

RINGS SATISFYING CERTAIN CONDITIONS EITHER ON SUBSEMIGROUPS OR ON ENDOMORPHISMS

A. CHERUBINI and A. VARISCO

(Received 23 May 1984; revised 11 October 1984)

Communicated by R. Lidl

Abstract

We characterize rings whose multiplicative subsemigroups containing 0 and the additive inverse of each element are subrings. In addition we consider commutative rings for which every non-constant multiplicative endomorphism that preserves additive inverses is a ring endomorphism, and we show that they belong to one of three easily-described classes of rings.

1980 *Mathematics subject classification* (*Amer. Math. Soc.*): primary 20 M 25; secondary 16 A 48.

1. Introduction

In this paper we study associative rings R possessing one of the following properties.

(α) Every (multiplicative) subsemigroup S of R such that $0 \in S$, and such that $a \in S$ if and only if $-a \in S$ (for every $a \in R$), is a subring of R .

(β) Every non-constant semigroup endomorphism ϕ of R such that $\phi(-a) = -\phi(a)$ (for every $a \in R$) is a ring endomorphism.

Throughout the paper these rings will be called α -rings and β -rings, respectively.

The results here contained (Theorems 2.1 and 3.3) extends Theorem 1 of [9] and Theorem 1 of [11], respectively, which are in turn generalizations of theorems obtained in [4] by Cresp and Sullivan. In addition we observe that a different generalization of the work in [4] and [9] was furnished by Ligh in [8].

This work was supported by the Italian M.P.I.

© 1986 Australian Mathematical Society 0263-6115/86 \$A2.00 + 0.00

In what follows R will denote an associative ring, the term subsemigroup (subgroup) of R will mean multiplicative subsemigroup (subgroup), and the multiplicative semigroup of R will be denoted as usual by (R, \cdot) .

2. Subsemigroups

The main result of this section is the following characterization of α -rings.

THEOREM 2.1. *A ring R is an α -ring if and only if R belongs to one of the following types.*

- (i) R is a finite field of order $2^m = p + 1$, where p is prime and m is a positive integer.
- (ii) R is a finite field of order $3^m = 2p + 1$, where p is prime and m is a positive integer.
- (iii) R is a nil ring of order ≤ 3 .
- (iv) R is the ring of order 4 whose additive group is cyclic and generated by a with $a^2 = 2a$.

The proof of the theorem will utilize the following lemmas, where $2R$ ($3R$) denotes the set $\{2a \mid a \in R\}$ ($\{3a \mid a \in R\}$). Moreover, we shall put $[y] = \{y^h \mid h \in \mathbf{Z}^+\}$ and $-[y] = \{-y^h \mid h \in \mathbf{Z}^+\}$ ($y \in R$).

LEMMA 2.2. *If an α -ring R has a non-zero idempotent e , then either $2R = 0$ or $3R = 0$, and e is the identity of R .*

PROOF. Since R is an α -ring, the subset $\{0, e, -e\}$ is a subring and contains $2e$. Then, either $2e = 0$ or $3e = 0$. Let $2e = 0$. Then, for every $x \in R$, the subset $-[2x] \cup [2x] \cup \{0, e\}$ is a subring by Property (α), so it contains $e + 2x$. Since $e \neq 0$, it is immediate that $e + 2x = e$, whence $2R = 0$. Analogously, if $3e = 0$, then by investigating the subring $-[3x] \cup [3x] \cup \{0, e, -e\}$, we find that $3R = 0$. When $2R = 0$, every subsemigroup of R contains the additive inverses of its own elements; thus e is the identity of R by Lemma 2 of [9]. Now suppose $3R = 0$. Let $x \in R$, and put $a = xe - exe$. Since $a^2 = ea = 0$, $ae = a$, and R is an α -ring, the subset $\{0, e, -e, a, -a\}$ is a subring and contains $a + e$. Hence it immediately follows that $a = 0$, that is, $xe = exe$. By a similar argument it is proved that $ex = exe$, so e is a central idempotent. At this point, the subset $-[x - xe] \cup [x - xe] \cup \{0, e, -e\}$ is a subring, by Property (α), and it contains $x + e - xe$. Now it is immediate that $x + e - xe = e$, that is, $x = xe$, and that e is the identity of R .

LEMMA 2.3. *If R is an α -ring with identity, and $2R = 0$, then R is a finite field of order $2^m = p + 1$, where p is prime and m is a positive integer.*

PROOF. If $2R = 0$, every subsemigroup of R contains the additive inverses of its own elements. Therefore the statement follows from Theorem 2 of [4].

LEMMA 2.4. *If R is an α -ring with identity, and $3R = 0$, then R is a periodic field.*

PROOF. Let e be the identity of R . For every $x \in R \setminus 0$, the subset $-[x] \cup [x] \cup \{0, e, -e\}$ is a subring by Property (α) , so it contains $x + e$. Hence it easily follows that $x = x^2f(x)$ for some polynomial $f(\lambda) \in \mathbb{Z}[\lambda]$. Thus R is commutative by a well-known theorem of Herstein [6], it is periodic by a theorem of Chacron [1, Proposition 2], and (R, \cdot) is union of groups [3, Theorem 4.3]. Furthermore, the only idempotents of R are 0 and e by Lemma 2.2; thus we may immediately conclude that R is a periodic field.

LEMMA 2.5. *Let R be an α -field. If $3R = 0$, then R has a unique element of order 2, and every finite subgroup of even order has order $2p$ with p prime ≥ 1 .*

PROOF. Let e be the identity of R . Since $3e = 0$ implies $-e \neq e$, and $(-e)^2 = e$, it follows that R contains an element of order 2. Let f be any element of R having order 2; since R is an α -field, the subset $H = \{0, e, -e, f, -f\}$ is a subring and, obviously, a finite field. Thus $H \setminus 0$ is a finite cyclic group, with a unique element of order 2. Hence $f = -e$. Now let G be a finite subgroup of R having even order $2rs$ with $r > 1, s > 1$. Then G contains $-e$, whence $-x = -ex \in G$ for every $x \in G$. So, by Property (α) , $G \cup 0$ is a subfield of R . From this and from $3G = 0$, it follows that $|G \cup 0| = 3^j$ for some positive integer j . Therefore

$$(1) \quad 2rs = 3^j - 1 \quad (j > 1),$$

Moreover G , being an abelian group, contains a subgroup A of order $2r$ and a subgroup B of order $2s$. The same argument employed above for G shows that $A \cup 0$ and $B \cup 0$ are subfields of $G \cup 0$, of orders 3^h and 3^k , respectively, (h, k positive integers). Then we have

$$(2) \quad 2r = 3^h - 1, \quad 2s = 3^k - 1, \quad (h, k > 1),$$

and, using relations (2) in (1), we deduce that

$$3^j = 2rs + 1 = \frac{(3^h - 1)(3^k - 1)}{2} + 1 = \frac{3^{h+k} - 3^h - 3^k + 3}{2}.$$

This is a contradiction, since $h, k, j > 1$. So G must have order $2p$ with p prime ≥ 1 .

LEMMA 2.6. *Let R be an α -field. If $3R = 0$, then R is a finite field of order $3^m = 2p + 1$ with p prime, $p \geq 1$ and m a positive integer.*

PROOF. Let e be the identity of R . If $R = \{0, e, -e\}$, we have $|R| = 3$ and the statement is true. Otherwise, we have $R \setminus \{0, e, -e\} \neq \emptyset$. Let $x, y \in R \setminus \{0, e, -e\}$ and let $X = \langle x, -e \rangle$ and $Y = \langle y, -e \rangle$ be the subgroups generated by $x, -e$ and by $y, -e$, respectively. By Lemma 2.4, X and Y have finite orders, which, moreover, are even numbers, since $-e \in X \cap Y$. Consequently, $|X| = 2p$, $|Y| = 2q$ and $|X \cap Y| = 2r$ for some primes $p, q > 1$ and $r \geq 1$, in view of Lemma 2.5. Suppose $X \neq Y$. Since $2r$ divides both $2p$ and $2q$, we have either $r = 1$, or $r = p = q$. In the first case XY is a subgroup of order $2pq$, in contradiction to Lemma 2.5. In the second we have $X = X \cap Y = Y$, which is another contradiction. Thus $X = Y$, whence $R \setminus 0 = X$. At this point, we may conclude that $|R| = 2p + 1$. Moreover, $3R = 0$ implies that $|R| = 3^m$ for some positive integer m , which proves the statement.

REMARK 2.7. The primes of the form $2^m - 1$ which appear in Lemma 2.3 are the well-known Mersenne primes, where m is necessarily prime. Analogously, it is easily verifiable that, if p is a prime and m a positive integer satisfying the condition $3^m = 2p + 1$, then m must be prime. In fact, suppose $m > 1$ and put $m = hq$ with q prime > 1 and h positive integer. Then $2p = 3^{hq} - 1 = (3^h - 1)(3^{h(q-1)} + \dots + 3^h + 1)$, whence $3^h - 1 = 2$. Thus $h = 1$, and $m = q$ is prime. Pairs (m, p) satisfying the above condition do actually exist; we include a small table of such pairs

m	1	3	7	13	...
p	1	13	1093	797161	...

LEMMA 2.8. *Let R be an α -ring without non-zero idempotents. Then, for every $x \in R$, either $x^2 = 0$ or $x^2 = 2x$.*

PROOF. Let $|R| > 1$, and let $x \in R \setminus 0$. The subset $H = -[x] \cup [x] \cup \{0\}$ is a subring by Property (α) and contains $x - x^2$. Since $x \neq x^2$, we have either $x - x^2 = x^h$ or $x - x^2 = -x^h$ for some positive integer h . If $h > 1$, we have $x = x^2 f(x) = x f(x) x$ for some polynomial $f(\lambda) \in \mathbf{Z}[\lambda]$, and $x f(x)$ is a non-zero idempotent, which is a contradiction. Thus, for every $x \in R$, we have either $x^2 = 0$ or $x^2 = 2x$.

In what follows we shall denote by R^2 the set $\{xy | x, y \in R\}$.

LEMMA 2.9. *Let R be an α -ring without non-zero idempotents. Then either $R^2 = 0$ and $|R| \leq 3$, or R is the ring of order 4 whose additive group is cyclic generated by an element a satisfying the relation $a^2 = 2a$.*

PROOF. Let $x \in R$ with $x^2 = 0$. Then the subset $\{0, x, -x\}$ is a subring by Property (α), and it contains $2x$. Hence it easily follows that either $2x = 0$ or $3x = 0$. Next, let $y \in R$ with $y^2 \neq 0$. Then from Lemma 2.8 it follows that $y^2 = 2y$ and $(-y)^2 = -2y$, whence $y^2 = 2y = -2y$, and also $y^3 = 2y^2 = 4y = 0$. At this point we may distinguish two cases:

(1) R satisfies the identity $x^2 = 0$. Then, for every $x \in R$, we have either $2x = 0$ or $3x = 0$. Since the subsets $H = \{x \in R \mid 2x = 0\}$ and $K = \{x \in R \mid 3x = 0\}$ are additive subgroups of $R = H \cup K$, we must have either $R = H$ or $R = K$. In the first case, every subsemigroup of R contains the zero and the additive inverses of its own elements. So, $R^2 = 0$ and $|R| \leq 2$ follows from Theorem 1 of [4]. If $R = K$, let us suppose $|R| > 1$ and let $x, y \in R \setminus \{0\}$. Then we have $0 = (x + y)^2 = xy + yx$, whence $xyx = 0$. Therefore, the subset $\{0, x, -x, xy, -xy\}$ is a subring by Property (α), and it contains $x + xy$. This implies that $xy = 0$. Hence, the subset $\{0, x, -x, y, -y\}$ is also a subring by Property (α), and it contains $x + y$. Now it is immediate that either $y = x$ or $y = -x$. Thus $R = \{0, x, -x\}$ and this implies that $R^2 = 0$ and $|R| = 3$.

(2) R contains an element y such that $y^2 \neq 0$. Then $4y = 0$ and, for every $w \in R$, we must have either $4w = 0$ or $3w = 0$. Repeating the argument used in (1), we see that $4w = 0$ for every $w \in R$. Now, for every $x \in R \setminus \{0\}$ with $x^2 = 0$, we have $2x = 0$. Consequently the subset $\{0, x, 2y\}$ is a subring by Property (α), and it contains $x + 2y$. Hence it easily follows that $x = 2y$, and that $2y$ is the unique element of R with index of nilpotence 2. Now, for every $z \in R$ with $z^2 \neq 0$, we have $z^2 = 2z = 2y$. Hence, $(yz)^2 \neq 0$ implies that $(yx)^2 = 2yz = z^3 = 0$, which is a contradiction. So we must have $(yz)^2 = 0$, whence $yz = 2y$. In the same way we find that $zy = 2y$; thus the subset $\{0, y, -y, z, -z, 2y\}$ is a subring by Property (α), and it contains $y + z$. At this point it is immediate that either $z = y$ or $z = -y$. So $R = \{0, y, -y, 2y\}$ is the ring of order 4 described in the lemma.

PROOF OF THEOREM 2.1. From the preceding lemmas we immediately deduce that every α -ring belongs to one of the types listed in the statement. The converse is immediately verifiable.

REMARK 2.10. Let R be a field of order $3^m (m \geq 1)$ with identity e . Since $3e = 0$, we have $2e \in R \setminus \{0, e\}$; thus R has a subsemigroup containing the zero which is not a subring. Next, let R be a nil ring of order 3. Since the additive

group of R is cyclic, we have $R = \{0, a, -a\}$ and $a^2 = 0$. Hence the subset $\{0, a\}$ is a subsemigroup of R containing the zero, but it is not a subring. Finally, let R be the ring of order 4 with the additive group generated by an element a satisfying the relation $a^2 = 2a$. It is immediate that the subset $\{0, a, 2a\}$ is a subsemigroup of R but not a subring. That being stated, let R be a ring all of whose subsemigroups containing the zero are subrings. Obviously, R is a α -ring, and consequently it is one of the rings listed in the statement of Theorem 2.1. But from the above it follows that if $|R| > 2$, then R is necessarily a field of order $2^m = p + 1$, where p is a prime [9, Theorem 1].

3. Endomorphisms

The purpose of this section is to describe commutative β -rings. We recall that an ideal I of a ring R is said to be *completely prime* if $a, b \in R$, $ab \in I$ imply $a \in I$ or $b \in I$. R is *completely prime* if the zero ideal is a completely prime ideal in R .

LEMMA 3.1. *Let R be a β -ring. If I is a proper, completely prime ideal of R , then $I = 0$.*

The proof is analogous to that of [7, Lemma 1].

In what follows we shall use the terminology of [10].

LEMMA 3.2. *Let R be a β -ring. If (R, \cdot) is a semilattice of archimedean semigroups, then either R is completely prime or R is a nil ring.*

PROOF. From [2, Theorem A and Theorem 1.3] it follows either that (R, \cdot) is archimedean, or that it contains a proper, completely prime semigroup ideal I . (We remark that in [2] the term “prime” stands for “completely prime”.) In the first case R is obviously a nil ring. In the second case, let ϕ be the map of R into R defined by $\phi(x) = 0$ for $x \in I$, and $\phi(x) = x$ for $x \in R \setminus I$. It is easily seen that ϕ is a non-constant semigroup endomorphism of R , and that $x \in I$ if and only if $-x \in I$. Hence $\phi(-x) = -\phi(x)$ and, since R is a β -ring, ϕ is a ring endomorphism whose kernel is I . Thus I is a ring ideal. Hence $I = 0$ by Lemma 3.1, and so R is completely prime.

Now we are able to state the following.

THEOREM 3.3. *A commutative β -ring belongs to one of the following types*

- (i) R is a ring of order ≤ 3 ;
- (ii) R is the ring of order 4 whose additive group is cyclic generated by a with $a^2 = 2a$;

(iii) $R = R^2$ is the direct sum of a ring P satisfying the identities $x^2 = 2x = 0$ and a ring Q satisfying the identities $x^3 = 3x = 0$.

PROOF. Let χ be the map of R in R defined by $\chi(a) = a^3$ for every $a \in R$. If χ is non-constant, then, since R is a commutative β -ring, χ is a ring endomorphism. Then R satisfies the identity

$$(3) \quad (a + b)^3 = a^3 + b^3.$$

If χ is constant, we have $a^3 = \chi(a) = \chi(0) = 0$, and (3) continues to hold. Analogously, utilizing the map ψ defined by $\psi(a) = a^5$ ($a \in R$), we obtain the identity

$$(4) \quad (a + b)^5 = a^5 + b^5.$$

Now we recall that, since R is commutative, (R, \cdot) is a semilattice of archimedean semigroups [3, Theorem 4.13]; consequently R is either completely prime or a nil ring, by Lemma 3.2. In the first case, if $|R| > 1$, we obtain from (3) that $3a + 3b = 0$ for every $a, b \in R \setminus 0$. Hence, when $a = b$, it follows that $6a = 0$. Utilizing these relations in (4), we find that $a^3 - a^2b - ab^2 + b^3 = 0$. Replacing a by $-a$ and summing the two relations, we obtain $2a^2b - 2b^3 = 0$, whence $2a^2 = 2b^2$. Moreover, $3a + 3b = 0$ implies that $9a^2 = 9b^2$, whence $a^2 = b^2$. Now if $a + b \neq 0$, then $(a + b)(a - b) = 0$ implies that $a = b$. Therefore, either $R = \{0, a\}$ or $R = \{0, a, -a\}$. Now let us suppose that R is a nil ring. If $R^2 \subset R$, let a be an element of $R \setminus R^2$, h the least positive integer such that $a^{2h} = 0$, and $J = R \setminus \{a, -a\}$. Let $\phi: R \rightarrow R$ be defined by $\phi(a) = a^h$, $\phi(-a) = -a^h$ and $\phi(x) = 0$ otherwise. Then ϕ is non-constant, and it is a ring endomorphism by Property (β) . Therefore, for every $x \in J$, we have $\phi(a + x) = a^h \neq 0$. Hence, either $a + x = a$ or $a + x = -a$, whence either $x = 0$ or $x = -2a$. So we have $R = \{0, a, -a, -2a\}$. At this point, either $|R| \leq 3$ or the elements $0, a, -a, -2a$ are distinct; in this case the additive group of R is cyclic, and $-2a = 2a$. Moreover, we cannot have $a^2 = 0$, since then we would have $h = 1$, whence $\phi(2a) = 2\phi(a) = 2a$, and $2a \in \{0, a, -a\}$, which is a contradiction. Thus $a^2 \neq 0$, and it is immediate that $a^2 = 2a$. Finally, we have to examine the case $R = R^2$. First, let us verify that $x^3 = 3x^2 = 6x = 0$ for every $x \in R$. In fact, putting $b = a^2$ in (3) and (4), we find that $3a^4 + 3a^5 = 0$ and $5a^6 + 10a^7 + 10a^8 + 5a^9 = 0$, whence $3a^4 = 5a^6 = 0$, and consequently $a^6 = 0$. Then $(a + b)^6 = 0$ for every $a, b \in R$ and, using again $3a^4 = a^6 = 0$, we obtain $20a^3b^3 = 0$. Moreover, from (3) it follows that $3a^2b + 3ab^2 = 0$, whence $3a^3b^3 = -3a^4b^2 = 0$. Therefore $a^3b^3 = 0$, and this, in view of the fact that $R = R^2$, implies that $x^3 = 0$ for every $x \in R$. Now $3a^2b + 3ab^2 = 0$ implies that $3a^2b^2 = 0$, whence $3x^2 = 0$ for every $x \in R$. Finally, $3(a + b)^2 = 0$ implies that $6ab = 0$, that is, $6x = 0$ for every $x \in R$. That being stated, we let $P = \{x \in R \mid 2x = 0\}$, and we let $Q = \{x \in R \mid 3x = 0\}$.

It is immediate that P and Q are ring ideals of R , that $P \cap Q = 0$ and that, for every $x \in R$, we have $x = 7x = 3x + 4x$, with $3x \in P$ and $4x \in Q$. Therefore R is the direct sum of P and Q . For every $x \in P$, we have $2x^2 = 0$ and, since we have shown that $3x^2 = 0$, we may conclude that $x^2 = 0$. So the proof is complete.

REMARK 3.4. It is immediate that the rings of types (i) and (ii) described in the statement of Theorem 3.3 are β -rings. As regards the rings of type (iii), Duncan and Macdonald have shown in [5] that rings like P (called *power rings* in [11]) do exist. A similar argument can be used to show that rings like Q also exist. At this point, the existence of rings satisfying condition (iii) is assured. But we do not know whether they are β -rings, and it is still not known whether power rings are ϵ' -rings.

REMARK 3.5. From Theorem 3.3 we may easily deduce Theorem 1 of [11]. In fact, if R is a ring of order 3, we have necessarily $R = \{0, a, -a\}$, and it is easily seen that the map ϕ defined by $\phi(0) = 0$, and $\phi(a) = \phi(-a)$ is a non-constant semigroup endomorphism which does not preserve addition. The same result may be obtained when R is the ring of type (ii), with the map ϕ defined by $\phi(0) = 0$, $\phi(a) = \phi(-a) = a$, and $\phi(2a) = 2a$. Further, let us suppose that R is a commutative ring with the property (ϵ') introduced in [11]. Obviously, R is a β -ring and, if $|R| > 2$, it follows from the above that R is of type (iii). Now the function ϕ defined by $\phi(x) = x^2$ for every $x \in R$ is a ring endomorphism by property (ϵ'), and it induces in R the identity $(a + b)^2 = a^2 + b^2$, whence $2ab = 0$. Since $R = R^2$, this implies that $2x = 0$ for every $x \in R$. Thus $Q = 0$, and $R = P$ is a power ring.

REMARK 3.6. In Theorem 3.3 the hypothesis of commutativity may be weakened. Following the terminology used for semigroups, we say that a ring R is *medial* if $abcd = acbd$ for every $a, b, c, d \in R$. A medial ring need not be commutative, as is shown by the ring of real square matrices of the form $\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$. The authors have proved that Theorem 3.3 continues to hold if the word “commutative” is replaced by “medial”, but the proof is here omitted.

References

- [1] M. Chacron, “On a theorem of Herstein”, *Canad. J. Math* **21** (1969), 1348–1353.
- [2] A. Cherubini and A. Varisco, “On Putcha’s Q -semigroups”, *Semigroup Forum* **18** (1979), 313–317.
- [3] A. H. Clifford and G. B. Preston, *The algebraic theory of semigroups* (Amer. Math. Soc., Providence, R. I., Vol. 1, 1961).

- [4] J. Cresp and R. P. Sullivan, "Semigroups in rings", *J. Austral. Math. Soc. (Ser. A)* **20** (1969), 172–177.
- [5] J. Duncan and I. D. Macdonald, "Some factorable nil rings of characteristic two", *Proc. Roy. Soc. Edinburgh Sect. A*, **82** (1979), 193–199.
- [6] I. N. Herstein, "The structure of a certain class of rings", *Amer. J. Math.* **75** (1953), 864–871.
- [7] Y. Hirano and H. Tominaga, "On rings whose non-constant semigroup endomorphisms are ring endomorphisms", *Math. J. Okayama Univ.* **23** (1981), 13–16.
- [8] S. Ligh, "On a class of semigroups admitting ring structure", *Semigroup Forum* **13** (1976), 37–46.
- [9] S. Ligh, "A note on semigroups in rings", *J. Austral. Math. Soc. (Ser. A)* **24** (1977), 305–308.
- [10] M. S. Putcha, "Semilattice decompositions of semigroups", *Semigroup Forum* **6** (1973), 12–34.
- [11] R. P. Sullivan, "Semigroup endomorphisms of rings", *J. Austral. Math. Soc. (Ser. A)* **26** (1978), 319–322.

Dipartimento di Matematica
Politecnico di Milano
Piazza Leonardo da Vinci 32
20133 Milano
Italy