*Glasgow Mathematical Journal* (2023), **65**, pp. 324–327
doi:10.1017/S0017089522000325

Glasgow
Mathematical
Journal

RESEARCH ARTICLE

# A characterization of potent rings

Greg Oman

Department of Mathematics, University of Colorado at Colorado Springs, Colorado Springs, CO 80918, USA
E-mail: goman@uccs.edu

**Received:** 8 May 2022; **Revised:** 28 September 2022; **Accepted:** 29 September 2022;
**First published online:** 2 November 2022

**Keywords:** Boolean ring, idempotent, Jacobson's theorem, nilradical, potent ring

**2020 Mathematics Subject Classification:** *Primary* - 16U40, *Secondary* - 06E75

**Abstract**
An associative ring $R$ is called *potent* provided that for every $x \in R$, there is an integer $n(x) > 1$ such that $x^{n(x)} = x$. A celebrated result of N. Jacobson is that every potent ring is commutative. In this note, we show that a ring $R$ is potent if and only if every nonzero subring $S$ of $R$ contains a nonzero idempotent. We use this result to give a generalization of a recent result of Anderson and Danchev for reduced rings, which in turn generalizes Jacobson's theorem.

## 1. Introduction

Boolean algebras play a significant role not only in mathematics but are also important tools in logic and computer science. Moreover, there is a natural correspondence between Boolean algebras and so-called Boolean rings: from a Boolean algebra, one may canonically construct a Boolean ring and vice versa (for details and an introduction to the subject, see [4]). We recall that an associative ring $R$ is *Boolean* provided every member of $R$ is idempotent, that is, $x^2 = x$ for every $x \in R$. It is well-known (and an exercise in many undergraduate algebra texts) that every Boolean ring is commutative (see [5], for example). In fact, if one replaces the exponent 2 in the previous equation with 3, $R$ is still commutative. Indeed, one can replace 2 with any integer greater than 1, and commutativity is guaranteed. Continuing to generalize, if one assumes only the existence of some such $n > 1$ for every $x \in R$ (which may depend on $x$), $R$ must be commutative. This beautiful result is due to Nathan Jacobson and generalizes Wedderburn's theorem that every finite division ring is a field ([13]).

**Proposition 1** (Jacobson's theorem [8]). *Let $R$ be an associative ring and suppose that for every $x \in R$, there is an integer $n(x) > 1$ such that $x^{n(x)} = x$ (that is, $R$ is a potent ring). Then, $R$ is commutative.*

We refer the reader to [2, 3], and [6] for further reading, and to [1] for a recent generalization of Jacobson's theorem.

Changing gears temporarily, the theory of idempotents contributes significantly to the theory of both commutative and non-commutative rings. Indeed, the number of different kinds of idempotents defined in the literature (orthogonal, central, primitive, local, irreducible, etc.) as well as rings defined in terms of idempotents (Baer, semisimple, von Neumann regular, Zorn, Rickart, etc.) indicates the utility of this notion in the structure theory of rings (see [11] for details). The purpose of this short note is to identify potency with a natural condition on the existence of idempotents. Specifically, we prove that an associative ring $R$ is potent if and only if every nonzero subring of $R$ contains a nonzero idempotent. We mention the classic texts [5] and [7] as references for some standard algebraic results utilized in the paper such as the Chinese remainder theorem, the division algorithm for polynomials over a field, and Lagrange's theorem.

*Throughout, a ring is assumed only to be associative and not to be commutative nor to contain an identity unless specified; subrings are also not assumed unital, even in rings with identity.*

## 2. Main result

Before presenting the main result of this paper, we prove the following lemma. For brevity, let us agree to call a ring with the property that every nonzero subring contains a nonzero idempotent *idempotent-rich*.[1]

**Lemma 1.** *The following hold:*

*(1) Every subring of an idempotent-rich ring is idempotent-rich.*
*(2) Every idempotent-rich ring is reduced.*
*(3) If $R$ is a nonzero reduced ring, then the polynomomial ring $XR[X] := \{Xf(X) : f(X) \in R[X]\}$ in the (commuting) variable $X$ is not idempotent-rich.*
*(4) If $R$ is idempotent-rich and $e \in R$ is idempotent, then the additive order of $e$ is a square-free integer.*

*Proof.* We establish each in succession.

(1) Trivial.
(2) Suppose by way of contradiction that $R$ is idempotent-rich but not reduced. Then, there is some nonzero $\alpha \in R$ such that $\alpha^2 = 0$. But now $\mathbb{Z}\alpha$ is a nonzero subring of $R$ with no nonzero idempotent, a contradiction.
(3) Let $R$ be a nonzero reduced ring. We claim $XR[X]$ has no nonzero idempotents. Indeed, consider an arbitrary $f := a_1X + \cdots + a_nX^n \in XR[X]$, where $a_n \neq 0$. Then because $R$ is reduced, it is easy to see that $f^2$ has degree $2n$ and thus $f^2 \neq f$.
(4) Let $R$ be idempotent-rich and let $e \in R$ be an idempotent. Then $\mathbb{Z}e$ is a subring of $R$ and, moreover, $\mathbb{Z}e \cong \mathbb{Z}/\langle n\rangle$ for some non-negative integer $n$. If $n = 0$, then by (1), we see that $\mathbb{Z}$ is idempotent-rich, but this is absurd as the subring $2\mathbb{Z}$ of $\mathbb{Z}$ has no nonzero idempotent. Thus, $n > 0$ (and hence $n = \mathrm{ord}(e)$). Suppose that $n$ is not square-free, and write $n = m^2q$, where $m,q$ are integers and $m > 1$. Then, $mq \pmod n$ is a nonzero nilpotent element of $\mathbb{Z}/\langle n\rangle$, a contradiction to (1) and (2) above. □

We are now ready to prove the main result of this note.

**Theorem 1.** *Let $R$ be a ring. Then, $R$ is potent if and only if every nonzero subring of $R$ contains a nonzero idempotent.*

*Proof.* Let $R$ be a ring. Suppose first that $R$ is potent. We will show that $R$ is idempotent-rich. Indeed, suppose that $S$ is a nonzero subring of $R$, and let $s \in S$ be nonzero. By our assumption, there is an integer $n > 1$ such that $s^n = s$. Then, $s^n(s^{n-2}) = s(s^{n-2})$, that is, $(s^{n-1})^2 = s^{2n-2} = s^{n-1}$. As $s^n = s$ and $s \neq 0$, clearly $s^{n-1} \neq 0$; since $n > 1$, $s^{n-1} \in S$. Hence, $S$ contains a nonzero idempotent.

Conversely, suppose that every nonzero subring of $R$ contains a nonzero idempotent. We shall prove that $R$ is potent. Suppose that $\alpha \in R$ is nonzero. We will show that

$$\text{the ring } \alpha\mathbb{Z}[\alpha] := \{\alpha f(\alpha) : f(X) \in \mathbb{Z}[X]\} \text{ is a finite product of finite fields.} \tag{2.1}$$

We first verify that the ring $X\mathbb{Z}[X]$ is Noetherian (that is, every ascending chain of ideals stabilizes). Indeed, notice that every ideal of $X\mathbb{Z}[X]$ is also an ideal of $\mathbb{Z}[X]$. As $\mathbb{Z}[X]$ is Noetherian, $X\mathbb{Z}[X]$ is as well. Next, since $\alpha\mathbb{Z}[\alpha]$ is a homomorphic image of $X\mathbb{Z}[X]$, we conclude that $\alpha\mathbb{Z}[\alpha]$ is a Noetherian ring. It

[1] This definition can be seen as a strengthening of the definition of a so-called *Zorn ring* (due to Kaplansky; see [10]), which is a ring for which every nonzero non-nil ideal contains a nonzero idempotent. Zorn rings need not be commutative.

https://doi.org/10.1017/S0017089522000325 Published online by Cambridge University Press

now follows immediately that $\alpha\mathbb{Z}[\alpha]$ does not contain an infinite internal direct sum of nonzero ideals. Therefore (see Lemma 4 of [12]),

$$\alpha\mathbb{Z}[\alpha] = I_1 \oplus I_2 \cdots \oplus I_n \text{ for some nonzero indecomposable ideals } I_1, \ldots, I_n \text{ of } \alpha\mathbb{Z}[\alpha]. \tag{2.2}$$

Next, fix $k$ with $1 \leq k \leq n$, and set $I := I_k$. Then, $I$ is a nonzero subring of $\alpha\mathbb{Z}[\alpha]$ and thus contains a nonzero idempotent $e$. Let $J := \{ie - i\colon i \in I\}$. Observe that $J$ is a subideal of $I$ and that $Ie + J = I$. We claim that the sum is direct: suppose that $xe = ye - y$ for some $x, y \in I$. Multiplying through by $e$ and using the fact that $e$ is idempotent, we see that $xe = ye - ye = 0$, proving the directness of the sum. Because $e$ is a nonzero element of $Ie$, and since $I$ is indecomposable, we have $Ie = I$. By (4) of Lemma 1, the additive order of $e$ is a square-free integer. As $\alpha\mathbb{Z}[\alpha]$ is commutative, this clearly implies that the additive order of every member of $Ie = I$ is also a square-free integer. Since $k$ was arbitrary, it follows easily from (2.2) above that the order of every member of $\alpha\mathbb{Z}[\alpha]$ is a square-free integer; in particular, the order of $\alpha$ is a square-free integer $m$. From this fact, we deduce that[2]

$$\text{the additive order of every element of } \alpha\mathbb{Z}[\alpha] \text{ is a factor of } m. \tag{2.3}$$

The map $\overline{a}_1 X + \cdots + \overline{a}_n X^n \to a_1\alpha + \cdots + a_n\alpha^n$ is now a well-defined ring surjection of $X\mathbb{Z}/\langle m\rangle[X]$ onto $\alpha\mathbb{Z}[\alpha]$. Thus,

$$\alpha\mathbb{Z}[\alpha] \cong X\mathbb{Z}/\langle m\rangle[X]/K \text{ for some ideal } K \text{ of } X\mathbb{Z}/\langle m\rangle[X]. \tag{2.4}$$

Write $m = p_1 p_2 \cdots p_n$, where the $p_i$ are distinct primes (recall above that $\alpha \neq 0$, and hence $m > 1$). As is well-known, a simple application of The Chinese Remainder Theorem yields that, as rings, $\mathbb{Z}/\langle m\rangle \cong \mathbb{Z}/\langle p_1\rangle \oplus \cdots \oplus \mathbb{Z}/\langle p_n\rangle$. We conclude that $X\mathbb{Z}/\langle m\rangle[X] \cong X\mathbb{Z}/\langle p_1\rangle[X] \oplus \cdots \oplus X\mathbb{Z}/\langle p_n\rangle[X]$. We may now view $K$ as an ideal of $X\mathbb{Z}/\langle p_1\rangle[X] \oplus \cdots \oplus X\mathbb{Z}/\langle p_n\rangle[X]$. Via this identification,

$$\alpha\mathbb{Z}[\alpha] \cong (X\mathbb{Z}/\langle p_1\rangle[X] \oplus \cdots \oplus X\mathbb{Z}/\langle p_n\rangle[X])/K. \tag{2.5}$$

Next, for $1 \leq i \leq n$, let $I_i := K \cap X\mathbb{Z}/\langle p_i\rangle[X]$. We claim that $I_i$ is nontrivial. If $I_i$ is trivial, then the mapping $y \mapsto K + y$ is a ring isomorphism of $X_i\mathbb{Z}/\langle p_i\rangle[X]$ into $(X\mathbb{Z}/\langle p_1\rangle[X] \oplus \cdots \oplus X\mathbb{Z}/\langle p_n\rangle[X])/K \cong \alpha\mathbb{Z}[\alpha]$. But then by (1) of Lemma 1, $X\mathbb{Z}/\langle p_i\rangle[X]$ is idempotent-rich, contradicting (3) of Lemma 1. So we see that each $I_i$ is a nonzero ideal of $X\mathbb{Z}/\langle p_i\rangle[X]$. But it is easy to see that $I_i$ is also a nonzero ideal of the PID $\mathbb{Z}/\langle p_i\rangle[X]$. The Division Algorithm for polynomials over a field shows that $\mathbb{Z}/\langle p_i\rangle[X]/I_i$ is finite and thus also

$$\text{each } X\mathbb{Z}/\langle p_i\rangle[X]/I_i \text{ is finite.} \tag{2.6}$$

Now observe that

$$(X\mathbb{Z}/\langle p_1\rangle[X] \oplus \cdots \oplus X\mathbb{Z}/\langle p_n\rangle[X])/(I_1 \oplus \cdots \oplus I_n) \cong X\mathbb{Z}/\langle p_1\rangle[X]/I_1 \oplus \cdots \oplus X\mathbb{Z}/\langle p_n\rangle[X]/I_n. \tag{2.7}$$

Invoking (2.6), it follows that $(X\mathbb{Z}/\langle p_1\rangle[X] \oplus \cdots \oplus X\mathbb{Z}/\langle p_n\rangle[X])/(I_1 \oplus \cdots \oplus I_n)$ is finite. Since $I_1 \oplus \cdots \oplus I_n \subseteq K$,[3] it is immediate that

$$\alpha\mathbb{Z}[\alpha] \cong (X\mathbb{Z}/\langle p_1\rangle[X] \oplus \cdots \oplus X\mathbb{Z}/\langle p_n\rangle[X])/K \text{ is finite.} \tag{2.8}$$

Thus, finally, we see that $\alpha\mathbb{Z}[\alpha]$ is a finite, reduced commutative ring. As is well-known (see p. 22 of [9], for example), this implies that $\alpha\mathbb{Z}[\alpha]$ has an identity. By the Chinese Remainder Theorem, $\alpha\mathbb{Z}[\alpha] = F_1 \oplus \cdots \oplus F_k$ for some finite fields $F_1, \ldots, F_k$, establishing (2.1). We claim that

$$\alpha^{(|F_1|-1)(|F_2|-1)\cdots(|F_k|-1)+1} = \alpha, \tag{2.9}$$

showing that $R$ is potent. To see this, fix $i$ with $1 \leq i \leq k$, and let $\pi_i\colon \alpha\mathbb{Z}[\alpha] \to F_i$ be projection onto the $i$th coordinate. It clearly suffices to establish that $(\pi_i(\alpha))^{(|F_1|-1)(|F_2|-1)\cdots(|F_k|-1)+1} = \pi_i(\alpha)$. If $\pi_i(\alpha) = 0_i$, this is patent, so assume that $\pi_i(\alpha) \neq 0$. Lagrange's Theorem implies that $\pi_i(\alpha)^{|F_i|-1} = 1_i$. Raising both sides

[2] Recall that an ideal $I$ of a ring $S$ is *indecomposable* provided $I \neq J \oplus K$ for any nonzero ideals $J$ and $K$ of $S$.

[3] Observe that since none of the rings $X\mathbb{Z}/\langle p_i\rangle[X]$ has an identity, we cannot necessarily decompose $K$ into a direct sum of ideals of the form $J_1 \oplus \cdots \oplus J_n$, where each $J_i$ is an ideal of $X\mathbb{Z}/\langle p_i\rangle[X]$.

https://doi.org/10.1017/S0017089522000325 Published online by Cambridge University Press

to the power $\prod_{j\neq i}|F_j|-1$ and then multiplying through by $\pi_i(\alpha)$ yields the desired equation, and (2.9) is established. The proof is now complete. □

The following equivalent formulation of Jacobson's theorem is immediate.

**Corollary 1** (Jacobson's Theorem, Alternative Form). *Let $R$ be a ring. If every nonzero subring of $R$ contains a nonzero idempotent of $R$, then $R$ is commutative.*

In [1], the authors show that if $R$ is a ring with identity such that for every $x\in R$, there are positive integers $m(x)$ and $n(x)$ of different parity such that $x^{m(x)}=x^{n(x)}$, then $R$ potent, and hence commutative. Note that the assumption that $R$ is unital cannot be dropped completely, since every nil ring trivially has this property, and there are noncommutative nil rings. However, if $R$ has no nonzero nilpotent elements, then we have the following stronger result.

**Corollary 2.** *Let $R$ be a reduced ring. Suppose that for every nonzero subring $S$ of $R$, there exists a nonzero $x\in S$ and distinct positive integers $m(x)$ and $n(x)$ such that $x^{m(x)}=x^{n(x)}$. Then, $R$ is commutative.*

*Proof.* Suppose that $R$ is reduced with the above property. It suffices to prove that every nonzero subring of $R$ contains a nonzero idempotent. Thus, let $S$ be a nonzero subring and let $x\in S$ be nonzero and such that $x^m=x^n$ for some distinct positive integers $m$ and $n$. Without loss of generality, we may assume that $m>n$. Let $l:=m-n$. Then, it follows easily by induction that for every positive integer $r$, we have $x^{m+rl}=x^n$. Thus, we may assume without loss of generality that $m>2n$. Now set $k:=m-2n$. Then, observe that $(x^{n+k})^2=x^{2(n+k)}=x^{m+k}=x^{n+k}$. As $R$ is reduced, $x^{n+k}$ is a nonzero idempotent of $S$, and the conclusion follows. □

**Conflicts of interest.** The author declares none.

## References

[1] D. D. Anderson and P. V. Danchev, A note on a theorem of Jacobson related to periodic rings, *Proc. Am. Math. Soc.* **148**(12) (2020), 5087–5089.
[2] S. Buckley and D. MacHale, Variations on a theme: rings satisfying $x^3=x$ are commutative, *Am. Math. Mon.* **120**(5) (2013), 430–440.
[3] S. W. Dolan, A proof of Jacobson's theorem, *Canad. Math. Bull.* **19**(1) (1976), 59–61.
[4] S. Givant and P. Halmos, *Introduction to Boolean Algebras*, Undergraduate Texts in Mathematics (Springer, New York, 2009).
[5] I. N. Herstein, *Topics in Algebra* (Blaisdell Publishing Co., New York-Toronto-London, 1964).
[6] I. N. Herstein, Wedderburn's theorem and a theorem of Jacobson, *Am. Math. Mon.* **68** (1961), 249–251.
[7] T. W. Hungerford, *Algebra. Reprint of the 1974 Original*, *Graduate Texts in Mathematics*, vol. **73** (Springer-Verlag, New York-Berlin, 1980).
[8] N. Jacobson, Structure theory for algebraic algebras of bounded degree, *Ann. Math. (2)* **46** (1945), 695–707.
[9] J. Jans, *Rings and Homology* (Holt, Rinehart, and Winston Inc., New York-Chicago-San Francisco-Toronto-London, 1964).
[10] I. Kaplansky, Topological representation of algebras. II, *Trans. Bitter. Math. Soc.* **68** (1950), 62–75.
[11] T. Y. Lam, *A First Course in Noncommutative Rings*, Graduate Texts in Mathematics, vol. **131**, 2nd edition (Springer-Verlag, New York, 2001).
[12] G. Oman and J. Stroud, Rings whose subrings have an identity, *Involve* **13**(5) (2020), 823–828.
[13] J. H. M. Wedderburn, A theorem on finite algebras, *Trans. Am. Math. Soc.* **6** (1905), 349–352.

https://doi.org/10.1017/S0017089522000325 Published online by Cambridge University Press