N°: 110/2021-C/MT

RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITÉ DES SCIENCES ET DE LA TECHNOLOGIE HOUARI BOUMEDIENE
FACULTÉ DE MATHÉMATIQUES

THÈSE DE DOCTORAT

Présentée pour l'obtention du grade de **DOCTEUR**
En: Mathématiques

Spécialité: Arithmétique, Codage et Combinatoire

Par: Ahmed Djamal Eddine BOUZIDI

Titre

EXPOSANTS DES POLYNÔMES TORDUS SUR LES ANNEAUX PÉRIODIQUES

Soutenue publiquement, le 27/09/2021, devant le jury composé de:

Mme. Leila BENFERHAT	Professeur	à l'USTHB	Présidente.
M. Ahmed CHERCHEM	Professeur	à l'USTHB	Directeur de thèse.
Mme. Schehrazad SELMANE	Professeur	à l'USTHB	Examinatrice.
M. Ahmed AÏT-MOKHTAR	Professeur	à l'ENS Kouba	Examinateur.
M. André LEROY	Professeur	à l'Université d'Atrois	Invité.

N°: 110/2021-C/MT

The Democratic and Popular Republic of Algeria

Ministry of Higher Education and Scientific Research

University of Sciences and Technology Houari Boumediene
Faculty of Mathematics

THESIS

Submitted to the Department of Algebra and Number Theory in partial fulfillment of the requirements for the degree of

Doctor in Mathematics

Domain: Arithmetic, Coding and Combinatorics

By: Ahmed Djamal Eddine Bouzidi

EXPONANTS OF SKEW POLYNOMIALS OVER PERIODIC RINGS

Publicly defended on Sunday, 27/09/2021, in front of the jury composed by:

Mme. Leila BENFERHAT	Professor	U.S.T.H.B.	Chairwoman.
Mr. Ahmed CHERCHEM	Professor	U.S.T.H.B.	Thesis Supervisor.
Mme. Schehrazad SELMANE	Professor	U.S.T.H.B.	Examiner.
Mr. Ahmed AÏT-MOKHTAR	Professor	E.N.S Kouba	Examiner.
Mr. André LEROY	Professor	University of Artois, Lens, France	invited.

Acknowledgements

In the name of Allah, the Most Gracious and the Most Merciful.

All praises to Allah and His blessing for the completion of this thesis. I would like to express my appreciation to all the individuals without whom the completion of this thesis would not be possible.

First and foremost, my deepest gratitude goes to my parents and may wife for their continuous encouragement and for allowing me the time and providing the supportive environment needed for study. I know this will be never enough to repay them for their sacrifices.

I would like to express my sincere gratitude to my supervisor Prof. **Ahmed CHERCHEM** for his patience, motivation, attention, encouragement during the periods of research. Thank you for providing me with adequate support when I really needed it. Thank you very much. You have made a significant contribution, not only to this thesis but also to my life.

I would also gratefully acknowledge Prof. **Leila BENFERHAT** for the honour to judge this work and to preside over the jury.

I am indebted to my defence committee members: Prof. **Schehrazad SELMANE**, Prof. **Ahmed AÏT-MOKHTAR** and Prof. **André LEROY** for offering their suggestions, pertinent and detailed comments. Their precious time and effort are priceless to me. I am extremely proud to be able to gather such a prestigious jury.

I am very grateful again to Prof. André LEORY for the time that he gave selflessly to provide me with direction and technical assistance, especially during my visit to Artois university. I would like to thank the members of the mathematical department of this institution for their warm welcome.

My appreciation also goes to my family members, brothers and sisters for their love and confidence over the years. Last but not least, I would like to thank everybody who was important to the successful realization of this thesis, as well as expressing my apology that I could not mention personally one by one

Notations

The following notations will be used throughout this thesis.

1. $\mathbb{N}$: The monoid of natural numbers.
2. $\mathbb{Z}$: The ring of integers.
3. $\mathbb{C}$: The field of complex numbers.
4. $\mathbb{R}$: The field of real numbers.
5. $\binom{n}{k}$: The binomial coefficient .
6. $\mathbb{Z}_{p^n}$: The residue ring of integers modulo p^n.
7. $\mathbb{F}_{p^n}$: The finite field with cardinal p^n.
8. $\overline{\mathbb{F}}_q$: The algebraic closure of $\mathbb{F}_q$.
9. $|R|$: The cardinal of R.
10. $GR(p^n, m)$: The Galois ring with characteristic p^n and cardinality p^{nm}.
11. $M_n(R)$: The set of $n \times n$ matrices with entries from R.
12. $T_n(R)$: The set of all $n \times n$ upper triangular matrices with entries from R.
13. $T(R, S, M)$: The generalized triangular matrix ring with R, S are rings and M is an (R, S)-bimodule
14. $diag(M)$: The diagonal of the matrix M.
15. $C(p)$(or C_p) : The companion matrix of p.
16. R^* : The set of nonzero elements of R.
17. $GL_n(R)$: The general linear group of $n \times n$ invertible matrices over R.
18. $U(R)$: The set of all units of R.
19. $N(R)$: The set of all nilpotent elements of R.
20. $J(R)$: The Jacobson radical of R.
21. $Id(R)$: The idealizer of R.

22. $End(R)$: The set of all endomorphisms on R.

23. $Aut(R)$: The set of all automorphisms on R.

24. $Hom_R(M, N)$: The set of all R-homomorphisms from M into N.

25. $End_R(M)$: The set of all endomorphisms of the left R-module M.

26. $Aut_R(M)$: The set of all automorphisms of the left R-module M

27. $R[t; \sigma, \delta]$: The skew polynomial ring (also called Ore extension).

28. (σ, δ)-PLT : The (σ, δ) pseudo-linear transformation.

29. S_k^n : The sum of the words in σ and δ of length n with k letters σ and $n - k$ letters δ.

30. f^* : The reciprocal polynomial of f.

31. $e_r(g; f)($ resp. $e_l(g; f))$: The right (resp. left) exponent of g relatively to f.

32. $e_r(g)($ resp. $e_l(g))$: The right (resp. left) exponents of g with respect to the variable t.

33. $N_i(a)$: The ith norm of a.

34. $ord_{(\sigma,\delta)}(a)$: The (σ, δ)-order of a.

35. $a \sim b$: Express that a and b are (σ, δ) conjugate.

36. *P.I.* ring : A ring that satisfies a polynomial identity.

Abstract

The exponent of a polynomial $f(x)$ with nonzero constant term in $\mathbb{F}_q[x]$ is a classical tool in the theory of finite field. It is connected with the order of the roots of $f(x)$ in the multiplicative group of the algebraic closure $\overline{\mathbb{F}}_q$ or to the order of its companion matrix in the group $GL_k(\mathbb{F}_q)$, where k is the degree of $f(x)$. This exponent also has a profound impact on the study of linear recurrence sequences and on linearized polynomials. We refer the reader to the book by Lidl and Niederreiter [21] for basic information about this notion. Generalizations of the concept of exponent for polynomials belonging to the skew polynomial rings $\mathbb{F}_q[t;\sigma]$ have been investigated in [9]. In the present work, we define exponent for polynomials $g(t) \in S = R[t;\sigma,\delta]$, where R is a periodic ring, σ is an automorphism of R, and δ is a σ-derivation of R. Noting that the equality $tS = St$ is true in $S = R[t;\sigma]$ but does no longer holds in $R[t;\sigma,\delta]$, we introduce in this setting a notion of relative exponents and prove that, for monic polynomials $f(t), g(t) \in S$, and under some mild assumptions, there exists a positive integer e such that $g(t)$ divides on the right the polynomial $f(t)^e - 1$. This encompasses the classical case where $f(t) = t \in \mathbb{F}_q[t]$ (or $f(t) = t \in \mathbb{F}_q[t;\sigma]$).

In order to make the thesis relatively self contained and also to put the goals in good perspective, we present some well-known properties of periodic rings and develop new ones. This covers most of the second section. In the third section, we define the notion of relative exponent and prove some properties of it. We are in particular interested in the left-right symmetry of the exponent. This leads to some cyclic properties of factorizations. In particular, we show that in quite general situations, the fact that $g(t)$ divides on the right a polynomial $t^e - 1$ implies that $g(t)$ also divides $t^e - 1$ on the left. we used the computer software SageMath and MAGMA for preparing some examples.

Contents

Introduction

This thesis is devoted to the study of the exponents of skew polynomials. Our focus is mainly about investigating new properties of skew polynomials and skew polynomial rings, both, on the arithmetical point of views (roots, polynomial factorizations), but also on the structure of ideals (generators of ideals, radicals, polynomial identities). This should lead to interesting applications in coding theory, recurrent sequences, cryptography and more. We shall try to generalize properties of skew polynomials over rings that are not necessarily finite nor commutative and also examine relationship between the classical case and the skew case.

Before diving into the subject of the thesis, let us mention briefly, but concretely, some of the areas where the classical notion of exponent is used. Let $\mathbb{F}_q$ be the finite field with q elements. We recall that for a polynomial $g(t) \in \mathbb{F}_q[t]$ such that $g(0) \neq 0$, the exponent of $g(t)$ is the smallest natural number $e = e(g)$ such that $g(t)$ divide $t^e - 1$ in $\mathbb{F}_q[t]$. The least period of a linear recurring sequence divides the order of its characteristic polynomial. When this characteristic polynomial is irreducible and has a nonzero independent term, then the sequence is periodic with least period equal to the order of the characteristic polynomial. More generally, the least period of a linear recurring sequence is equal to the order of its minimal polynomial. These are important since having sequences with large period has applications in areas such as random number generation.

Let us now motivate the introduction of new concepts in the theory of exponents. There are many interesting works, particularly in coding theory, where noncommutative algebra is used. For instance, noncommutative semigroups, group rings and skew polynomials of the automorphism type $\mathbb{F}_q[t;\sigma]$ have shown their efficiency in finding good codes. Our interest is focused in the last point, i.e., developing the tool of exponent in general Ore extensions of the form $R = A[t;\sigma,\delta]$ (see section 1.2 for definition). This case of Ore extension $R[t;\sigma]$, where R is a finite ring, was already developed in the work of A. Cherchem and A. Leroy, in [9]. There are several difficulties that appear when dealing with a general Ore extension. The first one is that the evaluation of polynomials and the underlying "norms" are much more complex, the second one is that the indeterminate t is not necessarily suitable for developing the exponent since Rt is no longer a two-sided ideal. The last difficulty comes from our desire (natural in the context of exponent) to develop the theory when the base ring A is a periodic ring instead of a finite ring. To motivate this last point, let us mention that in Lemma 2.1 in [9], it is shown that for f and g in a ring R, the existence of the left exponent of f relative to g is based on the fact that the passage to the quotient R/Rg is finite, therefore $f^i + Rg = f^k + Rg$ for some integers $i > k > 0$. This last point led us to think of periodic ring.

A ring R is called periodic if for any $x \in R$, there exist two different positive integers m and n such that $x^m = x^n$. The term " periodic " was first introduced by Chacron [7]. For other characterizations of periodic rings, see [10], [8]. Examples of periodic rings are finite rings, Boolean rings, nil rings, and direct sums of matrix rings over finite fields. In recent years, many mathematicians studied periodic rings. Amongst others, we shall mention M. Chacron, H. E. Bell, R. R. Khazal, A. Yaqub, H. Chen, and M. Sheibani. Regarding periodic rings, we can distinguish two main directions of research :

- The first is to find sufficient conditions for the commutativity of a periodic ring.
- The second direction is to find structural results for the periodic rings.

In our work we will be interested in the skew polynomials rings built on periodic rings. Of course, this is also related to automorphisms and skew derivations over such rings. This thesis is divided into four chapters. The organization of the present work is as follows:

– In the first chapter we recall some necessary background. We start by briefly introducing all the concepts and basic but essential terminology in ring theory used in this thesis. Then we give some preliminaries about skew polynomial rings and we pay a particular attention to pseudo-linear transformations, as they are a fundamental tool in studying Ore extensions $R = A[t; \sigma, \delta]$ over a ring A that is not necessarily a division ring. These transformations appear naturally associated with module over an extension of Ore. This property is at the heart of evaluation theory which is itself strongly related to exponents.

– In the second chapter, we give a brief survey of the work done by A. Cherchem and A. Leroy, in [9], who studied the skew exponents of polynomials on a finite field $\mathbb{F}_q$. Then we transform the relation given in [27], between exponent over finite field $\mathbb{F}_{p^m}$ and the Galois ring $GR(p^n, m)$ from the classical case to the skew case. After that, we generalize the study of the exponent over a finite field to an arbitrary finite ring. We finish this chapter by giving a commutativity relation of the divisors of $t^e - 1$ in $R[t, \theta]$. We develop new programs and commands in magma for the skew polynomials ring $R[t, \theta]$.

– The third chapter is dedicated to the investigation of periodic rings. In the first part of this chapter, we show some properties of periodic elements, we present a relationship between the Jacobson radical and the periodic ring, and we relate periodic ring with other kind of rings. Most part of this chapter is extracted from the literature but in a form adapted to the thesis. Moreover, there are also some novelty, in particular, we establish a new characterization of periodic ring (see Theorem 8). Other new results related to periodic rings are developed in the second part of this chapter where we study graded periodic rings and give a necessary and sufficient condition for a finite graded ring to be periodic (see corollary 3). In the last part, we try to answer the natural question : if R is periodic, is the ring of matrices $M_n(R)$ periodic ? In fact, we do not have an explicit answer to this question, but we found a positive answer for some special cases. We also answer questions related to matrices over a given periodic ring, which were suggested in [10]. Examples are presented all along the thesis.

– The fourth chapter is in fact the heart of this work. We will look at the (relative) exponent of polynomials and their properties in the case of skew polynomial ring with derivation (general Ore extensions) $S = R[t; \sigma, \delta]$. We first work in a general ring and then we concentrate on Ore extensions with periodic base rings. In the general context of an Ore extensions with nonzero σ derivation, it is not always possible to define an exponent. But, under some conditions, we do get the existence of the (relative) exponents. This is the case for instance for P.I. periodic rings (cf. Corollary 7). For this relative exponent we also have a left-right symmetry (cf. Lemma 15). Classically the exponent of a polynomial is equal to the order of its companion matrix inside the group of invertible matrices. The analogue of this in the case of a polynomial belonging to an Ore extension $R[t; \sigma, \delta]$ is give in theorem 16, where the order of the companion matrix in a (σ, δ) setting is used.

Chapter 1

Preliminaries

In the first section of this chapter, we will give a quick description of the basic notions used in the thesis. In later sections we will be more specific and present the definitions and most important results related to skew polynomials and pseudo-linear transformations. We will present all the necessary tools and techniques used in the second and third chapters.

1.1 Basic terminology

In this part, we give definitions of the notions and concepts used later (even the most elementary). This will give us the opportunity to fix notations and will make the reading easier.

Definition 1. *A ring is a set R together with operations $+$ and $.$ (called addition and multiplication) and distinguished elements 0 and 1, which satisfy the following properties:*

1. $(R, +)$ *is an abelian group.*
2. $(R, .)$ *is a monoid.*
3. $a(b + c) = ab + ac$ *and* $(b + c)a = ba + ca$ *for all a, b, c in R.*

A ring with identity is a ring R that contains an element 1 such that: $1.r = r.1 = r$, for all $r \in R$. If $ab = ba$ for all a, b in R, we say R is commutative. A subring of a ring is a subset which is itself a ring with the same operations $+$ and $.$ and having the same distinguished elements 0, 1.

We note R^* the set of nonzero elements in R.

Definition 2. *Let R be a ring with identity 1. The characteristic of R (written $Char(R)$) is the smallest positive integer q such that $q1 = 0$, where $q1$ is an abbreviation for $1 + 1 + \ldots + 1$ (q times). If $q1$ is never 0, we say that R has characteristic 0.*

Definition 3. *Let R be a ring and $I \subseteq R$. I is called a left ideal of R if*

1. *$(I, +)$ is a group.*

2. *For every $r \in R$ and every $x \in I$, the product rx is in I.*

A right ideal is defined similarly. A two-sided ideal (or just an ideal) is both a left and right ideal.

Let R be a nonzero ring. We say that R is a division ring (or skew field) if for all $r \in R^*$, there exist $s \in R^*$, such that $rs = sr = 1_R$.

A field is a division ring where the multiplication is commutative. A finite field is a field that contains a finite number of elements. A simple ring R is nonzero ring whose only (two-sided) ideals are R itself and zero.

Let us mention the fact that every commutative simple ring is a field.

Definition 4. *Let $(R, +, .)$ and $(S, \dot{+}, *)$ be rings with identity. A map $\phi : R \longrightarrow S$ is a ring homomorphism if :*

1. *$\phi(r_1 + r_2) = \phi(r_1) \dot{+} \phi(r_2)$, for all $r_1,\ r_2 \in R$.*

2. *$\phi(r_1.r_2) = \phi(r_1) * \phi(r_2)$, for all $r_1,\ r_2 \in R$.*

3. *$\phi(1_R) = 1_S$.*

A ring homomorphism $\phi : R \longrightarrow S$ that is bijective (resp. injective, surjective) is called an isomorphism (resp. a monomorphism, an epimorphism). We say that two rings R_1 and R_2 are isomorphic if there exists an isomorphism between them.

An injective ring homomorphism is called an embedding.

An endomorphism is a homomorphism from the ring to itself. The set of all endomorphisms on R is denoted $End(R)$.

A ring automorphism of a ring R is an isomorphism from the ring onto itself. The set of all automorphisms on R is denoted $Aut(R)$.

Example 1. *Crucial examples in coding theory are the finite fields. Let p be a prime number and $n \in \mathbb{N}$. There is a unique (up to isomorphism) finite field with $q = p^n$ elements usually denoted $\mathbb{F}_q$. This is a Galois extension of the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ with cyclic group of automorphisms generated by the Frobenius map denoted θ and defined by $\theta(a) = a^p$ for any $a \in \mathbb{F}_q$.*
The group of automorphisms of $\mathbb{F}_q$ is cyclic of order n generated by the Frobenius automorphism.

$$Aut(\mathbb{F}_q) = \{Id,\ \theta,\ \theta^2, \ldots,\ \theta^{n-1}\}.$$

In the context of coding theory, as mentioned earlier, rings that are not fields (or even not commutative) are more and more used. It is thus not surprising that for linear codes vector spaces are replaced by modules. So, we just briefly recall the definition.

Definition 5. *Given a ring R with identity 1_R. We define a left R-module to be an abelian group M (written additively), together with a map $R \times M \longrightarrow M$ called scalar multiplication, satisfying the following laws for all r_i in R and x_i in M:*

1. $r(x_1 + x_2) = rx_1 + rx_2$
2. $(r_1 + r_2)x = r_1x + r_2x$
3. $(r_1r_2)x = r_1(r_2x)$
4. $1_Rx = x$

A right R-module M is an abelian group with scalar multiplication $M \times R \longrightarrow M$ satisfying the right-handed version of these laws.

A submodule of an R-module M (or an R-submodule), is an additive subgroup N closed under the given scalar multiplication, i.e.: for any $n \in N$ and any $r \in R$, the product $r.n$ (or $n.r$ for a right R-module) is in N.

A (left or right) module M over a ring R is simple if M is non-zero and have no non-zero proper submodules.

A module is indecomposable if it is non-zero and cannot be written as a direct sum of two non-zero submodules.

A module over a ring is said to be semisimple if it is a direct sum of simple submodules.

A ring is semisimple if it is semisimple as a left module over itself, or, equivalently, if every (left) module over it is semisimple

Definition 6. *Let R be a ring and M be a left R-module. Then:*
The module M is said to be finitely generated if there exist $E = \{e_1, \ldots, e_n\}$ a subset of M, such that $M = \sum_{i=1}^{n} Re_i$. We say that E is a set of generators for M.
The set of generators E is linearly independent (or free generators) if for every subset $\{e_1, e_2, \ldots, e_m\}$ of distinct elements of E and $r_1, r_2, \ldots, r_m$ in R, we have $r_1e_1 + r_2e_2 + \cdots + r_me_m = 0_M$ implies that $r_1 = r_2 = \cdots = r_m = 0_R$. A linearly independent generating set for M is called a basis for M, and a free module is a module with a basis.

Remark 1. In general, working with modules quickly lead to problems that do not occur in the case of vector spaces. There are modules that are not free, there are modules that are free but with bases having different cardinals, there are elements with nonzero annihilators...This last point will be more relevant to us and is the subject of the next definition.

Definition 7. *Let R be a ring, and let M be a left R-module. For any element $m \in M$, the left ideal $Ann(m) = \{r \in R : \ rm = 0\}$ is called the annihilator of m. The ideal $Ann(M) = \{r \in R : rm = 0$ for all $m \in M\}$ is called the annihilator of M. The module M is called faithful if $Ann(M) = (0)$.*

Definition 8. *Let R be a ring, M and N be left R-modules. A map $\phi : M \longrightarrow N$ is called an R-homomorphism if:*

1. $\phi(m + m^{'}) = \phi(m) + \phi(m^{'})$

2. $\phi(rm) = r\phi(m)$

for all $r \in R$ and all $m, m^{'} \in M$. We denote by $Hom_R(M, N)$ the set of all R-homomorphisms from M to N . An R-homomorphism is an isomorphism if it is bijective.

Elements of $Hom_R(M, M)$ are called endomorphisms and the set of endomorphisms of the left R-module M will be denoted by $End_R(M)$. This is a ring under usual composition and addition of endomorphisms. In case M is a free module, this ring is isomorphic to matrices over R. Many concepts initially defined for rings have analogues for modules by just considering the endomorphism ring of the module.

An isomorphism in $End_R(M)$ is called an automorphism and the set of automorphisms of the left R module M is denoted by $Aut_R(M)$.

Let R and S be two rings. Then an (R, S)-bimodule is an abelian group $(M, +)$ such that:

1. *M is a left R-module and a right S-module.*

2. *For all r in R, s in S and m in M: $(rm)s = r(ms)$.*

An (R, R)-bimodule is also known as an R-bimodule.

To every right R module M_R we can attach an (S, R)-bimodule where $S = End_R(M)$ via the obvious action. For us this structure is particularly important in the frame of skew evaluation. In particular, it leads to nice way of "denumbering" the zeros of a skew polynomial generalizing Gordon-Motzkin Theorem (cf. [19], for instance).

Definition 9. *Let R be a ring with identity 1_R and let $r \in R$. We say that r is*

1. *of finite order (or root of unity) e if e is the least positive integer such that $r^e = 1_R$;*

2. *left invertible (or left unit) if $r \neq 0$ and there is $u \in R$ such that $ru = 1_R$, right inverses (right unit) are defined in a similar manner;*

3. *left zero-divisor if $r \neq 0$ and there is non-zero $b \in R$ such that $rb = 0$, right zero-divisors are defined in a like manner;*

4. *periodic if there exist different positive integers $m,\ n$ such that $r^m = r^n$;*

5. *potent if there exists some positive integer m, such that $r^m = r$;*

6. *nilpotent if there exists some positive integer n, such that $x^n = 0$;*

7. *idempotent if $r^2 = r$, and*

   (a) *Two idempotents a and b are called orthogonal if $ab = ba = 0$ and a set of idempotents e_i is said to be orthogonal if $e_i e_j = 0$ for all $i \neq j$.*

   (b) *A non-zero idempotent e is said to be primitive if it cannot be written as a sum of non-zero orthogonal idempotents $e = f_1 + f_2$. Equivalently, Re indecomposable as a right R-module.*

   (c) *A local idempotent e is an idempotent such that eRe is a local ring. This implies that eR is directly indecomposable, so local idempotents are also primitive.*

Many types of rings are related to the above notions and will be used in the thesis. For instance a ring is called Dedekind finite (resp. reversible) if for any $a, b \in R$ we have $ab = 1_R$ implies $ba = 1_R$ (resp. $ab = 0$ implies $ba = 0$). Fortunately, all our rings will be Dedekind finite but they will generally not be reversible. For later use, let us just collect the most important rings structure associated to the type of elements described above. These types of rings are important for us in particular since they are defined elementwise.

Definition 10. *Let R be a ring with identity 1_R. We say that R is*

1. *strongly clean if every element is the sum of a unit and an idempotent which commute;*

2. *strongly π-regular if for every a in R, there exist a positive integer $n(a)$ and an element b in R satisfying $a^{n(a)} = a^{n(a)+1}b$;*

3. *periodic if its elements are periodic;*

4. *potent if its elements are potent;*

5. *graded if there exists a family of additive subgroups $\{R_i\}_{i\in\mathbb{Z}}$ of R, where $R = \oplus_{i\in\mathbb{Z}} R_i$ and $R_n R_m \subseteq R_{n+m}$ for all $n, m \in \mathbb{Z}$;*

6. *locally finite if any finitely generated subring of R is finite;*

7. *stable range one, if for any a, $b \in R$ with $Ra + Rb = R$, there exists $y \in R$ such that $a + yb \in U(R)$*

We recall that a ring R, is said to be left (resp. right) Noetherian if, it does not contain an infinite ascending chain of left (resp. right) ideals, i.e. given any increasing sequence of left (or right) ideals : $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$, there exists an $N \in \mathbb{N}$ such that : $I_N = I_n$, for $n \geqslant N$ (This is called the ascending chain conditions). A ring is said to be Noetherian if it is both left and right Noetherian. For a ring R, the following are equivalent :

1. R is left (resp. right) Noetherian.

2. Every non-empty set of left (resp. right) ideals in R has a maximal element.

3. Every ascending chain of left (resp. right) ideals in R is stationary.

4. Every left (resp. right) ideal in R is finitely generated.

We have also that, If R is a Noetherian ring, then the polynomial ring $R[t]$ is Noetherian by the Hilbert's basis theorem, and If I is a two-sided ideal of R, then the quotient ring R/I is also Noetherian.

Another type of rings, which is related to the Noetherian rings, is Artinian ring. A ring is left (resp. right) Artinian if there is no infinite descending sequence of left (resp. right) ideals, i.e. for any decreasing sequence of left (resp. right) ideals $B_1 \supseteq B_2 \supseteq B_3 \supseteq \ldots$, there exists an $M \in \mathbb{N}$ such that $B_m = B_M$, for $m \geqslant M$ (This is called the descending chain conditions). A ring is called Artinian if it is both left and right Artinian.

The Artin–Wedderburn theorem characterizes every simple Artinian ring as a ring of matrices over a division ring. We have previously said that Noetherian and Artinian rings are related, and this is clearly shown by the Hopkins-Levitzki theorem : Let R be a right (resp, left) Artinian ring with identity. Then R is right (resp, left) Noetherian.

Definition 11. *Let R be a ring and let $A \subseteq R$. We say that A is nil if its elements are nilpotent. Let us notice that these rings don't have an identity.*

An ideal of R is a nil ideal if it is a nil subset of R.

An ideal I of R is said to be a nilpotent ideal if there exists $k \in \mathbb{N}^*$, such that $I^k = 0$.

The Jacobson radical of a ring R, denoted by $J(R)$, is defined to be the intersection of the maximal ideals of R.The Jacobson radical is named after Nathan Jacobson, who was the first to study it. The following proposition characterizing the elements of $J(R)$.

Proposition 1. *[18] Let R be a ring with identity and $y \in R$, the following statements are equivalent:*

1. *$y \in J(R)$;*

2. *$1 - xy$ is left-invertible for any $x \in R$;*

3. *$yM = 0$ for any simple left R-module M.*

Mention here that:
– A semilocal ring R is a ring for which $R/J(R)$ is a semisimple ring.
– A ring R is called semiperfect if R is semilocal, and idempotents of $R/J(R)$ can be lifted to R.
– The Jacobson radical of an Artinian ring is nilpotent and contains every one-sided nil ideal.

A ring R satisfies a polynomial identity, and we say that R is P.I., if there is a polynomial $f \in R$ in non commuting variables, which vanishes under substitutions from R. For example, commutative rings satisfy the polynomial identity

$$f(x, y) = xy - yx.$$

Definition 12. *Let R be a ring and S be a subring of R. We say that S is finitely generated subring (also called a subring of finite type) if there exists a finite set of elements $r_1, ..., r_n$ of R such that every element of S can be expressed as a polynomial in $r_1, ..., r_n$, with coefficients in R.*

Definition 13. *Let R be a ring, and $p(t) = \sum_{i=0}^{n} a_i t^i$ be a monic polynomial in $R[t]$. The companion matrix of p, denoted by $C(p)$, is defined by*

$$C(p) = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \\ 0 & 0 & 0 & \cdots & 1 \\ -a_0 & -a_1 & -a_2 & \cdots & -a_{n-1} \end{pmatrix} \in M_n(R)$$

We recall that a ring R is periodic if for each $x \in R$, the multiplicative set of all powers of x; $\{x, x^2, x^3, \dots\}$ is finite, equivalently to, for each $x \in R$, there are different positive integers m, n such that $x^m = x^n$. We give in the next proposition a characterization of periodic rings, which was mentioned in Theorem 3.4 [10].

Proposition 2. *Let R be a ring. The following are equivalent:*

1. *R is a periodic ring.*

2. *For each $a \in R$, $a = f + b$, where $f^n = f$ for some integer $n \geqslant 2$, $af = fa$ and $b \in Nil(R)$.*

3. *For each $a \in R$, $a = ev + b = ve + b$, where $e^2 = e \in R$, $v_{n-1} = 1$ for some integer $n \geqslant 2$ and $b \in Nil(R)$ with $ab = ba$.*

4. *For each $a \in R$, $a - a^n \in Nil(R)$ for some integer $n \geqslant 2$.*

5. *For each $a \in R$, there exists an integer $m \geqslant 1$ such that a^m is strongly nil clean in R.*

In chapter 3, we examine in detail periodic rings, we relate periodic ring with other kind of rings, and we will examine the direct product of periodic rings, and the direct limit of periodic rings. In the following, we recall the definition of direct limit of rings.

Definitions 1.

1. *A directed set I is a set with a partial order $\leqslant$ such that for every $i, j \in I$ there is $k \in I$ such that $i \leq k$ and $j \leq k$.*

2. *Let R be a ring. A directed system of R-modules indexed by a direct set I, is a family of R-modules $(M_i)_{i \in I}$ with an R-module homomorphisms $\mu_{ij} : M_i \longrightarrow M_j$, for each pair $i, j \in I$ with $i \leqslant j$, such that :*

   i) *μ_{ii} is the identity mapping of M_i, for all $i \in I$;*

   ii) *for any $i \leqslant j \leqslant k$ in I, $\mu_{ij} \circ \mu_{jk} = \mu_{ik}$.*

   The modules M_i and homomorphisms μ_{ij} are said to form a direct system over the directed set I, denoted by $(M_i; \mu_{ij})$.

3. *Let $(M_i)_{i \in I}$ be a direct system of R-modules, then there exists an R-module M with the following properties:*

   (a) *There are R-module homomorphisms $\mu_i : M_i \longrightarrow M$ for each $i \in I$, satisfying $\mu_i = \mu_j \circ \mu_{ij}$ whenever $i \leqslant j$.*

   (b) *If there is an R-module N such that there are R-module homomorphisms $\nu_i : M_i \longrightarrow N$ for each i and $\nu_i = \nu_j \circ \mu_{ij}$ whenever $i \leqslant j$; then there exists a unique R-module homomorphism $\nu : M \longrightarrow N$, such that $\nu_i = \nu \circ \mu_i$.*

   This module M is called the direct limit of the direct system $(M_i)_{i \in I}$, and denoted by $M = \varinjlim M_i$.

4. *Let $(A_i)_{i\in I}$ be a family of rings indexed by a directed set I, and for each pair $i \leqslant j$ in I let $\phi_{i,j} : A_i \longrightarrow A_j$ be a ring homomorphism, satisfying conditions (i) and (ii) of 2. Regarding each A_i as a $\mathbb{Z}$-module we can then form the direct limit $A = \varinjlim A_i$. The ring A is the direct limit of the system $(A_i, \phi_{i,j})$.*

Galois rings are special finite rings. They play an important role in the theory of finite rings. Galois rings are useful in classical information theory, especially in coding theory (in particular for linear codes). They are also of interest in quantum information.

A finite (commutative) ring R with identity, such that the set of its zero divisors including 0 constitutes a principal ideal $m = pR$ with p prime (i.e. R/pR is an integrity ring) is called a Galois ring. For example. Let p is a prime number and n is a positive integer, and let $\mathbb{Z}_{p^n}$ be the ring of integers modulo p^n, is a Galois ring with p^n elements and a unique maximal ideal $p\mathbb{Z}_{p^n}$.

Let $h(t) \in \mathbb{Z}_{p^n}[t]$, If $\overline{h(t)}$ (i.e. $h(t)$ modulo p), is an irreducible (resp. primitive) polynomial in $\mathbb{F}_p[t]$, then $h(t)$ is called a basic irreducible (resp. primitive) polynomial.

Let $p \in \mathbb{N}$ be a prime number and $m, n \in \mathbb{N}$ are a positive integers, let $h\,(t)$ be a basic irreducible polynomial of degree m over $\mathbb{Z}_{p^n}$. A Galois ring $GR(p^n, m) = R$ with characteristic p^n and cardinality p^{nm} is constructed as quotient ring $\mathbb{Z}_{p^n}\,[t]/(h\,(t))$. The ring R is a commutative local ring with maximal ideal pR and residue field $\mathbb{F}_{p^m}$. Let $^-$ denote the natural homomorphism from R to $\mathbb{F}_{p^m}$. This homomorphism naturally induces a ring homomorphism from $R\,[t]$ to $\mathbb{F}_{p^m}\,[t]$, we also denote it by the same notation $^-$.

If ξ is root of $h\,(t)$ of order $p^m - 1$, then $R = \mathbb{Z}_{p^n}\,[\xi]$ and all elements of R can be expressed uniquely as

$$a_0 + a_1\xi + a_2\xi^2 + ... + a_{m-1}\xi^{m-1}, \textit{ for } a_i \in \mathbb{Z}_{p^n}.$$

The set $\Gamma_m = \left\{0, 1, \xi, ..., \xi^{p^m-2}\right\}$ is called the Teichmüller set of R, and any element $c \in R$ can be written uniquely as

$$c = c_0 + c_1p + c_2p^2 + ... + c_{n-1}p^{n-1}, \textit{ for } c_i \in \Gamma_m.$$

This is called the p-adic representation of the element c.
The Frobenius automorphism θ of R over $\mathbb{Z}_{p^n}$ is defined by

$$\theta\,(c) = c_0^p + c_1^p p + c_2^p p^2 + ... + c_{n-1}^p p^{n-1}, \textit{ for } c_i \in \Gamma_m.$$

The group of automorphisms $Aut(GR(p^n, m))$ of the Galois ring $GR(p^n, m)$ is cyclic of order m and is generated by θ. The Frobenius automorphism $\theta \in Aut(GR(p^n, m))$ fixes pointwise the subring $GR(p^n, 1) = \mathbb{Z}_{p^n}$ of $GR(p^n, m)$. For more information and details on Galois rings, we refer the reader to [26].

1.2 Skew polynomial rings $R[t;\sigma,\delta]$

Let R be a ring, $\sigma \in End(R)$ and δ a σ-derivation of R. Recall that δ is an additive map such that for any $a,\ b \in R$, $\delta(ab) = \sigma(a)\delta(b) + \delta(a)b$. Of course, when $\sigma = Id$, δ is a usual derivation. As another example of σ-derivation, let us mention the inner σ-derivation induced by an element $a \in R$, and denoted by δ_a. This is defined by putting $\delta_a(x) = ax - \sigma(x)a$, for all $x \in R$. It is not difficult to show that the map δ_a indeed defines a σ-derivation of the ring R. The skew polynomial ring $S = R[t;\sigma,\delta]$ is a ring whose elements are polynomials $\sum_{i=0}^{n} a_i t^i$ and the product is based on the commutation rule

$$\forall r \in R,\ \ tr = \sigma(r)t + \delta(r). \tag{1.1}$$

By associativity and distribution, we have:

$$t^n r = \sum_{k=0}^{n} S_k^n(r)t^k,\ \forall n \in \mathbb{N},\ \forall r \in R, \tag{1.2}$$

where the additive maps S_k^n satisfy the recursion formula

$$S_k^n = \delta \circ S_k^{n-1} + \sigma \circ S_{k-1}^{n-1} \ \text{ and } \ S_0^0 = Id,\ S_0^1 = \delta,\ S_1^1 = \sigma. \tag{1.3}$$

This means that S_k^n $(0 \leq j \leq n)$ is a sum of all monomials in σ and δ of degree k in σ and degree $n-k$ in δ, e.g. :

$$S_n^n = \sigma^n,\ S_{n-1}^n = \sigma^{n-1}\delta + \sigma^{n-2}\delta\sigma + \cdots + \delta\sigma^{n-1}.$$

We call S the skew polynomial ring in t over R determined by σ and δ (a.k.a Ore extension). These rings were introduced and systematically studied by Oystein Ore in [24]. Such a ring is a commutative ring if and only if R is commutative, $\sigma = Id.$, and $\delta = 0$. If only $\delta = 0$ instead of $R[t;\sigma,0]$ we write $R[t;\sigma]$, and if σ is the identity we write $R[t;\delta]$. This last ring is called a differential polynomial ring in the literature. It appears first in works by Schlesinger (1897) and Landau (1902). If $\delta = 0$ and $\sigma = Id$, then $R[t;1,0]$ is just $R[t]$ the usual polynomial ring in a central indeterminate t (This case is usually referred to as the classical case). Let us mention the following basic but important lemma:

Lemma 1. *Let R be a ring, $\sigma \in End(R)$ and δ be a σ-derivation.*

1. *If there exists c in the center of R such that $\sigma(c) - c$ is invertible, then δ is an inner σ-derivation determined by the element $(c - \sigma(c))^{-1}\delta(c)$.*

2. *If $\delta = \delta_a$, then $S = R[t;\sigma,\delta_a] = R[t-a;\sigma]$.*

The last statement of this lemma says that in fact we can sometimes "erase the derivation". For more on this topic, we refer the reader to a paper by G. Cauchon. (see [6]).

Let us present some properties of S_k^n.

Proposition 3. *Let R be a ring, $\sigma \in End(R)$ and δ a σ-derivation of R. We have :*

1. *S_k^n is the sum of the words in σ and δ of length n with k letters σ and $n-k$ letters δ.*
2. *$S_k^n(ab) = \sum\limits_{j=k}^{n} S_k^n(a)S_j^k(b)$. (This generalizes the Leibniz rule)*
3. *Suppose $\sigma\delta = \delta\sigma$, then $S_k^n = \binom{n}{k}\sigma^k\delta^{n-k}$.*
4. *$S_k^n = \delta(S_k^{n-1}) + \sigma(S_{k-1}^{n-1}),\ n \geqslant i+1$*
5. *$S_k^{n+m} = \sum\limits_{i+j=k} S_i^n S_j^m$.*

Let $f(t) \in R[t;\sigma,\delta]$, as in the classical case f has unique written as $f(t) = a_n t^n + \cdots + a_0$, if $a_n \neq 0$ we define the degree of f as $deg(f) = n$. we say that f is monic if $a_n = 1$.

Definition 14. *A polynomial $f \in S = R[t;\sigma,\delta]$ is called right invariant if $fS \subseteq Sf$ (this means that the left ideal Sf is two-sided ideal of S). A polynomial $g(t) \in S = R[t;\sigma,\delta]$ is called right semi-invariant if $gR \subseteq Rg$. Left invariant and left semi-invariant polynomials are defined similarly.*

Examples 1.

1. The complex skew polynomial ring $\mathbb{C}[t;-]$ consists of all polynomials with complex coefficients and commutation rule $ta = \bar{a}t$, where $\bar{a}$ is the complex conjugate of a. let $P,\ Q \in \mathbb{C}[t;-]$, where $P = it + 1$ and $Q = t + i$, we have

$$PQ \quad = \quad it^2 + i\bar{i}t + t + i = it^2 + 2t + i$$

and

$$QP \quad = \quad \bar{i}t^2 + t - t + i = -it^2 + i.$$

The center of this ring is $\mathbb{R}[t^2]$, the ring of all real polynomials in t^2. The residue class ring mod $x^2 + 1$ is the field of real quaternions. Let us also notice that, since $t + i$ divides QP on the right we might say that $-i$ is a right root of PQ, but replacing t by $-i$ does not give zero. So the evaluation of a polynomial needs to be defined in another way. This will be analyzed later.

2. Let $\mathbb{F}_4\,[t;\theta]$ be the skew polynomial ring with $\mathbb{F}_4 = \left\{0, 1, a, a^2 = a+1\right\}$ and $\theta\,(a) = a^2$. Consider the polynomial $f\,(t) = t - a$ and $g(t) = at + a^2$. We have

$$\begin{aligned} f(t)g(t) &= \theta(a)t^2 + \theta(a^2)t + a^2t + w^3 \\ &= a^2t^2 + t + 1 \end{aligned}$$

and

$$\begin{aligned} g(t)f(t) &= at^2 + a\theta(a^2)t + a^2t + a^3 \\ &= at^2 + at + 1. \end{aligned}$$

We can see that in general the skew polynomial ring is not a unique factorization domain, for example, if we take $p(t) = t^6 + at^3 \in \mathbb{F}_4\,[t;\theta]$, we find that

$$\begin{aligned} p(t) &= (t^4 + at)t^2 \\ &= (t^4 + at^3 + t^2)(t^2 + at) \\ &= (t^4 + at^3)(t^2 + at + 1) \end{aligned}$$

3. Let K be a field and $D = K(x)$ the field of rational functions in an indeterminate x over K. Let δ be the derivation given by the usual derivative on D, i.e., for $f \in D$, $\delta(f) = f^{'} = \dfrac{df}{dx}$. This gives rise to a skew polynomial ring $S = D[t; Id, \frac{d}{dx}]$, the ring of differential operators. Consider the field of rational functions over $\mathbb{F}_2$ and the derivation δ given by the usual derivative, i.e. $\delta(f(x)) = f^{'}(x)$. Hence, let $S = \mathbb{F}_2(x)[t;\delta]$. It is easy to see that t is not invariant in S, as in the following : $tx = xt + (x)^{'} = xt + 1$.

Remarks 1. Let $R[t;\sigma,\delta]$ the skew polynomial ring, then :

1. We have seen earlier that if the σ-derivation δ is inner, induced by an element $a \in R$ (i.e.: $\delta(r) = ar - \sigma(r)a,\ r \in R$), then putting $t^{'} = t - a$, we have $t^{'}r = (t-a)r = (\sigma(r)t + \delta(r)) - ar$ $= \sigma(r)t + ar - \sigma(r)a - ar = \sigma(r)t^{'}$. In this situation $R[t;\sigma,\delta] = R[t-a;\sigma]$. It is worth to mention that $t - a$ is an example of a CV polynomials (CV=change of variables). Other such polynomials are the invariant and semi-invariant polynomials. These polynomials have their own arithmetic. Let us notice, for instance, that if $p(t) \in S$ is a monic invariant polynomial of degree n then we have $p(t)a = \sigma^n(a)p(t)$, for any $a \in R$. These polynomials play an essential role in the study of the center of the Ore extension S as well as in the study of the simplicity of S. They also determine the rings morphisms between different polynomial rings. (for more information on this subject in the case when the base ring R is a division ring, we refer the reader to [17] and[16]).

2. Similarly, if σ is an inner automorphism induced by $u \in U(R)$ (i.e. : $\sigma(r) = uru^{-1},\ r \in R$), and δ is a σ-derivation. We can use the change of variable by writing $t^{'} = u^{-1}t$, we find that $t^{'}r = u^{-1}tr = u^{-1}(\sigma(r)t + \delta(r)) = ru^{-1}t + u^{-1}\delta(r)$, hence $t^{'}r = rt^{'} + u^{-1}\delta(r)$, for all $r \in R$. Then $u^{-1}\delta$ is a usual derivation and $R[t;\sigma,\delta] = R[u^{-1}t; Id, u^{-1}\delta] = R[u^{-1}t; u^{-1}\delta]$.

In the following theorem, we see that the properties of R, reflected in those $R[t;\sigma,\delta]$, see [23]

Theorem 1. *[23] Let $S = R[t;\sigma,\delta]$ the skew polynomial ring in t over R determined by σ and δ, then we have*

1. *If σ is injective and R is an integral domain, then S is an integral domain.*
2. *If σ is injective and R is a division ring, then S is a principal right ideal domain.*
3. *If σ is an automorphism and R is prime ring, then S is prime ring.*
4. *If σ is an automorphism and R is right (resp. left) Noetherian, then S is right (resp. left) Noetherian.*

Classically the exponent of a polynomial is in close relation with its roots. Our next objective is to introduce the "skew evaluation", in other words the evaluation of polynomial from a skew polynomial ring $S = R[t;\sigma,\delta]$. Let $f(t)$ and $g(t)$ be in $R[t;\sigma,\delta]$. If the leading coefficient of $g(t)$ is invertible, then there exists $q(t), r(t) \in R[t;\sigma,\delta]$, such that $f(t) = g(t)q(t) + r(t)$ and $deg(r(t)) \leq deg(g(t))$. We call $q(t)$ (resp. $r(t)$) the right quotient (resp. the right remainder) of $f(t)$ by $g(t)$. if $r(t) = 0$ then $g(t)$ is a right divisor of $f(t)$ in $R[t;\sigma,\delta]$. The division results on the right and on the left are naturally different. This division process is at the base of the definition of right evaluation of a skew polynomial, as we see in the following definition.

Definition 15. *Let R be a ring, σ an endomorphism of R and δ a σ-derivation of R.*

1. *For a polynomial $f(t) \in S = R[t;\sigma,\delta]$ and $a \in R$, we define $f_r(a)$, the right evaluation of $f(t)$ at a, to be the only element in R such that $f(t) - f(a) \in S(t-a)$ i.e. $f(t) = q(t)(t-a) + f_r(a)$, for some polynomial $q(t) \in R[t;\sigma,\delta]$. An element $a \in R$ is a right zero of $f(t) = \sum_{i=0}^{n} f_i t^i$ in S, if $f_r(a) = 0$ i.e. if $f(t)$ is right divisible by $t - a$ in S.*
2. *Two elements $a, b \in R$ are (σ,δ) conjugate if there exists $c \in U(R)$, such that $b = \sigma(c)ac^{-1}$ $+\delta(c)c^{-1}$*

We will use the notations $a \sim b$ to express that a and b are (σ, δ) conjugate and $a^c := \sigma(c)ac^{-1} + \delta(c)c^{-1}$. It is easy to check that $\sim$ is an equivalence relation on R.

Examples 2. 1. Let us evaluate the powers of the indeterminate $t^n \in S = R[t; \sigma, \delta]$. We have $t = (t - a) + a$ so that, as usual, t evaluated at a is a. Let us continue and compute $t^2 = t(t-a) + ta = t(t-a) + \sigma(a)t + \delta(a) = (t + \sigma(a))(t-a) + \sigma(a)a + \delta(a)$, so that t^2 evaluated at a is $\sigma(a)a + \delta(a)$. When $\delta = 0$, live is much more easier and, in this case, we can quickly get the following: t^n evaluated at $a \in R$ is $\sigma^{n-1}(a)\sigma^{n-2}(a)\ldots\sigma(a)a$. This looks like a norm defined by σ and motivates the notation we will use in our next definition.

2. Let us remark that a skew polynomial ring even when its coefficients belong to a commutative field can have infinitely many nonzero right roots. For instance the right roots of $t^2 - 1 \in \mathbb{C}[t; -]$ are all the elements of $\mathbb{C}$ of norm one. We will mention later in this section the right way of evaluating the "number of roots".

3. Let $S = \mathbb{F}_4\,[t; \theta]$ as described in examples $1(2)$, $f(t) = t + a$ and $g(t) = at + 1$ are in S. We have $f(t) = a^2g(t) + 1$ and $f(t) = g(t)a + 0$. We see that $g(t)$ is a left divisor of $f(t)$ but not a right divisor.

Remarks 2. 1. It is, of course possible to define the left evaluation. In case when σ is an automorphism, this comes from the fact that, denoting the opposite ring of a ring R by R^{op}, we can check that $S^{op} = R^{op}[x; \sigma^{-1}, -\delta\sigma^{-1}]$. If an element $b \in R$ is not in the image of σ-evaluating on the left the polynomial bt at $a \in R$ is not possible.

One of the important formulas for evaluating skew polynomials is the product formula. We first introduce this formula in the case when $R = K$ is a division ring. We will place it in a more general context later in the text. Let K be a field, σ an endomorphism and δ a σ-derivation of the division ring K. Recalling that $a^c := \sigma(c)ac^{-1} + \delta(c)c^{-1}$

Theorem 2. *For $f(t),\ g(t) \in S = K[t; \sigma, \delta]$ and $a \in K$, we have*

$$(fg)_r(a) = \begin{cases} 0 & \text{if} \quad g_r(a) = 0, \\ f(a^{g_r(a)})_r g_r(a) & \text{if} \quad g_r(a) \neq 0. \end{cases}$$

Proof.

• If $g_r(a) = 0$ it means that $t - a$ divides $g(t)$ on the right and since $g(t)$ divide $f(t)g(t)$ on the right, hence fg is also divisible on the right by $t - a$, so $(fg)_r(a) = 0$.

• Otherwise, since $g_r(a) = c \neq 0$, we put $b = a^c$. Therefore, there exist $q(t), h(t) \in S$, such that $g(t) = q(t)(t-a) + c$ and $f(t) = h(t)(t-b) + f_r(b)$. Noticing that

$$\begin{aligned}
(t-b)c &= tc - bc \\
&= \sigma(c)t + \delta(c) - a^c c \\
&= \sigma(c)t + \delta(c) - \big(\sigma(c)ac^{-1} + \delta(c)c^{-1}\big)c \\
&= \sigma(c)t + \delta(c) - \sigma(c)a - \delta(c) \\
&= \sigma(c)t - \sigma(c)a \\
&= \sigma(c)(t-a),
\end{aligned}$$

we can use this last equality to write the product $f(t)g(t)$, we obtain that

$$\begin{aligned}
f(t)g(t) &= f(t)q(t)(t-a) + f(t)c \\
&= f(t)q(t)(t-a) + h(t)(t-b)c + f_r(b)c \\
&= f(t)q(t)(t-a) + h(t)\sigma(c)(t-a) + f_r(b)c \\
&= \big[f(t)q(t) + h(t)\sigma(c)\big](t-a) + f_r(b)c
\end{aligned}$$

and $f_r(b)c = f(a^{g_r(a)})_r g_r(a)$. Which gives the desired formula.

□

Definition 16. *Let R be a ring. For $a \in R$, we define the ith norm $N_i(a)$, by induction:*

$$N_0(a) = 1, \quad \text{for } i \geq 0,\ N_{i+1}(a) = \sigma(N_i(a))a + \delta(N_i(a)).$$

In general, if $\delta = 0$, therefore $N_i(a) = \sigma^{i-1}(a)\sigma^{i-2}(a)\cdots\sigma(a)a$.

The following lemma enables us to generalize the classical way of evaluating a polynomial.

Lemma 2. *Let $f(t) = \sum_{i=0}^{n} f_i t^i \in R[t;\sigma,\delta]$ and $a \in R$. Then $f_r(a) = \sum_{i=0}^{n} f_i N_i(a)$*

Example 2. *1. For $S = K(x)[t; Id, \frac{d}{dx}]$ (the ring of differential operators), we have :*

$$\begin{aligned}
N_2(x) &= x^2 + 1. \\
N_3(x) &= x^3 + 3x. \\
N_4(x) &= x^4 + 6x^2 + 3.
\end{aligned}$$

Definition 17. *Let $R,\ \sigma,\ \delta$ be a ring, an automorphism and a σ-derivation, respectively. An element $a \in R$ is of finite (σ,δ)-order if there exists a positive integer l such that $N_l(a) = 1$. When it exists, the smallest $l > 0$ such that $N_l(a) = 1$ is called the (σ,δ)- order of a and denoted by $ord_{\sigma,\delta}(a) = l$.*

Now, we introduce the definition of the norm in the special case when $\delta = 0$ and R is finite, and study some of its elementary properties.

Definitions 2. *Let G be a finite group and $\sigma \in Aut(G)$.*

1) Let $g \in G$ and $n \in \mathbb{N}$. We define the n'th norm of g, denoted $N_n(g)$ by $N_0(g) = 1$and, for $n \geqslant 1$,

$$N_n(g) = \sigma^{n-1}(g)\sigma^{n-2}(g)\cdots\sigma(g)g.$$

2) An element $g \in G$ is of finite σ-order if there exists $l \in \mathbb{N}$ such that $N_l(g) = 1$. In this case $ord_\sigma(g)$ is the smallest l such that $N_l(g) = 1$

(3) For two elements $x, g \in G$ we define $x \underset{\sigma}{\circ} g := \sigma(x)gx^{-1}$. We say that two elements $g, h \in G$ are σ-conjugate if there exists an element $x \in G$ such that $h = \sigma(x)gx^{-1}$.

In the particular case when $\delta = 0$ and R is finite, we have the following properties of the norm N_i.

Proposition 4. *Let g be an element of a finite group G and $\sigma \in Aut(G)$. Then we have the following*

a) $N_{l+s}(g) = \sigma^l(N_s(g))N_l(g) = \sigma^s(N_l(g))N_s(g)$.

b) For $l, q \in \mathbb{N}$ we have $N_{lq}(g) = \sigma^{l(q-1)}(N_l(g))\sigma^{l(q-2)}(N_l(g))\cdots\sigma^l(N_l(g))N_l(g)$.

c) Every element $g \in G$ is of finite σ-order.

d) $N_r(g) = 1$ if and only if $ord_\sigma(g)$ divides r.

e) If $\tau \in Aut(G)$ is such that $\sigma\tau = \tau\sigma$, then $ord_\sigma(g) = ord_\sigma(\tau(g))$.

f) For any $s \in \mathbb{N}$, $N_s(\sigma(g)hg^{-1}) = \sigma^s(g)N_s(h)g^{-1}$. With our notations this means:

$$N_s(g \underset{\sigma}{\circ} h) = g \underset{\sigma^s}{\circ} N_s(h).$$

g) If $\sigma^l = id$, then

i) $\sigma(N_l(g)) = gN_l(g)g^{-1}$.

ii) For any $i \in \mathbb{N}$, $N_{il}(g) = N_l(g)^i$.

iii) $ord_\sigma(g) | l \cdot ord(N_l(g))$.

Proof. a) We have $N_{l+s}(g) = \sigma^{l+s-1}(g)\cdots\sigma(g)g = \sigma^l\left(\sigma^{s-1}(g)\cdots\sigma(g)g\right)\sigma^{l-1}(g)\cdots\sigma(g)g$ $= \sigma^l(N_s(g))N_l(g)$. The second equality is shown similarly.

b) This follows easily from the statement a) above.

c) Since the group G is finite, for any $g \in G$, there must exist $l,\ s \in \mathbb{N}$ with $s \neq 0$, such that $N_{l+s}(g) = N_l(g)$. The statement a) above then implies that $N_s(g) = 1$. This yields the result.

d) Let us put $l := ord_\sigma(g)$. By definition we must have $N_l(g) = 1$ and $l \leq r$. Let us write $r = lq + s$, where $s < l$. We have $1 = N_r(g) = N_{lq+s}(g) = \sigma^s(N_{lq}(g))N_s(g)$. The point b) above then implies that $1 = N_s(g)$. Since $s < l$ this shows that $s = 0$, as desired. Conversely, suppose that $l := ord_\sigma(g)$ is such that l divides r, say $r = ls$ for some $s \in \mathbb{N}$. Using statement (b) above we get $N_r(g) = N_{ls}(g) = \sigma^{l(s-1)}(N_l(g))\sigma^{l(s-2)}(N_l(g))\cdots\sigma^l(N_l(g))N_l(g)$. Since $N_l(g) = 1$ we get that $N_r(g) = 1$, as desired.

e) Let us put $l := ord_\sigma(g)$, therefore $N_l(g) = 1$, so we have $\sigma^{l-1}(g)\sigma^{l-2}(g)\cdots\sigma(g)g = 1$. Apply τ, to this last equality, we get $\tau\big(\sigma^{l-1}(g)\sigma^{l-2}(g)\cdots\sigma(g)g\big) = \tau\big(\sigma^{l-2}(g)\big)\cdots\tau\big(\sigma(g)\big)\tau(g)$, and since $\sigma\tau = \tau\sigma$, we get $\sigma^{l-1}(\tau(g))\sigma^{l-2}(\tau(g))\cdots\sigma(\tau(g))\tau(g) = 1$, This means that $ord_\sigma(\tau(g)) = l$, so $ord_\sigma(g) = ord_\sigma(\tau(g))$.

f) For any $S \in \mathbb{N}$, we have

$$\begin{aligned} N_s(\sigma(g)hg^{-1}) &= \sigma^{n-1}(\sigma(g)hg^{-1})\sigma^{n-2}(\sigma(g)hg^{-1})\cdots\sigma(\sigma(g)hg^{-1})\sigma(g)hg^{-1} \\ &= \sigma^n(g)\sigma^{n-1}(h)\sigma^{n-1}(g^{-1})\sigma^{n-1}(g)\sigma^{n-2}(h)\sigma^{n-2}(g^{-1})\cdots\sigma^2(g)\sigma(h)\sigma(g^{-1})\sigma(g)hg^{-1} \\ &= \sigma^n(g)\big[\sigma^{n-1}(h)\sigma^{n-2}(h)\cdots\sigma(g)\big]g^{-1} \\ &= \sigma^s(g)N_s(h)g^{-1}. \end{aligned}$$

This yields the result.

g) i) We have

$$\begin{aligned} \sigma(N_l(g)) &= \sigma\big(\sigma^{l-1}(g)\sigma^{l-2}(g)\cdots\sigma(g)g\big) \\ &= \sigma^l(g)\sigma^{l-1}(g)\cdots\sigma^2(g)\sigma(g) \end{aligned}$$

and since $\sigma^l = id$, we find that

$$\begin{aligned} \sigma^l(g)\sigma^{l-1}(g)\cdots\sigma^2(g)\sigma(g) &= g\sigma^{l-1}(g)\cdots\sigma^2(g)\sigma(g)gg^{-1} \\ &= gN_l(g)g^{-1} \end{aligned}$$

ii) comes from the statement b) above.

For $iii)$, we compute: $\sigma(N_l(g)) = \sigma^l(g)\sigma^{l-1}(g)\cdots\sigma(g) = gN_l(g)g^{-1}$.

iv) Since $\sigma^l = id.$, statement $ii)$ above shows that $N_{ls}(g) = N_l(g)^s$. If s is the order of $N_l(g)$ in G, we get $N_{ls}(g) = N_l(g)^s = 1$. Part d) above then implies that $ord_\sigma(g)$ divides $ls = l \cdot ord(N_l(g))$. □

In the case of a finite cyclic group, the last point of the previous lemma is more precise.

Corollary 1. *Let $G =< g >$ be a finite cyclic group and let l be the order of an automorphism $\sigma \in Aut(G)$. Then we have $ord_\sigma(g) = l \cdot ord(N_l(g))$.*

Proof. We already know that $ord_\sigma(g)$ divides $l \cdot ord(N_l(g))$. Let $p, n \in \mathbb{N}$ be such that $\sigma(g) = g^p$ and $n := |G| = ord(g)$. Since $\sigma^l = id$, we have that $g^{p^l} = \sigma^l(g) = g$ and hence $g^{p^l-1} = 1$. Since $n = ord(g)$, we conclude that n divides $p^l - 1$. We write $ord_\sigma(g) = il + r$ for $i \in \mathbb{N}$ and $0 \leq r < l$ and, using the above lemma, we have $1 = N_{il+r}(g) = N_l(g)^i N_r(g) = g^{i[l]+[r]}$, where $[l] = \frac{p^l-1}{p-1}$ and $[r] = \frac{p^r-1}{p-1}$. This implies that n divides $i[l] + [r]$. Hence there exists $m \in \mathbb{N}$ such that $n(p-1)m = i(p^l - 1) + (p^r - 1)$. The fact that n divides $p^l - 1$ implies that n also divides $p^r - 1$. This shows that, for any $g \in G$, $\sigma^r(g) = g^{p^r} = g$. Since $0 \leq r < l$ and l is the order of σ, we must have $r = 0$ and $1 = g^{i[l]} = N_l(g)^i$. This yields that $ord(N_l(g))$ divides i and hence $l \cdot ord(N_l(g))$ divides $li = ord_\sigma(g)$, as desired. □

1.3 Pseudo-linear transformations

In this part, we give the most important result of pseudo-linear transformations used in the next chapters. For more information see [20]. Let us remind a few technical matters.

Definition 18. *Let R be a ring, σ an endomorphism of R and δ a σ-derivation of R. Let also V stand for a left R-module. A map $T : V \longrightarrow V$ such that,*

1. *$T(v_1 + v_2) = T(v_1) + T(v_2)$ for all $v_1,\ v_2 \in V$,*
2. *$T(\alpha v) = \sigma(\alpha)T(v) + \delta(\alpha)v$ for $\alpha \in R$ and $v \in V$,*

is called a (σ, δ) pseudo-linear transformation (or a (σ, δ)-PLT, for short).

In case V is a finite dimensional vector space and σ is an automorphism, the pseudo-linear transformations were introduced by Jacobson in [14]. They appear naturally in the context of modules over an Ore extension $S = R[t; \sigma, \delta]$. This is explained in [19].

If V is a finitely generated free left R-module, $\underline{e} = \{e_1, \ldots, e_n\}$ is an ordered set of free generators of V, and T is an endomorphism of the left R-module V, let us write $T(e_i) = \sum_{j=1}^n a_{ij}e_j$, $a_{ij} \in R$, or with matrix notation $T(\underline{e}) = A\underline{e}$, where $A = (a_{ij}) \in M_n(K)$. The matrix A will be denoted $M_{\underline{e}}(T)$.

Proposition 5. *Let R be a ring, $\sigma \in End(R)$ and δ a σ-derivation of R. For an additive group $(V, +)$, the following conditions are equivalent:*

(1) V has a left $S = R[t;\sigma,\delta]$-module structure;

(2) V is a left R-module endowed with a (σ,δ) pseudo-linear transformation $T : V \longrightarrow V$;

(3) There exists a ring homomorphism $\Lambda : S \longrightarrow End(V,+)$.

Examples 3. 1. *If $a \in R$, $T_a : R \longrightarrow R$ given by $T_a(r) = \sigma(r)a + \delta(r)$ is a (σ,δ)-PLT. Remark that $T_0 = \delta$.*

2. *As is well known (cf.[19], [20]), if $f(t) = \sum_{i=0}^{n} a_i t^i$, we have $f(a) = \sum_{i=0}^{n} a_i N_i(a)$. In fact, we also have $f(a) = f(T_a)(1) = \sum_{i=0}^{n} a_i (T_a)^i(1)$.*

3. *If $g(t) \in S = R[t;\sigma,\delta]$, the (σ,δ)-PLT corresponding to S/Sg (cf. Proposition 5) is given by the action of t. If $g(t)$ is monic of degree n, S/Sg is a left R-free module with basis $(\overline{1},\overline{t},\ldots,\overline{t^{n-1}})$ and the elements of S/Sg correspond to vectors in R^n. With this point of view, the left multiplication by t on S/Sg corresponds to the PLT $T_g : R^n \longrightarrow R^n$ given by $T_g(\underline{v}) = \sigma(\underline{v})C_g + \delta(\underline{v})$, where C_g is the companion matrix of $g(t)$ (cf. [19]).*

We will need the following lemma that can be found in [20], Lemma 3.3 (b).

Lemma 3. *Let V be a left free R-module with basis $e = (e_1, ..., e_n)$ and $T : V \to V$ a (σ,δ)-PLT. Let $A = (a_{ij}) = M_e(T) \in M_n(R)$ be the matrix representing T in this basis. Let $g(t) \in R[t;\sigma,\delta]$. Then $g(T)(e_i) = \sum_{j=1}^{n} g(A)_{ij} e_j$ for $i = 1, ..., n$ or in matrix form*

$$M_{\underline{e}}(g(T)) = g(M_{\underline{e}}(T)),$$

where σ and δ are naturally extended to matrices and the evaluation of g at $M_{\underline{e}}(T)$ is as given in the above definition.

In the next proposition we give a formula which generalizes the standard one (theorem 2) for the evaluation of a product of polynomials at a point $c \in R$.

Proposition 6. *[20] Let R be a ring, σ an endomorphism of R and δ a σ-derivation of R and let $f(t),\ g(t)$ be polynomials in $S = R[t;\sigma,\delta]$. Then for any $c \in R$ we have :*

$$(f(t).g(t))_r(c) = f(T_c)_r(g_r(c)).$$

In particular if $g(c)$ is invertible in R we have $(f(t).g(t))_r(c) = f(c^{g_r(c)})_r g_r(c)$.

Chapter 2

Exponents in general finite rings

We are going to attach an integer to a nonzero polynomial, this is known as the exponent (or order) of polynomial. We define the exponent of the polynomial $f(t)$ as the least positive integer e such that $f(t)$ divides $t^e - 1$. In [21], chapter 3, part 1, we find a study of this notion over finite field (i.e. exponent of polynomial over $\mathbb{F}_q[t]$), we refer the reader to review this part for more information and to have a clear view of this concept.

Exponent of polynomial is very important in the theory of polynomials over finite fields and in coding theory, it also has great importance in linear recurring sequences. In 2016, A. Cherchem and A. Leroy generalized the notion of exponent from the classical case over $\mathbb{F}_q[t]$ to the skew case $\mathbb{F}_q[t;\theta]$, and introduced the notion of a relative exponent for two elements in a finite ring and apply this to define and study the skew exponent of a polynomial in an Ore extension of the form $\mathbb{F}_q[t;\theta]$.

In this chapter we present a short survey of this work. We focus our attention to important results that shall motivate next sections and the last chapter of this thesis and we propose programs in computer software MAGMA.The interested reader may consult [9] for more properties and details. We begin by the definition of the exponent over a ring.

Definition 19. *Let R be a ring and $f(t) \in R[t]$. If there exists a positive integer $e = e(f)$ such that $f(t)|\ t^e - 1$, the least such e is called the exponent of $f(t)$ (a.k.a. order or period of $f(t)$).*

We note that the polynomial t is invariant in the polynomial ring $R[t;\sigma]$ i.e. $Rt = tR$, but in a general Ore extension $R[t;\sigma,\delta]$ the polynomial t is no longer invariant. However, there will often exists an invariant polynomial that can play its role. This leads us to define the relative exponent of two polynomials in a quite general setting.

Definition 20. *Let R be a ring and $f, g \in R$. The right exponent of g relative to f is the smallest strictly positive integer $e = e_r(g, f)$, when it exists, such that $f^e - 1 \in Rg$, i.e. g is a right divisor of $f^e - 1$. Similarly, we can define the notion of left exponent of g relative to f.*

The next lemma examines the existence of the relative exponent over finite rings and gives some conditions for this. We will only prove part (b), as it will be the starting point for a generalization of the relative exponent, presented in chapter 4.

Lemma 4. *[9] Let R be a finite ring with $1_R \in R$ and $f,\ g \in R$ be such that $fg \in Rf$. Let $r_g : R/Rf \to R/Rf$ the right multiplication by g. Consider the following statements:*

(i) The map r_g is one-to-one.

(ii) For any $h \in R$, if $hg \in Rf$ then $h \in Rf$.

(iii) There exists a positive integer e such that $f^e - 1 \in Rg$.

(iv) The map r_g is onto.

(v) $Rg + Rf = R$.

Then:

a) We always have (i)⇔(ii) and (iii)⇒(iv)⇔(v).

b) If $|R/Rg| < \infty$ and f is not a zero divisor and is such that $fR = Rf$, we also have (ii)⇒(iii).

c) If conditions b) are satisfied and moreover $|R/Rf| < \infty$, then statements (i) to (v) are equivalent.

Proof. (b) Since $|R/Rg| < \infty$, there exist integers $0 < l < s$ such that $(1 - f^{s-l})f^l \in Rg$ and hence there exists $h \in R$ such that $(1 - f^{s-l})f^l = hg \in Rf$. Statement (ii) and the fact that $Rf = fR$ ensure that there exists $q_1, q_1' \in R$ such that $h = q_1 f = f q_1'$. Since f is not a zero divisor we have $f^{l-1}(1 - f^{s-l}) = q_1' g \in Rf$. Repeating this argument leads to the existence of $q_2', q_3', \ldots, q_l' \in R$ such that $f^{l-i}(1 - f^{s-l}) = q_i' g$. In particular, we have $1 - f^{s-l} = q_l' g \in Rg$. □

Remarks 3. *In the proof we only use $Rf \subseteq fR$. But for the analogue of the above result for right modules we will need the other inclusion. Moreover when f is a non zero divisor and R/Rf is finite the inclusion $Rf \subseteq fR$ is equivalent to $fR \subseteq Rf$.*

Let us give some basic properties related to the notion of relative exponent.

Lemma 5. *[9] Suppose that $f, g, h \in R$ such that $e_r(g, f)$ and $e_r(h, f)$ exist. Then:*

a) g is a right factor of $f^l - 1$ if and anly if $e_r(g, f)$ divides l;

b) g is a right factor of h if and anly if $e_r(g, f)$ divides $e_r(h, f)$;

c) if $Rg \cap Rh = Rm$, then $e_r(m, f)$ exists and it is equal to the least common multiple of $e_r(g, f)$ and $e_r(h, f)$.

2.1 Skew exponents over $\mathbb{F}_q[t;\theta]$

Now let's take the finite field as an example. Let $n \in \mathbb{N}^*$, p a prime, and $q = p^n$. Consider the skew polynomials ring $\mathbb{F}_q[t;\theta]$, where $\theta : \mathbb{F}_q \to \mathbb{F}_q$ is the Frobenius automorphism defined by : $\theta(a) = a^p$. Let $f(t), g(t) \in \mathbb{F}_q[t;\theta]$ such that $g(0) \neq 0$ and $f(t) = t$, so that condition (i) of Lemma 4 is satisfied . This leads to the following proposition.

Proposition 7. *Let $\mathbb{F}_q$ be a finite field and θ be the Frobenius automorphism of $\mathbb{F}_q$, and let $f(t)$ $\in \mathbb{F}_q\left[t;\theta\right]$. If $f\left(0\right) \neq 0$, then there exists a positive integer e such that $f(t)|x^e - 1$ on the right.*

The right exponent of f is defined to be the least integer e such that $f(t)|x^e - 1$. We denote it by $e_r\left(f\right) := e_r(f, t)$.

Example 3. *Let $\mathbb{F}_4\left[t;\theta\right]$ be the skew polynomial ring with $\mathbb{F}_4 = \left\{0, 1, a, a^2 = a + 1\right\}$ and $\theta\left(a\right) = a^2$. Consider the polynomial $f\left(t\right) = t - a$. In the classical case, when $f \in \mathbb{F}_4\left[t\right]$, the exponent is 3. However, when $f \in \mathbb{F}_4\left[t;\theta\right]$, we have $\left(t - a^2\right)\left(t - a\right) = t^2 - ta - a^2t + a^3 = t^2 - (\theta\left(a\right) + a^2)t + 1$ $= t^2 - 1$. Then $e_r\left(f\right) = 2$.*

In the sequel, we shall write $e\left(f\right)$ for the (right) exponent of f.

The study of exponents is related to a notion of order of an element in a group with an automorphism. We introduce this definition and study some of its elementary properties.

Definitions 3. *Let G be a group and $\sigma \in Aut(G)$.*

1) Let $g \in G$ and $n \in \mathbb{N}$. We define the nth norm of g, denoted $N_n(g)$ by $N_0(g) = 1$ and, for $n \geqslant 1$,

$$N_n(g) = \sigma^{n-1}(g)\sigma^{n-2}(g)\cdots\sigma(g)g.$$

2) An element $g \in G$ is of finite σ-order if there exists $l \in \mathbb{N}^*$ such that $N_l(g) = 1$. In this case $ord_\sigma(g)$ is the smallest l such that $N_l(g) = 1$.

(3) For two elements $x, g \in G$. We define $x \underset{\sigma}{\circ} g := \sigma(x)gx^{-1}$. We say that two elements $g, h \in G$ are σ-conjugate if there exists an element $x \in G$ such that $h = \sigma(x)gx^{-1}$.

We give in the following proposition some relations between the above definitions.

Proposition 8. *[9] Let $q = p^l$, where p is prime, $l \in \mathbb{N}^*$, and let $g, g_1, ..., g_s$ be monic polynomials in $\mathbb{F}_q[t;\theta]$ with nonzero constant terms. Then:*

a) the polynomial g is a right (resp., left) factor of $t^c - 1$, where c is a positive integer, if and only if $e(g)$ divides c;

b) if g is a right (resp., left) factor of h, then $e(g)$ divides $e(h)$;

c) we denote by $[g_1, ..., g_s]_l$ the least left common multiple of $g_1, \ldots, g_s$. We have :

$e([g_1, \ldots, g_s]_l) = lcm(e(g_1), \ldots, e(g_s))$;

d) for $\alpha \in \mathbb{F}_q^*$, $e(t - \alpha) = ord_\theta(\alpha)$;

e) if α is a primitive element of $\mathbb{F}_q = \mathbb{F}_{p^l}$, then $e(t - \alpha) = l(p - 1)$;

f) If $\alpha \in \overline{\mathbb{F}}_q$ is such that $t - \alpha$ is a right (resp., left) factor of $g(t)$ in $\overline{\mathbb{F}}_q[t;\theta]$ and $g(t)$ is irreducible in $\mathbb{F}_q[t;\theta]$, then $e(g) = ord_\theta(\alpha)$.

Example 4. Let us denote $\mathbb{F}_4 = \mathbb{F}_2(a)$ with $a^2 + a + 1 = 0$ and $\mathbb{F}_{16} = \mathbb{F}_4(b)$ with $b^2 + b + a = 0$. Consider $R = \mathbb{F}_{16}[t;\theta]$, where θ is the Frobenius automorphism defined by $\theta(c) = c^2$, for all $c \in \mathbb{F}_{16}$. One can check that the left R-modules $R/R(t - a)$ and $R/R(t - ab)$ are isomorphic (i.e. the two polynomials $t - a$ and $t - ab$ are similar) but the exponents of these polynomials are different. Indeed, we easily check that $\theta(a)a = 1$ and hence the θ-order of a is 2 and, by the statement (d) in the proposition 8, the exponent of $t - a$ is two as well (look also at Example 3). Now, the θ-order of ab is equal to 4, is bigger than 2 and hence the exponent of $t - ab$ is bigger than two as well.

If $C = (c_{ij})_{0 \leq i,j \leq n}$ is a matrix with entries in $\mathbb{F}_q$, we set $\theta(C) = (\theta(c_{ij}))_{0 \leq i,j \leq n}$. One can check easily that θ is then an automorphism of $GL_n(\mathbb{F}_q)$. In the next theorem we present concrete ways of computing this exponent over the ring $\mathbb{F}_q[t;\theta]$.

Theorem 3. *[9] Let $g\left(t\right)=t^{n}+g_{n-1}t^{n-1}+\cdots+g_{0}\in\mathbb{F}_{q}\left[t;\theta\right]$ and*

$$C_g=\begin{pmatrix}0&1&0&\cdots&0\\0&0&1&\cdots&0\\\vdots&\vdots&\vdots&\ddots&\vdots\\0&0&0&\cdots&1\\-g_0&-g_1&-g_2&\cdots&-g_{n-1}\end{pmatrix}$$

the companion matrix of g. Then:

(a) $ord_{\theta}\left(C_g\right)=e_r(t-C_p)$;

(b) $e_r\left(g\right)=ord_{\theta}\left(C_g\right)$.

Proof. (a) Remarking that $t-C_p\in M_n(\mathbb{F}_q[t;\theta])$ this is then an immediate consequence of the fact (d) in Proposition 8 (and the remark following it).

(b) Put $m:=ord_{\theta}(C_p)$ and remark that, thanks to the part (a) of the Theorem, there exists a polynomial $q(t)=(q_{ij}(t))\in M_n(\mathbb{F}_q)[t;\theta]=M_n(\mathbb{F}_q[t;\theta])$ such that $q(t)(t-C_p)=t^m-1$. Equating the first row entries on both side we get

- $q_{11}(t)t+q_{1n}(t)a_0=t^m-1$ for the (11) entry,
- $-q_{1i}(t)t+q_{1,i+1}(t)t+q_{1,n}(t)a_i=0$ for the entries $(1,i)$ and $2\leq i\leq n-2$,
- $-q_{1,n-1}(t)+q_{1,n}(t)(t+a_{n-1})=0$ for the $(1,n)$ entries.

Going backwards we then get successively $q_{1,n-1}(t)=q_{1,n}(t)(t+a_{n-1})$ and replacing $q_{1,n-1}(t)$ in the previous equation leads to $q_{1,n-2}(t)=q_{1,n}(t)(t^2+a_{n-1}t+a_{n-2})$. More generally, for $1\leq i\leq n-1$, we obtain

$$q_{1,n-i}(t)=q_{1,n}(t)(t^i+a_{n-1}t^{i-1}+\cdots+a_{n-i})\quad\text{for } 1\leq i\leq n-1.$$

In particular, $q_{1,1}(t)=q_{1,n}(t)(t^{n-1}+\cdots+a_2t+a_1)$. Replacing this value in the first equation $q_{11}(t)t+q_{1n}(t)a_0=t^m-1$ above we get $q_{1,n}p(t)=t^m-1$. This shows that $e_r(p(t))$ divides m. For the converse suppose that $e=e_r(p(t))$ and let $q(t)p(t)=t^e-1\in R:=\mathbb{F}_q[t;\theta]\subset M_n(\mathbb{F}_q)[t;\theta]$. We have $t^e-1\in Rp$ and hence by Theorem 1.10 in [19] we have that $(T_p^e-1)(I,0,\ldots,0)=(0,0,\ldots,0)$ where the entries of the vectors are square matrices of size $\deg(p)$. This leads to $\theta^e(I,0,\ldots,0)N_e(C_p)=(I,0,\ldots,0)$ and hence $N_e(C_p)=I$. So that $ord_{\theta}(C_p)$ divides e. This yields the desired result. □

Theorem 4. *[9] The left and right exponent of a monic polynomial $g(t)\in\mathbb{F}_q[t;\theta]$ are equal.*

Proof. We must show that, for $e = e_r(g)$, $g(t)$ divides $t^e - 1$ on the right and on the left. Now $e_r(g) = ord_\theta(C_g)$. Working in $M_s(\mathbb{F}_q)[t;\theta]$ with $s = \deg g(t)$, we have $ord_\theta(C_g) = e_r(t - C_g)$. In $M_s(\mathbb{F}_q)[t;\theta]$ $t - C_g$, is a right factor of $t^e - 1$ if and only if

$$\theta^{e-1}(C_g) \cdots \theta(C_g) C_g = 1.$$

Appling θ^{1-e} to this equality, we get

$$C_g \theta^{-1}(C_g) \cdots \theta^{1-e}(C_g) = 1.$$

This means that $t - C_g$ is a left factor of $t^e - 1$. Hence $e_r(t - C_g) = e_l(t - C_g)$.

□

From Theorem 3, we can see that the computing of exponent, is in fact an algebraic calculation in the finite field $\mathbb{F}_q$. The following program defines a command $\texttt{Exp}(f, p^i)$ in MAGMA which determines the exponent of any skew polynomial $f(t) \in \mathbb{F}_q[t;\theta]$, with $\theta(r) = r^{p^i}$ for all $r \in \mathbb{F}_q$. We note here that in [25], the authors give a program in MAGMA to compute the exponent of skew polynomials of degree 2 only.

Program 1.

```
q:= ... ;
F<a>:=GF(q);
R<t>:=PolynomialRing(F);
f(t):= ... ;

FrobM:=function(M,n,theta)
     for i in [1..n], j in [1..n] do
       M[i][j]:=M[i][j]^theta;
     end for;
     return M;
end function;

Exp:= function(poly,theta)
  M:=CompanionMatrix(poly);
  n:=Nrows(M);
  pr:=1;
  Id:=Matrix(IdentitySparseMatrix(Parent(M[1][1]),n));
  i:=0;
  repeat
     pr:=M*pr;
     M:=FrobM(M,n,theta);
     i:=i+1;
     until (pr eq Id);
 return i;
end function ;

Exp(f, ... );
```

Example 5. *Let $\mathbb{F}_{27} = \mathbb{F}_3(b)$ be a finite field with $b^3+2b+1 = 0$ and θ the Frobenius automorphism defined by $\theta(r) = r^3$ for all $r \in \mathbb{F}_{27}$. Consider $R = \mathbb{F}[t;\theta]$ and Let $f(t) = t^3 + t + b \in R$. Let's use* ***Program*** *1 to calculate the exponent*

```
# We begin by definir our ring and  f(t).
F<b>:=GF(3^3);
R<t>:=PolynomialRing(F);
f:=t^3+t+b;
# We implement the program on Magma.
FrobM:=function(M,n,theta)
   for i in [1..n], j in [1..n] do
     M[i][j]:=M[i][j]^theta;
   end for;
return M;
end function;

Exp:= function(pol,theta)
   M:=CompanionMatrix(pol);
   n:=Nrows(M);
   pr:=1;
   Id:=Matrix(IdentitySparseMatrix(Parent(M[1][1]),n));
   i:=0;
```

```
  repeat
    pr:=M*pr;
    M:=FrobM(M,n,theta);
    i:=i+1;
    until (pr eq Id);
return i;
end function ;
# We use command Exp(f,3) to compute the exponent of f(t).
Exp(f,3);
```

We find that `Exp(f,3)=9` *and* $(t^9-1)=(t^3+t+b)(x^6+2x^4+a^{14}x^3+x^2+a^{22}x+a^{12})$*. We can check the results obtained using the following commands in MAGMA.*

```
F<b>:=GF(27);
R<t>:=SkewPolynomialRing(F,1);
f:=t^3+t+b;
(t^9-1) mod f;
```

We have seen, in (f), Theorem 8, that if we have $g(t)\in\mathbb{F}[t;\theta]$ is irreducible and $\alpha\in\overline{\mathbb{F}}_q$ is a root of $g(t)$ in $\overline{\mathbb{F}}_q[t;\theta]$ (i.e. $t-\alpha$ is a right factor of $g(t)$ in $\overline{\mathbb{F}}_q[t;\theta]$), then $e(g)=ord_\theta(\alpha)$. So, as in the classical case, we can compute the exponent of a polynomial using the θ-order of its root. In the following we give a program on MAGMA to compute the exponent using the θ-order of its root. Before that, let's mention some basic definitions and skills.

Proposition 9. *Let* $f(t)=\sum\limits_{i=0}^{n}a_it^i\in\mathbb{F}_q[t;\theta]$ *and* $\alpha\in\overline{\mathbb{F}}_q$*, then the right remainder of the Euclidean division on the right of* $f(t)$ *by* $t-\alpha$ *is:*

$$\sum_{i=0}^{n}a_iN_i(\alpha).$$

Proof. Let $f(t)=a_nt^n+\cdots+a_0\in\mathbb{F}_q[t;\theta]$, then we have the following equality, for any integer $i\geqslant 1$:

$$t^i-N_i(\alpha)=\left[t^{i-1}+\theta^{i-1}(\alpha)t^{i-2}+\theta^{i-1}(\alpha)\theta^{i-2}(\alpha)t^{i-3}+\cdots+N_i(\alpha)\right](t-\alpha).$$

Multiplying these equations by a_i and summing over i, with $1\leq i\leq n$, we get:

$$\sum_{i=1}^{n}a_it^i-a_iN_i(\alpha)=Q(t)(t-\alpha).$$

By adding a_0, we get:

$$\sum_{i=0}^{n}a_it^i-a_iN_i(\alpha)=Q(t)(t-\alpha).$$

This proves the proposition. □

Corollary 2. *Let $f(t) = \sum_{i=0}^{n} a_i t^i \in \mathbb{F}_q[t;\theta]$ and $\alpha \in \overline{\mathbb{F}}_q$, then α is a root of $f(t)$ if and only if:*

$$\sum_{i=0}^{n} a_i N_i(\alpha) = 0.$$

We observe that if $\theta(\alpha) = \alpha^{q_0}$ and $\theta \neq id$, then $N_i(\alpha) = \theta^{i-1}(\alpha)\dots(\alpha) = \alpha^{q_0^{i-1}}\dots\alpha$, then :

$$N_i(\alpha) = \alpha^{\sum_{j=0}^{i-1} q_0^j} = \alpha^{\frac{q_0^i - 1}{q_0 - 1}}.$$

We deduce the following proposition:

Proposition 10. *Let $f(t) = \sum_{i=0}^{n} a_i t^i \in \mathbb{F}_q[t;\theta]$ and $\alpha \in \overline{\mathbb{F}}_q$, then α is a root of $f(t)$ if and only if α is root of the following polynomial of $\mathbb{F}_q[Y]$:*

$$P_f = \sum_{i=0}^{n} a_i Y^{\frac{q_0^i - 1}{q_0 - 1}}.$$

This polynomial P_f is a polynomial of the commutative ring $\mathbb{F}_q[Y]$, is denoted with the indeterminate Y to not confuse it with skew polynomials.

In [19], we find a study of the polynomial P_f (called $[p]$-polynomial) previously defined. They show that the question of the irreducibility of a polynomial $f(t) \in \mathbb{F}_q[t;\theta]$ can be translated in terms of factorization in $\mathbb{F}_q[x]$, as the following proposition show and in the case of a skew polynomial ring $\mathbb{F}_q[t;\theta]$ where $q = p^n$ and θ is the Frobenius automorphism, the splitting field of a polynomial $f(t) \in \mathbb{F}_q[t;\theta]$ is the splitting field of the polynomial P_f over $\mathbb{F}_q[Y]$.

Proposition 11. *[19] A polynomial $f(t) \in \mathbb{F}_q[t;\theta]$ is irreducible if and only if $P_f \in \mathbb{F}_q[Y]$ has no non trivial factor belonging to $\mathbb{F}_q[Y]$.*

In the following MAGMA program, we define a command $\texttt{RemPol}(f(t), p^i)$ which gives the polynomial P_f of the skew polynomial $f(t) \in \mathbb{F}_q[t;\theta]$, with $\theta(r) = r^{p^i}$ for all $r \in \mathbb{F}_q$.

Program 2.

```
RemPol:=function(poly,theta)
 p:=theta;
 t:=Coefficients(poly);
 s:=t[1];
 for i in [2..#t] do
```

```
   s:=s+t[i]*t^((p^(i-1)-1) div (p-1) );
 end for;
return s;
end function;
```

Example 6. *Let us denote $\mathbb{F}_4 = \{0, 1, a, a+1\}$. Consider $R = \mathbb{F}_4[t;\theta]$, where $\theta(a) = a^2$. Let $f(t) = t^2 + at + 1 \in R$, let's compute P_f in MAGMA with **Program** 2.*

```
# We define our ring and f(t).
F<a>:=GF(4);
R<x>:=PolynomialRing(F);
po:=x^2+a*x+1;
# We implement the program on MAGMA.
RemtPol:=function(poly,theta)
  p:=theta;
  t:=Coefficients(poly);
  s:=t[1];
  for i in [2..#t] do
    s:=s+t[i]*x^((p^(i-1)-1) div (p-1) );
  end for;
return s;
end function;
# We use the command RemPol(f,2).
RemPol(f,2);
>x^3 + a*x + 1
```

We get $P_f(Y) = Y^3 + aY + 1$.

We recall that for an element $a \in \mathbb{F}_q$, the nth norm $N_l(a) = \theta^{n-1}(a)\theta^{n-2}(a)\dots\theta(a)a$ and a is of finite θ-order, if there exists $l \in \mathbb{N}$ such that $N_l(a) = 1$. The smallest l such that $N_l(a) = 1$ is the θ-order of a, and it is denoted by $ord_\theta(a)$. We propose in the following a program to compute it, using the command `ThetaOrd`(a, p^i), where $\theta(a) = a^{p^i}$.

Program 3.

```
ThetaOrd:=function(elem,theta)
 p:=1;
 i:=0;
 repeat
   p:=p*elem;
   elem:=elem^theta;
   i:=i+1;
   until (p eq 1);
return i;
end function;
```

Now, with **Programs** 2 and 3 we are able to use MAGMA to compute the exponent of irreducible polynomial in $\mathbb{F}_q[t;\theta]$ using the θ-order of its root in $\overline{\mathbb{F}}_q$.

Example 7. *Let $f(t) = t^2 + at + 1 \in \mathbb{F}_4[t;\theta]$, where $\theta(a) = a^2$, as described in Example 6 above. let's compute $e(f,t)$ with MAGMA.*

```
# We define our ring and f(t).
F<a>:=GF(4);
R<x>:=PolynomialRing(F);
f:=x^2+a*x+1;
# We implement programs 2 and 3 on MAGMA.
RemPol:=function(poly,theta)
p:=theta;
t:=Coefficients(poly);
s:=t[1];
for i in [2..#t] do
s:=s+t[i]*x^((p^(i-1)-1) div (p-1) );
end for;
return s;
end function;

ThetaOrd:=function(elem,theta)
p:=1;
i:=0;
repeat
p:=p*elem;
```

```
elem:=elem^theta;
i:=i+1;
until (p eq 1);
return i;
end function;
# We use the command RemPol(f,2) to compute P(f).
RemPol(f,2);
>x^3 + a*x + 1
# we test the irreducibility of P(f).
Factorization(x^3 + a*x + 1);
[
<x^3 + a*x + 1, 1>
]
# We define the splitting field of P(f)
F1<w>:=ext<F | x^3+a*x+1>;
# We use the command ThetaOrd(w,2) to compute the O-order of the root w of P(f).
ThetaOrd(w,2);
>6
```

Therefore $ord_\theta(w) = 6$*, where* $w \in \dfrac{\mathbb{F}_4[t]}{(P_f)}$ *and* $P_f(w) = 0$*, then* $Exp(f,t) = 6$.

In next theorem, we generalize a relationship (see [27]) between the exponent in a finite field and in a Galois ring from the classical case to the skew case. We follow the same proof method used in ([27]). For this we need the following lemma.

Lemma 6. *Let* $f \in GR(p^n, m)\,[t;\theta]$ *and* $l \in \mathbb{N}^*$*. If* $f \equiv 1\,\left[p^l\right]$*, then* $f^p \equiv 1\,\left[p^{l+1}\right]$.

Proof. We have the classical equality in a noncommutative ring :

$$b^i - a^i = (b-a)b^{i-1} + a(b-a)b^{i-2} + \cdots + a^{i-1}(b-a).$$

From this equality, we can deduce the decomposition of $f^p - 1$:

$$\begin{aligned} f^p - 1 &= (f-1)f^{p-1} + (f-1)f^{p-2} + \ldots + (f-1) \\ &= (f-1)\left(f^{p-1} + f^{p-2} + \ldots + 1\right). \end{aligned}$$

we have by hypothesis $f \equiv 1\,\left[p^l\right]$, then p^l divides $(f-1)$ and

$$\begin{aligned} f^{p-1} + f^{p-2} + \ldots + 1 &\equiv 1 + \cdots + 1\,\left[p^l\right] \\ &\equiv p\left[p^l\right] \end{aligned}$$

So p divides $(f^{p-1}+f^{p-2}+\cdots+1)$, therefore $p^{l+1}|(f-1)(f^{p-1}+f^{p-2}+...+1)$, we get then $p^{l+1}|f^p-1$ and $f^p\equiv 1\left[p^{l+1}\right]$. □

In the following theorem, we use the notation $e_\theta(f)$ (resp. $e_\theta(\overline{f})$) to express the exponent $e(f,t)$ in the skew polynomials ring $GR(p^n,m)\,[t,\theta]$ (resp., $\mathbb{F}_{p^m}\,[t,\theta]$).

Theorem 5. *Let $R=GR(p^n,m)$ be a Galois ring and $f\,(t)=\sum\limits_{i=0}^{k}a_it^i$ be a skew polynomial in $R\,[t,\theta]$. Then,we have the following :*

1) $f(t)$ have an exponent if and only if $a_0\in U(R)$;

2) If $e_\theta(\overline{f})=e$, then $e_\theta(f)=p^ie$, where $0\le i<n$.

Proof. 1) If $f(t)$ have an exponent, so there exist a positive integer $e\in\mathbb{N}^*$ and a polynomial $g\,(t)\in R\,[t;\theta]$ such that $t^e-1=f\,(t)\,g\,(t)$, then $f\,(0)\,g\,(0)=-1$ and clearly $f(0)=a_0$ is unite. Conversely, if $a_0\neq 0$, the condition (i) of Lemma 4 is satisfied, then $f(t)$ have an exponent.

2) Now suppose $a_0\in U(R)$, so then there exists $e\in\mathbb{N}^*$ with $\overline{f}\,(t)\,|t^e-1$ in $\mathbb{F}_{p^m}[t;\theta]$. Suppose $g\,(t)\in GR(p^n,m)\,[t;\theta]$ such that $t^e-1=f\,(t)\,g\,(t)\,(mod\,p)$, so $t^e-f\,(t)\,g\,(t)=1(mod\,p)$. Taking p^i-th powers on both sides, by Lemma 6, we have :

$$(t^e-f\,(t)\,g\,(t))^{p^i}=1(mod^{\cdot}p^{i+1})$$

Note that p^n is the characteristic of $GR(p^n,m)$. Letting $i=n-1$, we have :

$$(t^e-f\,(t)\,g\,(t))^{p^{n-1}}=1$$

which leads to,

$$t^{ep^{n-1}}=1\ (mod^{\cdot}f\,(t))$$

then, $r|p^{n-1}e$, where $r=e_\theta(f)$. On the other hand, from $f\,(t)\,|(t^r-1)$,we get $\overline{f}(t)|t^r-1$ and $e|r$. Thus $r=p^ie$, where $0\le i<n$.

□

Example 8. *Let $GR(4,2)=\mathbb{Z}_4\,[\xi]=\{0,1,2,3,\xi,\xi+1,...,3\xi,3\xi+1,3\xi+2,3\xi+3\}$, where $\xi^2=-\xi-1$ and $\theta\,(a_0+a_1\xi)=a_0+a_1\xi^2$, for $a_i\in\mathbb{Z}_4$.*

The exponent of $f\,(t)=t^2+t+\xi\in GR(4,2)\,[t;\theta]$ is 8, and we have

$$t^8-1=\left(t^6+3t^5+(3\xi+1)t^4+2t^3+(2\xi+1)t^2+t+\xi+1\right)\left(t^2+t+\xi\right)$$

The exponent of $f\,(t)=t^2+t+a\in\mathbb{F}_4\,[t;\theta]$ is 4, and we have

$$t^4-1=\left(t^2+t+a^2\right)\left(t^2+t+a\right)$$

2.2 Skew exponents in general finite ring R

Somewhat more generally, we can consider a finite ring A, an automorphism $\sigma \in Aut(A)$ and $f(t) = t \in R = A[t;\sigma]$. If $g(t) \in R$ is such that its independent term is invertible then $Rg + Rt = R$ and all the conditions of the Lemma 4 will be satisfied.

Theorem 6. *Let R be finite ring with identity 1_R and $\sigma \in Aut(R)$ be such that $\sigma^l = id_R$ for some $l \in \mathbb{N}^*$. Let $f(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_0 \in R[t,\sigma]$ with $a_0 \in U(R)$ and let*

$$C_f = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \\ 0 & 0 & 0 & \cdots & 1 \\ -a_0 & -a_1 & -a_2 & \cdots & -a_{n-1} \end{pmatrix} \in M_n(R)$$

be the companion matrix of $f\,(t)$. Then $e_r(f) = ord_\sigma(C_f)$.

Proof. Let $f(t) = \sum\limits_{i=0}^{n} a_i t^i \in R[t;\sigma]$. We denote $R[t;\sigma]f(t)$ by (f) and put $T = R[t;\sigma]/(f)$. let V^k denote the transpose of the vector $(\overline{t^k}, \overline{t^{k+1}}, \overline{t^{k+2}}, \ \ldots\ , \overline{t^{k+n-1}})$, where $\overline{t} = t + (f)$ and $k \in \mathbb{N}$. Firstly, let us prove that

$$N_k(C_f).V^0 = V^k, \forall k \in \mathbb{N}^*. \tag{2.1}$$

For $k = 1$, we find that $C_f.V^0 = V^1$. We suppose that equality (2.1) is true for all positive integers smaller or equal to k, and we prove it for $k+1$.
We have $N_{k+1}(C_f).V^0 = \sigma^k(C_f).N_k(C_f).V^0 = \sigma^k(C_f).V^k$ by hypothesis. Since $\overline{t^n} = -\sum\limits_{i=0}^{n-1} \overline{a_i t^i}$ in T, then $\overline{t^{k+n}} = \overline{t^k}\,\overline{t^n} = -\sum\limits_{i=0}^{n-1} \overline{t^k a_i t^i} = -\sum\limits_{i=0}^{n-1} \overline{\sigma^k(a_i) t^{k+i}}$, therefore $\sigma^k(C_f).V^k = V^{k+1}$.
Now, the ring $M_n(R)$ is periodic because R is finite, so a nonzero divisor matrix must be invertible. If we suppose that C_f is a zero-divisor, then there exists $0 \neq M \in M_n(R)$ such that $MC_f = 0$. But the fact that $a_0 \in U(R)$ implies that $M = 0$, a contradiction. Hence C_f is invertible. This leads to $\sigma^k(C_f)$ is invertible, for all $k \in \mathbb{N}$. Notice also that $N_k(C_f) \in M_n(S)$, where S is the subring of R generated by $\{\sigma^k(a_i),\ 0 \leq k \leq l,\ 0 \leq i < n\}$. This implies that $M_n(S)$ is finite. By Proposition 4, (c), in [9], C_f is of finite σ-order r, where r is a positive integer. If we put $k = r$ in (2.1), we get $N_r(C_f)V^0 = I_n V^0 = V^r$, so $\overline{t^r} = \overline{1}$. This yields that $e_r(f)$ divides r, from (a) of lemma 5. On the other hand, if we set $e_r(f) = e$, then f divides $t^e - 1$ on the right, hence $\overline{t^e} = \overline{1}$. Now if we put $k = e$ in (2.1), we get $N_e(C_f)V^0 = V^e = V^0$, so $(N_e(C_f) - Id)V^0 = 0$. Since $\{\overline{1}, \overline{t}, \overline{t^2}, \ \ldots\ , \overline{t^{n-1}}\}$ is a basis of T as a left R-module, then $N_e(C_f) = Id$, which means that e divides $ord_\sigma(C_f)$. □

Now, we give a commutativity relation of $t^e - 1$ in $R[t;\theta]$. We prove that in quite general situations, the fact that $g(t)$ divides on the right the polynomial $t^e - 1$ implies that $g(t)$ also divides $t^e - 1$ on the left.

Theorem 7. *Let R be a ring and $f(t), g(t) \in R[t;\theta]$ be such that f is monic and $f_0 g_0 = g_0 f_0$, where f_0 and g_0 are the constant terms of $f(t)$ and $g(t)$ respectively. Assume that $f(t)g(t) = t^e - 1$ for a positive integer e. Then we have also $g(t)f(t) = t^e - 1$.*

Before going on into the proof we need the following lemma.

Lemma 7. *Let k be a non-zero positive integer and $a(i,r)$ be a formula in i and r. Then we have*

(i) $\sum\limits_{i=1}^{k}\sum\limits_{r=1}^{i} a(i,r) = \sum\limits_{i=1}^{k}\sum\limits_{r=0}^{k-i} a(i+r,i)$,

(ii) $\sum\limits_{i=1}^{k}\sum\limits_{r=0}^{k-i} a(i,r) = \sum\limits_{i=1}^{k} a(i,0) + \sum\limits_{i=1}^{k-1}\sum\limits_{r=1}^{k-i} a(i,r)$.

Proof. **(i)** We shall use the following formula mentioned in [[11], page 36]:

$$\sum_{i=1}^{k}\sum_{r=1}^{k} a(i,r) = \sum_{r=1}^{k}\sum_{i=r}^{k} a(i,r) = \sum_{i=1}^{k}\sum_{r=i}^{k} a(r,i).$$

We use the change of variable $s = r - i$, so we have

$$\sum_{i=1}^{k}\sum_{r=1}^{k} a(i,r) = \sum_{i=1}^{k}\sum_{r=i}^{k} a(r,i) = \sum_{i=1}^{k}\sum_{s=0}^{k-i} a(i+s,i).$$

Replacing s by r, we obtain

$$\sum_{i=1}^{k}\sum_{r=1}^{k} a(i,r) = \sum_{i=1}^{k}\sum_{r=0}^{k-i} a(i+r,i).$$

(ii) The proof is trivial. □

Proof. of the theorem

Let $f(t) = \sum\limits_{i=0}^{n} f_i t^i$ and $g(t) = \sum\limits_{j=0}^{m} g_j t^j$, so

$$f(t)g(t) = \sum_{i=0}^{n}\sum_{j=0}^{m} f_i\theta^i(g_j)t^{i+j} = \sum_{k=0}^{m+n} A_k t^k,$$

where $A_k = \sum\limits_{i+j=k} f_i\theta^i(g_j)$. Similarly

$$g(t)f(t) = \sum_{j=0}^{m}\sum_{i=0}^{n} g_j\theta^j(f_i)t^{i+j} = \sum_{k=0}^{n+m} B_k t^k$$

with $B_k = \sum\limits_{i+j=k} g_j\theta^j(f_i)$.
Assume that $f(t)g(t) = t^{n+m} - 1$. Then we have

$$\begin{aligned} A_0 &= -1, \\ A_1 &= A_2 = ... = A_{n+m-1} = 0, \\ A_{n+m} &= 1. \end{aligned}$$

We shall prove that

$$\begin{aligned} B_0 &= -1, \\ B_1 &= B_2 = ... = B_{n+m-1} = 0, \\ B_{n+m} &= 1. \end{aligned}$$

We have $A_0 = f_0g_0 = -1$, so $B_0 = g_0f_0 = -1$, and $A_{n+m} = B_{n+m} = 1$ since f and g are monic. Now we need to prove that

$$B_1 = B_2 = ... = B_{n+m-1} = 0.$$

In order to do that, we use finite induction. First, we verify that $B_1 = 0$, where $B_1 = g_0f_1 + g_1\theta(f_0)$. We have
$B_0 = g_0f_0 = -1$ and $A_1 = f_0g_1 + f_1\theta(g_0) = 0$. Multiplying A_1 by g_0 on the left and by $\theta(f_0)$ on the right, we obtain

$$\begin{aligned} g_0A_1\theta(f_0) &= (g_0f_0)g_1\theta(f_0) + g_0f_1\theta(g_0).\theta(f_0) \\ &= (g_0f_0)g_1\theta(f_0) + g_0f_1\theta(g_0f_0) \\ &= -g_1\theta(f_0) - g_0f_1 = -B_1 \end{aligned}$$

Thus $A_1 = 0$ implies $B_1 = 0$, and the first step of induction is proved.
Now we suppose that $B_t = 0$ for all $t \in \{1, 2, ..., k\}$ and we prove that $B_{k+1} = 0$, where $0 < k < m + n - 1$.
For that, we will show that

$$g_0A_{k+1}\theta^{k+1}(f_0) = -B_{k+1}. \tag{2.2}$$

We know that

$$\begin{aligned} B_{k+1} &= \sum_{i+j=k+1} g_i\theta^i(f_j) \\ &= \sum_{i=0}^{k+1} g_i\theta^i(f_{k-i+1}) \\ &= g_0f_{k+1} + \sum_{i=1}^{k} g_i\theta^i(f_{k-i+1}) + g_{k+1}\theta^{k+1}(f_0), \end{aligned}$$

and

$$\begin{aligned} A_{k+1} &= \sum_{i+j=k+1} f_i\theta^i(g_j) \\ &= \sum_{i=0}^{k+1} f_i\theta^i(g_{k-i+1}) \\ &= f_0g_{k+1} + \sum_{i=1}^{k} f_i\theta^i(g_{k-i+1}) + f_{k+1}\theta^{k+1}(g_0). \end{aligned}$$

As in the first step, multiplying A_{k+1} by g_0 on the left and by $\theta^{k+1}(f_0)$ on the right, we obtain

$$\begin{aligned} g_0A_{k+1}\theta^{k+1}(f_0) &= g_0(f_0g_{k+1} + \sum_{i=1}^{k} f_i\theta^i(g_{k+1-i}) + f_{k+1}\theta^{k+1}(g_0)\theta^{k+1}(f_0) \\ &= -g_{k+1}\theta^{k+1}(f_0) + g_0\sum_{i=1}^{k} f_i\theta^i(g_{k-i+1})\theta^{k+1}(f_0) - g_0f_{k+1} \\ &= -g_0f_{k+1} + g_0\sum_{i=1}^{k} f_i\theta^i(g_{k-i+1})\theta^{k+1}(f_0) - g_{k+1}\theta^{k+1}(f_0) \end{aligned}$$

Identifying the coefficients of B_{k+1} and $g_0A_{k+1}\theta^{k+1}(f_0)$, we see that proving the equality (1) is equivalent to showing that

$$g_0\sum_{i=1}^{k} f_i\theta^i(g_{k+-i+1})\theta^{k+1}(f_0) = -\sum_{i=1}^{k} g_i\theta^i(f_{k-i+1}).$$

Let us evaluate $g_0 \sum\limits_{i=1}^{k} f_i\theta^i(g_{k+-i+1})\theta^{k+1}(f_0)$.

By hypothesis $B_i = 0$ for all i, where $0 < i \leqslant k$, and $B_i = \sum\limits_{r+s=i} g_r\theta^r(f_s) = \sum\limits_{r=0}^{i} g_r\theta^r(f_{i-r})$. Multiplying B_i on the right by $\theta^i(g_{k-i+1})$, and summing up from $i = 1$ to k, we obtain

$$\sum_{i=1}^{k} B_i\theta^i(g_{k-i+1}) = \sum_{i=1}^{k}\sum_{r=0}^{i} g_r\theta^r(f_{i-r})\theta^i(g_{k-i+1}) = 0.$$

By isolating the term when $r = 0$ in the last sum, we get

$$\sum_{i=1}^{k} g_0f_i\theta^i(g_{k-i+1}) = -\sum_{i=1}^{k}\sum_{r=1}^{i} g_r\theta^r(f_{i-r})\theta^i(g_{k-i+1}).$$

From lemma 7, (i), we find

$$\sum_{i=1}^{k} g_0 f_i \theta^i(g_{k-i+1}) \quad = \quad -\sum_{i=1}^{k}\sum_{r=0}^{k-i} g_i \theta^i(f_r)\theta^{i+r}(g_{k-i-r+1}).$$

Using lemma 7, (ii), we deduce that

$$\begin{aligned}\sum_{i=1}^{k} g_0 f_i \theta^i(g_{k-i+1}) &= -\sum_{i=1}^{k} g_i \theta^i(f_0)\theta^i(g_{k-i+1}) - \sum_{i=1}^{k-1}\sum_{r=1}^{k-i} g_i \theta^i(f_r)\theta^{i+r}(g_{k-i-r+1})\\ &= -\sum_{i=1}^{k} g_i \theta^i(f_0 g_{k-i+1}) - \sum_{i=1}^{k-1}\sum_{r=1}^{k-i} g_i \theta^i(f_r)\theta^{i+r}(g_{k-i-r+1}).\end{aligned}$$

Now, we evaluate $f_0 g_{k-i+1}$. We know that $A_{k-i+1} = 0$ for all $0 < i \leq k$, so

$$A_{k-i+1} = \sum_{r+s=k-i+1} f_r \theta^r(g_s) = \sum_{r=0}^{k-i+1} f_r \theta^r(g_{k-i-r+1}) = 0.$$

When we pick out the term for $r = 0$, we obtain

$$f_0 g_{k-i+1} = -\sum_{r=1}^{k-i+1} f_r \theta^r(g_{k-i-r+1}).$$

Replacing $f_0 g_{k-i+1}$ by its value, we get

$$\begin{aligned}\sum_{i=1}^{k} g_0 f_i \theta^i(g_{k-i+1}) &= -\sum_{i=1}^{k} g_i \theta^i\Big(-\sum_{r=1}^{k-i+1} f_r \theta^r(g_{k-i-r+1})\Big) - \sum_{i=1}^{k-1}\sum_{r=1}^{k-i} g_i \theta^i(f_r)\theta^{i+r}(g_{k-i-r+1})\\ &= \sum_{i=1}^{k}\sum_{r=1}^{k-i+1} g_i \theta^i(f_r)\theta^{i+r}(g_{k-i-r+1}) - \sum_{i=1}^{k-1}\sum_{r=1}^{k-i} g_i \theta^i(f_r)\theta^{i+r}(g_{k-i-r+1}).\end{aligned}$$

Isolating the term for $r = k - i + 1$, we obtain

$$\begin{aligned}\sum_{i=1}^{k} g_0 f_i \theta^i(g_{k-i+1}) = \sum_{i=1}^{k} g_i \theta^i(f_{k-i+1})\theta^{k+1}(g_0) \quad &+ \sum_{i=1}^{k-1}\sum_{r=1}^{k-i} g_i \theta^i(f_r)\theta^{i+r}(g_{k-i-r+1})\\ &- \sum_{i=1}^{k-1}\sum_{r=1}^{k-i} g_i \theta^i(f_r)\theta^{i+r}(g_{k-i-r+1}),\end{aligned}$$

then

$$\sum_{i=1}^{k} g_0 f_i \theta^i(g_{k-i+1}) = \sum_{i=1}^{k} g_i \theta^i(f_{k-i+1})\theta^{k+1}(g_0).$$

Finally, we multiply the last equality from the right side by $\theta^{k+1}(f_0)$, then we have

$$\begin{aligned}g_0 \sum_{i=1}^{k} f_i \theta^i(g_{k-i+1})\theta^{k+1}(f_0) &= \sum_{i=1}^{k} g_i \theta^i(f_{k-i+1})\theta^{k+1}(g_0)\theta^{k+1}(f_0)\\ &= \sum_{i=1}^{k} g_i \theta^i(f_{k-i+1})\theta^{k+1}(g_0 f_0)\\ &= -\sum_{i=1}^{k} g_i \theta^i(f_{k-i+1}),\end{aligned}$$

therefore,

$$g_0 \sum_{i=1}^{k} f_i \theta^i(g_{k-i+1}) \theta^{k+1}(f_0) = -\sum_{i=1}^{k} g_i \theta^i(f_{k-i+1}).$$

The last equality proves that $g_0 A_{k+1} \theta^{k+1}(f_0) = -B_{k+1}$, and since $A_{k+1} = 0$, we conclude that $B_{k+1} = 0$.

This completes the proof □

Chapter 3

Periodic graded rings and *P.I.* rings

3.1 New characterizations of periodic rings

If R is a periodic ring, then the element $1_R + 1_R$ is periodic and this easily leads to the first statement of the following lemma. The second is true for any ring of positive characteristic.

Lemma 8. *Let R be a periodic ring, then*

1. *R has a positive characteristic.*

2. *If $q > 0$ is the characteristic of R and $q = p_1^{n_1} \dots p_s^{n_s}$ is a decomposition of q as product of prime integers, then the ring R is isomorphic to $R_1 \times \cdots \times R_s$, where, for $1 \leq i \leq s$, $R_i = \frac{q}{p_i^{n_i}} R$.*

Remark 2. *We mention that, if R is periodic and $R = R_1 \times \cdots \times R_s$ is the decomposition from Lemma 8, then the rings R_i, $1 \leq i \leq s$, are stable under the action of σ and δ. This leads to the decomposition $S = R[t;\sigma,\delta] = R_1[t_1;\sigma_1,\delta_1] \times \cdots \times R_s[t_s;\sigma_s,\delta_s]$ with the obvious notations.*

Periodic rings have many nice properties. First, let us notice some properties of periodic elements.

Lemma 9.

1. *Let r be a periodic element in a ring R. If $r^n = r^m$ with $m < n$, then for any $k \in \mathbb{N}$ and $j \geq m$, we have $r^{k(n-m)+j} = r^j$.*

2. *If S is a finite subset of periodic elements in a ring R, there exist positive integers l, n with $l > n$ such that, for every $s \in S$, $s^l = s^n$.*

3. *If $u \in U(R)$ is periodic, there exists a positive integer n such that $u^n = 1$.*

4. *The periodic elements of the Jacobson radical are nil.*

5. *If $a \in R$ is periodic, there exists $l = l(a) \in \mathbb{N}$ such that a^l is an idempotent.*

6. *If $a, b \in R$ are such that ab is periodic, then ba is periodic.*

Proof. (1) We have $r^m r^{n-m} = r^m$, this easily gives that for any $k \in \mathbb{N}$, $r^m r^{k(n-m)} = r^m$ and hence also $r^{k(n-m)+j} = r^j$ for all $j \geq m$.

(2) It is enough to consider the case when S has two elements, say s_0, s_1. Since R is periodic, there exist integers $l_0 > n_0$ and $l_1 > n_1$ such that $s_0^{l_0} = s_0^{n_0}$ and $s_1^{l_1} = s_1^{n_1}$. From Part 1 above, we get $s_0^{(l_0-n_0)(l_1-n_1)+j} = s_0^j$ and $s_1^{(l_0-n_0)(l_1-n_1)+j} = s_1^j$ for any $j \geq max\{n_0, n_1\}$.

(3) If $u \in U(R)$ is periodic, there exist integers $m > n$ such that $u^m = u^n$, then $u^{m-n} = 1$.

(4) If $a \in J(R)$ is periodic, there exist integers $m < l$ such that $a^m(a^{l-m} - 1) = 0$. Since $a^{l-m} \in J(R)$, $a^{l-m} - 1 \in U(R)$ and $a^m = 0$.

(5) If $a \in R$ and $l > m$ are integers such that $a^l = a^m$, and if $k \in \mathbb{N}$ is such that $j := k(l-m)-m > 0$, then, according to the point 1 above, we have $a^{2(m+j)} = a^{2k(l-m)} = a^{m+j+k(l-m)} = a^{m+j}$.

(6) We have $(ab)^m = (ab)^n$, with m, n an integers and $m > n$. Multiplying both sides of the previous equation by a on the right and b on the left, we obtain $(ba)^{m+1} = (ba)^{n+1}$. □

Let us now give a useful characterization of periodic rings. This can be obtained from results in the literature but we offer here a short independent proof.

Proposition 12. *Let R be a ring and $J = J(R)$ its Jacoson radical. Then R is periodic if and only if J is nil and R/J is periodic.*

Proof. Assume J nil and R/J periodic. These hypotheses imply that, for any $a \in R$, there exist $l, m, s \in \mathbb{N}$ such that $l < m$ and $(a^m - a^l)^s = 0$. This is true in particular for the element $2 = 1_R + 1_R \in R$. This shows that there exists $0 \neq q \in \mathbb{N}$ such that $qR = 0$. Using the above equality we get that, for any $a \in R$, there exists $r \geq 1$ such that $a^r = \sum_{i=0}^{r-1} \alpha_i a^i$, where $\alpha_i \in \{0, 1, \ldots, q-1\}$. This shows that the subring generated by a in R is finite and hence a is periodic. The converse is an immediate consequence of Part 4 of the precedent lemma. □

We now relate periodic rings with other kind of rings. Let us first recall, that a ring is strongly π-regular (resp. strongly clean) if and only if for any $a \in R$, there exists $n \geq 1$ (resp. there exist $e = e^2$ and $u \in U(R)$) such that $a^n \in a^{n+1}R$ (resp. $a = e + u$ and $ue = eu$). A ring R has stable range 1 if whenever $a, b \in R$ are such that $aR + bR = R$, there exists $x \in R$ with $ax + b$ right invertible. As it is well-known this notion is left-right symmetric.

Proposition 13. *Let R be a periodic ring. Then*

1. *R is Dedekind finite.*

2. *R is strongly π-regular.*

3. *R has stable range 1.*

4. *R is strongly clean.*

Proof. (1) Let $a, b \in R$ be such that $ab = 1$, we know that there exist $l, s \in \mathbb{N}$ such that $a^l = a^s$ and $l > s$. Define $e_{ij} = b^i(1 - ba)a^j$, then we have for any $i, j, k, l \in \mathbb{N}$, $e_{ij}e_{kl} = 0$ if $j \neq k$ and $e_{ij}e_{kl} = e_{il}$ if $j = k$, so $e_{is}e_{li} = 0$. This implies that

$$\begin{aligned} 0 &= b^i(1-ba)a^s b^l(1-ba)a^i \\ &= b^i(1-ba)a^l b^l(1-ba)a^i \\ &= b^i(1-ba)(1-ba)a^i \\ &= b^i(1-ba)a^i \end{aligned}$$

Left and right multiplying by a^i and b^i respectively, we get $ba = 1$.

(2) Since a ring R is strongly π-regular if and only if for any $a \in R$ the descending chain $aR \supseteq a^2R \supseteq a^3R \dots$ (equivalently $Ra \supseteq Ra^2 \supseteq Ra^3 \dots$) is finite.

(3) According to a Theorem 4 of P. Ara (cf. [1]), every strongly π-regular ring has stable range 1.

(4) We must show that any element $a \in R$ can be written as $a = e + u$, where $e^2 = e$ is an idempotent, u is an invertible element and moreover $ue = eu$. Thanks to Lemma 9 (3), we know that there exists $n \in \mathbb{N}$ such that $f = a^n$ is an idempotent. We can check that $(a - (1 - f))(a^{n-1}f - (1 + a + \cdots + a^{n-1})(1 - f)) = 1$. This yields the thesis □

We will now give one more characterization of periodic rings. We will need the following easy lemma.

Lemma 10. *Let R be a ring of positive characteristic q. If $a, b \in R$ are periodic and $ab = ba$, then $a + b$ is periodic.*

Proof. It is enough to show that the set $P := \{(a + b)^i : i \in \mathbb{N}\}$ of powers of $a + b$ is finite. Since a and b are periodic and commute, there is only a finite number of words in a and b. This means that the set $\{a^i b^j : i, j \in \mathbb{N}\}$ is finite. So, for any $i \in \mathbb{N}$, $(a + b)^i$ is a sum of words $\alpha a^i b^j$, where i and j are both bounded (since a and b are periodic), and $\alpha \in \{0, 1, 2, \dots q - 1\}$ (since $qR = 0$, where q denote the finite characteristic of R) . This yields that P is finite, as desired. □

Remark 3. *Let us remark that a similar proof as in 10 shows that if a and b are periodic elements and $p(t) \in \mathbb{Z}[t]$ such that $ab = p(a)b$, then $a + b$ is periodic. We will not need this fact.*

Theorem 8. *A ring R is periodic if and only if the followings hold:*

1. *R is of positive characteristic,*
2. *R is strongly clean,*
3. *The invertible elements of R are roots of unity.*

Proof. Thanks to Lemmas 8 and 9 and Proposition 13, we only need to prove that the above conditions are sufficient for the ring R to be periodic.

Assume that R is a ring that satisfies (1), (2) and (3), let $a \in R$. We can thus write $a = u + e$, where u is invertible, e is an idempotent element and $eu = ue$. So, we have $e^2 = e$, and there exists $n \in \mathbb{N}$ such that $u^n = 1$ so that the elements e and u are periodic and commute. Lemma 10 above shows that a is then periodic, as required. □

3.2 Periodic graded rings

Theorem 9. *Let $R = \oplus_{i\in\mathbb{N}} R_i$ be a graded ring such that R_0 is a periodic ring. Let $f = a_0 + a_1 + ... + a_m \in R$, $a_i \in R_i$ for $i \in \{0, ..., m\}$ and $f^n = \sum\limits_{k=0}^{nm} A_k^n$, where A_k^n is the homogeneous component of f^n of degree k. Then, for all $k \in \mathbb{N}$, there exist $l, s \in \mathbb{N}$ with $l > s$ and $A_k^l = A_k^s$.*

Proof. Let $f = \sum_{i=0}^{m} a_i \in R$. Since R_0 is periodic, there exist positive integers e, p with $p < e$ and $a_0^e = a_0^p$. Let us notice that A_k^n is the sum of all words in $a_0, a_1, ..., a_m$ of length n and degree k. Any word in $a_0, a_1, ..., a_m$ of length n and degree k is of the form $a_0^{j_1} a_{c_1} a_0^{j_2} a_{c_2} ... a_{c_y} a_0^{j_y+1}$, with $0 \leq j_l \leq e$ and $\sum_{b=1}^{y} c_b = k$. The number, say h, of such words is finite and is independent of n. If $w_1, ..., w_h$ are all the words in $a_0, a_1, ..., a_m$ of length n and degree k, then for all $n \in \mathbb{N}$, $A_k^n = \alpha_1 w_1 + ... + \alpha_h w_h$, $\alpha_i \in \mathbb{N}$. Lemma 8 shows that $0 \leq \alpha_i \leq q - 1$. Therefore, for all $k \in \mathbb{N}$, there exist $l, s \in \mathbb{N}$, $l > s$ such that $A_k^l = A_k^s$, as desired. □

Corollary 3. *Let $R = \oplus_{i\in\mathbb{N}} R_i$ be a graded ring and $l \in \mathbb{N}$. Suppose that $R_i = 0$ for $i \geq l$. Then R is periodic if and only if R_0 is periodic.*

Proof. It is enough to use Part 2 of Lemma 9. □

We saw in Theorem 9 that the homogeneous components A_k are periodic. In the next proposition, we give a period for each homogeneous component. We keep the notations used in Theorem 9.

Proposition 14. *Let $R = \oplus_{i\in\mathbb{N}} R_i$ be a graded ring with R_0 periodic, and such that $qR_0 = 0$ for $q \in \mathbb{N}^*$. Then, for $f = \sum\limits_{k=0}^{m} a_k \in R$, with $a_k \in R_k$ for $0 \le k \le m$ and $a_0 \neq 0$, we have*

1. *For any positive integers n and k,*

$$A_k^n = \sum_{i=0}^{n-1}\sum_{j=0}^{k-1} A_{k-j-1}^i a_{j+1} a_0^{n-i-1}.$$

2. *If $a_0^l = a_0^s$ with $l, s \in \mathbb{N}$ and $l > s$, then, for all $k \in \mathbb{N}$, $A_k^{q^k l} = A_k^{q^k s}$. Moreover, for all $a, b \in \mathbb{N}$ with $b \geqslant q^k s$, $A_k^{aq^k(l-s)+b} = A_k^b$.*

Proof. 1. Let $f = \sum\limits_{k=0}^{m} a_k \in R$, and $f^{n-1} = \sum\limits_{k=0}^{(n-1)m} A_k^{n-1}$, then

$$f^{n-1} f = \sum_{i=0}^{(n-1)m}\sum_{j=0}^{m} A_i^{n-1} a_j = \sum_{k=0}^{nm} A_k^n,$$

where $A_k^n = \sum\limits_{i+j=k} A_i^{n-1} a_j = \sum\limits_{j=0}^{k} A_{k-j}^{n-1} a_j$, $A_0^0 = 1$ and $A_i^0 = 0,\ i > 0$.
It is clear that $A_0^n = a_0^n$ for all $n \in \mathbb{N}^*$. Let us prove that, for any positive integers k and n, we have

$$A_k^n = \sum_{i=0}^{n-1}\sum_{j=0}^{k-1} A_{k-j-1}^i a_{j+1}\, a_0^{n-i-1}.$$

First, for $n = 1$ and $k \in \mathbb{N}^*$, we have $A_k^1 = \sum\limits_{j=0}^{k-1} A_{k-j-1}^0\, a_{j+1} = a_k$. We suppose that the formula giving A_k^n is true for all positive integers k and n, and we prove that it is true for A_k^{n+1}. For all $k \in \mathbb{N}^*$, we have

$$\begin{aligned} A_k^{n+1} &= \sum_{j=0}^{k} A_{k-j}^n a_j = A_k^n a_0 + \sum_{j=1}^{k} A_{k-j}^n a_j \\ &= \sum_{i=0}^{n-1}\sum_{j=0}^{k-1} A_{k-j-1}^i a_{j+1}\, a_0^{n-i} + \sum_{j=0}^{k-1} A_{k-j-1}^n a_{j+1} \\ &= \sum_{i=0}^{n}\sum_{j=0}^{k-1} A_{k-j-1}^i\, a_{j+1}\, a_0^{n-i}, \end{aligned}$$

as desired.

2. We have $A_0^l = A_0^s$, and from Part 1 of Lemma 9, $A_0^{a(l-s)+b} = A_0^b$ for all $a, b \in \mathbb{N}$ with $b \geqslant s$. We use now induction on k. We suppose that

$$A_\lambda^{q^\lambda l} = A_\lambda^{q^\lambda s} \text{ and } A_\lambda^{aq^\lambda(l-s)+b} = A_\lambda^b$$

for all $\lambda \in \{0, 1, ..., k\}$ and for all positive integers a, b with $b \geqslant q^\lambda s$, and we prove that

$$A_{k+1}^{q^{k+1}l} = A_{k+1}^{q^{k+1}s} \text{ and } A_{k+1}^{aq^{k+1}(l-s)+b} = A_{k+1}^b,$$

with $a, b \in \mathbb{N}$ and $b \geqslant q^{k+1}s$. From (1), we have

$$A_{k+1}^{aq^{k+1}(l-s)+b} = \sum_{i=0}^{aq^{k+1}(l-s)+b-1} \sum_{j=0}^{k} A_{k-j}^i \; a_{j+1} \; a_0^{aq^{k+1}(l-s)+b-i-1}.$$

Divide the first sum on the right into three parts. Firstly, we note that, for each $\lambda \in \{0, 1, ..., k\}$ and $v \in \mathbb{N}^*$, we have

$$\sum_{i=0}^{q^k s-1} A_\lambda^i \; a_v \; a_0^{aq^{k+1}(l-s)+b-i-1} = \sum_{i=0}^{q^k s-1} A_\lambda^i \; a_v \; a_0^{b-i-1},$$

because of $b - i - 1 \geqslant s$. Secondly, we also have

$$\sum_{i=q^k s}^{aq^{k+1}l-q^k s(aq-1)-1} A_\lambda^i \; a_v \; a_0^{aq^{k+1}(l-s)+b-i-1} = q \sum_{i=q^k s}^{q^k l-1} A_\lambda^i \; a_v \; a_0^{aq^{k+1}(l-s)+b-i-1} = 0,$$

since it is easy to see, thanks to our hypothesis, that

$$\begin{aligned}
\sum_{i=q^k s}^{q^k l-1} A_\lambda^i \; a_v \; a_0^{aq^{k+1}(l-s)+b-i-1} &= \sum_{i=q^k l}^{2q^k l-q^k s-1} A_\lambda^i \; a_v \; a_0^{aq^{k+1}(l-s)+b-i-1} \\
&\vdots \\
&= \sum_{i=q^k l(aq-1)-q^k s(aq-2)}^{aq^{k+1}l-q^k s(aq-1)-1} A_\lambda^i \; a_v \; a_0^{aq^{k+1}(l-s)+b-i-1}.
\end{aligned}$$

Thirdly, we now show the following equality

$$\sum_{i=aq^{k+1}l-q^k s(aq-1)}^{aq^{k+1}(l-s)+b-1} A_\lambda^i \; a_v \; a_0^{aq^{k+1}(l-s)+b-i-1} = \sum_{i=q^k s}^{b-1} A_\lambda^i \; a_v \; a_0^{b-i-1}.$$

For that, we use the change of variable $u = i - aq^{k+1}(l - s)$, then

$$\sum_{i=aq^{k+1}l-q^k s(aq-1)}^{aq^{k+1}(l-s)+b-1} A_\lambda^i \; a_v \; a_0^{aq^{k+1}(l-s)+b-i-1} = \sum_{u=q^k s}^{b-1} A_\lambda^{aq^{k+1}(l-s)+u} \; a_v \; a_0^{b-u-1},$$

and, since $u \geqslant q^k s$, then, by hypothesis

$$\sum_{u=q^k s}^{b-1} A_\lambda^{aq^{k+1}(l-s)+u} \; a_v \; a_0^{b-u-1} = \sum_{u=q^k s}^{b-1} A_\lambda^u \; a_v \; a_0^{b-u-1}.$$

Using the values of these three parts, we finally conclude that for all $\lambda \in \{0, 1, ..., k\}$ and for all integers a, b, v such that $v > 0$ and $b \geqslant q^{k+1}s$, we have

$$\sum_{i=0}^{aq^{k+1}(l-s)+b-1} A_\lambda^i \; a_v \; a_0^{aq^{k+1}(l-s)+b-i-1} = \sum_{i=0}^{b-1}\sum_{j=0}^{k} A_\lambda^i \; a_v \; a_0^{b-i-1}.$$

Therefore,

$$A_{k+1}^{aq^{k+1}(l-s)+b} = A_k^b.$$

□

The following lemma is well-known, but we give a short proof for the sake of completeness.

Lemma 11. *A finite direct product of periodic rings is periodic.*

Proof. Let $n \in \mathbb{N}^*$ and $R = \prod_{i=1}^{n} R_i$, where, for every $1 \leq i \leq n$, R_i is a periodic ring. Let $r = (r_1, r_2, ..., r_n) \in R$ with $r_i \in R_i$. For every $i \in \{1, 2, ..., n\}$, there exist $s_i < l_i \in \mathbb{N}$ such that $r_i^{l_i} = r_i^{s_i}$. Thanks to Part 1 of Lemma 9, $r_i^{k(l_i - s_i)+j} = r_i^j$ for any positive integer k and any $j \geqslant s_i$. So, if we choose $s = max\{s_i : i \in \{1, 2, ..., n\}\}$ and $l = \prod_{i=1}^{n}(l_i - s_i) + s$, then $l > s$ and $r^l = r^s$. □

3.3 Periodic matrix rings

Let $T(R, S, M)$ denote the generalized (or formal) triangular matrix ring, that is, a ring of the form $\begin{pmatrix} R & M \\ 0 & S \end{pmatrix}$ under the usual matrix operations, where R, S are rings and M is an (R, S)-bimodule.

Theorem 10. *Let $T(R, S, M)$ be the generalized triangular matrix ring. Then R and S are periodic if and only if $T(R, S, M)$ is periodic.*

Proof. Let R and S be periodic rings. We can consider $T = T(R, S, M)$ as a graded ring with $T = T_0 \bigoplus T_1$, where $T_0 = \begin{pmatrix} R & 0 \\ 0 & S \end{pmatrix}$ and $T_1 = \begin{pmatrix} 0 & M \\ 0 & 0 \end{pmatrix}$. Therefore, from Lemma 11, T_0 is periodic and then, by Corollary 3, T is periodic. The converse is obvious.

□

By an easy induction, this theorem can be extended to the more general situation of generalized triangular matrix rings. Such rings are denoted $T(R_i, M_{ij} \mid 1 \leq i < j \leq n)$, where R_i and $M_{i,j}$ are respectively periodic rings and (R_i, R_j)-bimodules equipped with maps guaranteeing that the multiplication of the matrices is well defined and satisfies the usual associativity property. If $n = 3$, this gives that the triangular matrix ring $S = \begin{pmatrix} R_1 & M_{12} & M_{13} \\ 0 & R_2 & M_{23} \\ 0 & 0 & R_3 \end{pmatrix}$ is periodic, because $S = \begin{pmatrix} A & M \\ 0 & R_3 \end{pmatrix}$, with $A = \begin{pmatrix} R_1 & M_{12} \\ 0 & R_2 \end{pmatrix}$ and $M = \begin{pmatrix} M_{13} \\ M_{23} \end{pmatrix}$, where R_1, R_2, R_3 are periodic rings, and M_{12}, M_{23}, M_{13} are respectively (R_1, R_2)-,(R_2, R_3)-,(R_1, R_3)-bimodules equipped with a map $\psi : M_{1,2} \times M_{2,3} \longrightarrow M_{1,3}$.

Of course, the usual upper triangular matrix over a ring R can be seen in this perspective and we get the point one of the following corollary. The second point of this result is an easy consequence of Part 2 of Proposition 14.

Corollary 4. *Let R be a periodic ring.*

1. *The ring of all upper triangular matrices $T_n(R)$ is periodic.*

2. *Let $M \in T_n(R)$. Then there exist integers l, s in $\mathbb{N}$ and $l > s$ such that $diag(M)^l = diag(M)^s$ and $(M)^{q^n l} = (M)^{q^n s}$, where $q \in \mathbb{N}^*$ is such that $qR = 0$.*

Examples 4. *let R be a periodic ring and $2R = 0$, and let $M = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ 0 & a_{22} & a_{23} \\ 0 & 0 & a_{33} \end{pmatrix}$ where $(a_{11}, a_{22}, a_{33})^2 = (a_{11}, a_{22}, a_{33})$, then $M^{16} = M^8$.*

We need the following theorem " the classical commutativity theorem ", due to Jacobson (cf. [12], Theorem 3.1.2).

Theorem 11 (Jacobson)**.** *Let R be a ring in which for every $a \in R$ there exists an integer $n(a) > 1$, depending on a, such that $a^{n(a)} = a$, then R is commutative.*

Remarks 4. 1. *Part 1 of Corollary 4 was proved in [8] with different techniques.*

2. *We can now answer the following two questions, which were raised in [10].*

   - *If R is a ring such that the equality $x^m = x$ holds for all $x \in R$ and a fixed $m \in \mathbb{N}^*$, when is the ring $M_n(R)$ periodic?*

- *If R is a ring with nil Jacobson radical and such that $R/J(R)$ is a finite direct product of periodic rings, is R periodic?*

Since a ring R such that for any $x \in R$, there exists $n \in \mathbb{N}$, with $x^n = x$ is commutative and hence P.I., the first question is an obvious consequence of Theorem 14 below. The answer to the second question is also positive. This is a direct consequence of Lemma 11 and Proposition 12.

In Section 3, we will use the assumption that for some ring R, the ring $M_n(R)$ is periodic. We will now mention some cases where this assumption is satisfied.

Lemma 12. *If a ring R is locally finite, then, for any $n \geq 1$, $M_n(R)$ is periodic.*

Proof. For any matrix $A \in M_n(R)$ and for any $l \in \mathbb{N}$, we have $A^l \in M_n(S)$, where S is the ring generated by the entries of A. Our hypothesis implies that S is a finite ring and hence so is $M_n(S)$. This gives the result. □

Proposition 15. *Let D be a division ring that is periodic. Then*

1. *D is a field.*

2. *D is locally finite.*

3. *For any $n \geq 1$, $M_n(D)$ is periodic.*

Proof. (1) Since D is periodic and any nonzero $d \in D$ is invertible, we get that for any $d \in D$, there exists $0 \neq n_d \in \mathbb{N}$ such that $d^{n_d} = d$ and theorem 11, implies that D is commutative.

(2) This is clear since D is periodic commutative and there exists a positive integer q such that $qD = 0$.

(3) This is a direct consequence of Lemma 12. □

Proposition 16. *Let R be an Artinian periodic ring, then $M_n(R)$ is periodic for any $n \geq 1$.*

Proof. Since R is periodic, $J(R)$ is nil and hence nilpotent because R is also Artinian. This implies that $J(M_n(R)) = M_n(J(R))$ is also nilpotent. On the other hand, $M_n(R)/J(M_n(R))$ $= M_n(R/J)$ and R/J is artinian semisimple. Now, R/J is artinian semisimple and hence, by the Wedderburn-Artin theorem, $R/J \cong \prod_{i=1}^{s} M_{l_i}(D_i)$, where $D_1, \ldots, D_s$ are division rings. Since R/J is periodic, the division rings $D_1, \ldots, D_s$ are periodic and Proposition 15 implies that $M_n(R/J) \cong \prod_{i=1}^{s} M_{nl_i}(D_i)$ is periodic. The conclusion follows since, according to Proposition 12, a ring R is periodic if and only if R/J is periodic and J is nil. □

Theorem 12. *Let R be a left (right) Noetherian periodic ring. Then*

1. *The Jacobson radical $J(R)$ is nilpotent.*

2. *$R/J(R)$ is semisimple artinian.*

3. *For any $n \geq 1$, $M_n(R)$ is periodic.*

Proof. (1) Since R is periodic, Lemma 9 shows that $J(R)$ is nil, and the fact that R is left Noetherian implies that $J(R)$ is nilpotent.

(2) Let us first notice that the ring R is Noetherian, and hence doesn't contain an infinite set of orthogonal idempotents. We claim that primitive idempotents in R are in fact local idempotents. Theorem 1 in [22] will then show that R is semiperfect and hence $R/J(R)$ is semisimple artinian. So, let e be a primitive idempotent. We need to show that e is a local idempotent, i.e. that eRe is a local ring. Let $x \in eRe \setminus J(eRe)$. We have to prove that x is invertible in eRe. The left ideal $eRex$ of eRe cannot be nil since it is not contained in J, hence there exists $0 \neq b \in eRex$ that is not nilpotent. Since R is periodic, a power of b is a nonzero idempotent, say f, and we have $Rf \subseteq Rx \subseteq Re$. The fact that e is primitive leads to $Rf = Re = Rx$. Writing $e = rx$ for some $r \in R$, we get $(ere)x = erx = e$, showing that x is indeed invertible in eRe. By Mueller's result mentioned above, we get that R/J is semisimple artinian.

(3) By (1), we know that $J(R)$ is nilpotent and hence the same holds for $J(M_n(R))$. On the other hand, R/J is Artinian and hence Theorem 16 implies that $M_n(R/J) \cong \frac{M_n(R)}{J(M_n(R))}$ is periodic. Proposition 12 then implies that $M_n(R)$ is periodic. □

Theorem 13. *[13] Let R be a periodic $P.I.$ ring and let S be a finitely generated subring of R. Then S is a finite ring.*

Theorem 14. *Let R be a $P.I.$ ring and $n \in \mathbb{N}^*$. Then R is periodic if and only if the matrix ring $M_n(R)$ is periodic.*

Proof. If R is a periodic $P.I.$ ring, then Theorem 13 implies that R is locally finite, and the above Lemma 12 shows that $M_n(R)$ is periodic. Since R is a subring of $M_n(R)$, the converse statement is clear. □

Corollary 5. *Let R be a potent ring. Then, for any $n \geq 1$, the matrix ring $M_n(R)$ is periodic.*

Proof. The classical commutativity theorem implies that a potent ring is commutative. The corollary is then an obvious consequence of Theorem 14. □

Definition 21.

Let $e \in \mathbb{N}^*$. A ring R is called periodic of bounded index of periodicity e if for every $x \in R$, there exist $m, n \in \mathbb{N}$ such that $x^n = x^m$ with $m < n \leq e$. A ring R is called periodic of bounded index of nilpotence if R is periodic and there exists $n \in \mathbb{N}^*$ such that, for every $x \in N(R), x^n = 0$.

Lemma 13. *Any periodic ring of bounded index (of nilpotence or periodicity) satisfies a polynomial identity.*

Proof. Let $x \in R$. Since the ring is periodic, there exist $m, n \in \mathbb{N}$, such that $x^n = x^m$ with $n > m \in \mathbb{N}$. Therefore, $x^{k(n-m)+j} = x^j$ for each positive integer k and each $j \geqslant m$. Now, as R is of bounded index of periodicity e, then $n - m \in \{1, 2, ..., (e-1)\}$, so for all x in R, we have $x^{(e-1)!+e} = x^e$. This gives a $P.I.$ for R.

The case of bounded index of nilpotence is proved in Proposition 1 in [13]. □

Corollary 6. *Let R be a periodic ring. If R is of bounded index (of nilpotencity or periodicity), then $M_n(R)$ is a periodic ring.*

Some infinite matrix rings over a periodic ring can also give rise to periodic rings. Let us briefly mention two examples. Let R be a periodic ring such that, for any $n \geq 1$, $M_n(R)$ is also periodic. Consider the ring T of matrices with entries in R whose rows and columns are indexed by an infinite set J. Let S be the subring of T consisting of the matrices that are of the form $A + rI$, where A is an infinite matrix that has only a finite number of nonzero rows and rI is the diagonal matrix having the same element r all along the diagonal. It can be shown that this ring S is indeeed periodic. The ring S contains the ring T of matrices of the form $A + rI$, where A is a finite matrix.

In fact, in case J is the set of natural numbers, T can also be viewed as a direct limit of the set of finite matrix rings, and the fact that T is periodic can be deduced from the following proposition.

Proposition 17. *A direct limit of periodic rings is periodic.*

Proof. Let I be a direct set, and let $(R_i)_{i \in I}$ a family of periodic rings. Put $R = \varinjlim R_i$, and let $r \in R$. Then there exist $i \in I$, a ring homomorphism $\phi_i : R_i \longrightarrow R$, and an element $r_i \in R_i$ satisfying $\phi_i(r_i) = r$. Since the ring R_i is periodic, there exist positive integers $m < n$ such that $r_i^m = r_i^n$. Therefore, $r^m = \phi_i(r_i^m) = \phi_i(r_i^n) = r^n$. □

In 1930, G.Köthe raised the following question which is known as the Köthe conjecture: Does a ring R with nonzero one-sided nil ideal have a nonzero two-sided ideal ?. Despite the considerable efforts of many researchers, it still remains open. However, many equivalent properties have been found. Below we list some of them. The followings are equivalent. [see [18], p 171]

1. The Köthe conjecture. (the sum of two nil left ideals in any ring is nil)
2. In any ring, the sum of two one-sided nil ideals is nil.
3. For any ring R and for any nil ideal I of R, the matrix ideal $M_2(I)$ is a nil ideal of $M_2(R)$.
4. For any ring R and for any nil ideal I of R, the matrix ideal $M_n(I)$ is a nil ideal of $M_n(R)$ for every n.

Remark 4. *Since periodic rings have a nil Jacobson radical, the class of periodic rings satisfy the Köthe conjecture, i.e. if I and J are two right (left) nil ideals of a periodic ring, then the sum $I + J$ is also nil. The question whether the matrix rings $M_n(R)$ are periodic when R is periodic is strongly connected to the Köthe conjecture itself. We intend to come back to this problem in a future work.*

Chapter 4

Exponents of polynomials over $P.I.$ periodic rings

We begin this section with the following proposition, which shows that periodic rings may appear as homomorphic image of a skew polynomial ring.

Proposition 18. *Let R be a periodic ring with positive characteristic q, and let $n \in \mathbb{N}^*$. Then the ring $R[t;\sigma]/[t^n]$ is periodic.*

Proof. The polynomial ring $R[t;\sigma]$ is a $\mathbb{Z}$-graded ring with $R_i = Rt^i$ for $i \geqslant 0$, and $R_i = 0$ for $i < 0$. Let $f(t) \in R[t;\sigma]$. Since R is periodic, Theorem 9 shows that the coefficients of the same degree in the successive powers of f form a finite set. Then, in the quotient ring $R[t;\sigma]/(t^n)$, all the coefficients of all the powers of f form a finite set. This shows that $\{f^k + (t^n) : k \in \mathbb{N}\}$ must be finite and hence $f(t) + (t^n)$ is periodic.

□

Example 9. *Let R be a periodic ring of characteristic 2 and $\sigma \in End(R)$. Let $f(t) = at + b$ in $R[t;\sigma]/(t^2)$ with $b^3 = b$. Then we have $f(t)^2 = b^2 + (ba + a\sigma(b))t$ and $f(t)^3 = b + \alpha t$, where $\alpha = b^2a + ba\sigma(b) + a\sigma(b^2)$. Therefore, $f(t)^3 f(t)^3 = b^2 + (b\alpha + \alpha\sigma(b))t$ and $b\alpha + \alpha\sigma(b) = ba + a\sigma(b)$, hence $f(t)^6 = f(t)^2$.*

The notion of exponent is a classical one for polynomials with coefficients in a finite field. More general concepts have been introduced in [9]. The following definition recalls this notion in a general setting.

Definition 22. *Let f, g be two elements in a ring S. When it exists, the smallest nonzero integer $e \in \mathbb{N}$ such that $f^e - 1 \in Sg$ (resp. $f^e - 1 \in gS$) is called the right (resp. left) exponent of g relatively to f and denoted $e_r(g, f)$ (resp. $e_l(g, f)$). In the more classical case, when $f(t) = t$, the exponents of g with respect to the variable t will be denoted by $e_r(g)$ and $e_l(g)$.*

The notion of relative exponent appears naturally while working with polynomials of a general Ore extensions $S = R[t; \sigma, \delta]$. In this setting, it is not always possible to define an exponent of $g \in S$ with respect to t, but, under some circumstances (related to the non simplicity of S, for instance), we might find an invariant (semi invariant) polynomial $f \in S$ for which we have $fa = \sigma^n(a)f$, for $a \in R$ and $n = degf$. It is then often possible to compute the exponent of g with respect to f. We will be particularly concerned with exponents of polynomials $g \in R[t; \sigma, \delta]$ with respect to t when R is a periodic ring. Notice that the exponent may not exist (e.g. $e_r(0, f)$ exists only if f is root of unity) and some conditions will be imposed to obtain existence of the relative exponents. We first work in a general ring and then will concentrate on Ore extensions with periodic base rings.

Lemma 14. *Let f, g, f_1 be elements of a ring S such that g is neither a left nor a right zero divisor in S, $gf = f_1 g$, and $Sg + Sf = S$. Suppose that the endomorphism ring $End(S/Sg)$ is periodic, then*

1. *$End(S/gS)$ is also periodic.*

2. *$gS + f_1 S = S$.*

3. *There exists a positive integer e such that $f^e - 1 \in Sg$ and $f_1^e - 1 \in gS$.*

4. *If $fg \in gS$, there exists $e \in \mathbb{N}$ such that $f^e - 1 \in Sg \cap gS$.*

Proof. (1) The idealizer $Idl(Sg) = \{h \in S : gh \in Sg\}$ is a subring of S which is the maximal one in which Sg is a two-sided ideal. Moreover, the quotient $T = Idl(Sg)/Sg \cong End_S(S/Sg)$. Elements of $End_S(S/Sg)$ are right multiplication by elements from $Idl(Sg)$. If $c \in Idl(Sg)$, there exists $c_1 \in S$ with $gc = c_1 g$. But then $c_1 \in Idl(gS)$ and left multiplication by c_1 gives rise to an element of $End(S/gS)$. Since g is not a zero divisor, the element c_1 coresponding to c is unique and, writing the endomorphisms on the opposite side of the action of S, the map $\psi : End_S(S/Sg) \to End_S(S/gS)$ sending the right multiplication by c to the left multiplication by c_1 is indeed a ring isomorphism. This allows us to conclude that $End_S(S/gS)$ is also periodic.

(2) The assumption that $Sg+Sf = S$ can be translated by saying that the right multiplication by f, denoted R_f, in $End_S(S/Sg)$ is onto. Since $End_S(S/Sg)$ is periodic and hence Dedekind

finite (cf. Proposition 13), R_f is in fact an isomorphism. Let us denote the left multiplication by f_1 as L_{f_1}. We have $\psi(R_f) = L_{f_1}$, where ψ is the ring isomorphism defined in (1) above. This implies that L_{f_1} is also an isomorphism and, in particular, it is onto. Hence, we get $gS + f_1S = S$.

(3) Since the ring $End_S(S/Sg)$ is periodic, hence Dedekind finite, we have seen in (2) above that $R_f \in End(S/Sg)$ is an isomorphism. Part 3 of Lemma 9 implies that $f^e - 1 \in Sg$. Similarly the element $L_{f_1} \in End_S(S/gS)$ is invertible and we get $f_1^e - 1 \in gS$.

(4) Let us suppose that $fg = gf_2$. The second equality of the above statement (3), with f_1 replaced by f, leads to $f^e - 1 \in gS$ and gives the conclusion. □

Let us now consider the existence of relative exponents in the case of skew polynomials.

Theorem 15. *Let R be a ring and $n \geq 1$ be such that $M_n(R)$ is a periodic ring, and let g be a monic polynomial in $S = R[t; \sigma, \delta]$ of degree n. Then*

1. *The ring $T = Idl(Sg)/Sg$ is periodic, where $Idl(Sg) = \{h \in S : gh \in Sg\}$.*
2. *If $f \in S$ is a monic polynomial such that $Sf + Sg = S$, and $gf \in Sg$, then there exists $e \in \mathbb{N}^*$ such that $f^e - 1 \in Sg$. In particular, $e_r(g, f)$ exists.*

Proof. (1) The set $Idl(Sg) = \{h \in S : gh \in Sg\}$ is the idealizer of Sg. Since any S-endomorphism of S/Sg is also an R-endomorphism, we have an embedding of $T = Idl(Sg)/Sg \cong End_S(S/Sg)$ in $End_R(S/Sg)$. The fact that g is monic implies that the module S/Sg is a free left R-module of dimension n. We thus have that $End_S(S/Sg)$ is embedded in $M_n(R)$ and our hypothesis implies that $T = Idl(Sg)/Sg$ is periodic.

(2) Since $T = Idl(Sg)/Sg$ is periodic, the above Lemma 14 yields the conclusion. □

Remarks 5. *1) Of course, a statement similar to that of Theorem 15 holds if, with the same notations, we have $gS + fS = S$ and $fg \in gS$.*

2) As an obvious consequence of Part 1 of Theorem 15, let us mention that if $g \in S$ is monic and such that $Sg = gS$, then S/Sg is periodic.

3) There is a more concrete point of view on the eigenring T in the proof above. As mentioned $T \cong End_S(S/Sg)$ and this ring is in fact isomorphic to the kernel of the additive map $T_C - L_C$ acting on $M_n(R)$, where $n = deg(g)$, C is the companion matrix of g, L_C is the left multiplication by C, and T_C is the (σ, δ) pseudo-linear transformation induced by C (i.e. $T_c(B) = \sigma(B)C + \delta(B)$ for any $B \in M_n(R)$).

The following corollary is an immediate consequence of Theorems 15 and 14.

Corollary 7. *Let R be a periodic $P.I.$ ring, and let $f, g \in S = R[t; \sigma, \delta]$ be monic polynomials such that $fS = Sf$. If $Sf + Sg = S$, then there exists a positive integer e such that $f^e - 1 \in Sg$.*

The next result is then obtained from the above corollary 7 and lemma 13..

Corollary 8. *Let R be a bounded periodic ring and $g \in R[t; \sigma]$ with invertible constant term. Then there exists a positive integer e such that $t^e - 1 \in R[t; \sigma]g$.*

We now give some properties of exponents.

Proposition 19. *Let f, f_1, f_2, g, h be elements in a ring R, and suppose that g is neither a right nor a left zero divisor.*

1. *Suppose $gf = f_1 g$. For any $e \geq 1$, we have $f^e - 1 = hg$ if and only if $f_1^e - 1 = gh$.*

2. *Suppose that $gf = f_1 g$ and $fg = gf_2$. For any $e \geq 1$, we have $f^e - 1 = hg$ if and only if $f^e - 1 = gh$.*

Proof. (1) Suppose we have $f^e - 1 = hg$. Left multiplying by g, we get $gf^e = g + ghg = (1 + gh)g$. Our hypothesis then gives $f_1^e g = (1 + gh)g$. This leads to the conclusion since g is not a right zero divisor. Retracing our steps, we get the proof of the converse statement.

(2) First, notice that we have $f_1 g^2 = gfg = g^2 f_2$. Now, suppose we have $f^e - 1 = hg$. By the preceding statement, we have $f_1^e - 1 = gh$ and hence $f_1^e g^2 - g^2 = ghg^2$. Using our hypotheses, we successively get $g^2 f_2^e - g^2 = ghg^2$ and hence $f^e g^2 - g^2 = ghg^2$. The fact that g is not a right zero divisor then gives $f^e - 1 = gh$. The converse implication is obtained similarly or just by symmetry. □

The next lemma lists some elementary properties of the relative exponents. The last statement of this lemma is a direct consequence of Proposition 19. The other statements come from [9].

Lemma 15. *Suppose that f, g, h are elements in a ring R such that $e_r(g, f)$ and $e_r(h, f)$ exist. Then :*

(1) g is a right factor of $f^l - 1$ if and only if $e_r(g, f)$ divides l;

(2) If g is a right factor of h, then $e_r(g, f)$ divides $e_r(h, f)$;

(3) If $Rg \cap Rh = Rm$, then $e_r(m, f)$ exists and it is equal to the least common multiple of $e_r(g, f)$ and $e_r(h, f)$;

(4) If g is such that $gR = Rg$, then $e_r(g,f) = e_l(g,f)$.

We will now look at the properties of exponents in the case of skew polynomial rings in the form $S = R[t;\sigma,\delta]$. Remark that the classical exponent for polynomials refers to the exponent of $g(t) \in \mathbb{F}_q[t]$ relative to the variable t. A bit more general is the case of exponents of polynomials $g(t) \in R[t;\sigma] = S$ with respect to t, where R is periodic. Remark that, in this case, $tS = St$. We will thus assume that our polynomial f is also such that $fS = Sf$. This assumption will also lead to left right symmetry, as we will show quite generally in the following proposition.

Proposition 20. *Let f,g,h be a monic polynomials in $S = R[t;\sigma,\delta]$, and suppose that $Sf = fS$. Then $hg = f^e - 1$ if and only if $gh = f^e - 1$. In particular, when they exist, we have:*

$$e_r(g,f) = e_l(g,f).$$

Proof. Let $g_1 \in S$ be such that $f^e g = g_1 f^e$ and notice that g_1 is then a monic polynomial with $deg(g_1) = deg(g)$. Multiplying $hg = f^e - 1$ on the left by g_1, we obtain $g_1 f^e - g_1 = g_1 hg$ and hence $(f^e - g_1 h)g = g_1$. Since g and g_1 are monic polynomials of the same degree, we get that $f^e - g_1 h = 1$, and also $g = g_1$. The other implication is obtained similarly and leads to the desired conclusion. □

Corollary 9. *Let R be a ring, $R[t;\sigma]$ the skew polynomial ring over R with automorphism σ, and $g,h \in R[t;\sigma]$ be such that h is monic. Then $hg = t^e - 1$ for a positive integer e if and only if $gh = t^e - 1$. In particular, if the exponent e of g exists, then $e = e_r(g) = e_l(g)$ and the coefficients of g are fixed by σ^e.*

Proof. The first part of the corollary follows directly from Proposition 20 with $f = t$. We extend σ to the Ore extension $S = R[t;\sigma]$ by defining $\sigma(t) = t$. Since e is the order of g, there exists $h \in S$ such that $gh = hg = t^e - 1$ and we get $gt^e - g = g(t^e - 1) = ghg = (t^e - 1)g = \sigma^e(g) - g$. This gives $gt^e = \sigma^e(g)t^e$ and hence $\sigma^e(g) = g$, as desired. □

When σ and δ commute, we can extend σ to the Ore extension $S = R[t;\sigma,\delta]$ itself by putting $\sigma(t) = t$ This can be easily checked. We continue to write σ for this extended map hence σ becomes an automorphism of S. With this in mind and statement (e) of Proposition 4, we have the following corollary .

Corollary 10. *Let R, σ, δ be a ring, an automorphism of R and a σ-derivation of R such that $\sigma\delta = \delta\sigma$. If $g(t)$ is a monic polynomial such that $e(g) = e(g,t)$ exists then $e(g) = e(\sigma(g))$.*

Definition 23. *Let $g(t) = \sum_{i=0}^{n} a_i t^i \in S = R[t;\sigma]$, with σ an automorphism of R. The reciprocal polynomial, denoted g^*, is defined by $g^* = \sum_{i=0}^{n} \sigma^i(a_{n-i})t^i$*

The notion of reciprocal polynomial is important in coding theory where the reciprocal of a check polynomial of a cyclic code is the generator polynomial of the dual code. Codes using polynomials over Ore extensions have been studied, e.g. in [3] and [4]. The reciprocal polynomial is known only in the case of Ore extension of automorphism type (i.e. $\delta = 0$). This was presented together with some of its properties in [3].

Proposition 21. *Let $g \in R[t;\sigma]$ and suppose that $e(g) = e(g,t)$ is the exponent of g, then :*

$$e(g) = e(g^*).$$

Proof. The proof is a direct consequence of the definition of the exponent and of the formulas $(fh)^* = \sigma^k(h^*)f^*$ and $(f^*)^* = \sigma^k(f)$, where $k = deg(f)$. □

Examples 5.

1. *Let $\mathbb{F}_{16} = \mathbb{F}_2(\alpha)$ be the finite field with $\alpha^4 = \alpha + 1$, and let σ be the Frobenius automorphism defined by $\sigma(a) = a^2$, $a \in \mathbb{F}_{16}$. The order of σ is 4. Consider the polynomials in $\mathbb{F}_{16}[t;\sigma]$ defined by $f(t) = t^3 + \alpha^5 t^2 + \alpha^5 t + \alpha^{10}$ and $g(t) = t^3 + \alpha^{10}t^2 + \alpha^5 t + \alpha^5$. Then we have $f(t)g(t) = g(t)f(t) = t^6 - 1$.*

   If f is not monic, the result is not true as the following example shows.

2. *Let $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$ with $\alpha^2 = \alpha + 1$ and let σ be the Frobenius automorphism defined by $\sigma(a) = a^2$, $a \in \mathbb{F}_4$. Now, consider the polynomials in $\mathbb{F}_4[t;\sigma]$ defined by $f(t) = \alpha t^3 + \alpha t + \alpha^2$ and $g(t) = \alpha t^4 + \alpha t^2 + \alpha t + \alpha$. Then we have $f(t)g(t) = t^7 - 1$, while $g(t)f(t) = \alpha^2 t^7 - 1$.*

Corollary 9 can be useful to factorize polynomials of the form $t^n - 1 \in R[t;\sigma]$. If we have $t^n - 1 = f_1...f_r$, with f_i monic for $1 \leq i \leq r$, then we obtain $r - 1$ other factorizations of $t^n - 1$ by cyclic permutation of the factors.

We now intend to relate the exponent of a monic polynomial $g(t) = \sum_{i=0}^{n} a_i t^i \in S = R[t;\sigma,\delta]$ with the order of its companion matrix $C = C_g \in GL_n(R)$, where

$$C_g = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \\ 0 & 0 & 0 & \cdots & 1 \\ -a_0 & -a_1 & -a_2 & \cdots & -a_{n-1} \end{pmatrix} \in M_n(R)$$

We have seen that the left S-module $V := S/Sg$ played an important role in the proof of Theorem 15. The (σ, δ)-PLT attached to this module (see Proposition 5) is given by the left multiplication by t. The matrix corresponding to this PLT in the basis $\{\overline{1}, \overline{t}, \dots, \overline{t^{n-1}}\}$ is just $C = C_g$. Since we are working with twisted polynomials, it is expected that the order of C_g is not the usual one. Using the definition (c) in 18, we now introduce the following notion.

Definition 24. *Let R, σ, δ be a ring, an automorphism and a σ-derivation, respectively. An element $a \in R$ is of finite (σ, δ)-order if there exists a positive integer l such that $N_l(a) = 1$. When it exists the smallest $l > 0$ such that $N_l(a) = 1$, is called the (σ, δ)- order of a and denoted $ord_{\sigma,\delta}(a) = l$.*

When $\delta = 0$, this notion was introduced in [9] and we refer the reader to this paper for more details and information about the σ-order and its elementary properties. In the next proposition we extend naturally both σ and δ to any matrix ring over R, and hence we have the notion of (σ, δ)-order for matrices over the ring R. Let us first establish the following easy lemma.

Lemma 16. *Let $f(t) = \sum_{i=0}^{l} a_i t^i, g(t) \in S = R[t; \sigma, \delta]$ be such that $g(t)$ is monic of degree n, and let us denote its companion matrix by $C_g \in M_n(R)$. Then*

1. *The left multiplication by t on S/Sg is a (σ, δ) pseudo-linear transformation. Its associated matrix in the basis $(\overline{1}, \overline{t}, ..., \overline{t^{n-1}})$ is C_g.*

2. *The matrix in the basis $(\overline{1}, \overline{t}, ..., \overline{t^{n-1}})$ corresponding to the left multiplication by $f(t)$ is given by $\sum_{i=0}^{l} a_i N_i(C_g)$.*

3. *If the row $\underline{v} \in R^n$ represents the coordinates of $\overline{h(t)} \in S/Sg$, then the coordinates of $\overline{f(t)h(t)}$ in this basis are given by*
$$\sum_{i=0}^{l} \sum_{k=0}^{i} a_i f_k^i(\underline{v}) N_k(C_g),$$
where the map f_k^i is the sum of all the words in σ and δ with k letters σ and $i - k$ letters δ.

4. *The polynomial $f(t)$ is right divisible by $g(t)$ if and only if $\sum_{i=0}^{l} a_i (1, 0 \dots, 0) N_i(C_g) = (0, \dots, 0)$.*

Proof. (1) This is clear.

(2) This is exactly the content of Lemma 3.

(3) It is enough to show that the matrix of left multiplication by t^k is given by $N_k(C_g)$. We prove this by an easy induction: so, let $\underline{v}$ be a column in R^n. We have $t^{k+1}.\underline{v} = t.t^k.\underline{v}$ $= t.(N_k(C_g)\underline{v}) = \sigma(N_k(C_g))t.\underline{v} + \delta(N_k(C_g))\underline{v} = \sigma(N_k(C_g))C_g\underline{v} + \delta(N_k(C_g))\underline{v} = N_{k+1}(C_g)\underline{v}$.

(4) Remark first that $f_i^k((1,0,\ldots,0)) = (0,\ldots,0)$, if $i < k$, and $f_k^k((1,0,\ldots,0)) = \sigma^k((1,0,\ldots,0))$ $= (1,0,\ldots,0)$. Using this, the fact that $f(t) \in Sg$ if and only if $f(t).\overline{1} = \overline{0}$ easily implies that

$$\sum_{i=0}^{l} a_i(1,0,\ldots,0)N_i(C_g) = \overline{0}.$$

□

Theorem 16. *Let R, σ, δ be a ring, an automorphism and a σ-derivation of R, respectively. Denote by S and A the Ore extensions $S = R[t;\sigma,\delta]$ and $A = M_n(R)[t;\sigma,\delta]$. We suppose that $g \in S$ is a monic polynomial of degree n which is such that $ord_{\sigma,\delta}(C_g) = l$. Then*

1. $e_r\left(t - C_g\right) = ord_{\sigma,\delta}\left(C_g\right).$
2. $e_r\left(g\right) = ord_{\sigma,\delta}\left(C_g\right).$

Proof. (1) We have :

$$\begin{aligned} l &= ord_{\sigma,\delta}(C_g) \\ &= min\{r \in \mathbb{N}^* : N_r(C_g) = I_n\} \\ &= min\{r \in \mathbb{N}^* : t^r - I_n \in A(t - C_g)\} \\ &= e_r\left(t - C_g\right) \end{aligned}$$

(2) Let us denote $\beta = \{\overline{1}, \overline{t}, \ldots, \overline{t^n}\}$ the basis of S/Sg over R. The matrix of $(T_{C_g})^l$ relative to this basis is $N_l(C_g) = I_n$. We thus have, in particular, $(t.)^l.\overline{1} = \overline{1}$, i.e. $t^l - 1 \in Sg$. We conclude that $e_r(g(t))$ divides $l = ord_{\sigma,\delta}\left(C_g\right)$.

Conversely, if $g(t)$ divides $t^r - 1$ in $S \subset A = M_n(R)[t;\sigma,\delta]$, for $\underline{v} = (I_n, 0, 0, \ldots, 0) \in (M_n(R))^n$, the statement (4) in Lemma 16 $\tilde{}$leads to $T_g^r(\underline{v}) = \underline{v}N_r(C_g)$. This quickly leads to $N_r(C_g) = I_n$ $\in M_n(R)$, and hence we have $l = ord_{\sigma,\delta}(C_g) < r$. This yields the conclusion.

□

If we use the notation introduced earlier for the evaluation of a skew polynomial, we can write $\sum_{i=0}^{l} a_i N_i(C_g) = f(C_g)$. With this in mind, we have the following corollary.

Corollary 11. *Let $R, \sigma, \delta, f(t), g(t)$ be a ring, an automorphism of R, a σ-derivation of R, and monic polynomials in $S = R[t;\sigma,\delta]$, respectively. Then, denoting $C_g \in M_n(R)$ the companion matrix of $g(t)$, we have $f(t)^r - 1 \in Sg(t)$ if and only if $(1,0,\ldots,0)f^r(C_g) = (1,0,\ldots,0)$.*

In particular,

$$t^r - 1 \in Sg(t) \Longleftrightarrow N_r(C_g) = I_n.$$

Furthermore, when they exist, the exponent of $g(t)$ (with respet to t) and the (σ,δ)-order of C_g are equal.

The above corollary shows the importance of knowing when the companion matrix C_g of the polynomial g is of finite (σ,δ)-order. In full generality, it is a very challenging question but, if $\delta = 0$, the situation is much more tractable.

Theorem 17. *Let R be a periodic P.I. ring, and $\sigma \in Aut(R)$ be such that $\sigma^l = id_R$ for some $l \in \mathbb{N}^*$. Let $g(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_0 \in R[t,\sigma]$ be a monic polynomial with $a_0 \in U(R)$, and denote C_g the companion matrix of $g(t)$. Then C_g is of finite σ-order and $e_r(g) = ord_\sigma(C_g)$.*

Proof. The equality between the σ-order of C_g and the exponent comes directly from the above theorem 16. We only have to show that C_g is indeed of finite σ-order. Now, from Theorem 14, the ring $M_n(R)$ is periodic, so a nonzero divisor matrix must be invertible. If we suppose that C_g is a zero-divisor, then there exists $0 \neq M \in M_n(R)$ such that $MC_g = 0$. But the fact that $a_0 \in U(R)$ implies that $M = 0$, a contradiction. Hence C_g is invertible. This leads to $\sigma^k(C_g)$ is invertible, for all $k \in \mathbb{N}$. Notice also that $N_k(C_g) \in M_n(S)$, where S is the subring of R generated by $\{\sigma^k(a_i) : \ 0 \leq k < l, \ 0 \leq i < n\}$. Theorem 13 implies that $M_n(S)$ is finite. By Statement c of Proposition 2.1 in [9], C_g is of finite σ-order. □

Remark 5. *One of the problems that arises when trying to extend the above Theorem 17 to the case when $\delta \neq 0$, is that, in this case, even if C_g is invertible, $N_i(C_g)$ need not be invertible.*

Examples 6.

1. *Let R be a ring of characteristic 2, $\sigma = Id$, and let $f(t) = t^2 + at + 1 \in R[t;\sigma]$, with $a^4 = a^2$. The companion matrix of $f(t)$ is $C_f = \begin{pmatrix} 0 & 1 \\ 1 & a \end{pmatrix}$. By computing the powers of C_f, we obtain $N_{12}(C_f) = C_f^{12} = I_2$. We can verify that*

$$t^{12}+1 = \left(t^2 + at + 1\right)\left(t^{10}+at^9+(a^2+1)t^8+a^3t^7+t^6+(a^3+a)t^5+t^4+a^3t^3+(a^2+1)t^2+at+1\right).$$

2. *Consider the Galois ring $R = \mathbb{Z}/4\mathbb{Z}\left[\xi\right] = \left\{a + b\xi : a, b \in \mathbb{Z}/4\mathbb{Z}, \xi^2 + \xi + 1 = 0\right\}$. Let σ be an automorphism of R defined by $\sigma\left(a + b\xi\right) = a + b\xi^2$, for all $a, b \in \mathbb{Z}/4\mathbb{Z}$. The exponent of $f\left(t\right) = t^2 + t + \xi \in R\left[t;\sigma\right]$ is 8, and we have*

$$t^8 - 1 = \left(t^2 + t + \xi\right)\left(t^6 + 3t^5 + (3\xi + 1)t^4 + 2t^3 + (2\xi + 1)t^2 + t + \xi + 1\right).$$

Example 10. *If $t^6 - 1 \in \mathbb{F}_{16}[t;\sigma]$ is as described in Example 5(1) above, we have*

$$t^6 - 1 = (t^2 + \alpha^{10})(t^2 + \alpha^5)(t + \alpha^5)(t + \alpha^{10}).$$

By shifting the polynomials, we obtain

$$\begin{aligned} t^6 - 1 &= (t^2 + \alpha^5)(t + \alpha^5)(t + \alpha^{10})(t^2 + \alpha^{10}) \\ &= (t + \alpha^5)(t + \alpha^{10})(t^2 + \alpha^{10})(t^2 + \alpha^5) \\ &= (t + \alpha^{10})(t^2 + \alpha^{10})(t^2 + \alpha^5)(t + \alpha^5). \end{aligned}$$

Conclusion and Perspectives

We have shown how the notion of exponents could be generalized from their natural initial setting (i.e., polynomials with coefficients in a finite field) to polynomials of the ring $R = A[t; \sigma, \delta]$ where A is a periodic ring $\sigma \in Aut(A)$ and δ is a σ-derivation. So in this definition we not only pass from a finite field to a periodic ring, but as well twist the variables. This required the use of relative exponents which was already introduced in a more restricted case in a paper by A. Cherchem and A. Leroy. We have also shown how the classical results related to the exponents can be extended to our settings. For getting these, we needed to use the notion of evaluation of the skew polynomials and to replace the usual power of an element by the "generalized" power $N_r(a)$. The use of pseudo-linear maps was very helpful in all the computations, either explicitly or in a more disguised way.

This thesis also leads to a few questions and opens new perspective and area for future research. Let us mention briefly a few of these:

-The exponents is used in different area, in particular for periodic sequences. Classical periodic sequences are very often defined on finite fields and their minimal period is related to the period of their attached polynomial (which gives the recurring formula) . It is thus quite natural to introduce the skew periodic sequences and hope to get similar behaviour as the one for "classical" periodic sequences. Some preliminary work has already been done in this area, in particular A. Cherchem and A. Leroy are currently working on this project.

-In the recent years, there has been many works on multivariate Ore extensions. This seems to be a very wide area where skew evaluations similar as the one that appears in this thesis already exists. It is for sure possible to develop the theory of pseudo-linear maps in this settings and it could be interesting to study these and insider for instance the notion of algebraicity of a PLT, eigenvalues,...in the setting of multivariate polynomials.

-In the case when $R = A[t; \sigma, \delta]$ where A is a division ring, it is well known that looking at the (skew) roots in a specific skew conjugacy class leads to the notion of exponential sums and gives a generalization and more precise form of the Gordon-Motzkin theorem (this says that the number of classical conjugacy classes containing roots of a polynomial is bounded by the degree of this polynomial). Using pseudo linear transformations as introduced in the thesis, it is a challenging question to determine some classes of noncommutative rings where this generalization is valid.

-Other kind of extensions Iterated Ore, quantum planes...could also be explored using the tools developed in the thesis

-In the thesis a σ-order is defined for elements of a finite group where σ is an automorphism of the group. It is natural to wonder what could be developed with these notions.

-Skew polynomial rings of automorphism types (more precisely of the form $\mathbb{F}_q[t;\sigma,\delta]$) have been used to create codes with prescribed distance. It could be an interesting topic to consider the more general kind of skew polynomial rings over finite rings and periodic rings.

-Classically the period of a polynomial $p(x) \in \mathbb{F}_q[x]$ of degree k is a factor of $q^k - 1$. Is it possible to get the same kind of result in our general setting assuming for instance that the periods of the elements of the base ring are bounded?

-A very important question we will try to work on in the future, which is strongly connected to the Köthe conjecture : if the Köthe conjecture holds, then the matrix rings $M_n(R)$ are periodic if and only if R is periodic.

Bibliography

[1] Ara, P. (1996). *Strongly π-regular rings have stable range one*. Proceedings of the American Mathematical Society, 124(11), 3293-3298.

[2] Bell, H. (1977). *A commutativity study for periodic rings,* Pacific Journal of Mathematics, 70(1), 29-36

[3] Boucher, D. Ulmer, F. *A Note on the Dual Codes of Module Skew Codes,* IMACC 2011. Lecture Notes in Comput. Sci., vol 7089. pp 230-243.

[4] Boulagouaz, A. Leroy, A. *(σ, δ)-codes,* Adv. Math. Commun., 2013, 7(4): 463-474.

[5] Bouzidi, A. D. Cherchem, A. Leroy, A. *Exponents of skew polynomials over periodic rings*. Communications in Algebra, 2021, vol. 49, no 4, p. 1639-1655.

[6] Chacron, M. *On a theorem of Herstein,* Canad. J. Math, Vol 21, (1969), 1348-1353

[7] Chacron, M. *On quasi periodic rings,* J. Algebra 12 (1969), 49–60

[8] Chen, H. Sheibani, M. *Periodicity and J-clean-like rings*, Math. Reports, 2016.

[9] Cherchem, A. Leroy, A. *Exponents of skew polynomials*, Finite Fields Appl, 37, (2016), 1-13.

[10] Cui, J. Danchev, P. *Some new characterizations of periodic rings,* J. Algebra Appl., 2019.

[11] Graham, R. L. Knuth, D. E. Patashnik, O. *Concrete mathematics,* a foundation for computer science. Computers in Physics, 3(5), 106-107, 1989.

[12] Herstein, I. N. *Noncommutative rings* Math. Assoc. Amer, 1968.

[13] Hirano, Y. *On periodic P.I. rings and locally finite rings,* Math. J. Okayama Univ. 33 , 115-120, 1991.

[14] Jacobson, N. *Pseudo-linear transformations*, Ann. of Math. **38** (1937), 484-507.

[15] Khazal, R. Breaz, S. Călugăreanu, G. *On torsion-free periodic rings,* Int. J. Math. Math. Sci., 2005.

[16] Lam, T. Y. Leroy, A. *Algebraic conjugacy classes and skew polynomial rings.* (English) Zbl 0694.16002 Perspectives in ring theory, Proc. NATO Adv. Res. Workshop, Antwerp/Belg. 1987, NATO ASI Ser., Ser. C 233, 153-203 (1988).

[17] Lam, T. Leung, K. H. Leroy, A. Matczuk, J. *Invariant and semi-invariant polynomials in skew Ore extensions.* Ring theory 1989. In honor of S. A. Amitsur, Proc. Symp. and Workshop, Jerusalem/Isr. 1988/89, Isr. Math. Conf. Proc. 1, 247-291 (1989)

[18] Lam, T. Y. *A First Course in Noncommutative Rings,* Grad. Texts in Math 131, 2001.

[19] Leroy, A. *Noncommutative polynomial maps*, J. Algebra Appl, Vol. 11, No. 04, (2012), 1793-6829.

[20] Leroy, A. *Pseudo linear transformations and evaluation in Ore extensions*, Bull. Belg. Math. Soc. 2 (1995), 321–347.

[21] Lidl, R. Niederreiter, H. *Introduction to finite fields and their applications*, Cambridge University Press, 1994.

[22] Mueller, B. J. *On semi-perfect rings*, Illinois J. Math. 14(3) (1970), 464–467.

[23] McConnell, J. C. Robson, J. C. Small, L. W. *Noncommutative Noetherian rings,* American Mathematical Soc., 2001.

[24] Ore, O. *Theory of non-commutative polynomials,* Ann. of Math. 34, 1933.

[25] Valdebenito, A. E. A. Andrea, A. l. *On the dual codes of skew constacyclic codes,* Advances in Mathematics of Communications, 12(4), 659, (2018).

[26] Wan, Z. X. *Lectures on Finite Fields and Galois Rings,* 2003.

[27] Zhang, X. Hu, L. *Periods of polynomials over a Galois ring*, Sci. China Math. 56, 1761–1772 (2013).