PERIODIC AND POTENT ELEMENTS

GUANGLIN MA, ANDRÉ LEROY*, AND MEHRDAD NASERNEJAD

Abstract. In this paper, our main aim is to study periodic and potent elements of a ring. We specially study periodic elements of graded rings and generalize some classical results related to idempotent of polynomial rings. We show that a (von Neumann) quasi-inverse of a potent element is a root of unity. We study the isomorphism of potent elements and analyze some closure properties of the set $Pot(R)$ of potent elements of a ring R. The potent elements of the endomorphism ring of a Fitting module are described, and we apply this to matrices over division rings. In the case of matrices over finite fields, we connect features of potent elements with the exponent of their minimal polynomials.

Keywords: Potent, periodic elements, von Neumann regular elements, clean elements, Commutatively closed sets

MSC2020: 16U40,16W50,16U60.

1. Introduction

Periodic rings were introduced by Chacron [4] in his study of Herstein's commutativity theorems [8]. Many works have been published around this theme, let us mention for instance the references [2],[3],[4],[5],[11],[12],[9], and [13]. Lifting idempotents is a classical topic while trying to lift the structural properties of quotient rings. Recently lifting properties have been studied for periodic elements in [11], [12]. Finite rings form an important family of periodic rings. Applications have been given with a flavor of polynomial arithmetic over finite fields ([3]). Periodic elements are fascinating since they present different decompositions and connect with many other types of elements such as the clean, nil clean, (von Neumann) regular, unit regular. In this paper, we focus on periodic and potent elements. Potent, idempotent, and nilpotent elements form important subclasses of periodic elements and appear naturally.

Let us now briefly describe the content of the paper. We are trying, as far as possible, to develop the theory assuming the properties on one element without requiring all the elements of the ring to have this property. Another

*Corresponding author.

feature of the paper is that it is essentially self-contained. In Section 2, we present, with short direct proofs, some characterizations and properties of periodic elements in Propositions 2.4 and 2.5. We analyze periodic elements in graded rings $R = \bigoplus_{i \in \mathbb{N}} R_i$. We first state a result for idempotents in such rings and use it to get a property of periodic elements (cf. Theorem 2.12). This ensures that, under some conditions, the periodic elements come from the zero component R_0. We also consider periodic elements of domains and of polynomial rings.

The potent elements are studied in Section 3. We first show that, in any ring, potent elements are unit regular and obtain various properties of the unit regular decomposition. In particular, the quasi inverse of a potent element is a root of unity. We obtain necessary and sufficient conditions for two potents with the same level of potency to be isomorphic, generalizing the classical result of idempotents. We then study the commutative closure of potent elements. We analyze the potent elements in matrix rings over fields. In the case of finite fields we connect the potent matrices with the exponent of polynomials.

All the rings considered in this paper are assumed to have an identity except in some explicitly mentioned cases. Ring homomorphisms respect the identity. If R is a ring, we denote $U(R), Per(R), Pot(R)$, and $Nil(R)$ the set of units, periodic, potent, and nilpotent elements of R. In addition, $J(R)$ stands for the Jacobson radical of R. The symbol $\mathbb{N}$ (respectively, $\mathbb{N}^*$) denotes the nonnegative integers (respectively, positive integers).

2. Periodic elements

In this section, we study periodic elements of general rings. We are particularly interested in the case of graded rings.

Definitions 2.1. *An element a of a ring R is periodic if there exist integers $0 < m < l$ such that $a^m = a^l$. When $m = 1$, we say that the element is potent. In this case, the smallest $l > 1$ such that $a^l = a$ is called the level of potency. A ring R is periodic (π-potent) if all its elements are periodic (potent).*

If R is a periodic ring, then the element $1_R + 1_R$ is periodic and this easily leads to the fact that there exists $q \in \mathbb{N}^*$ such that $qR = 0$. For completeness, we provide short proofs of a few well-known useful facts. Notice that we focus on elements and don't require the ring to be periodic.

Lemma 2.2. *Let R be a ring, $a, b \in R$, $f(x) \in \mathbb{Z}[x]$ be a monic polynomial of degree n, and $q \in \mathbb{N}^*$. Then the following statements hold:*

(1) *If $f(a) = qa = 0$, then a is periodic.*
(2) *If a, b are periodic, $qa = qb = 0$, and $ba = f(a)b$, then the subring (without one) generated by a and b is periodic.*

Proof. (1) We may assume that the constant term of $f(x)$ is zero. It is easy to check that the elements of the set $\{a, a^2, a^3, \ldots, a^l, \ldots\}$ are of the form $\sum_{i=0}^{n-1} \alpha_i a^i$ with, for $1 \leq i \leq n-1$, $-q+1 \leq \alpha_i \leq q-1$. Since there are only a finite number of such expressions we conclude that the set of powers of a is finite, and hence we can find distinct $m, n \in \mathbb{N}$ such that $a^m = a^n$, as desired.

(2) Suppose that there exist distinct $l, m \in \mathbb{N}$ $(l > m)$ and distinct $s, t \in \mathbb{N}$ $(s > t)$ such that $a^l = a^m$ and $b^s = b^t$. Since by the hypothesis $ba = f(a)b$, this implies that the monomials in a and b are of the form $a^i b^j$ with $0 < i < l$ and $0 < j < s$. Since there exists an integer $q > 0$ such that $qa = qb = 0$, we obtain that the subring (without identity) generated by a and b is a finite ring, and hence is periodic. □

Let us mention a classical result due to Chacron (cf. [4]) that strengthens (1) in Lemma 2.2.

Proposition 2.3. *Let R be a ring such that for any element $a \in R$, there exist $m \in \mathbb{N}$ and a polynomial $f(x) \in \mathbb{Z}[x]$ such that $a^m = a^{m+1} f(a)$. Then R is periodic.*

Proposition 2.4. *Let a be an element in a ring R. Then the following are equivalent:*

(1) *There exist $m, l \in \mathbb{N}$, $l > m$, such that $a^m = a^l$, i.e., a is periodic.*
(2) *There exist $m, l \in \mathbb{N}$, $l > m$, such that for any $k \in \mathbb{N}$ and any $j \geq m$ we have $a^j = a^{j+k(l-m)}$.*
(3) *If $a^l = a^m$ with $l > m$, then $a^{m(l-m)}$ is an idempotent.*
(4) *There exists $r \in \mathbb{N}^*$ such that $a^r R \oplus a(1-a^r)R = aR$.*
(5) *There exists $r \in \mathbb{N}^*$ such that $Ra^r \oplus Ra(1-a^r) = Ra$.*
(6) *There exists $r \in \mathbb{N}^*$ such that $a^r R \cap a(1-a^r)R = \{0\}$.*
(7) *There exists $r \in \mathbb{N}^*$ such that $Ra^r \cap Ra(1-a^r) = \{0\}$.*

Proof. (1) ⇒ (2) We have $a^m = a^m a^{l-m} = a^m a^{2(l-m)} = \cdots = a^{m+k(l-m)}$ and hence also $a^j = a^{j+k(l-m)}$ for any $j \geq m$.

(2) ⇒ (3) Using (2), we get $(a^{m(l-m)})^2 = a^{m(l-m)+m(l-m)} = a^{m(l-m)}$.

(3) ⇒ (1) This is straightforward.

(3) ⇒ (4) Suppose that there exists $r \geq 1$ such that a^r is an idempotent. This implies that $a^r R \cap a(1-a^r)R \subseteq a^r R \cap (1-a^r)R = \{0\}$, and clearly

$a^rR + a(1-a^r)R \subseteq aR$. Now, if $ab \in aR$, then we can deduce that

$$ab = (a^r + (1-a^r))ab = (a^{r+1} + a(1-a^r))b \in a^rR + a(1-a^r)R.$$

(4) $\Rightarrow$ (6) This is straightforward.

(6) $\Rightarrow$ (3) Due to $a^r - a^{2r} = a^r(1-a^r) \in a^rR \cap a(1-a^r)R = \{0\}$, we thus get a^r is an idempotent.

(3) $\Rightarrow$ (5) and (5) $\Rightarrow$ (7) and (7) $\Rightarrow$ (3) are proved similarly. □

Although the fact that periodic elements are strongly clean seems to be part of folklore, we present a short proof of this fact in Proposition 2.5 (4). Notice also that the first three statements of this proposition are *equivalent* if the *ring* R is periodic (cf. Corollary 2.6).

Proposition 2.5. *For an element $a \in R$, consider the following assertions:*

(1) *a is periodic and $a^l = a^m$ for some $l, m \in \mathbb{N}^*$ with $m < l$.*
(2) *For any $k \in \mathbb{N}$, we have $a = p + n$, where $p = a^{1+k(l-m)}$ is potent and $n = a(1 - a^{k(l-m)}) \in Nil(R)$ are such that $pn = np$.*
(3) *There exists a prime integer p such that $a - a^p$ is nilpotent.*
(4) *a is strongly clean, i.e., $a = e + u$, where $e = e^2$ and u is a unit, and $eu = ue$.*

Then we have (1) $\Rightarrow$ (2), (2) $\Rightarrow$ (3), (2) $\Rightarrow$ (4). *Moreover, if we suppose that there exists $q \in \mathbb{N}$ such that $qa = 0$, then the first three assertions are equivalent.*

Proof. (1) $\Rightarrow$ (2) For any $k \in \mathbb{N}$, we have $a = p+n$, where $n = a(1-a^{k(l-m)})$ and $p = a^{1+k(l-m)}$. Thanks to (2) in Lemma 2.4, we have $n^m = 0$. Moreover, if k is such that $k(l-m)+1 \geq m$, then one obtains

$$p^{1+k(l-m)} = a^{(1+k(l-m))^2} = a^{1+k(l-m)+(1+k(l-m))k(l-m)} = a^{1+k(l-m)} = p.$$

The fact that $pn = np$ is straightforward.

(2) $\Rightarrow$ (3) By (2) in Lemma 2.4 and the proof of (1) $\Rightarrow$ (2), we know that, for any $k \geq m$, we get $a - a^{1+k(l-m)}$ is nilpotent. Since 1 and $l - m$ are coprime, the Dirichlet's result yields the proof.

(2) $\Rightarrow$ (4) By (2), we know that $a = p + n$, where p is potent and n is nilpotent, $pn = np$, and $pa = ap$. We will show that p is strongly clean. Suppose $p^l = p$. We then obtain $1 - p^{l-1}$ is idempotent and we easily check that, for $i \geq 1$, we have $(-1+p+p^{l-1})p^i = p^{i+1}$. This leads to the fact that $(-1+p+p^{l-1})(-1+p^{l-2}+p^{l-1}) = 1$. We can thus write $p = e + u$, where $e = 1-p^{l-1}$ is an idempotent element and $u = -1+p+p^{l-1}$ is an invertible element. Notice that $pu = up$. Now, our periodic element a can be written

as $a = p + n = e + u + n = e + u(1 + u^{-1}n)$. Since $un = nu$, we deduce that $1 + u^{-1}n$ is invertible. This yields the proof.

To prove that the first three assertions are equivalent if there exists some $q \in \mathbb{N}^*$ such that $qa = 0$, it is enough to show that under this hypothesis (3) $\Rightarrow$ (1). But remember that $a - a^p \in Nil(R)$, we get a monic polynomial $f(x) \in \mathbb{Z}[x]$ such that $f(a) = 0$. Due to $qa = 0$, Lemma 2.2 (1), yields the conclusion. □

The comments just after definition 2.1 and the above proposition immediately leads to the following classical result.

Corollary 2.6. *If R is a periodic ring, then, for any element $a \in R$, the first three statements in Proposition 2.5 are equivalent.*

Remarks 2.7. (1) From Proposition 2.5 we see that π-potent rings are periodic and reduced.

(2) Proposition 2.5 (2) above shows that strongly nil clean rings are periodic.

Let us make some comments on periodic rings. First, let us recall that a periodic ring is Dedekind-finite [3]. More information about these rings can be found in [6]

Proposition 2.8. (1) *If a domain A is periodic, then it is a subfield of the algebraic closure of a finite field $\mathbb{F}_p$, for some prime integer $p > 0$.*

(2) *Let I be the nil ideal of a ring R. Then R is periodic if and only if R/I is periodic. In particular, this is true for the prime radical of R.*

Proof. (1) Let R be a periodic domain. Then the nonzero elements of R are potent and invertible. This gives that R is a commutative field. Moreover, we know that a periodic ring has a nonzero characteristic. Since R is a field, the characteristic is a prime positive integer, say $p > 0$. Moreover, R is algebraic over its prime field, and hence R is a subfield of the algebraic closure of $\mathbb{F}_p$.

(2) This is an immediate consequence of the fact that, if for every $a \in R$, there exist $m, l, n \in \mathbb{N}$ such that $(a^m - a^l)^n = 0$; then the ring R is periodic by using Proposition 2.3. □

We remark that while considering potent rings, (2) implies that we can assume the ring R to be semiprime.

Definition 2.9. *A ring R is an $\mathbb{N}$-graded ring if $R = \bigoplus_{i\in\mathbb{N}} R_i$, where R_i are additive subgroups of $(R,+)$ and, for $i,j \in \mathbb{N}$, $R_iR_j \subseteq R_{i+j}$.*

We continue to focus on periodic elements. The next theorem was proved in [3] when the base ring R_0 was assumed to be periodic. The same proof works for elements and we reproduce it here for the sake of completeness.

Theorem 2.10. *Let $R = \bigoplus_{i\in\mathbb{N}} R_i$ be a graded ring and let $f = \sum_{i=0}^{m} a_i \in R$, $a_i \in R_i$ for $i \in \{0,\ldots,m\}$, and $f^n = \sum_{k=0}^{nm} A_k^n$, where A_k^n is the homogeneous component of f^n of degree k. Then, if a_0 is periodic and such that $qa_0 = 0$ for some $q \in \mathbb{N}$, then for all $k \in \mathbb{N}$, there exist $l,s \in \mathbb{N}$ with $l > s$ and $A_k^l = A_k^s$. In particular, this holds if R_0 is a periodic ring.*

Proof. Let $f = \sum_{i=0}^{m} a_i \in R$. Suppose that a_0 is periodic so that there exist positive integers e,p with $p < e$ and $a_0^e = a_0^p$. Let $k \in \mathbb{N}$ be fixed and notice that A_k^n is the sum of all words in $a_0, a_1, \ldots, a_m$ of length n and degree k. Any word in $a_0, a_1, \ldots, a_m$ of length n and degree k is of the form $a_0^{j_1} a_{c_1} a_0^{j_2} a_{c_2} \cdots a_{c_y} a_0^{j_{y+1}}$, with $0 \le j_l \le e$ and $\sum_{b=1}^{y} c_b = k$. If $n > k$ in any such word the letter a_0 will appear. The number, say h, of such words is finite and is independent of $n > k$ when n is big enough. If $w_1, \ldots, w_h$ are all the words in $a_0, a_1, \ldots, a_m$ of length n and degree k with $n > k$, then for all $n \in \mathbb{N}$, $A_k^n = \alpha_1 w_1 + \cdots + \alpha_h w_h$, $\alpha_i \in \mathbb{N}$. The fact that the letter a_0 appears in the words $w_1, \ldots, w_h$ and our assumption shows that $0 \le \alpha_i \le q-1$. Therefore, for k fixed, the set $\{A_k^n \mid n \in \mathbb{N}\}$ is finite and hence, 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. □

The next theorem generalizes to periodic elements a result that is well-known for idempotents of a polynomial ring. We first re-prove the case of idempotent elements in a graded ring.

Lemma 2.11. *Let $R = \bigoplus_{i\in\mathbb{N}} R_i$ be a graded ring and $e = \sum_{i=0}^{n} e_i \in R$ be an idempotent. If $e_ie_0 = e_0e_i$, for every $i \ge 0$, then $e = e_0$. In particular, if R_0 is abelian, then $E(R) = E(R_0)$.*

Proof. It is clear that e_0 is an idempotent of R. Assume that $e \ne e_0$ and let $k > 0$ be the least index such that $e_k \ne 0$. Comparing the degree k coefficients of e^2 and e, we get $2e_ke_0 = e_k$. Multiplying this equality by e_0 on the right, we obtain $e_ke_0 = e_0e_k = 0$, and hence also $e_k = 0$. This contradiction yields the result. □

The following theorem generalizes Lemma 2.11.

Theorem 2.12. *Let $R = \bigoplus_{i\in\mathbb{N}} R_i$ be a graded ring and $p = \sum_{i=0}^n p_i$ be a periodic element such that $[p_0, p_i] = 0$. If $p^l = p^m$, for some $l > m$, we put $r = m(l-m)$ and assume that $r1_R$ is a nonzero divisor in R. Then $p^{m^2} = p_0^{m^2} \in R_0$. In particular, under these conditions, if p is potent, then $m = 1$ and $p \in R_0$.*

Proof. Let us assume that $p = \sum_{i=0}^n p_i$, with $p_i \in R_i$, is such that $p^l = p^m$, where $l > m$. We put $r := m(l-m)$; hence, Proposition 2.4(3) implies that p^r is idempotent. Now, Lemma 2.11 shows that $p^r \in R_0$, and hence $p^r = p_0^r$. We also have

$$p^{m^2} = (p^m)^m = (p^l)^m = p^{lm} = p^{m^2+m(l-m)} = p^{m^2}p^r = p^{m^2}p_0^r.$$

We write $p^{m^2} = \sum_{i=0}^t q_i$, $q_i \in R_i$, and obtain

$$\sum_{i=0}^t q_i = p^{m^2} = p^{m^2}p_0^r = (\sum_{i=0}^t q_i)p_0^r.$$

This gives that, for any $0 \le i \le t$, $q_i = p_0^r q_i$, and thus $q_i = p_0^{sr} q_i$ for any $s \in \mathbb{N}$. Since $p^r = p_0^r$, the sum of degree $i \ge 1$ terms of p^r is zero. We now prove, by induction on i, that for any $i \ge 1$, we have $p_0^{i(r-1)} p_i = 0$. If $i = 1$, then the degree 1 term of p^r gives $rp_0^{r-1}p_1 = 0$. The fact that $r1_R$ is not a zero divisor gives $p_0^{r-1}p_1 = 0$. The induction hypothesis shows that $p_0^{(i-1)(r-1)}$ annihilates all the elements of $p_1, \dots, p_{i-1}$. The fact that the sum of the degree i terms of p^r is zero leads to $rp_0^{r-1}p_i + w = 0$, where w is a sum of words that contain at least one p_j with $j < i$. Multiplying this last equality by $p_0^{(i-1)(r-1)}$ leads to $rp_0^{i(r-1)}p_i = 0$. Our hypothesis says that $r1_R$ is not a zero divisor leads to the claim.

We get $p^{m^2} = \sum_{i=0}^t q_i$, so $q_i \in R_i$ is a sum of products of p_j for $j \le i$. Therefore, $p_0^{ir} q_i = 0$. But we know that $q_i = p_0^{ir} q_i$. This implies that, for $i \ge 1$, we have $q_i = 0$. We thus conclude that $p^{m^2} \in R_0$, as required. □

Remark 2.13. The proof of Theorem 2.12 shows that we only require the graded ring R to be such that, for any $a \in S$, where S is the set of monomials in the p_i's, we have $ra = m(l-m)a = 0$ implies that $a = 0$.

The following result should be compared with (2) and (3) in Proposition 2.5.

Proposition 2.14. *Let $R = \bigoplus_{i\in\mathbb{N}} R_i$ be a graded ring and $p = \sum_{i=0}^n p_i \in Per(R)$ be such that $p_ip_0 = p_0p_i$ for $1 \le i \le n$. Suppose there exists a natural number q such that $qp_i = 0$ for $0 \le i \le n$. Then $p - p_0$ is nilpotent.*

Proof. On account of p and p_0 are periodic and commute and $qp = qp_0 = 0$, we know, by Lemma 2.2(2), that $p - p_0$ is also periodic. This yields that $p - p_0 := p_1 + p_2 + p_3 + \cdots + p_s$ is such that $p - p_0$ is periodic. So there exist $l, m \in \mathbb{N}$ such that $(p - p_0)^l = (p - p_0)^m$ with $l > m$. This gives that $(p - p_0)^m(1 - (p - p_0)^{l-m}) = 0$. If $(p - p_0)^{l-m} = 0$, then we are done. If $(p - p_0)^{l-m} \neq 0$, then $1 - (p - p_0)^{l-m}$ is not a zero divisor, since its zero component is 1. We thus deduce that $(p - p_0)^m = 0$, as desired. □

As a direct application of the last results, let us mention the following corollary. We recall that if σ is an automorphism of a ring R_0, then the skew polynomial ring $R_0[x; \sigma]$ is the set of polynomials $\sum_{i=0}^{n} a_i x^i$ with coefficients $a_i \in R_0$ written on the left. This set is a ring with usual addition and multiplication based on the commutation rule $xa = \sigma(a)x$, for $a \in R_0$. This ring is graded by the degree.

Corollary 2.15. *Let R_0 be a ring and σ an automorphism of R_0. If $e(x) = \sum e_i x^i \in R = R_0[x; \sigma]$ is an idempotent and $p = p(x) = \sum p_i x^i \in R$ is a periodic element, then*

(1) *If $e_i e_0 = e_0 e_i$, then $e(x) = e_0 \in R_0$.*
(2) *If $p^l = p^m$ is such that $[p_i, p_0] = 0$ and $m(l - m)1_R$ is not a zero divisor, then we have $p^{m^2} \in R_0$.*

Examples 2.16. (1) The polynomial $p(x) = 4x + 1 \in (\mathbb{Z}/8\mathbb{Z})[x]$ is such that $p(x)^3 = p(x)$. So, in this case we have $l = 3$, $m = 1$, and $r = 2$. This shows that the condition mentioned in Theorem 2.12 (or in Remark 2.13(1)) is not satisfied.

(2) Consider the ring $M_3(k)[x]$, where k is a field. Let $p(x) = p_0 + p_1 x$ be such that

$$p_0 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \quad \text{and} \quad p_1 = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix}.$$

One can check that $p(x)^3 = 1$, and hence $p(x)$ is potent but we remark that $p_0 p_1 \neq p_1 p_0$, so that we cannot apply Theorem 2.12.

Corollary 2.17. (1) *If $a = \sum a_i \in R = \bigoplus_{i \in \mathbb{N}} R_i$ is such that $a^l = a$ (a is a potent element) with $[a_0, a_i] = 0$ and $(l - 1)1_R$ is not a zero divisor, then $a = a_0$.*

(2) *Let R be 2-primal and let T be a set of central indeterminates. Then $S := R[T]$ is 2-primal and if $a \in Per(S)$ then $a = a_0 + a_1$ where $a_0 \in Per(R)$ and $a_1 \in Nil(R)[T] \setminus R$. Thus, in this case, we have $Per(R[T]) \subseteq Per(R) + (Nil(R)[T] \setminus R)$.*

Proof. (1) is a direct consequence of our earlier results and is left to the reader.

(2) To prove that S is 2-primal it is enough to show that $Nil(S) \subseteq P(S)$, where $P(S)$ is the prime radical of S. It is well-known that $P(S) = P(R)[T]$ (cf. [13], P. 160). So that $S/P(S) = \frac{S}{P(R)[T]} = \frac{R}{P(R)}[T]$. Since R is 2-primal, we get that $R/P(R)$ is reduced and hence $S/P(S)$ is also reduced. This implies that S itself is 2-primal.

Let P be a minimal prime ideal of R. Then P is a completely prime ideal of R, so R/P is a domain. If $f \in R[T]$, then $f \in R[T_0]$ where $T_0 = t_1, \dots, t_n$ is a finite subset of T. We thus write $f = \sum_{i \in I} a_i t^i$, where $I \subseteq \mathbb{N}^n$, $a_i \in R$, and for $i = (i_1, \dots, i_n) \in I$, $t^i = t_1^{i_1} t_2^{i_2} \dots t_n^{i_n}$. For any $f \in Per(R[T])$, there exist distinct $m, n \in \mathbb{N}$ such that $\overline{f}^m = \overline{f}^n \in R[T]/P[T]$ $(m > n)$. Comparing the degree zero coefficients of f^n and f^m, we get a_0 is periodic. Now, to end the proof, it is enough to show that for each minimal prime ideal P of R, every $a_i \in P$ $(i \neq 0)$. Also, $R[T]/P[T] \cong \frac{R}{P}[T]$. Then $\overline{f} \in Per(\frac{R}{P}[T])$. Since $\frac{R}{P}[T]$ is a domain, we have $\overline{f} = \bar{0}$ or $\overline{f}^{m-n} = \bar{1}$. If $\overline{f} = \bar{0}$, then $f \in P[T]$. If $\overline{f}^{n-m} = \bar{1}$, then $\overline{f} \in \frac{R}{P}[T]$ is invertible. Since R/P is a domain, this implies that $\bar{a}_i = \bar{0}$ for $i \neq 0$, and hence $a_i \in P$, $i \neq 0$. In both cases, we get $a_i \in P$ for $i \neq 0$. Because for every minimal primal ideal P we get $a_i \in P$ for $i \neq 0$, we obtain $a_i \in \bigcap P = Nil(R)$ for $i \neq 0$. We conclude that $Per(R[T]) \subseteq Per(R) + (Nil(R)[T] \setminus R)$. □

Example 2.18. Let R be the commutative ring $\mathbb{Z}[y]/(y^2)$. Consider $1+yx \in R[x]$. Clearly, 1 is periodic and y is nilpotent, but $(1+yx)^n = 1 + nyx$ is not periodic for any $n \in \mathbb{N}$. This shows the reverse inclusion in Corollary 2.17(2) does not always hold.

3. Potent elements

This section starts with some properties of potent elements in general rings. We first connect these elements with the von Neumann elements. It is well-known and obvious that idempotents are (von Neumann) unit regular. Theorem 3.2 shows that the same is true for potent elements.

Lemma 3.1. *A potent element is always von Neumann regular. A π-potent ring is a commutative von Neumann regular ring. In particular, it is unit regular.*

Proof. Let $a = a^l$ be a potent element of R. If $l = 2$, then a is an idempotent, and hence unit regular. If $l > 2$, then we have $a = a^l = aa^{l-2}a$ so that a

is regular. If R is a π-potent ring, then it is a commutative von Neumann regular ring. Such a ring is always unit regular (cf. [7, Corollary 4.2]). $\square$

Since a strongly regular element is unit regular ([7]), we conclude that a potent element is unit regular. The next theorem gives a direct proof of this fact and moreover shows that a quasi inverse of a potent element is a root of unity.

Theorem 3.2. *Every potent element is unit regular and has a root of unity as quasi inverse.*

Proof. Let $x \in Pot(R)$, say $x^l = x$ with $l \geq 2$. If $l = 2$, x is an idempotent and the result is clear. So we may assume that $l \geq 3$. We want to prove that there exists $y \in U(R)$ such that $x = xyx$. We get $x = xx^{l-2}x$ and $x(1 - x^{l-1}) = 0$. This gives $x(1 - x^{l-1} + x^{l-2})x = x^l = x$.

Since $(1 - x^{l-1})x^{l-2} = 0$ and $1 - x^{l-1}$ is an idempotent, we get that $(1 - x^{l-1} + x^{l-2})^{l-1} = 1 - x^{l-1} + (x^{l-2})^{l-1} = 1$

$\square$

We now collect some features of a potent element in the following corollary.

Corollary 3.3. *Let $a^l = a \in Pot(R)$ with l being the level of potency of a. We put $u = -1 + a + a^{l-1}$, $e = 1 - a^{l-1}$, $v = 1 + a^{l-2} - a^{l-1}$. Then the following statements hold:*

(1) *The element a^{l-1} is an idempotent, $u \in U(R)$, and $a = e + u$, with $eu = ue$.*
(2) *The element a is unit regular, more precisely, $a = ava$, where $v \in U(R)$ is such that $v^{l-1} = 1$ and l is the level of potency of v.*
(3) *We have $av = f = f^2$, $f = a^{l-1} = 1 - e$, $u = -1 + a + a^{l-1} = a - e$, and $v = a^{l-2} + a - u$.*

Proof. (1) This can be extracted from the proof of Proposition 2.5(4).

(2) The fact that $a = ava$, where $v = 1 + a^{l-2} - a^{l-1} = a^{l-2} + e \in U(R)$ comes from the proof of Theorem 3.2. This proof also shows that $v^{l-1} = 1$, and hence $v^l = v$. Let us now show that the level of potency of v is l. Assume that $v^s = v$, with $1 < s < l$. Following the proof of Theorem 3.2, we get $v = v^s = (1 + a^{l-2} - a^{l-1})^s = 1 + a^{l-s-1} - a^{l-1} = v = 1 + a^{l-2} - a^{l-1}$. This leads to $a^{l-s-1} = a^{l-2}$. So, $a = a^l = a^{l-s+1}$. Since $1 < l - s + 1 < l$, this contradicts the fact that l is the level of potency of a. This shows that l is also the level of potency of v.

(3) This is straightforward and left to the reader. $\square$

Remark 3.4. If $a \in R$ is periodic, say $a^l = a^m$ with $l > m$, we put $r = m(l-m)$. Following the proof of Proposition 2.5 we can express the summands of these decompositions in terms of a. In fact, we have $a = p + n = e + u$, where $p = a^{r+1}$ is potent, $n = a - a^{r+1}$ is nilpotent, and $e = 1 - p^r$ $u = -1 + p + p^r$. In addition, the proof of Theorem 3.2 gives that $p = pvp$, where $v = 1 + a^{r-1} - a^r$ is invertible (with inverse v^{r-1}). The element $f = pv$ is then idempotent and we get $f^2 = f = a^r$.

Lemma 3.5. *Let a, b be elements in a ring R. Then, the following statements hold:*

(1) *If $ab \in Pot(R)$, then $(ba)^s \in Pot(R)$ for any $s \geq 2$.*
(2) *If $ab \in Pot(R)$ and $ab \in U(R)$, then $ba \in Pot(R)$.*

Proof. (1) Let $(ab)^l = ab$. Then direct computations give that

$$\begin{aligned}(ba)^{sl} &= b(ab)^{(s-1)l+l-1}a = b((ab)^l)^{s-1}(ab)^{l-1}a = b(ab)^{s-1}(ab)^{l-1}a \\ &= b(ab)^{s+l-2}a = b(ab)^{s-2}(ab)^l a = b(ab)^{s-2}(ab)a \\ &= b(ab)^{s-1}a = (ba)^s.\end{aligned}$$

This shows that $(ba)^s$ is a potent element, as required.

(2) If $(ab)^l = ab$ and $ab \in U(R)$, then $(ab)^{l-1} = 1$, this gives that $(ba)^l = b(ab)^{l-1}a = ba$. So that ba is potent. □

The next proposition gives more information about the relations between ab and $(ba)^2$ when ab is potent. Let us notice that if $ab \in Pot(R)$, then by Proposition 3.5 (1), we have $(ba)^2 \in Pot(R)$ and these elements are strongly clean. We can thus write $ab = e + u$ and $(ba)^2 = f + v$, where e, f are idempotents and u, v are units such that $eu = ue$ and $fv = vf$.

Proposition 3.6. *With the above notations we have the following:*

(1) *$afb = 0$.*
(2) *$baf = bea$.*
(3) *$b(af - ea) = (af - ea)b = 0$.*
(4) *$b(u + e)a = f + v$ and $a(f + v)b = avb$.*

Proof. (1) According to Corollary 3.3 we have $f = 1 - (ba)^{2(l-1)}$, and hence

$$\begin{aligned}afb &= a(1 - (ba)^{2(l-1)})b = ab - (ab)^{2(l-1)+1} \\ &= ab - (ab)^l(ab)^{l-1} = ab(1 - (ab)^{l-1}) = 0.\end{aligned}$$

(2) We have the following equalities

$$\begin{aligned} baf &= ba(1-(ba)^{2(l-1)}) = ba - b(ab)^{2(l-1)}a = ba - b(ab)^{l-1}a \\ &= ba - (ba)^l = b(1-(ab)^{l-1})a = bea. \end{aligned}$$

(3) The first equality is clear from (2), and the second one is a direct consequence of the fact that $e = 1-(ab)^{l-1}$.

(4) Note that $f+v = (ba)^2 = b(ab)a = b(e+u)a$. Also, Corollary 3.3 implies that $v = -1+(ba)^2+(ba)^{2(l-1)}$. This leads to the following equalities

$$\begin{aligned} avb &= a(-1+(ba)^2+(ba)^{2(l-1)})b = -ab+(ab)^3+(ab)^{2(l-1)+1} \\ &= (ab)^3 = a(ba)^2b = a(f+v)b. \end{aligned}$$

This finishes the proof. □

It is worth considering the relationship between periodic and regular elements. We say an element $a \in R$ is *strongly regular* if there exists $x \in R$ such that $a = axa$, where $ax = xa$. We denote the set of strongly regular elements as $sReg(R)$. Theorem 3.2 and its proof show that potent elements are strongly regular. We have the following proposition.

Proposition 3.7. *Let R be any ring. We have:*

$$Per(R) \cap sReg(R) = Pot(R).$$

Proof. It is enough to show that $Per(R) \cap sReg(R) \subseteq Pot(R)$. To do this, let $a \in Per(R) \cap sReg(R)$. There exist $l, m \in \mathbb{N}$ and $x \in R$ such that $l > m$, $a = a^2x$, $ax = xa$, and $a^l = a^m$. We suppose that l is minimal. Assume that $a \notin Pot(R)$. We thus have $m \geq 2$. This gives rise to

$$a^{l-1} = a^l x = a^m x = a^{m-2}a^2x = a^{m-1}.$$

This is a contradiction with the minimality of l. □

Example 3.8. Proposition 3.7 is untrue if we just consider the intersection of $Per(R)$ with $Reg(R)$, the set of regular elements. To see this, consider the ring $R = M_2(\mathbb{F}_2)$. This finite ring is periodic and regular but not all elements of R are potent.

The following proposition generalizes the classical criterion for isomorphic idempotents (cf. [14], section 21).

Proposition 3.9. *Suppose $c, d \in R$ and $n \geq 2$ are such that $c^n = c$ and $d^n = d$. Then*

$$cR \cong dR \Leftrightarrow \exists\, a, b \in R \text{ such that } c = bd^{n-2}a \text{ and } d = ac^{n-2}b.$$

Proof. Suppose that $\theta : cR \to dR$ is an R-module isomorphism and let $a = d\alpha \in dR$ be such that $\theta(c) = a$. We thus have $a = \theta(c) = \theta(c^n) = \theta(c)c^{n-1} = ac^{n-1}$. By a similar argument, if $b = c\beta \in cR$ is such that $\theta^{-1}(d) = b$, we obtain $b = \theta^{-1}(d)d^{n-1} = bd^{n-1}$. We then get

$$c = \theta^{-1}(\theta(c)) = \theta^{-1}(a) = \theta^{-1}(d)\alpha = bd^{n-1}\alpha = bd^{n-2}a.$$

We can deduce $d = ac^{n-2}b$ in the same way.

Conversely, suppose $c^n = c \in R$ and $d^n = d \in R$ are such that $c = bd^{n-2}a$ and $d = ac^{n-2}b$. We thus have the following

$$ac^{n-1} = ac^{n-2}c = ac^{n-2}bd^{n-2}a = dd^{n-2}a = d^{n-1}a \in dR.$$

Similarly, we obtain $bd^{n-1} = c^{n-1}b \in cR$. We then define $\theta : cR \to dR$ via $\theta(c) = ac^{n-1}$ and $\theta' : dR \to cR$ via $\theta'(d) = bd^{n-1}$. These maps are well-defined and we compute, for every $x \in R$,

$$\begin{aligned}\theta'(\theta(cx)) &= \theta'(ac^{n-1}x) = \theta'(d^{n-1}ax) = \theta'(d)d^{n-2}ax \\ &= bd^{n-1}d^{n-2}ax = bd^{n-2}ax = cx.\end{aligned}$$

Similarly, we have $\theta(\theta'(dx)) = dx$ for every $x \in R$. This shows that θ is an isomorphism of right R-modules with $\theta' = \theta^{-1}$. □

The symmetry of Proposition 3.9 gives immediately the following corollary.

Corollary 3.10. *Suppose $c, d \in R$ and $n \geq 2$ are such that $c^n = c$ and $d^n = d$. Then $cR \simeq dR$ if and only if $Rc \simeq Rd$.*

Remark 3.11. Let us mention that, for a potent element $c \in R$, say $c^n = c$, for $n > 1$, we have that $cR = c^{n-1}R$ where c^{n-1} is an idempotent. Hence, if $d \in R$ is another potent element such that $d^n = d$ then $cR \simeq dR$ if and only if $c^{n-1}R \simeq d^{n-1}R$. So we could also use the characterization of the isomorphic idempotents c^{n-1} and d^{n-1} to get a characterization of the isomorphic potent elements c and d, but this would have involved powers of c and d.

Let us mention, without proof, the following lemma. For more information on direct limit we refer the reader to [18].

Lemma 3.12. *Let R_1, R_2 and R_i $i \in I$ be rings. Then the following statements hold:*

1. *$Pot(R_1 \times R_2) = Pot(R_1) \times Pot(R_2)$.*
2. *If $(I, \leq)$ is a directed set and $(R_i)_{i\in I}$ is a directed system of rings, then $Pot(R_i)$ is a directed system of sets and $\varinjlim Pot(R_i) = Pot(\varinjlim R_i)$.*

It is easy to remark that $Pot(R) \cap Nil(R) = \{0\}$. We will provide some more remarks related to $Pot(R)$ in the next theorem. To do this, we need the following definition (cf. [1]).

Definitions 3.13. *A subset S of a ring is called commutatively closed if for any $a, b \in R$, we have $ab \in S$ implies $ba \in S$. If $a, b \in R$, we write $a \underset{1}{\sim} b$ if there exists $c, d \in R$ such that $a = cd$ and $b = dc$, and we define by induction $a \underset{n}{\sim} b$ iff there exists $c \in R$ such that $a \underset{1}{\sim} c$ and $c \underset{n-1}{\sim} b$. If S is a subset of R, we define*

$$\overline{S} = \{x \in R \mid \exists\, n \in \mathbb{N},\ \exists\, s \in S \text{ with } x \underset{n}{\sim} s\}.$$

This definition is motivated by the fact that it leads to a characterization of Dedekind-finite rings, reversible rings, and is related to regular elements, clean elements, Jacobson Lemma, and many other classical topics (cf. [1] and [15], for more information).

Theorem 3.14. *Let R be a ring. Then the following statements hold:*

(1) *$Per(R)$ is commutatively closed (i.e., $ab \in Per(R)$ if and only if $ba \in Per(R)$).*
(2) *$\overline{Pot(R)} \subseteq Per(R)$.*
(3) *If $x \in \overline{Pot(R)}$, then there exists $l \in \mathbb{N}$ such that $x^l \in Pot(R)$.*
(4) *$\overline{Pot(R)} \cap Nil(R) = \overline{\{0\}}$*
(5) *$\overline{Pot(R)} \cap Jac(R) \subseteq \overline{\{0\}}$*

Proof. (1) This is straightforward and left to the reader.

(2) Due to $Pot(R) \subseteq Per(R)$, we get $\overline{Pot(R)} \subseteq \overline{Per(R)} = Per(R)$.

(3) If $x \in \overline{Pot(R)}$, then x is periodic, and so a power of x is idempotent by Proposition 2.4.

(4) If $x \in \overline{Pot(R)} \cap Nil(R)$, then there exist $n \in \mathbb{N}$ and $y \in Pot(R)$ such that $x \underset{n}{\sim} y$ and, since $x \in Nil(R)$, $y \in Nil(R)$, as well. This means that y is potent and nilpotent, so that $y = 0$ and the fact that $x \underset{n}{\sim} y$ implies $x \in \overline{\{0\}}$.

Conversely, let $a \in \overline{\{0\}}$. Thanks to $\overline{\{0\}} \subset Nil(R)$, we obtain $a \in Nil(R)$. On the other hand, since $0 \in Pot(R)$, we have $\overline{0} \subseteq \overline{Pot(R)}$, and therefore $a \in Nil(R) \cap \overline{Pot(R)}$, as desired.

(5) If $x \in \overline{Pot(R)} \cap Jac(R)$, we have that there exists $r \in \mathbb{N}$ such that x^r is an idempotent and belongs to $J(R)$. This implies that $x^r = 0$ and hence the statement (4) above shows that $x \in \overline{Pot(R)} \cap Nil(R) = \overline{\{0\}}$, as required. □

Let us notice that the commutative closure gives rise to a topology on a ring. In particular, the intersection of two closed subsets is closed. This immediately gives the inclusion $\overline{\{0\}} \subseteq Nil(R) \cap \overline{Pot(R)}$ in Theorem 3.14(4).

Recall that a ring is *reversible* if for $a, b \in R$, $ab = 0$ implies $ba = 0$.

Corollary 3.15. *A ring R is reversible if and only if $\overline{Pot(R)} \cap Nil(R) = \{0\}$.*

Proof. The definitions imply that R is reversible if and only if $\overline{\{0\}} = \{0\}$. Theorem 3.14(4) yields the conclusion. □

Example 3.16. We give an example such that the set of potent elements is not commutatively closed. Let $\mathbb{F}$ be a field and

$$a = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \in M_2(\mathbb{F}) \quad \text{and} \quad b = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{F}).$$

Then $ab = 0$ is potent but $0 \neq ba$ is nilpotent, and hence not potent.

Before stating the next proposition let us make the following remark.

Remark 3.17. A word of caution about definitions is in order. A ring R is said to be potent if each left ideal of R that is not contained in the Jacobson radical contains a nonzero idempotent and idempotents lift modulo the Jacobson radical. This definition is left-right symmetric and was introduced by Nicholson [16]. In some literature (cf., e.g. [17]) the π-potent rings are called potent rings. We will continue to use the classical definition of potent rings given by Nicholson. Nicholson proved that every exchange ring is a potent ring (cf. [16]). We have the following result relating π-potent rings and potent rings.

Proposition 3.18. *A π-potent ring is a potent ring.*

Proof. If R is a π-potent ring, then according to [17] every nonzero subring of R not contained in the Jacobson radical contains an idempotent element. Since a left ideal of R is a subring, the definition of a potent ring immediately gives that R is potent. The Jacobson radical of a potent ring being zero we thus get the result. □

Proposition 3.19. *If the zero divisors of a ring are nilpotent, then the potent elements are roots of unity. This is the case of right Artinian local rings.*

Proof. If R is a ring satisfying our hypothesis and $a \in R$ is a nonzero potent element, say $a^l = a$, for $l \in \mathbb{N}$, $l > 1$, we can deduce that $a(1 - a^{l-1}) = 0$. Our hypothesis then shows that either a is nilpotent or $1 - a^{l-1} = 0$. On account of a is potent and nonzero, it cannot be nilpotent. This finishes the proof. □

The ring $\mathbb{Z}/p^n\mathbb{Z}$, where p is a prime number, is a concrete example for Proposition 3.19.

We recall that a module M_R over a ring R is said to be a Fitting module if for every $\alpha \in End_R(M)$ there exists $s \in \mathbb{N}$ such that

$$M = Ker(\alpha^s) \oplus Im(\alpha^s)$$

We now study potent elements in the endomorphism ring of a Fitting module. As a corollary this will give a concrete decomposition of matrices over division rings.

Theorem 3.20. *Let M_R be a Fitting module, $\alpha \in End_R(M)$ and $s \in \mathbb{N}$ be such that $M = Ker(\alpha^s) \oplus Im(\alpha^s)$. Then α is potent if and only if $\alpha^l|_{M_1} = id.$ and $\alpha|_{M_0} = 0$, where $M_0 = Ker(\alpha^s)$ and $M_1 = Im(\alpha^s)$.*

Proof. Suppose that $\alpha^m = \alpha$, for some $m \in \mathbb{N}$. We decompose $\alpha = \alpha_0 + \alpha_1$ where $\alpha_0, \alpha_1 \in End_R(M)$ are such that $\alpha_0|_{M_0} = \alpha|_{M_0}, \alpha_0|_{M_1} = 0$ and $\alpha_1|_{M_1} = \alpha|_{M_1}, \alpha_1|_{M_0} = 0$. M_0 and M_1 are stable under the action of α. Moreover $\alpha_0^s = 0$, $\alpha_0\alpha_1 = \alpha_1\alpha_0 = 0$ and α_1 is an injection on M_1. Moreover we have $\alpha = \alpha^m = (\alpha_0 + \alpha_1)^m = \alpha_0^m + \alpha_1^m = \alpha = \alpha_0 + \alpha_1$ and hence $\alpha_0^m = \alpha_0$ and $\alpha_1^m = \alpha_1$. Since α_0 is nilpotent we get $\alpha_0 = 0$ and $\alpha = \alpha_1$ with $\alpha_1^m = \alpha_1$ and the fact α_1 is an injection on M_1 yields the result with $l = m - 1$.

For the converse notice that, with the above notation, $\alpha = \alpha_1$ and hence $\alpha^{l+1} = \alpha$. □

In the rest of this section, we will briefly study potent matrices. Recall that if a matrix with coefficients in a division ring D is idempotent, then there exists a matrix $P \in GL_n(D)$ such that $PAP^{-1} = diag(1, \ldots, 1, 0, \ldots, 0)$. As a corollary of Theorem 3.20, we obtain the following generalization of this fact for potent matrices.

Corollary 3.21. *Suppose that D is a division ring and $A \in R = M_n(D)$ is such that $A^l = A$. Then there exists $P \in GL_n(D)$ such that $PAP^{-1} = diag(A_1, 0)$, where $A_1^{l-1} = I$, $A_1 \in GL_r(D)$, and $r = rank(A)$.*

Proof. Since D_D^n is a Fitting module, we apply Theorem 3.20 and obtain that there exists $P \in GL_n(D)$ such that $PAP^{-1} = diag(A_1, A_0)$, where $A_1 \in GL_r(D)$ and A_0 is nilpotent. The fact that $A^l = A$ implies that $A_1^l = A_1$ and $A_0^l = A_0$. Since A_0 is potent and nilpotent, we obtain that $A_0 = 0$. □

An invertible element $a \in R$ is potent if and only if a is a root of unity. In the next propositions we focus on noninvertible potent matrices.

Corollary 3.22. *Let $A \in M_2(D)$ be a noninvertible matrix over a commutative integral domain D. Then A is potent if and only if $det(A) = 0$ and $tr(A)$ is a root of unity in D.*

Proof. Let F be the quotient field of D and consider $A \in M_2(D) \subseteq M_2(F)$. Theorem 3.21 shows that A is similar to a matrix $\begin{pmatrix} a_1 & 0 \\ 0 & 0 \end{pmatrix}$. Moreover the element a_1 is a root of unity and we have that $Tr(A) = a_1$. This shows that the condition is necessary. The converse is left to the reader. □

An easy example of a potent matrix is a diagonal matrix with potent elements on the diagonal. We now give another more subtle construction of potent matrices.

Example 3.23. (1) Let R be a ring. To construct $A \in M_n(R)$ such that $A^l = A$, we consider l row vectors $\{\underline{u_1}, \underline{u_2}, \dots, \underline{u_l}\} \subseteq M_{1\times n}(R)$ and l column vectors $\{\overline{v_1}, \overline{v_2}, \dots, \overline{v_l}\} \subseteq M_{n\times 1}(R)$ such that, there exists $k \in \mathbb{N}$ with, for every $1 \leq i, j \leq l$, the products $\underline{u_i}\overline{v_j} = 0$ if $i \neq j$ and $(\underline{u_i}\overline{v_i})^k = 1 \in R$. Then the matrices

$$A = \begin{pmatrix} \overline{v_1}, \dots, \overline{v_l} \end{pmatrix} \begin{pmatrix} \underline{u_1} \\ \vdots \\ \underline{u_l} \end{pmatrix} \in M_{n\times n}(R) \text{ and } B = \begin{pmatrix} \underline{u_1} \\ \vdots \\ \underline{u_l} \end{pmatrix} \begin{pmatrix} \overline{v_1}, \dots, \overline{v_l} \end{pmatrix} \in M_{l\times l}(R),$$

are such that $B^k = I_{l\times l}$ and $A^{k+1} = A$. Let us give particular concrete instances of this construction. Let $\mathbb{R}$ be the set of real numbers, and suppose $\underline{u_1}, \dots, \underline{u_l}$ form a part of an orthogonal basis of $\mathbb{R}^n$. Taking $\overline{v_i} = \underline{u_i}^t$ (the transpose of $\underline{u_i}$), one obtains $\underline{u_i}\overline{v_j} = \delta_{ij}$, and hence $A^2 = A \in M_{n\times n}(\mathbb{R})$. As a very special case if $x, y, z, t \in \mathbb{R}$ are such that $(xy + zt)^k = 1$, for some $k \in \mathbb{N}$, then the matrix $A = \begin{pmatrix} y \\ t \end{pmatrix} \begin{pmatrix} x & z \end{pmatrix} \in M_{2\times 2}(\mathbb{R})$ is such that $A^{k+1} = A$.

The notion of exponent of polynomials with coefficients in a finite field is classical. The following lemma is a well-known result.

Lemma 3.24. *Let $p(X) \in \mathbb{F}_q[X]$ be such that $p(0) \neq 0$, then there exists $e \in \mathbb{N}$ such that $p(X)$ divides $X^e - 1$.*

Proof. Since the element $\overline{X}$ of the finite ring $\mathbb{F}_q[X]/p(X)$ is not a zero divisor, it must be a potent element. This finishes the proof. □

With the notations of the above lemma, the minimal e such that $p(X)$ divides $X^e - 1$ is called the *exponent* or the *period* of $p(X)$ and will be denoted by $Exp(p(X))$. There are generalizations of this result, in particular for polynomials over periodic rings, we refer to [3] for more details. Let us recall that if $p(X) \in \mathbb{F}_q[X]$ is such that $p(X)$ divides $X^l - 1$, then $Exp(p(X))$ divides l.

We remark that if $p(X) \in \mathbb{F}_q[X]$ has a nonzero independent coefficient, then any matrix (of any size) annihilating this polynomial will be invertible and potent. Now, in the next lemma, we look at noninvertible matrices in $M_n(\mathbb{F}_q)$.

Lemma 3.25. *Let $A \in M_n(\mathbb{F}_q)$ be a noninvertible matrix such that $A^l = A^m$ with m minimal. Then m is the highest power of X dividing the minimal polynomial $\mu_A(X)$ of A.*

Proof. Since A is not invertible, its minimal polynomial is of the form $\mu_A(X) = p(X)X^s$, where $p(0) \neq 0$ and $s \geq 1$. It follows from Lemma 3.24 that there exists $e \in \mathbb{N}$ such that $p(X)$ divides $X^e - 1$. Hence, $\mu_A(X)$ divides $(X^e - 1)X^s$, and therefore $A^{e+s} - A^s = 0$. The minimality of m shows that $m \leq s$. On the other hand, since $A^l - A^m = 0$, we can deduce that the polynomial $\mu_A(X) = p(X)X^s$ divides $(X^{l-m} - 1)X^m$, and thus $s \leq m$. This concludes the proof. □

We close this paper with the following proposition.

Proposition 3.26. *Let $0 \neq A \in M_n(\mathbb{F}_q)$ be a noninvertible matrix. Then $A^l = A^m$ for some $l \in \mathbb{N}$ with $l > m$ if and only if X^m is the highest power of X dividing $\mu_A(X)$ and $Exp(\frac{\mu_A(X)}{X^m})$ divides $l - m$.*

Proof. Assume that $A^l = A^m$. Then $\mu_A(X)|X^l - X^m$ and $\frac{\mu_A(X)}{X^m}|X^{l-m} - 1$. This gives that $Exp(\frac{\mu_A(X)}{X^m})|l - m$.

Conversely, if X^m is the highest power of X dividing $\mu_A(X)$, then we can deduce that $Exp(\frac{\mu_A(X)}{X^m})$ exists and, by our hypothesis, it follows that $Exp(\frac{\mu_A(X)}{X^m})|l - m$. This gives $\frac{\mu_A(X)}{X^m}|X^{l-m} - 1$, and hence $\mu_A(X)|X^l - X^m$. Consequently, $A^l - A^m = 0$, as desired. □

Acknowledgment

This work was done while Guanglin Ma was visiting the Artois University during her one-year doctoral internship sponsored by the China Scholarship Council (No.202209040018). She would like to thank the staff of this institution for the warm welcome she received.

ORCID

Guanglin Ma: https://orcid.org/0000-0003-2638-9985,
André Leroy: https://orcid.org/0000-0002-8486-584X,
Mehrdad Nasernejad: https://orcid.org/0000-0003-1073-1934.

References

[1] M. Abdi and A. Leroy, *Graphs of commutatively closed sets,* Linear Multilinear Algebra **70** (2022), no. 21, 6965–6977.

[2] L.P. Belluce, I.N. Herstein, S.K. Jain, *Generalized commutative rings,* Nagoya Math. J. **7**,(1966), 1-5 .

[3] A. D. Bouzidi, A. Cherchem, and A. Leroy, *Exponents of skew polynomials over periodic rings*, Comm. Algebra **49** (2021), no. 4, 1639–1655.

[4] M. Chacron, *Certains anneaux périodiques,* (French) Bull. Soc. Math. Belg. **20** (1968), 66–78.

[5] M. Chacron, *On a theorem of Herstein*, Canadian J. Math. **21** (1969), 1348–1353.

[6] H. Chen and M. Sheibani Abdolyousefi, Theory of clean rings and matrices. World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2023. xi+680 pp.

[7] K. R. Goodearl, von Neumann regular rings. Second edition. Robert E. Krieger Publishing Co., Inc., Malabar, FL, 1991, xviii+412 pp.

[8] I. N. Herstein, *The structure of a certain class of rings,* Amer. J. Math. **75** (1953), 866-871.

[9] S.K. Jain, P.K. Menon, *Note on generalized commutative rings,* J. Indian Math. Soc., n. Ser. **33**, 1-5 (1969).

[10] P. Kanwar, A. Leroy, and J. Matczuk, *Clean elements in polynomial rings,* Noncommutative rings and their applications, Contemp. Math., **634**, Amer. Math. Soc. (2015), 197-204.

[11] D. Khurana, *Lifting potent elements modulo nil ideals,* J. Pure Appl. Algebra **225** (2021), no. 11, Paper No. 106762, 7 pp.

[12] D. Khurana and P. P. Nielsen, *Periodic elements and lifting connections,* J. Pure Appl. Algebra **227** (2023), no. 11, Paper No. 107421, 9 pp.

[13] T. J. Laffey, *Commutative subrings of periodic rings,* Math. Scand. **39** (1976), no. 2, 161–166.

[14] T. Y. Lam, A first course in noncommutative rings. Graduate Texts in Mathematics, **131**. Springer-Verlag, New York, 1991. xvi+397 pp.

[15] A. Leroy and M. Nasernejad, *Symmetric closure of modules and rings*, 2023, To appear in Communications in Algebra. `https://doi.org/10.1080/00927872.2023.2240888`

[16] W. K. Nicholson, *Lifting idempotents and exchange rings,* Trans. Amer. Math. Soc. **229** (1977), 269–278.

[17] G. Oman, *A characterization of potent rings,* Glasg. Math. J. **65** (2023), no. 2, 324–327.

[18] J. J. Rotman, An introduction to homological algebra. Second edition. Universitext. Springer, New York, 2008. xiv+709 pp.

•School of Mathematics and Statistics, Nanjing University of Science and Teconology, China, email: linlinguangma@163.com

•Univ. Artois, UR 2462, Laboratoire de Mathématiques de Lens (LML), F-62300 Lens, France, email: andre.leroy@univ-artois.fr

•Univ. Artois, UR 2462, Laboratoire de Mathématiques de Lens (LML), F-62300 Lens, France, email: m_nasernejad@yahoo.com