{\frac{1}{2}}(e_1^2) = 0$. Proposition 2.8 tells us that (A, ω) is a train algebra of rank at most $m + 1$.
• If $\text{Card}(\text{Support}(e_1^2)) = 2$, then without loss of generality, set $a_{12} \neq 0$ and $a_{1i} = 0$ for $3 \leq i \leq n$. Since $a_{12} \neq 0$, the equality $e_1^2 = e_1^2e_1^2 = e_1^2 + a_{12}^2e_2^2$ leads to $a_{12}^2e_2^2 = 0$, i.e. $e_2^2 = 0$ and we have $e_1^2e_2 = 0$. Furthermore, $e_1^2e_j = 0$ for $3 \leq j \leq n$. It follows that $A_{\frac{1}{2}}(e_1^2) = 0$ and (A, ω) is a train algebra of rank at most $m + 1$. $\square$

Lemma 3.4. Let (A, ω) be a baric evolution F -algebra of dimension $n \geq 3$ and satisfying the identity (3) for some $m > 3$. If $\text{Card}(\text{Support}(e_1^2)) = n - 1$, then the algebra A satisfies the identity (2).

Proof. Without loss of generality, we set $a_{1n} = 0$, $a_{1j} \neq 0$ for $2 \leq j \leq n-1$ and $x = x_1e_1 + \sum_{j=2}^{n-1} x_je_j + x_ne_n \in A$. We have $x^2 = x_1^2e_1^2 + \sum_{j=2}^{n-1} x_j^2e_j^2 + x_n^2e_n^2$ and $x^3 = x_1^3e_1^3 + z$ with $z = x_n^3e_n^3 + \sum_{j=2}^{n-1} (x_1^2x_je_1^2e_j + x_n^2x_je_n^2e_j + x_j^2x_ne_j^2e_n + \sum_{k=2}^{n-1} x_j^2x_ke_j^2e_k) \in A_{\frac{1}{2}}(e_1^2)$ because $e_n^3, e_1^2e_j, e_n^2e_j, e_j^2e_n, e_j^2e_k \in A_{\frac{1}{2}}(e_1^2)$ for $2 \leq j, k \leq n-1$. It follows that $x^3x^3 = x_1^6e_1^6 + x_1^3xz = x_1^3(x_1^3e_1^3 + z) = \omega(x)^3x^3$. Thus, we obtain the lemma. $\square$

Proposition 3.5. There is no baric evolution algebra of dimension 3 or 4 satisfying strictly the identity (3) for $m > 3$.

Proof. • Suppose that $\dim(A) = 3$, then $\text{Card}(\text{Support}(e_1^2)) = 1, 2$ or 3. Thus, the algebra A is either a Bernstein algebra or a train algebra. In the particular case where $\text{Card}(\text{Support}(e_1^2)) = 2$, it verifies the identity (2) and it is a train algebra of rank at most 4.
• It is assumed that $\dim(A) = 4$, $\text{Card}(\text{Support}(e_1^2)) = 1, 2, 4 - 1$ or 4, then A is a Bernstein algebra, a train algebra or satisfies the identity (2). $\square$

Lemma 3.6. Let $A = Fe_1^2 \oplus A_{\frac{1}{2}}(e_1^2) \oplus A_0(e_1^2)$ be a Peirce decomposition of baric evolution algebra of dimension $n \geq 3$ and satisfying the identity (3) for some $m > 3$. If there is a unique $i_0 \in \{2, \dots, n\}$ such that $e_{i_0}^2 \notin A_{\frac{1}{2}}(e_1^2)$, then the algebra A verifies the identity (2).

Proof. Without loss the generality, we set $i_0 = n$ and let $x = x_1 e_1 + \sum_{j=2}^{n-1} x_j e_j + x_n e_n \in A$. We have $x^2 = x_1^2 e_1^2 + \sum_{j=2}^{n-1} x_j^2 e_j^2 + x_n^2 e_n^2$, $x^3 = x_1^3 e_1^2 + z$ with $z = x_1^2 x_n e_1^2 e_n + x_n^3 e_n^3 + \sum_{j=2}^{n-1} (x_1^2 x_j e_1^2 e_j + x_n^2 x_j e_n^2 e_j + x_j^2 x_n e_j^2 e_n) + \sum_{j,k=2}^{n-1} x_j^2 x_k e_j^2 e_k \in A_{\frac{1}{2}}(e_1^2)$ because for all $2 \leq j, k \leq n-1$, we have $e_1^2 e_j, e_1^2 e_n, e_n^2 e_j, e_j^2 e_n, e_j^2 e_k, e_n^3 \in A_{\frac{1}{2}}(e_1^2)$. It follows that $x^3 x^3 = x_1^6 e_1^2 + x_1^3 z = \omega(x)^3 x^3$ and the algebra A verifies the identity (2). $\square$

Lemma 3.7. Let $A = Fe_1^2 \oplus A_{\frac{1}{2}}(e_1^2) \oplus A_0(e_1^2)$ be a Peirce decomposition of baric evolution algebra of dimension $n \geq 3$ satisfying the identity (3) for some $m > 3$. For all $i, j \in \{2, \dots, n\}$ verifying $a_{ii} = a_{jj} = 0$, there is an integer $k_0 \geq 1$ such that $(e_i + e_j)^{2k_0} = (a_{ij} a_{ji})^{k_0-1} (e_i^2 + e_j^2) \in A_{\frac{1}{2}}(e_1^2)$. Moreover, if $a_{ij} a_{ji} \neq 0$, then $e_i^2, e_j^2 \in A_{\frac{1}{2}}(e_1^2)$.

Proof. Let $i, j \in \{2, \dots, n\}$, we have $(e_i + e_j)^2 = e_i^2 + e_j^2 = (a_{ij} a_{ji})^{1-1} (e_i^2 + e_j^2)$ and suppose that $(e_i + e_j)^{2k} = (a_{ij} a_{ji})^{k-1} (e_i^2 + e_j^2)$. Then, $(e_i + e_j)^{2(k+1)} = (a_{ij} a_{ji})^{k-1} ((e_i^2 + e_j^2)(e_i + e_j))(e_i + e_j) = (a_{ij} a_{ji})^{k-1} ((a_{ij} e_j^2 + a_{ji} e_i^2))(e_i + e_j) = (a_{ij} a_{ji})^k (e_i^2 + e_j^2)$. We denote by k_0 , the smallest integer such that $2k_0 \geq m$. Since $(e_i + e_j)^m \in A_{\frac{1}{2}}(e_1^2)$, we have $(e_i + e_j)^{2k_0} = (a_{ij} a_{ji})^{k_0-1} (e_i^2 + e_j^2) \in A_{\frac{1}{2}}(e_1^2)$. Furthermore, for $a_{ij} a_{ji} \neq 0$, we will get $e_j^2 + e_i^2 \in A_{\frac{1}{2}}(e_1^2)$ and by multiplying the vector $e_j^2 + e_i^2$ by e_j and e_i respectively, we obtain $e_i^2 e_j, e_j^2 e_i \in A_{\frac{1}{2}}(e_1^2)$, i.e. $e_i^2, e_j^2 \in A_{\frac{1}{2}}(e_1^2)$. $\square$

Proposition 3.8. Let (A, ω) be a baric evolution algebra of dimension 5 satisfying strictly the identity (3) with $m > 3$. It is assumed that A is neither a Bernstein algebra nor a power-associative algebra. Then A is isomorphic to the algebra $A(\gamma, \gamma_1, \gamma_2, \gamma_3) : e^2 = e, eu = \frac{1}{2}u, uv_1 = \gamma u, v_2^2 = \gamma_1 u + v_1, v_3^2 = \gamma_2 u + \gamma_3 v_1 + v_2$ with $\gamma_1, \gamma_2, \gamma_3 \in K$ and $\gamma \in K^*$. The products that are not mentioned are void.

Proof. It is assumed that A is an evolution algebra with the natural basis $B = \{e_1, \dots, e_5\}$. If $\text{Card}(\text{Support}(e_1^2)) = 1, 2, 5 - 1, 5$ then A is a Bernstein algebra, a train algebra or verifies the identity (2). Thus, $\text{Card}(\text{Support}(e_1^2)) = 3$ and without loss of generality, we assume that $a_{12} a_{13} \neq 0$ and $a_{14} = a_{15} = 0$. We deduce that $e_2^2, e_3^2 \in A_{\frac{1}{2}}(e_1^2)$ and $e_4, e_5 \in A_0(e_1^2)$.

- The equality $e_1^2 = e_1^2 e_1^2 = e_1^2 + a_{12}^2 e_2^2 + a_{13}^2 e_3^2$ leads to

$$e_3^2 = -a_{13}^{-2} a_{12}^2 e_2^2.$$

We deduce that $A_{\frac{1}{2}}(e_1^2) = Fe_2^2$.

- The equality $e_2^2 = 2e_1^2 e_2^2 = 2(a_{12} a_{22} e_2^2 + a_{13} a_{23} e_3^2) = 2a_{12}(a_{22} - a_{13}^{-1} a_{12} a_{23}) e_2^2$ gives

$$a_{22} = \frac{1}{2} a_{12}^{-1} + a_{13}^{-1} a_{12} a_{23}.$$

- Lemma 3.6 and Proposition 2.15 tell us that $a_{24} = a_{25} = a_{44} = a_{55} = 0$, otherwise e_4^2 or e_5^2 would belong to $A_{\frac{1}{2}}(e_1^2)$ and the algebra A would be a Bernstein algebra or would satisfy the identity (2).
- The relation $0 = e_2^2 e_2^2 = a_{22}^2 e_2^2 + a_{23}^2 e_3^2 = (\frac{1}{4} a_{12}^{-2} + a_{13}^{-1} a_{23}) e_2^2$ leads to

$$a_{23} = -\frac{1}{4} a_{12}^{-2} a_{13} \text{ and } a_{22} = \frac{1}{4} a_{12}^{-1}.$$

- Lemma 3.7 tells us that $a_{45} a_{54} = 0$, otherwise A would be a Bernstein algebra. Thus, we distinguish three cases:

- $a_{45} = a_{54} = 0$, then $e_4^2 = a_{42} e_2 + a_{43} e_3$, $e_5^2 = a_{52} e_2 + a_{53} e_3$ and we set $x = x_1 e_1 + \sum_{j=2}^5 x_j e_j$. We have $x^2 = x_1^2 e_1^2 + \sum_{j=2}^5 x_j^2 e_j^2$ and $x^3 = x_1^3 e_1^2 + z$ with $z = \sum_{j=2}^5 (x_1^2 x_j e_1^2 e_j + \sum_{k=2}^5 x_j^2 x_k e_j^2 e_k) \in A_{\frac{1}{2}}(e_1^2)$ because for all $2 \leq j, k \leq 5$, $e_1^2 e_j, e_j^2 e_k \in A_{\frac{1}{2}}(e_1^2)$. We deduce that $(x^3)^2 = x_1^6 e_1^2 + x_1^3 z = \omega(x)^3 x^3$. It follows that the algebra A verifies the identity (2).

- (ii) $a_{45} = 0$ and $a_{54} \neq 0$, then $e_4^2 = a_{42}e_2 + a_{43}e_3$ and $e_5^2 = a_{52}e_2 + a_{53}e_3 + a_{54}e_4$. Since the family (e_2^2, e_5^2) is linearly independent, Lemma 3.6 indicate that the family (e_2^2, e_4^2) is linearly independent otherwise the algebra A would satisfy the identity (2). It follows that $(a_{42} + a_{12}a_{13}^{-1}a_{43}) \neq 0$.
- (iii) $a_{45} \neq 0$ and $a_{54} = 0$, then if we swap the vectors e_4 and e_5 of the natural basis, we return to the previous case.

From above, we deduce that the multiplication table of (A, ω) in the natural basis

$B = (e_1, e_2, e_3, e'_4, e_5)$, where $e'_4 = a_{54}e_4$, is the following:

$$\begin{cases} e_1^2 &= e_1 + a_{12}e_2 + a_{13}e_3, \\ e_2^2 &= \frac{1}{4}a_{12}^{-2}(a_{12}e_2 - a_{13}e_3), \\ e_3^2 &= -a_{13}^{-2}a_{12}^2e_2^2, \\ e_4'^2 &= a_{42}'e_2 + a_{43}'e_3, \\ e_5^2 &= a_{52}e_2 + a_{53}e_3 + e_4', \end{cases} \quad \text{with } a_{42}' + a_{12}a_{13}^{-1}a_{43}' \neq 0.$$

We have $(\ker \omega)^2 = \langle e_2^2, e_4'^2, e_5^2 \rangle$, $(\ker \omega)^3 = \langle e_2^2, e_4'^2 \rangle$ and $(\ker \omega)^4 = \langle e_2^2 \rangle = A_{\frac{1}{2}}(e_1^2)$. Set $e = e_1^2$, $u = 2a_{12}e_2^2$, $v_1 = e_2 - 2e_1^2e_2$, $v_2 = e_4'$ and $v_3 = e_5$. Solving the system

$$\begin{cases} u = \frac{1}{2}e_2 - \frac{1}{2}a_{12}^{-1}a_{13}e_3, \\ v_1 = \frac{1}{2}e_2 + \frac{1}{2}a_{12}^{-1}a_{13}e_3, \end{cases}$$

we get $e_2 = u + v_1$ and $e_3 = -a_{12}a_{13}^{-1}(u - v_1)$. Thus, the multiplication table of the algebra A in the basis $\{e, u, v_1, v_2, v_3\}$ is given by: $e^2 = e$, $eu = \frac{1}{2}u$, $uv_1 = \frac{1}{4}a_{12}^{-1}u$, $v_2^2 = (a_{42}' - a_{12}a_{13}^{-1}a_{43}')u + (a_{42}' + a_{13}^{-1}a_{12}a_{43}')v_1 = \delta_1 u + \delta_2 v_1$ with $\delta_2 \neq 0$, $v_3^2 = (a_{52} - a_{12}a_{13}^{-1}a_{53})u + (a_{52} + a_{13}^{-1}a_{12}a_{53})v_1 + v_2 = \delta_3 u + \delta_4 v_1 + v_2$. Furthermore, the equality $(\ker \omega)^4 = A_{\frac{1}{2}}(e_1^2)$ and Theorem 2.9 tell us that the algebra A verifies the identity (3) with $m = 4$. By setting $v_1' = \delta_2 v_1$, we get the desired algebra. $\square$

Proposition 3.9. Assume that F is an algebraically closed field and (A, ω) is the algebra defined in Proposition 3.8. Then, the automorphism group of the algebra A is given by Table 1 below:

Table 1

Conditions on structural constants	$\text{Aut}_K(A)$	Conditions on the matrix coefficients
$\gamma_1 = \gamma_2 = \gamma_3 = 0$	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & \beta & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & \varepsilon_{33}^2 & 0 \\ 0 & 0 & 0 & 0 & \varepsilon_{33} \end{pmatrix}$	$\varepsilon_{33}^4 = 1$ and $\beta \neq 0$
$\gamma_1 = \gamma_2 = 0$ and $\gamma_3 \neq 0$	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & \beta & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & \varepsilon_{33} \end{pmatrix}$	$\varepsilon_{33}^2 = 1$ and $\beta \neq 0$
$\gamma_1 = \gamma_3 = 0$ and $\gamma_2 \neq 0$	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & \varepsilon_{33}^2 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & \varepsilon_{33}^2 & 0 \\ 0 & 0 & 0 & 0 & \varepsilon_{33} \end{pmatrix}$	$\varepsilon_{33}^4 = 1$
$\gamma_1 \neq 0$ and $\gamma_2 = \gamma_3 = 0$	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & \varepsilon_{33}^2 & 0 \\ 0 & 0 & 0 & 0 & \varepsilon_{33} \end{pmatrix}$	$\varepsilon_{33}^4 = 1$

Table 1

Conditions on structural constants	$\text{Aut}_K(A)$	Conditions on the matrix coefficients
$(\gamma_1\gamma_2, \gamma_1\gamma_3, \gamma_2\gamma_3) \neq 0$	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & \varepsilon_{33} \end{pmatrix}$	$\varepsilon_{33}^2 = 1$

Proof. Let $\sigma \in \text{Aut}_K(A)$. The assertions (ii) to (iii) of Proposition 2.13 tell us that $\sigma(e_1^2) = e_1^2 + \alpha u$, $f_\sigma(u) = \beta u$ and we set $g_\sigma(v_i) = \varepsilon_{i1}v_1 + \varepsilon_{i2}v_2 + \varepsilon_{i3}v_3$ with $1 \leq i \leq 3$.

(1) The assertion (iv) of Proposition 2.13 leads to:

- $\gamma f_\sigma(u) = f_\sigma(uv_1) = f_\sigma(u)g_\sigma(v_1) = \beta\varepsilon_{11}uv_1$, i.e. $\gamma\beta(\varepsilon_{11} - 1)u = 0$. Since $\gamma\beta \neq 0$, we have $\varepsilon_{11} = 1$.
- For $i = 2$ or 3 , we have $0 = f_\sigma(uv_i) = f_\sigma(u)g_\sigma(v_i) = \gamma\beta\varepsilon_{i1}u$, i.e. $\varepsilon_{21} = \varepsilon_{31} = 0$.

(2) The assertion (v) of Proposition 2.13 gives:

- $0 = g_\sigma(v_1^2) = ((v_1 + \varepsilon_{12}v_2 + \varepsilon_{13}v_3)^2)_0 = (\varepsilon_{12}^2 + \varepsilon_{13}^2\gamma_3)v_1 + \varepsilon_{13}^2v_2$. It follows that $\varepsilon_{12} = \varepsilon_{13} = 0$ and $g_\sigma(v_1) = v_1$.
- $v_1 = g_\sigma(v_1) = g_\sigma((v_2^2)_0) = ((g_\sigma(v_2))^2)_0 = (\varepsilon_{22}^2 + \varepsilon_{23}^2\gamma_3)v_1 + \varepsilon_{23}^2v_2$. We deduce that $\varepsilon_{23} = 0$, $\varepsilon_{22}^2 = 1$ and $g_\sigma(v_2) = \varepsilon_{22}v_2$.
- $0 = g_\sigma(v_2v_3) = (g_\sigma(v_2)g_\sigma(v_3))_0 = \varepsilon_{32}\varepsilon_{22}v_1$, i.e. $\varepsilon_{32} = 0$. So $g_\sigma(v_3) = \varepsilon_{33}v_3$.
- $\gamma_3v_1 + \varepsilon_{22}v_2 = g_\sigma((v_3^2)_0) = ((g_\sigma(v_3))^2)_0 = \varepsilon_{33}^2\gamma_3v_1 + \varepsilon_{33}^2v_2$, i.e. $\varepsilon_{33}^2 = \varepsilon_{22}$ and $\gamma_3(\varepsilon_{33}^2 - 1) = 0$.

(3) The assertion (vi) of Proposition 2.13 gives:

- $0 = f_\sigma(v_1^2) = -4g_\sigma(v_1)(\alpha u g_\sigma(v_1)) = -4v_1(\alpha uv_1) = -4\alpha\gamma^2u$, i.e. $\alpha = 0$ and $\sigma(e_1^2) = e_1^2$.
- $\gamma_1\beta u = f_\sigma((v_2^2)_{\frac{1}{2}}) = ((g_\sigma(v_2))^2)_{\frac{1}{2}} = \varepsilon_{22}^2\gamma_1u$, i.e. $\gamma_1(\beta - 1) = 0$.
- $\gamma_2\beta u = f_\sigma((v_3^2)_{\frac{1}{2}}) = ((g_\sigma(v_3))^2)_{\frac{1}{2}} = \varepsilon_{33}^2\gamma_2u$ i.e. $\gamma_2(\beta - \varepsilon_{33}^2) = 0$.

From the above, we deduce that the matrix of σ in the basis $(e_1^2, u, v_1, v_2, v_3)$ is of the form:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & \beta & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & \varepsilon_{33}^2 & 0 \\ 0 & 0 & 0 & 0 & \varepsilon_{33} \end{pmatrix}$$

with

$$\beta \neq 0, \varepsilon_{33}^4 = 1, \gamma_1(\beta - 1) = 0, \gamma_2(\beta - \varepsilon_{33}^2) = 0 \text{ and } \gamma_3(\varepsilon_{33}^2 - 1) = 0. \quad (13)$$

Taking into account the identities in the relation (13), we obtain automorphism group of the algebra A given by Table 1. $\square$

From Proposition 3.8 and Proposition 3.9, we deduce the corollary below:

Corollary 3.10. *Let F be an algebraically closed field and (A, ω) be a five-dimensional baric evolution F -algebra satisfying strictly the identity (3). It is assumed that A is neither a Bernstein algebra nor a power-associative algebra. Then, the algebra A is isomorphic to one of the following pairwise non-isomorphic algebras (where $\gamma \neq 0$ and the products that are not mentioned are void):*

- $A_1(\gamma): e^2 = e; eu = \frac{1}{2}u; uv_1 = \gamma u; v_2^2 = v_1; v_3^2 = v_2$.
- $A_2(\gamma, \gamma_3): e^2 = e; eu = \frac{1}{2}u; uv_1 = \gamma u; v_2^2 = v_1; v_3^2 = \gamma_3v_1 + v_2$ with $\gamma_3 \neq 0$.
- $A_3(\gamma, \gamma_2): e^2 = e; eu = \frac{1}{2}u; uv_1 = \gamma u; v_2^2 = v_1; v_3^2 = \gamma_2u + v_2$ with $\gamma_2 \neq 0$.
- $A_4(\gamma, \gamma_1): e^2 = e; eu = \frac{1}{2}u; uv_1 = \gamma u; v_2^2 = \gamma_1u + v_1; v_3^2 = v_2$ with $\gamma_1 \neq 0$.
- $A_5(\gamma, \gamma_1, \gamma_2, \gamma_3): e^2 = e; eu = \frac{1}{2}u; uv_1 = \gamma u; v_2^2 = \gamma_1u + v_1; v_3^2 = \gamma_2u + \gamma_3v_1 + v_2$ with $(\gamma_1\gamma_2, \gamma_1\gamma_3, \gamma_2\gamma_3) \neq 0$.

Proposition 3.11. Suppose that $F = \mathbb{R}$ and (A, ω) is the algebra defined in Proposition 3.8. Then, the automorphism group of the algebra A is given by Table 2 below:

Table 2

Conditions on structural constants	$\text{Aut}_K(A)$	Conditions on the matrix coefficients
$\gamma_1 = \gamma_2 = 0$	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & \beta & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & \varepsilon_{33} \end{pmatrix}$	$\varepsilon_{33}^2 = 1$ and $\beta \neq 0$
$(\gamma_1, \gamma_2) \neq 0$	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & \varepsilon_{33} \end{pmatrix}$	$\varepsilon_{33}^2 = 1$

Proof. This proposition is an immediate consequence of the previous proposition because the equation $\varepsilon_{33}^4 = 1$ is equivalent to $\varepsilon_{33}^2 = 1$ on $\mathbb{R}$. $\square$

From Proposition 3.8 and Proposition 3.11, we deduce the corollary below:

Corollary 3.12. Let (A, ω) be a five-dimensional baric evolution $\mathbb{R}$ -algebra satisfying strictly the identity (3). It is assumed that A is neither a Bernstein algebra nor a power-associative algebra. Then, the algebra A is isomorphic to one of the following pairwise non-isomorphic algebras (where $\gamma \neq 0$; $\gamma_3 \in K$ and the products that are not mentioned are void):

- $A_1(\gamma, \gamma_3)$: $e^2 = e$; $eu = \frac{1}{2}u$; $uv_1 = \gamma u$; $v_2^2 = v_1$; $v_3^2 = \gamma_3 v_1 + v_2$.
- $A_2(\gamma, \gamma_1, \gamma_2, \gamma_3)$: $e^2 = e$; $eu = \frac{1}{2}u$; $uv_1 = \gamma u$; $v_2^2 = \gamma_1 u + v_1$; $v_3^2 = \gamma_2 u + \gamma_3 v_1 + v_2$ with $(\gamma_1, \gamma_2) \neq 0$.

4 Derivations

Let F be a commutative field and A be an F -algebra. A *derivation* d of A is a linear operator on A satisfying the following condition:

$$d(xy) = d(x)y + xd(y) \text{ for all } x, y \in A.$$

Since, the commutator $[d, d'] = d \circ d' - d' \circ d$ of two derivations is still a derivation, the set $\text{Der}_K(A)$ of all derivations of A is a subalgebra of $(\text{End}_K(A), [,])$. Thus, $\text{Der}_K(A)$ is a Lie algebra, called the *Lie algebra of derivations of A* [15].

In [16, Proposition 5.2], the authors give a characterisation of the derivation of a baric evolution algebra satisfying the identity (2). The following proposition shows that this characterisation does not depend on the integer m .

Proposition 4.1. Let $A = Fe_1^2 \oplus A_{\frac{1}{2}}(e_1^2) \oplus A_0(e_1^2)$ be a Peirce decomposition of evolution algebra of dimension n satisfying the identity (3) for some $m > 3$. The linear operator $d \in \text{End}_K(A)$ is a derivation of the algebra A if, and only if, the following assertions are satisfied:

- $d(e_1^2) = 0$;
- the subspaces $A_{\frac{1}{2}}(e_1^2)$ and $A_0(e_1^2)$ are invariants with respect to d . Let $d_{\frac{1}{2}}$ and d_0 be the endomorphisms induced by d on $A_{\frac{1}{2}}(e_1^2)$ and $A_0(e_1^2)$ respectively;
- $d_{\frac{1}{2}}(x_{\frac{1}{2}}x_0) = d_{\frac{1}{2}}(x_{\frac{1}{2}})x_0 + x_{\frac{1}{2}}d_0(x_0)$ for all $x_{\frac{1}{2}} \in A_{\frac{1}{2}}(e_1^2)$ and $x_0 \in A_0(e_1^2)$;
- $d_{\frac{1}{2}}((x_0y_0)_{\frac{1}{2}}) = (d_0(x_0)y_0 + x_0d_0(y_0))_{\frac{1}{2}}$ for all $x_0, y_0 \in A_0(e_1^2)$;

(v) $d_0((x_0 y_0)_0) = (d_0(x_0) y_0 + x_0 d_0(y_0))_0$ for all $x_0, y_0 \in A_0(e_1^2)$.
 Furthermore, if d is a derivation of A , then $d_{\frac{1}{2}}$ is a derivation of $A_{\frac{1}{2}}(e_1^2)$.

Proof. Assume that d is a derivation of the algebra A and let $d(e_i) = \sum_{k=1}^n d_{ik} e_k$. For $e_j \in \text{ann}(A)$, we have $e_j^2 = 0$ and the relation $0 = d(e_1 e_j) = d(e_1) e_j + e_1 d(e_j) = d_{j1} e_1^2$, leads to $d_{j1} = 0$. For $e_j \notin \text{ann}(A)$ with $2 \leq j \leq n$, the family (e_1^2, e_j^2) is linearly independent and we have $d_{j1} = d_{1j} = 0$. We deduce that $d(e_1) = d_{11} e_1 + z$ with $z \in \text{ann}(A)$ and $d(e_j) \in \ker(\omega)$ for all $2 \leq j \leq n$.

- We have $d(e_1^2) = 2e_1 d(e_1) = 2d_{11} e_1^2$ and $d(e_1^2 e_1^2) = 2e_1^2 (d(e_1^2)) = 4d_{11} e_1^2 e_1^2 = 4d_{11} e_1^2$. The equality $d(e_1^2) = d(e_1^2 e_1^2)$ gives $d_{11} = 0$ and it follows that $d(e_1^2) = 0$. We obtain the assertion (ii).
- For $x_{\frac{1}{2}} \in A_{\frac{1}{2}}(e_1^2)$ and $x_0 \in A_0(e_1^2)$, the equalities $\frac{1}{2} d(x_{\frac{1}{2}}) = d(e_1^2 x_{\frac{1}{2}}) = e_1^2 d(x_{\frac{1}{2}})$ and $0 = d(e_1^2 x_0) = e_1^2 d(x_0)$ tell us that the subspaces $A_{\frac{1}{2}}(e_1^2)$ and $A_0(e_1^2)$ are invariants with respect to d . Thus, we set $d_{\frac{1}{2}}$ and d_0 the induced endomorphisms by d on $A_{\frac{1}{2}}(e_1^2)$ and on $A_0(e_1^2)$ respectively. By the same reasoning as in the proof of [16, Corollary 5.4], we deduce that the endomorphism $d_{\frac{1}{2}}$ is a derivation of the algebra A . Thus, we get the assertion (iii).
- The assertions (iii) to (v) follow from a direct calculation of $d(x_{\frac{1}{2}} x_0)$ and $d(x_0 y_0)$ and identifying the traces on $A_{\frac{1}{2}}(e_1^2)$ and $A_0(e_1^2)$.

The proof of the reciprocal is identical to [16, Proof of Proposition 5.3]. Indeed, the Peirce decomposition and the product between the Peirce subspaces of the evolution algebra satisfying the identity (3) for some $m > 3$ and one verifying the identity (2) are identical. $\square$

Proposition 4.2. *Let (A, ω) be the algebra defined in Proposition 3.8. Then, the Lie algebra of derivations of A is the abelian algebra.*

Proof. Let d be a derivation of A . Set $d_{\frac{1}{2}}(u) = \alpha u$ and $d_0(v_i) = \sum_{k=1}^3 d_{ik} v_k$ for $1 \leq i \leq 3$.

- We have $\gamma \alpha u = d_{\frac{1}{2}}(u v_1) = d_{\frac{1}{2}}(u) v_1 + u d_0(v_1) = \gamma \alpha u + d_{11} \gamma u$, i.e. $d_{11} = 0$. Also, for $j = 2$ or 3 , we have $0 = d_{\frac{1}{2}}(u v_j) = d_{\frac{1}{2}}(u) v_j + u d_0(v_j) = d_{j1} \gamma u$, i.e. $d_{j1} = 0$.
- For $j = 2$ or 3 , we have $0 = d_0((v_1 v_j)_0) = (d_0(v_1) v_j + v_1 d_0(v_j))_0 = (d_{1j} v_j^2)_0$. Thus, for $j = 2$, we have $0 = d_{12} v_1$, i.e. $d_{12} = 0$ and for $j = 3$, we have $0 = d_{13}(\gamma_3 v_1 + v_2)$, i.e. $d_{13} = 0$. We deduce that $d_0(v_1) = 0$.
- We have $0 = d_0(v_1) = d_0((v_2^2)_0) = 2(v_2 d_0(v_2))_0 = 2d_{22} v_1$, i.e. $d_{22} = 0$ and $d_{23} v_3 = d_0(v_2) = d_0((v_3^2)_0) = 2(v_3 d_0(v_3))_0 = 2d_{33}(\gamma_3 v_1 + v_2)$, i.e. $d_{23} = d_{33} = 0$. It follows that $d_0(v_2) = 0$ and $d_0(v_3) = d_{32} v_2$. Also, we have $0 = d_0((v_2 v_3)_0) = (v_2 d_0(v_3))_0 = d_{32} v_2^2$, i.e. $d_{32} = 0$ and $d_0(v_3) = 0$.
- We have $\gamma_1 \alpha u = d_{\frac{1}{2}}((v_2^2)_{\frac{1}{2}}) = 2(v_2 d_0(v_2)) = 0$, i.e. $\gamma_1 \alpha = 0$ and $\gamma_2 \alpha u = d_{\frac{1}{2}}((v_3^2)_{\frac{1}{2}}) = 2(v_3 d_0(v_3)) = 0$, i.e. $\gamma_2 \alpha = 0$.

From above, we deduce that the matrix of the derivation d in the basis $\{e_1^2, u, v_1, v_2, v_3\}$ is

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & \alpha & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Particulary, when $\gamma_1 \neq 0$ or $\gamma_2 \neq 0$ the only derivation is the zero one. Moreover, for $d, d' \in \text{Der}_K(A)$, we have $[d, d'] = 0$ and we get the proposition. $\square$

Acknowledgement. The authors thank the referee for his/her pertinent comments, which improved the reading of this paper.

References

- [1] V. M. Abraham, "Linearizing quadratic transformations in genetic algebras", Proc. Lond. Math. Soc. 40(3) (1980), 346–363. <https://doi.org/10.1112/plms/s3-40.2.346>
- [2] A. A. Albert, "A theory of power-associative commutative algebras", Trans. Am. Math. Soc. 69 (1950), 503–527. <https://doi.org/10.2307/1990496>
- [3] J. Bayara, A. Conseibo, M. Ouattara and A. Micali, "Train algebras of degree 2 and exponent 3", Discrete Contin. Dyn. Syst., Ser. S 4(6) (2011), 1371–1386. <https://doi.org/10.3934/dcdss.2011.4.1371>
- [4] J. Bayara, A. Conseibo, M. Ouattara and F. Zitan, "Power associative algebras that are train algebras", Journal of Algebra 324 (2010), 1159–1176. <https://doi.org/10.1016/j.jalgebra.2010.06.012>
- [5] P. Beremwidougou and A. Conseibo, "Classification and derivations of four-dimensional almost Bernstein algebras", JP J. Algebra Number Theory Appl. 56 (2022), 1–25. <https://doi.org/10.17654/0972555522022>
- [6] S. Bernstein, "Principe de stationnarité et généralisation de la loi de Mendel", Comptes rendus de L'Acad. des Sci. Paris 177 (1923), 581–584.
- [7] A. Conseibo, S. Savadogo and M. Ouattara, "Duplicate, Bernstein Algebras and Evolution algebras", Le Matematiche LXXVI(1) (2021), 193–209. <https://doi.org/10.4418/2021.76.1.11>
- [8] A. Elduque and A. Labra, "Evolution algebras and graphs", J. Algebra Appl. 14(7) (2015), P10. <https://doi.org/10.1142/S0219498815501030>
- [9] P. Holgate, "Genetic algebras satisfying Bernstein's stationarity principle", J. Lond. Math. Soc., II. Ser. 9 (1975), 613–623. <https://doi.org/10.1112/jlms/s2-9.4.613>
- [10] D. Kabre and A. Conseibo, "Structure of baric algebras satisfying a polynomial identity of degree six", JP J. Algebra Number Theory Appl. 61(1) (2023), 37–52. <https://doi.org/10.17654/0972555523010>
- [11] Yu. I. Lyubich, "Basic concept and theorems of the evolutionary generics of free populations", Russian Math. Surveys 26(5) (1971), 51–123.
- [12] Yu. I. Lyubich, "Algebraic methods in evolutionary genetics", Biom. J. 20 (1978), 511–529. <https://doi.org/10.1002/bimj.4710200508>
- [13] M. Ouattara and S. Savadogo, "Evolution train algebras", Gulf J. Math. 8(1) (2020), 37–51. <https://gjom.org/index.php/gjom/article/view/299>
- [14] M. Ouattara and S. Savadogo, "Power-associative evolution algebras", Associative and non-associative algebras and applications. Proceedings of the 3rd Moroccan Andalusian meeting on algebras and their applications, MAMAA 2018, Chefchaouen, Morocco, April 12–14, 2018 : 23–49 Cham : Springer(2020). https://doi.org/10.1007/978-3-030-35256-1_2
- [15] R. D. Schafer, "An introduction to nonassociative algebras", Pure Appl. Math., Academic Press, 22 (1966), P166.

- [16] J. Tenkodogo, S. Savadogo, A. Conseibo and A. Dembega, *Evolution algebras satisfying train identity of degree 2 and exponent 3*, Gulf J. Math. 15(1) (2023), 158–172. <https://doi.org/10.56947/gjom.v15i1.1387>
- [17] J. P. Tian and P. Vojtěchovský, "Mathematical concepts of evolution algebras in non-Mendelian genetics", Quasigroups Relat. Syst. 14(1) (2006), 111–122.
- [18] A. Wörz-Busekros, "Algebras in genetics", Lect. Notes Biomath, 36, (1980).
- [19] W. A. Zangre and A. Conseibo, "On train algebras of degree 2 and exponent 4", Gulf J. Math. 13(1) (2022), 41–53. <https://gjom.org/index.php/gjom/article/view/926/373>