Semigroup Forum (2013) 86:272–278
DOI 10.1007/s00233-012-9442-y

RESEARCH ARTICLE

Rings whose multiplicative endomorphisms are power functions

Greg Oman

Received: 12 March 2012 / Accepted: 14 September 2012 / Published online: 9 November 2012

Abstract Let R be a commutative ring. For any positive integer m, the power function $f : R \to R$ defined by $f(x) := x^m$ is easily seen to be an endomorphism of the multiplicative semigroup $(R, \cdot)$. In this note, we characterize the commutative rings R with identity for which every multiplicative endomorphism of $(R, \cdot)$ is equal to a power function. Specifically, we show that every endomorphism of $(R, \cdot)$ is a power function if and only if R is a finite field.

Keywords Local ring · E-ring · Multiplicative endomorphism · Nilradical

1 Introduction

In his classic text, Abelian Groups (Fuchs [3]), Laszlo Fuchs posed the following problem (Problem 45, p. 232):

$$\textit{Characterize the rings } R \textit{ for which } End(R^+) \cong R,$$

where $End(R^+)$ is the ring (under addition and composition of functions) of endomorphisms of the abelian group R^+. P. Schultz was among the first mathematicians to attack this question. In Schultz [13], he coined the term *E-ring*, which is a ring R for which every endomorphism of R^+ is a left multiplication in R. This is to say that if $f \in End(R^+)$, then there exists some $r \in R$ for which $f(x) = rx$ for all $x \in R$ (it makes no difference whether r acts on the left or right). Moreover, every E-ring is commutative; this is proved in Lemma 6 of [13]. Note that conversely, if $r \in R$, then the map $f_r : R \to R$ defined by $f_r(x) := rx$ is an endomorphism of R^+. Thus,

Communicated by Benjamin Steinberg.

G. Oman (✉)
Department of Mathematics, The University of Colorado, Colorado Springs, CO 80918, USA
e-mail: goman@uccs.edu

in a sense, one may view an E-ring as a ring in which all additive endomorphisms of R are "canonical". There is an extensive literature on the theory of E-rings. It is not our purpose to give an account of this theory; we refer the reader instead to the bibliographies of Dugas [2], Göbel [5], and Herden [7] for historical background and a sampling of topics of current interest.

In this note, we keep the spirit of Fuchs' original question, but we change the focus from addition to multiplication. To wit, let R be a commutative ring with identity $1 \neq 0$, and let m be a positive integer. Then the power function $f : R \to R$ defined by $f(x) := x^m$ is easily seen to be an endomorphism of the multiplicative semigroup $(R, \cdot)$. Informally, the power functions are the canonical endomorphisms of $(R, \cdot)$. The purpose of this paper is to answer the following question:

For which commutative rings R with identity are all endomorphisms of $(R, \cdot)$ canonical? That is, for which commutative rings R with identity is every endomorphism of $(R, \cdot)$ equal to a power function?

For the purposes of this note, let us call such a ring a *P-ring*. In the sequel, we will show that a commutative ring R with identity is a P-ring if and only if R is a finite field.

We end the introduction with a few remarks on notation and terminology. Let R be a commutative ring with identity. The ideal $Nil(R) := \{x \in R : x^n = 0$ for some positive integer $n\}$ is the *nilradical* of R. We will denote the multiplicative group of units of R by $U(R)$. If $r_1, r_2, \ldots, r_k \in R$, then the ideal generated by the r_i will be denoted by $\langle r_1, r_2, \ldots, r_k \rangle$. We recall that R is *local* provided R has a unique maximal ideal. We remind the reader that a ring R is local if and only if the set of non-units of R forms an ideal of R. If G is a group and $g_1, g_2, \ldots, g_k \in G$, then the subgroup generated by $g_1, g_2, \ldots, g_k$ will be denoted by $(g_1, g_2, \ldots, g_k)$. Finally, if S is a monoid with 0, then we assume that every endomorphism $f : S \to S$ satisfies the conditions $f(0) = 0$ and $f(1) = 1$ (in other words, f is a 0-preserving monoid endomorphism).

2 Main result

We begin this section by stating that *all rings are now assumed to be commutative with identity* $1 \neq 0$. Our principal result (Theorem 1) is that a ring R is a P-ring if and only if R is a finite field. Our work commences with the following lemma, which is essentially folklore. We include a proof for completeness.

Lemma 1 *Let G be an abelian group (written additively). Then G is a finite cyclic group if and only if every endomorphism $f : G \to G$ has the form $f(g) = mg$ for some positive integer m.*

Proof Assume first that G (written additively) is a finite cyclic group of order n; say $G = (g_0)$. Now let $f : G \to G$ be an arbitrary endomorphism of G. Then $f(g_0) = mg_0$ for some m, $1 \leq m \leq n$. Now let $g \in G$ be arbitrary. We claim that $f(g) = mg$. To wit, $g = ig_0$ for some i, $1 \leq i \leq n$. Thus $f(g) = f(ig_0) = if(g_0) = i(mg_0) = m(ig_0) = mg$. This establishes the trivial direction.

Conversely, assume that every endomorphism f of the abelian group G has the form $f(g) = mg$ for some positive integer m. We will prove that G is a finite cyclic group. Clearly we may assume that G is nontrivial. Note first that the zero map $f : G \to G$ defined by $f(g) := 0$ for all $g \in G$ is an endomorphism of G. Thus there exists a positive integer m such that $f(g) = mg$ for all $g \in G$. But this implies that $mG = \{0\}$, whence G is a bounded torsion group (that is, there is a finite bound (namely, m) on the orders of the elements of G). Hence there exists a finite collection $\{p_1, p_2, \ldots, p_k\}$ of prime numbers such that

$$G = G_{p_1} \oplus G_{p_2} \oplus \cdots \oplus G_{p_k}, \tag{2.1}$$

where G_{p_i} (the p_i-component of G) is the subgroup of G consisting of the elements of G whose orders are a power of p_i. Since every G_{p_i} is bounded, it follows from Prüfer's Theorem that every G_{p_i} is a direct sum of cyclic groups, each of order a power of p_i (this follows from Theorem 11.2 of [3], for example). Fix an i with $1 \leq i \leq k$. We claim that G_{p_i} is cyclic. Suppose not. Then (by virtue of (2.1)) there exist positive integers r and s with $r \geq s$ such that

$$G = \mathbb{Z}/(p_i^r) \oplus \mathbb{Z}/(p_i^s) \oplus H \tag{2.2}$$

for some subgroup H of G. Define $f : \mathbb{Z}/(p_i^r) \oplus \mathbb{Z}/(p_i^s) \oplus H \to \mathbb{Z}/(p_i^r) \oplus \mathbb{Z}/(p_i^s) \oplus H$ by:

$$f(\overline{a}, \overline{b}, h) := (\overline{0}, \overline{a}, 0). \tag{2.3}$$

One checks easily that f is a well-defined endomorphism of G. Thus there exists some positive integer m such that $f(g) = mg$ for all $g \in G$. Note that by (2.3), we have $f((\overline{1}, \overline{0}, 0)) = (\overline{0}, \overline{1}, 0)$. However, $f(g) = mg$ for all $g \in G$. Thus also $f((\overline{1}, \overline{0}, 0)) = (\overline{m}, \overline{0}, 0)$. But then $\overline{1} = \overline{0}$ (in $\mathbb{Z}/(p_i^s)$), and this is a contradiction. We conclude that G_{p_i} is cyclic. As $1 \leq i \leq k$ was arbitrary, we deduce that each G_{p_j} is a finite cyclic group. Furthermore, as the orders of the cyclic groups G_{p_j} are pairwise relatively prime and since $G = G_{p_1} \oplus G_{p_2} \oplus \cdots \oplus G_{p_k}$, we deduce that G is a finite cyclic group. This completes the proof. □

Before proceeding, we pause to remind the reader that we defined a ring R to be a *P-ring* provided every endomorphism f of $(R, \cdot)$ is of the form $f(x) = x^m$ for some positive integer m. We now show that every P-ring is local.

Lemma 2 *Let R be a P-ring. Then R is local with maximal ideal $J = Nil(R)$.*

Proof Suppose that R is a P-ring, and let J be an arbitrary maximal ideal of R. Now define the function $f : R \to R$ by:

$$f(x) = \begin{cases} 0 & \text{if } x \in J, \\ x & \text{if } x \notin J. \end{cases}$$

Since R is a commutative ring with identity and J is maximal, we see that J is also prime. This implies that f is an endomorphism of $(R, \cdot)$. Since R is a P-ring, there

is a positive integer m such that $f(x) = x^m$ for all $x \in R$. In particular, if $x \in J$, then $0 = f(x) = x^m$. This proves that $J \subseteq Nil(R)$. Since J is maximal, we obtain $J = Nil(R)$, as required. □

The following corollary is immediate.

Corollary 1 *If R is a P-ring, then every element of R is either nilpotent or a unit.*

Our first proposition will play a pivotal role in the proof of the main theorem.

Proposition 1 *Let R be a P-ring. Then R is a finite local ring and $U(R)$ (the multiplicative group of units of R) is cyclic.*

Proof We assume that R is a P-ring. We first show that $U(R)$ is a finite cyclic group. By Lemma 1, it suffices to show that every endomorphism $f : U(R) \to U(R)$ is of the form $f(u) = u^m$ for some positive integer m. Indeed, let $f : U(R) \to U(R)$ be an arbitrary endomorphism. Now define $g : R \to R$ as follows:

$$g(x) = \begin{cases} 0 & \text{if } x \in Nil(R), \\ f(x) & \text{if } x \in U(R). \end{cases}$$

Of course, $Nil(R) \cap U(R) = \varnothing$, and by Corollary 1, every element of R belongs to either $Nil(R)$ or $U(R)$. We conclude that g is well-defined. It is trivial to verify that g is an endomorphism of $(R, \cdot)$. Hence there exists a positive integer m such that $g(x) = x^m$ for all $x \in R$. Thus if $u \in U(R)$, then $f(u) = g(u) = u^m$, and we see that $f(u) = u^m$ for all $u \in U(R)$. We conclude that $U(R)$ is a finite cyclic group. Recall again that every element of R is a member of either $U(R)$ or $Nil(R)$. Thus to prove that R is finite, it now suffices to show that $Nil(R)$ is finite. But this is easy. The map defined by $x \mapsto 1 + x$ is an injection from $Nil(R)$ into $U(R)$. This completes the proof. □

Some time ago, Robert Gilmer gave a complete description of the finite local rings with a cyclic group of units. After proving two technical lemmas, we will use his characterization to show that the P-rings are exactly the finite fields.

Lemma 3 *Let R be a finite local ring, and suppose $Nil(R)$ is a principal ideal; say $Nil(R) = \langle \alpha \rangle$. Then $Nil(R) = \{u\alpha^n : u \in U(R), n > 0\}$.*

Proof Suppose that R is a finite local ring and that $Nil(R) = \langle \alpha \rangle$. Then $Nil(R)$ is the unique maximal ideal of R, and every $x \in R\text{-}Nil(R)$ is a unit. Let $x \in Nil(R)$ be arbitrary. We will show that there exists some $u \in U(R)$ and some $n > 0$ such that $x = u\alpha^n$. Clearly we may assume that $x \neq 0$. Choose n to be largest such that $x = r\alpha^n$ for some $r \in R$ (such n and r exist since $Nil(R) = \langle \alpha \rangle$, $x \neq 0$, and α is nilpotent). We claim that r is a unit. If not, then r is nilpotent. Thus $r = s\alpha$ for some $s \in R$. But then $x = r\alpha^n = s\alpha\alpha^n = s\alpha^{n+1}$, contradicting the maximality of n. This completes the proof. □

Lemma 4 *Suppose that R is a finite local ring and that $Nil(R)$ is both nonzero and principal. Then R is a not a P-ring.*

Proof We assume that R has the above properties, and we suppose for the purpose of contradiction that R is a P-ring. Again, since R is finite and local, $Nil(R)$ is the unique maximal ideal of R, and every $x \in R\text{-}Nil(R)$ is a unit. Lemma 3 implies that $Nil(R) = \{u\alpha^n : u \in U(R), n > 0\}$. We define the following function f on R:

$$f(x) = \begin{cases} \alpha^n & \text{if } x = u\alpha^n \text{ for some unit } u \text{ and some positive integer } n, \\ 1 & \text{if } x \in U(R). \end{cases}$$

To conclude that f is a function, we must show that f is well-defined on $Nil(R)$. Toward this end, suppose that

$$u\alpha^i = u'\alpha^j, \tag{2.4}$$

where $u, u' \in U(R)$ and i, j are positive integers. We must show that $\alpha^i = \alpha^j$. Let k be the least positive integer for which $\alpha^k = 0$ (the *nilpotency* of α). Suppose first that $i \geq k$ or $j \geq k$. Without loss of generality, we may assume that $i \geq k$. Since $u\alpha^i = u'\alpha^j$ and since u' is a unit, it is clear that $\alpha^i = \alpha^j = 0$. Now assume that $i < k$ and $j < k$. To prove that $\alpha^i = \alpha^j$, clearly it suffices to show that $i = j$. Suppose not. Without loss of generality, suppose that $i < j$. Setting $\beta := (u')^{-1}u$, (2.4) becomes

$$\beta\alpha^i = \alpha^j. \tag{2.5}$$

An easy induction argument shows that

$$\beta^n\alpha^i = \alpha^{n(j-i)+i} \tag{2.6}$$

for all positive integers n. Choose n large enough so that $n(j-i)+i \geq k$. Then the right side of (2.6) above is zero, whence also $\beta^n\alpha^i = 0$. Since β^n is a unit, we deduce that $\alpha^i = 0$. But $i < k$, and this gives a contradiction to the minimality of k. We have shown that f is well-defined.

Now that we have shown that f is well-defined, it is a simple matter to check that f is an endomorphism of $(R, \cdot)$. Since we have assumed for the purposes of contradiction that R is a P-ring, we conclude that there exists a positive integer m such that $f(x) = x^m$ for every $x \in R$. In particular, $\alpha = f(\alpha) = \alpha^m$. Since $Nil(R) = \{u\alpha^n : u \in U(R), n > 0\}$ is nonzero, clearly $\alpha \neq 0$. But since $\alpha = \alpha^m$ and α is nonzero and nilpotent, we are forced to conclude that $m = 1$. Now let $u \in U(R)$ be arbitrary. Then $1 = f(u) = u^1 = u$. It follows that 1 is the *unique* unit of R. But α is nilpotent, whence $1 + \alpha$ is a unit. Thus $1 + \alpha = 1$, and $\alpha = 0$. This is a contradiction. Hence R cannot be a P-ring, and the proof is complete. □

We recall the following result of Gilmer (to which we alluded earlier) and then prove our main theorem.

Proposition 2 (Gilmer [4], Theorems 3 and 4) *Let R be a finite local ring. Then $U(R)$ is cyclic if and only if R is isomorphic to one of the following rings*:

(1) $\mathbb{F}_{p^n}$ (*the field of order* p^n),
(2) $\mathbb{Z}/\langle p^n\rangle$, *where* p *is an odd prime and* $n > 1$,
(3) $\mathbb{Z}/\langle 4\rangle$,
(4) $\mathbb{F}_p[x]/\langle x^2\rangle$,
(5) $\mathbb{F}_2[x]/\langle x^3\rangle$, *or*
(6) $\mathbb{Z}[x]/\langle 4, 2x, x^2 - 2\rangle$.

Theorem 1 *Let R be a ring. Then every multiplicative endomorphism $f : R \to R$ has the form $f(x) = x^m$ for some positive integer m if and only if R is a finite field.*

Proof Consider first a finite field F. Suppose that $f : F \to F$ is an endomorphism of $(F, \cdot)$. We will show that there exists a positive integer m such that $f(x) = x^m$ for all $x \in F$. We first claim that

$$\text{If } x \in F \text{ and } x \neq 0, \text{ then } f(x) \neq 0. \tag{2.7}$$

Suppose by way of contradiction that there exists some nonzero $a \in F$ such that $f(a) = 0$. Then note that $f(1) = f(aa^{-1}) = f(a)f(a^{-1}) = 0 \cdot f(a^{-1}) = 0$, and this contradicts $f(1) = 1$.

We conclude from (2.7) that f is an endomorphism of the cyclic group F^* (the group of nonzero elements of F under multiplication). Lemma 1 implies that there exists a positive integer m such that $f(x) = x^m$ for all $x \in F^*$. Since $f(0) = 0$, we see that $f(x) = x^m$ for all $x \in F$, and the proof of the first implication is complete.

Suppose now that R is a ring and that every endomorphism f of $(R, \cdot)$ is of the form $f(x) = x^m$ for some positive integer m. We will show that R is a finite field. Recall from Proposition 1 that R is a finite local ring and that $U(R)$ is cyclic. The proof will be complete if we can show that R is not isomorphic to any of the rings (2)–(6) of Proposition 2. Toward this end, it suffices by Lemma 4 to show that if R is any ring in families (2)–(6), then $Nil(R)$ is a principal ideal (all rings in families (2)–(6) have nonzero nilradical). Note that if R is a PID and I is an ideal of R, then R/I is a principal ideal ring. As $\mathbb{Z}$ and $\mathbb{F}_p[x]$ are PIDs, we conclude that any ring R in families (2)–(5) is a principal ideal ring. In particular, $Nil(R)$ is a principal ideal. Lastly, we must dispose of $R := \mathbb{Z}[x]/\langle 4, 2x, x^2 - 2\rangle$. As noted earlier, since R is finite and local, $Nil(R)$ is the unique maximal ideal of R. Let $I := \langle 4, 2x, x^2 - 2\rangle$. It is clear that $I \subseteq \langle 2, x\rangle$ and $\langle 2, x\rangle$ is a maximal ideal of $\mathbb{Z}[x]$. It follows that $Nil(R) = \langle 2, x\rangle/I$. Moreover, one checks easily that $\langle 2, x\rangle = \langle 2x, x^2 - 2, x + 2\rangle$. We conclude that $Nil(R) = \langle 2, x\rangle/I = \langle 2x, x^2 - 2, x + 2\rangle/I = \langle x + 2\rangle/I$. Hence $Nil(R)$ is a principal ideal, and the proof is complete. □

There is an alternate way to present the main result of this paper. A semigroup $(S, \cdot)$ is said to be a *ring semigroup* provided there exists an addition $+$ on S such that $(S, +, \cdot)$ is a ring. Such semigroups are well-studied in the literature. We refer the reader to Bell [1], Hannah [6], Jones [8], Ligh [9], Mazurek [10], and Oman [11], [12] for a sampling of what is known on ring semigroups. Theorem 1 can now be restated as follows:

Theorem 2 (Theorem 1, Alternate Version) *Let S be a commutative ring semigroup with $1 \neq 0$. Then every endomorphism of S is equal to a power function if and only if S is a cyclic group with 0 of order p^n for some prime number p and positive integer n.*

It is not hard to show (using the techniques presented in this paper) that if S is a commutative semigroup with $1 \neq 0$ and with no nonzero nilpotent elements, then every endomorphism of S is equal to a power function if and only if S is a finite cyclic group with 0. This leads naturally to the following more general problem:

Problem 1 Characterize the commutative semigroups S (with or without 0 or 1) with the property that every endomorphism of S is equal to a power function.

References

1. Bell, H.E.: Commutativity in ring semigroups. In: Words, Languages and Combinatorics, II, Kyoto, 1992, pp. 24–31. World Scientific, Singapore (1994)
2. Dugas, M., Mader, A., Vinsonhaler, C.: Large E-rings exist. J. Algebra **108**(1), 88–101 (1987)
3. Fuchs, L.: Abelian Groups. Publishing House of the Hungarian Academy of Sciences, Budapest (1958)
4. Gilmer, R.: Finite rings having a cyclic multiplicative group of units. Am. J. Math. **85**, 447–452 (1963)
5. Göbel, R., Herden, D., Shelah, S.: Absolute E-rings. Adv. Math. **226**(1), 235–253 (2011)
6. Hannah, J., Richardson, J.S., Zeleznikow, J.: Completely semisimple ring semigroups. J. Aust. Math. Soc. A **30**(2), 150–156 (1980)
7. Herden, D., Shelah, S.: An upper cardinal bound on absolute E-rings. Proc. Am. Math. Soc. **137**(9), 2843–2847 (2009)
8. Jones, P.: Rings with a certain condition on subsemigroups. Semigroup Forum **47**(1), 1–6 (1993)
9. Ligh, S.: On a class of semigroups admitting ring structure. Semigroup Forum **13**(1), 37–46 (1976/1977)
10. Mazurek, R.: On semigroups admitting ring structure. Semigroup Forum **83**(2), 335–342 (2011)
11. Oman, G.: Ring semigroups whose subsemigroups form a chain. Semigroup Forum **78**(2), 374–377 (2009)
12. Oman, G.: Ring semigroups whose subsemigroups intersect. Semigroup Forum **79**(2), 413–416 (2009)
13. Schultz, P.: The endomorphism ring of the additive group of a ring. J. Aust. Math. Soc. **15**, 60–69 (1973)