EXPONENTS OF SKEW POLYNOMIALS OVER PERIODIC RINGS

A. DJAMEL BOUZIDI, AHMED CHERCHEM, AND ANDRÉ LEROY

Abstract. We investigate properties of periodic rings R in view of studying general skew polynomials $f(t) \in R[t;\sigma,\delta]$. We introduce exponents for these polynomials and give some properties of this notion. We show, in particular, that this notion is right-left symmetric. Using the skew evaluation, we generalize the classical connection between the exponent of a polynomial and the order of its companion matrix.

1. Introduction and preliminaries

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 fields. 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 [15] 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 [7]. In the present paper, 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 hold 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 paper 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.

Let us mention some definition that we will use freely in the text.

A ring is called strongly clean if every element is the sum of a unit and an idempotent which commute. A ring R is called strongly π-regular if for every a in R, there exist a positive integer $n(a)$ and an element b in R satisfying $a^{n(a)} = a^{n(a)+1}b$. An element r of a ring R is periodic if there exist different positive integers m, n such that $r^m = r^n$. A ring

R is periodic if its elements are periodic. Since these rings are crucial for our purpose, we refer the reader to [2], [12], and [5] for more information about them. We mention that R is periodic if and only if for each $r \in R$, $r = p + n$ where p is potent (i.e. there exists $l > 1$ such that $p^l = p$), n is nilpotent and $rp = pr$. Obviously a periodic ring is strongly π-regular. We will say that R is Dedekind finite if for any $a, b \in R$, $ab = 1$ implies $ba = 1$. A ring R is 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 $n, m \in \mathbb{Z}$. Let $U(R)$, $N(R)$ and $J(R)$ denote the set of all units, the set of all nilpotent elements and the Jacobson radical of R, respectively. A ring is $P.I.$ if it satisfies a polynomial identity. A ring R is locally finite if any finitely generated subring of R is finite. Unless mentioned otherwise, all our rings will have an identity. The set of ring endomorphisms of a ring R is denoted $End(R)$. In Section 3, we used the computer software SageMath for preparing some examples.

We now present some tools related to Ore extensions and pseudo-linear maps. 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 $a, b \in R$, $\delta(ab) = \sigma(a)\delta(b) + \delta(a)b$. 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

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

In this setting, let us remind a few technical matters.

Definitions 1.1. 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) An additive map $T : V \longrightarrow V$ such that, for $\alpha \in R$ and $v \in V$,

$$T(\alpha v) = \sigma(\alpha)T(v) + \delta(\alpha)v$$

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

b) For $f(t) \in S = R[t; \sigma, \delta]$ and $a \in R$, we define $f(a)$, the right evaluation of $f(t)$ at $a \in R$, to be the only element in R such that $f(t) - f(a) \in S(t - a)$.

c) For $a \in R$, we define $N_i(a)$, 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 case V is a finite dimensional vector space and σ is an automorphism, the pseudo-linear transformations were introduced by Jacobson in [11]. They appear naturally in the context of modules over an Ore extension $S = R[t; \sigma, \delta]$. This is explained in [13].

If V is a finitely generated free left R-module, $\underline{e} = \{e_1, \dots, e_n\}$ 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 1.2. *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 1.3. (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.[13], [14]), 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 1.2) 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 $(\overline{1}, \overline{t}, \dots, \overline{t^{n-1}})$ 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. [13]).

We will need the following lemma that can be found in [14], Lemma 3.3 (b).

Lemma 1.4. *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.

2. Periodic graded rings and *P.I.* 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 2.1. *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 $R_1 \times \dots \times R_s$, where, for $1 \le i \le s$, $R_i = \frac{q}{p_i^{n_i}} R$.*

Remark 2.2. We mention that, if R is periodic and $R = R_1 \times \dots \times R_s$ is the decomposition from Lemma 2.1, then the rings R_i, $1 \le i \le s$, are stable under the action of σ and δ. This leads to the decomposition $S = R[t;\sigma,\delta] = R_1[t_1;\sigma_1,\delta_1] \times \dots \times R_s[t_s;\sigma_s,\delta_s]$ with the obvious notations.

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

Lemma 2.3. (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) This is clear.

(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) This is left to the reader. □

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

Proposition 2.4. *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 from the introduction, 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 2.5. *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) This is clear.

(3) According to a theorem 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 2.3 (3), we know that there exists $n \in \mathbb{N}$ such that $f = a^n$ is an idempotent. The reader can check that $(a-(1-f))(a^{n-1}f-(1+a+\cdots+a^{n-1})(1-f)) = 1$. This yields the thesis $\square$

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

Lemma 2.6. *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 $\{a^ib^j : i, j \in \mathbb{N}\}$ is finite. So, for any $i \in \mathbb{N}$, $(a + b)^i$ is a sum of words αa^ib^j, where i and j are both bounded (since a and b are periodic), and $\alpha \in \{0, 1, 2, \ldots q - 1\}$ (since $qR = 0$, where q denotes the finite characteristic of R) . This yields that P is finite, as desired. $\square$

Remark 2.7. Let us remark that a similar proof as in 2.6 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 2.8. *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 2.1 and 2.3 and Proposition 2.5, 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), and 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 2.6 above shows that a is then periodic, as required. □

Theorem 2.9. *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 2.1 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 2.10. *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 2.3. □

We saw in Theorem 2.9 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 2.9.

Proposition 2.11. *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 $0 \leq k \leq m$ 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

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

187 as desired.

(2) We have $A_0^l=A_0^s$, and from Part 1 of Lemma 2.3, $A_0^{a(l-s)+b}=A_0^b$ 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 2.12. *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 2.3, $r_i^{k(l_i - s_i)+j} = r_i^j$ 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 $r^l = r^s$. $\square$

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 2.13. *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 2.12, T_0 is periodic and then, by Corollary 2.10, T is periodic. The converse is obvious. $\square$

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 2.11.

Corollary 2.14. *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 $qR = 0$.*

Remarks 2.15. (1) Part 2 of Corollary 2.14 was proved in [6] with different techniques.

(2) We can now answer the following two questions, which were raised in [8].

- 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 2.21 below . The answer to the second question is also positive. This is a direct consequence of Lemma 2.12 and Proposition 2.4.

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 2.16. *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 2.17. *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 a classical result, due to Jacobson (cf. [9]), 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 2.16. □

Proposition 2.18. *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 2.17 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 2.4, a ring R is periodic if and only if R/J is periodic and J is nil. □

Theorem 2.19. *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 2.3 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 [16] 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 2.18 implies that $M_n(R/J) \cong \frac{M_n(R)}{J(M_n(R))}$ is periodic. Proposition 2.4 then implies that $M_n(R)$ is periodic. □

Theorem 2.20. [10] *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 2.21. *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 2.20 implies that R is locally finite, and the above Lemma 2.16 shows that $M_n(R)$ is periodic. Since R is a subring of $M_n(R)$, the converse statement is clear. □

Corollary 2.22. *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 2.21. □

Definition 2.23.
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 2.24. *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 [10]. □

Corollary 2.25. *Let R be a periodic ring. If R is of bounded index (of nilpotence 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. We leave the proof of it to the reader.

Proposition 2.26. *A direct limit of periodic rings is periodic.*

Remark 2.27. 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.

3. 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 3.1. *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 2.9 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 3.2. 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 $\alpha = b^2 a + ba\sigma(b) + a\sigma(b^2)$. 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 [7]. The following definition recalls this notion in a general setting.

Definition 3.3. 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 $n = deg f$. 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 3.4. *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 corresponding to c is unique and, writing the endomorphisms on the opposite side of the action of S, we leave it to the reader to check that 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 2.5), 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 $gS + f_1 S = S$.

(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 2.3 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 3.5. *Let R be a ring and $n \geq 1$ be such that $M_n(R)$ is a periodic ring, and let $g \in S = R[t; \sigma, \delta]$ be a monic polynomial 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 3.4 yields the conclusion. □

Remarks 3.6. 1) Of course, a statement similar to that of Theorem 3.5 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 3.5, 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 3.5 and 2.21.

Corollary 3.7. *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 3.7 and lemma 2.24.

Corollary 3.8. *Let R be a periodic ring of bounded index of periodicity 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 3.9. *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. $\square$

The next lemma lists some elementary properties of the relative exponents. The last statement of this lemma is a direct consequence of Proposition 3.9. The other statements come from [7].

Lemma 3.10. *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 $S = R[t;\sigma,\delta]$. 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 3.11. *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 3.12. *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 3.11 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, the reader can easily check the following corollary.

Corollary 3.13. *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 3.14. 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 3.15. *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 $k = deg(f)$. $\square$

Examples 3.16. (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 3.12 can be useful to factorize polynomials of the form $t^n - 1 \in R[t;\sigma]$. If $t^n - 1 = f_1 ... f_r$, with f_i monic for $1 \le i \le r$, 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 3.5. The (σ,δ)-PLT attached to this module (see Proposition 1.2) 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 1.1, we now introduce the following notion.

Definition 3.17. 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 [7] 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 3.18. *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 $\sum_{i=0}^{l} a_i(1,0\ldots,0)N_i(C_g) = (0,\ldots,0)$.*

Proof. (1) This is clear.
(2) This is exactly the content of Lemma 1.4.
(3) This is left to the reader.
(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 3.19. *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) $e_r(t - C_g) = ord_{\sigma,\delta}(C_g)$.
(2) $e_r(g) = ord_{\sigma,\delta}(C_g)$.

Proof. (1) We have $l = ord_{\sigma,\delta}(C_g) = min\{r \in \mathbb{N}^* : N_r(C_g) = I_n\} = min\{r \in \mathbb{N}^* : t^r - I_n \in A(t - C_g)\} = e_r(t - C_g)$.
(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 $l = ord_{\sigma,\delta}(C_g)$.

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 3.18 leads to $\widetilde{T_g^r}(\underline{v}) = \underline{v}N_r(C_g)$. 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 3.20. *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,

$$t^r - 1 \in Sg(t) \quad \text{if and only if} \quad N_r(C_g) = I_n.$$

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 3.21. *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 3.19. We only have to show that C_g is indeed of finite σ-order. Now, from Theorem 2.21, 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 2.20 implies that $M_n(S)$ is finite. By Statement c of Proposition 2.1 in [7], C_g is of finite σ-order. □

Remark 3.22. One of the problems that arises when trying to extend the above Theorem 3.21 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 3.23. (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

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

(2) Consider the Galois ring $R = \mathbb{Z}/4\mathbb{Z}\,[\xi] = \{a + b\xi : a, b \in \mathbb{Z}/4\mathbb{Z}, \xi^2 + \xi + 1 = 0\}$. Let $\sigma \in Aut(R)$ defined by $\sigma\,(a + b\xi) = a + b\xi^2$, for all $a, b \in \mathbb{Z}/4\mathbb{Z}$. The exponent of $f\,(t) = t^2 + t + \xi \in R\,[t;\sigma]$ 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 3.24. If $t^6-1 \in \mathbb{F}_{16}[t;\sigma]$ is as described in Example 3.16(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

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

Acknowledgments

This work was done while the first author visited the University of Artois during a Ph.D. stage. He would like to thank the members of the mathematical department of this institution for their warm welcome. The three authors would like to thank the referee for a very careful reading.

References

[1] P. Ara *Strongly π-regular rings have stable range one*, Proc. Amer. Math. Soc. 124 (1996), no. 11, 32933298.
[2] H. E. Bell, *A commutativity study for periodic rings,* Pacific J. Math. 70 (1977), no. 1, 2936.
[3] D. Boucher, F. Ulmer, *A Note on the Dual Codes of Module Skew Codes*, IMACC 2011. Lecture Notes in Comput. Sci., vol 7089. pp 230-243.
[4] A. Boulagouaz, A. Leroy, *(σ,δ)-codes*, Adv. Math. Commun. 2013, 7(4): 463-474.
[5] M. Chacron, *On a theorem of Herstein,* Canad. J. Math, Vol 21, (1969), 1348-1353
[6] H. Chen, M. Sheibani, *Periodicity and J-clean-like rings*, Math. Reports, 2016.
[7] A. Cherchem, A. Leroy, *Exponents of skew polynomials*, Finite Fields Appl. 37, (2016), 1-13.
[8] J. Cui, P. Danchev, *Some new characterizations of periodic rings,* J. Algebra Appl. 2019.
[9] I. N. Herstein, *Noncommutative rings* Math. Assoc. Amer. 1968.
[10] Y. Hirano, *On periodic P.I. rings and locally finite rings,* Math. J. Okayama Univ. 33 , 115-120, 1991.
[11] N. Jacobson, *Pseudo-linear transformations*, Ann. of Math. 38 (1937), 484-507.
[12] R. Khazal, S. Breaz, G. Călugăreanu, *On torsion-free periodic rings,* Int. J. Math. Math. Sci. 2005.
[13] A. Leroy, *Polynomial maps*, J. Algebra Appl. Vol. 11, No. 04, (2012), 1793-6829.
[14] A. Leroy, *Pseudo linear transformations and evaluation in Ore extensions*, Bull. Belg. Math. Soc. 2 (1995), 321347.
[15] R. Lidl and H. Niederreiter, *Introduction to finite fields and their applications*, Cambridge University Press, 1994.
[16] B. J. Mueller, *On semi-perfect rings*, Illinois J. Math. 14(3) (1970), 464–467.

Mathematics Faculty, Department of Algebra and Number Theory LA3C Laboratory, USTHB, Bp 32, Bab Ezzouar, Algiers, Algeria, email: dbouzidi@usthb.dz

Mathematics Faculty, Department of Algebra and Number Theory LA3C Laboratory, USTHB, Bp 32, Bab Ezzouar, Algiers, Algeria, email: acherchem@usthb.dz

Jean Perrin Faculty, Artois University, Jean Souvraz 62 307, Lens, France, email: andre.leroy@univ-artois.fr