On $E_k$-rings


Persistent URL: http://dml.cz/dmlcz/102241

Terms of use:

© Institute of Mathematics AS CR, 1988

Institute of Mathematics of the Czech Academy of Sciences provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these Terms of use.
ON $E_k$-RINGS

Alessandra Cherubini and Ada Varisco, Milano*)

(Received May 12, 1986)

In [4] a non idempotent semigroup $S$ has been called an $E_k$-semigroup ($k$ positive integer) if every subsemigroup of $S$ containing $k$ idempotents either is idempotent or contains all the idempotents of $S$. A similar definition can be given for rings, merely substituting the word "semigroup" by the word "ring". But, since every subring of a ring $R$ always contains an idempotent, namely the zero of $R$, we prefer to modify the definition slightly in the following way.

Let $R$ be a non idempotent ring, with set of idempotents $E$, and $|E| > 1$. For every positive integer $k$ we shall say that $R$ is an $E_k$-ring if every subring of $R$ containing $k$ non zero idempotents either contains $E$ or is contained in $E$. We shall call trivial $E_k$-rings those for which $|E| = k + 1$.

In the first part of this note we shall prove that the only $E_1$-rings are the trivial ones. The second part is devoted to characterize non-trivial $E_2$-rings, whose actual existence is shown by some examples.

Throughout this paper $Z$ will denote the center of the ring $R$ and $E$ the set of idempotents of $R$. The term "subsemigroup of $R" means "multiplicative subsemigroup"," and $(R, \cdot)$ denotes as usual the multiplicative semigroup of $R$. Non defined terminology may be found in [6] and [7].

1. $E_1$-RINGS

The purpose of this section is to prove the following.

**Theorem 1.1.** $R$ in an $E_1$-ring if and only if $E$ is a proper subset of $R$ having order two.

The proof of the theorem will be preceded by some Lemmas.

**Lemma 1.1.** If $R$ is a non-trivial $E_1$-ring, then $E$ is a subsemigroup of $R$, and $Re = 0$ for every $e \in E$.

**Proof.** Let $e, f \in E \setminus 0$. Then we have either $eR \supseteq E$ or $eR \subseteq E$, and in both cases we immediately see that $ef \in E$. Thus $E$ is a subsemigroup of $R$. Now, let

*) This work is supported by the Italian M.P.I.
\( u \in E \) with \( 2u \neq 0 \). Then \( 2u \in R \setminus E \), hence \( uR \cap Ru \supseteq E \) and \( u \) is the identity of \( E \). From the uniqueness of the identity it follows that \( 2e = 0 \) for every \( e \in E \setminus u \). Since \( |E| > 2 \), there exists \( e \in E \setminus \{0, u\} \), and we have \((e + u)^2 = e + 2eu + u = e + u + u \neq e + u \), whence \( 2(e + u) = 0 \) and \( 2u = 0 \), a contradiction.

**Lemma 1.2.** If \( R \) is a non-trivial \( E_1 \)-ring, then \( E \) is not commutative.

**Proof.** Suppose that \( E \) is commutative. Then, for every \( e, f \in E \), we have \((e + f)^2 = e + f \) (Lemma 1.1), hence \( E \) is a subring of \( R \). Moreover, it is well-known that \( E \) is contained in the center. At this point there are two cases, each of which leads to a contradiction.

1) \( E \) is not an ideal. Since \( E \subseteq Z \), we have \( uR \not\subseteq E \) for some \( u \in E \). Then \( uR \supseteq E \), hence \( u \) is the identity of \( E \). From the uniqueness of the identity it follows that \( eR \subseteq E \) for every \( e \in E \setminus u \). Now, taking \( e \in E \setminus \{u, 0\} \), we have \( u + e \in E \setminus u \), whence \( uR \subseteq E \), a contradiction.

2) \( E \) is an ideal. Let us preliminarily show that \( ae \neq 0 \) for every \( a \in R \setminus E, e \in E \). In fact, suppose that \( ae = 0 \) for some \( a \in R \setminus E, e \in E \), and consider the subring \( \langle a, e \rangle \) generated by \( a \) and \( e \). Since there exists \( f \in E \setminus \{e, 0\} \), and \( \langle a, e \rangle \supseteq E \), there is a polynomial \( P(t) \in Z[t] \) with zero constant term, such that \( f = P(a) + he \), where \( h \in Z_2 \) (Lemma 1.1). Hence \( P(a) \in E \setminus 0 \). Moreover, \( P(a) e = 0 \). Thus the annihilator \( A(e) \) contains \( E \), whence \( e = 0 \), a contradiction. Then \( ae \neq 0 \) for every \( a \in R \setminus E, e \in E \). Now, since \( E \) is an ideal, we have \( ae = (ae)^2 = a^2e \), whence \( ae(a - e) = 0 \). But this contradicts the fact that \( ae \in E \setminus 0 \) and \( a - e \in R \setminus E \).

**Lemma 1.3.** If \( R \) is a non-trivial \( E_1 \)-ring, then \( E \setminus 0 \) is a left (right) zero semigroup of order 2.

**Proof.** Since \( E \) is not commutative (Lemma 1.2), there exist \( e, f \in E \) such that \( ef \neq fe \). Then, we may suppose that \( fe \neq efe \) and, since \( fe - efe \) is nilpotent, the subring \( \langle e, fe - efe \rangle \) contains \( E \). On the other hand, we have \( \langle e, fe - efe \rangle = \{0, e, fe - efe, e + fe - efe\} \), whence \( E = \{0, e, e + fe - efe\} \). Thus \( f = e + fe - efe \) and \( ef = e, fe = f \). Analogously, if \( ef \neq efe \), \( E \setminus 0 \) turns out to be a right zero semigroup.

**Proof of theorem 1.1.** Let \( R \) be an \( E_1 \)-ring. If \( R \) is not trivial, \( E \setminus 0 \) is a left (right) zero semigroup of order 2, by Lemma 1.3. Suppose that \( E \setminus 0 \) is a left zero semigroup and that \( E = \{0, e, f\} \). Since \( eR \supseteq E \) implies that \( e \) is a left identity of \( E \), it must be \( eR \subseteq E \). Then, for every \( a \in R \), we have \( ea = e(ea) = e \), whence \( (ae)^2 = ae \), which implies \( Re \subseteq E \). At this point we have \( e + f = (e + f) e \in E \), a contradiction. The converse is obvious.

2. STRUCTURE OF \( E_2 \)-RINGS

In this section we shall study non-trivial \( E_2 \)-rings, which will be characterized by the following theorem.
Theorem 2.1. R is a non-trivial $E_2$-ring if and only if E is a proper subsemigroup of $R$ satisfying one of the following conditions:

i) $E$ is commutative of order 4 with identity.

ii) $E \setminus 0$ is a left (right) zero semigroup of prime order $p > 2$, and there are two elements $e, a \in E \setminus 0$ such that $E \setminus 0 = \{e + ka | k = 0, 1, \ldots, p - 1\}$.

In preparation for the proof of the theorem, we establish the following Lemmas.

Lemma 2.1. A finite Boolean ring has the identity ([5], Theorem 39).

Lemma 2.2. Let R be a non-trivial $E_2$-ring. If E is commutative, then E is a subsemigroup of $R$ of order 4, with identity.

Proof. First of all, let us recall that E, being commutative, is a subsemigroup of $R$ contained in the center. That being established, we have to examine the two following cases.

1) $E$ is not an ideal. Since $E \subseteq Z$, we have $eR \neq E$ for some $e \in E$. Then, let $f \in E \setminus \{0, e\}$. Now, if $ef \in E \setminus \{0, e\}$, we get $eR \supset E$, which implies that e is the identity of $E$. Then, suppose $ef = e$. Since $eR + fR \supset E$, for every $u \in E$ there exist $x, y \in R$ such that $u = ex + fy$. Consequently, $fu = fex + fyu = u$, hence u is the identity of E. Finally, if $ef = 0$, we have $e + f \in E \setminus \{0, e\}$. Then, $eR + (e + f)R \supset E$, and for every $u \in E$, there exist $z, w \in R$ such that $u = ez + (e + f)w$. Thus $(e + f)u = (e + f)ez + (e + f)w = u$, hence $e + f$ is the identity of E. At this point, we have proved that in any case E has the identity, which will be denoted by 1. Moreover, the idempotent e for which $eR \supsetneq E$ may be supposed different from 1. In fact, if $uR \subseteq E$ would hold for every $u \in E \setminus \{0, 1\}$, we should have also $(1 - u)R \subseteq E$, since $1 - u \in E \setminus \{0, 1\}$. But this should imply $1R \subseteq E$, whence $eR \subseteq E$ for every $e \in E$, a contradiction. Now, let us suppose that E has order greater than 4. This means that, in addition to the four idempotents 0, 1, $e$, $1 - e$, there exists another idempotent $f$. Moreover, $1 - f$ is also an idempotent distinct from all the preceding. Eventually exchanging $f$ with $1 - f$, we may suppose $ef \neq 0$. Now, we cannot have $ef = e$, since this would imply $eR \supset E$, and e would be the identity of E, while $e \neq 1$. Thus $ef = e$. But, in this case we have $Rf \supset E$, since $Rf$ contains the distinct idempotents f and $ef = e$, and $Rf \supsetneq Re$; so $f$ is the identity of E, contrary to $f \neq 1$. Thus we have proved that $|E| = 4$.

2) $E$ is an ideal. If we show that $|E| = 4$, E turns out to be a finite Boolean ring, and the statement follows from Lemma 2.1. Thus we may suppose $|E| > 4$, and start by proving that there exist two idempotents $e, f$ such that

\[ e \text{ is not the identity of } E, \]
\[ ef \in E \setminus \{0, e\} \]

In fact, it is easily seen that $E$ contains two elements $u, v$ such that $u, v, u + v$ are distinct from each other, from zero and from the eventual identity. Now, if $uv \in E \setminus \{0, u\}$, it is enough to take $e = u, f = v$. If $uv = u$, it suffices to take $e = v, f = u$. Finally, if $uv = 0$, we have $u(u + v) = u$, hence we may take $e = u + v,$
Let \( f = u \). That being stated, let \( a \) be an element of \( R \setminus E \). Then, the subring \( \langle a, e, ef \rangle \) generated by \( a, e, ef \) contains \( E \); consequently, for every \( w \in E \), there exist an element \( b \in R \) and a polynomial \( P(t) \in \mathbb{Z}[t] \) with zero constant term, such that \( w = P(a) + eb \). Since \( e \) is not the identity of \( E \), by (1), we have \( P(a) \neq 0 \) for at least an idempotent \( w \). Moreover, since \( E \) is an ideal, we have \( P(a) = w - eb \in E \). Thus \( P(a) \in E \setminus 0 \). At this point we have shown that, for every \( a \in R \), there exists a polynomial \( P(t) \in \mathbb{Z}[t] \) with zero constant term, such that \( P(a) \in E \setminus 0 \). Now, let us verify that \( 2a = 0 \) for every \( a \in R \). For the elements of \( E \) this is induced by the fact that \( E \) is an ideal, so we may suppose \( a \in R \setminus E \). If \( 2a \in E \), we have \( 4a = 0 \), whence \( 2a = 4a^2 = 0 \). If, on the contrary, \( 2a \in R \setminus E \), from the above it follows that there exists a polynomial \( P(t) \in \mathbb{Z}[t] \) with zero constant term, such that \( P(2a) \in E \setminus 0 \). But \( P(2a) = 2Q(a) \) for some \( Q(t) \in \mathbb{Z}[t] \) and, since \( 2P(2a) = 0 \), we have \( P(2a) = 2^2[Q(a)]^2 = 2P(2a)Q(a) = 0 \), a contradiction. This result, together with the preceding, allows us to conclude that every element of \( R \) is an algebraic co-integer, hence \( R \) is a periodic ring by Proposition 2 of [2]. Now, let us recall that in a ring every periodic element is the sum of a potent element (i.e. an element \( x \) such that \( x = x^m \) for some integer \( m > 1 \)) and a nilpotent (see [1], Lemma). If \( R \) contains some nilpotent, then there exists \( a \in R \) with \( a^2 = 0 \), and the subring \( \langle a, e, ef \rangle \) contains \( E \), as above remarked. But, since \( ae = (ae)^2 = a^2e = 0 \), we have \( \langle a, e, ef \rangle = \{ha + ke + jef \mid h, k, j \in \mathbb{Z}_2\} \), whence \( E = \{0, e, ef, e + ef\} \), contrary to \( |E| > 4 \). Thus, every element of \( R \) is potent. Then, for every \( x \in R \), there exists an integer \( m > 1 \) such that \( x = x^m = xx^{m-1} \in E \), since \( x^{m-1} \) is idempotent. This implies \( R = E \), which contradicts the hypothesis.

**Lemma 2.3.** Let \( R \) be a non-trivial \( E_2 \)-ring. If \( E \setminus Z \neq \emptyset \), the elements of \( E \setminus Z \) are all right identities (all left identities).

**Proof.** Let \( e \in E \setminus Z \). Then, \( ex = xe \) for some \( x \in R \). If \( xe \neq exe \), the subring \( Re \) contains the distinct idempotents \( 0, e, e + xe - exe \) and the nilpotent \( xe - exe \), hence \( Re \supset E \), and \( e \) is a right identity of \( E \). If, on the contrary, \( xe = exe \), we obviously have \( ex \neq exe \), and in the same way we may conclude that \( e \) is a left identity of \( E \). Since a right and a left identity may not co-exist, the statement is proved.

**Lemma 2.4.** Let \( R \) be a non-trivial \( E_2 \)-ring. If \( E \) is not commutative, then \( E \setminus 0 \) is a left (right) zero semigroup.

**Proof.** If \( Z \cap E = 0 \), the statement easily follows from Lemma 2.3. Otherwise, there exist \( u \in E \setminus Z \) and \( v \in (E \cap Z) \setminus 0 \). Since the subring \( \langle u, v \rangle \), which is commutative, cannot contain \( E \), it must be \( \langle u, v \rangle \subseteq E \). Thus \( 2u = 0 \), and we have \( (u + v)^2 = u + v \). Moreover, \( u + v \in Z \) implies \( u \in Z \), in contradiction with the hypothesis; so it must be \( u + v \in E \setminus Z \). Hence, by Lemma 2.3, we have \( v = v(u + v) = uv + v = 2v \), another contradiction.

**Lemma 2.5.** Let \( R \) be a ring with set of idempotents \( E \). If \( E \setminus 0 \) is a left (right)
zero semigroup, and $e, f \in E \setminus 0$, putting $a = f - e$, we have $a^2 = 0$, $ea = 0$, $ae = a$ ($a^2 = 0$, $ae = 0$, $ea = a$).

The proof is immediate.

**Lemma 2.6.** Let $R$ be a non-trivial $E_2$-ring. If $E \setminus 0$ is a left (right) zero semigroup, there exist a prime $p > 2$, an element $e \in E \setminus 0$ and an element $a \in R \setminus 0$, such that $E \setminus 0 = \{e + ka \mid k = 0, 1, \ldots, p - 1\}$.

**Proof.** Let $e, f$ be two distinct element of $E \setminus 0$. Since $(f - e)^2 = 0 \neq f - e$, the subring $\langle e, f \rangle$ contains $E$. Then, for every $u \in E \setminus 0$ there exist two positive integers $h, k$ such that $u = he + kf$, whence $(h + k - 1)e = 0$. Then we have $u = e + (h - 1)e + kf = e + k(f - e)$, hence, putting $f - e = a$, we find $u = e + ka$. Moreover, making use of Lemma 2.5, we have $(e + ja)^2 = e + ja = 0$ for every integer $j$; consequently $E \setminus 0 = \{e + ka \mid k \in \mathbb{Z}\}$. Now, let us suppose that $na \neq 0$ for every integer $n$. Then, the two idempotents $e$ and $e + 2a$ are distinct. Moreover, $2a$ is not idempotent, since $2a \neq 0$. Thus, $\langle e, e + 2a \rangle \supset E$. Then, $a = f - e \in \langle e, e + 2a \rangle$ and there exist two integers $\alpha, \beta$ such that $a = \alpha e + \beta(e + 2a)$. Since $\alpha e = 0$, by Lemma 2.5, we easily obtain $2\beta - 1 \alpha = 0$, which contradicts the hypothesis. Therefore $a$ has finite additive order $r$. If $r$ is not prime, suppose that $p$ is a prime factor of $r$. Since $pa \in R \setminus E$, the subring $H = \langle e, e + pa \rangle$ contains $E$, hence $a \in H$. Then there exist two positive integers $\gamma, \delta$ such that $a = \gamma e + \delta(e + pa)$. In the same way as above, we find $(\delta p - 1) a = 0$, hence it follows that $\delta p - 1 \equiv 0 \mod r$, in contradiction to the fact that $p$ divides $r$. At this point we may conclude that $E \setminus 0 = \{e + ka \mid k = 0, 1, \ldots, p - 1\}$, and $|E| = p + 1$ for some prime $p$. Since $p = 2$ implies $|E| = 3$, $p$ must be odd. Thus the statement is completely proved.

**Proof of Theorem 2.1.** The “only if part” easily follows from the preceding Lemmas, so it suffices to prove the “if part”. Suppose that $R$ is a ring satisfying condition i) of the statement. Then we have necessarily $E = \{0, 1, e, 1 - e\}$ and every subring of $R$ containing $E$ contains the whole $E$; so $R$ is a non-trivial $E_2$-ring. Now, suppose that $R$ satisfies condition ii), and let $A$ be a subring of $R$ containing two distinct non zero idempotents $u, v$. Then, we may assume that $u = e + ka, v = e + ja$ with $k, j$ integers and $0 \leq k < j < p$. Let us show that $a$ is an element of $A$. In fact, we have: $(j - k)a = v - u \in A$, where $(j - k, p) = 1$. Consequently, there exist two integers $\lambda, \mu$ such that $1 = \lambda p + \mu(j - k)$, hence $a = \lambda pa + \mu(j - k)a$. Now, let us verify that $pa = 0$. Making use of Lemma 2.5, we have $(e + pa)^2 = e + pa = 0$, whence $e + pa = e + ka$ for some integer $k$ with $0 \leq k < p$. If $k = 0$, we obviously have $pa = 0$. If $k \neq 0$, we have $(p - k)a = 0$, in contradiction to the fact that $|E| = p + 1$. At this point, $a = \mu(j - k)a \in A$; moreover, $e = u - k \in A$, hence $E \subset A$. Thus $R$ is a non-trivial $E_2$-ring.

**Remark.** From the proof of the “if part” of Theorem 2.1, we may easily derive
the following proposition: A non idempotent ring $R$ is a non-trivial $E_2$-ring if and only if every subring of $R$ containing two distinct non zero idempotents contains $E$.

Now, we shall consider the particular case of regular $E_2$-rings, for which the following characterization holds.

**Theorem 2.2.** $R$ is a non-trivial regular $E_2$-ring if and only if it is the direct sum of two division rings and $|R| > 4$.

**Proof.** If $R$ is the direct sum of two division rings, it is immediate that $R$ is regular. Moreover, $R$ has exactly four idempotents, which form a commutative semigroup with identity. Thus, since $|R| > 4$, $R$ turns out to be a non-trivial regular $E_2$-ring, by Theorem 2.1.

Conversely, let $R$ be a non-trivial regular $E_2$-ring. If $E$ is not commutative, by Theorem 2.1, we may assume that $E \setminus 0$ is a left zero semigroup. Let $e, f$ be two distinct non zero idempotents. Then we have $e - f = (e - f)x(e - f)$ for some $x \in R$. But $u = (e - f)x$ is idempotent, hence $e - f = u(e - f) = ue - uf = 0$, a contradiction. Therefore, by Theorem 2.1, $E = \{0, 1, e, 1 - e\}$ is commutative, hence $E \subseteq Z$. Then $(R, \cdot)$ is a union of four groups $G_0 = 0, G_1, G_e, G_{1-e}$ (see e.g. Theorem IV.1.6 of [7]). On the other hand, 1 turns out to be the identity of the regular ring $R$, so it is easily verifiable that $R$ is the direct sum of the two ideals $eR$ and $(1 - e)R$. To complete the proof, it suffices to show that $eR$ and $(1 - e)R$ are division rings. Let $ex \in eR \setminus 0$. Then, if $ex \in G_1$, we have $exy = 1$ for some $y \in R$. If $ex \in G_{1-e}$, we have $exz = 1 - e$ for some $z \in R$. In both cases we deduce the contradiction $1 = e$, so $ex$ must lie in $G_e$. Thus, there exists $w \in R$ such that $e = exw = exw$. This shows that $eR$ and $(1 - e)R$ (by a similar argument) are division rings.

We wish to conclude this note by some information on periodic $E_2$-rings. To this end we state the following.

**Lemma 2.7.** Let $R$ be a ring with set of nilpotents $N$. If $N$ is an ideal of $R$, $\phi$ the canonical homomorphism of $R$ onto $R/N$, and $T$ a $t$-archimedean subsemigroup of $R$ with idempotent $e$, then $\phi(T)$ is a subgroup of $R/N$ with identity $N + e$.

**Proof.** It is well-known that every homomorphical image of a $t$-archimedean semigroup with idempotent is itself $t$-archimedean with idempotent, so $\phi(T)$ is $t$-archimedean with the idempotent $N + e$. Now, it suffices to prove that $N + e$ is the identity of $\phi(T)$. In fact, let $N + a$ be an element of $\phi(T)$. This means that $a \in T$, and therefore $ae = ea$; hence there exists a positive integer $h$ such that $a^h = a^h$. Thus we have $(ae - a)^h = a^he - ha^he + \ldots + (-1)^h a^h = 
\sum_{i=0}^{h} (-1)^i \binom{h}{i} a^h = 0$. Hence $ae - a \in N$, and $(N + a)(N + e) = N + a$.

Now we are able to prove the following.

**Theorem 2.3.** Let $R$ be a ring with set of idempotents $N$. $R$ is a periodic non-
trivial $E_2$-ring with central idempotents if and only if the following conditions are satisfied:

i) $|R| > 4,$

ii) $(R, \cdot)$ is a strongly reversible semigroup,

iii) $N$ is an ideal of $R$,

iv) $R/N$ is the direct sum of two periodic fields.

Proof. Let $R$ be a periodic non-trivial $E_2$-ring with central idempotents. Then, by definition, $|R| > 4.$ Moreover, for every $a, x, y \in R,$ there exists a positive integer $h$ such that $(yx)a^h, (ay)x^h, (ax)\overline{x}^h$ are idempotents. Therefore we have

$$\begin{align*}
(xay)^{h+1} &= x(ayx)^h ay = xa^2y(xay)^{h-1} xy, \\
(xay)^{h+1} &= xa(ayx)^h y = xy(xay)^{h-1} xa^2y, \\
(xa^2y)^{h+1} &= xa(ayx)^h ay = xayz = wxy,
\end{align*}$$

for some $z, w \in R.$ Thus, by the well-known result of Putcha [8], and the fact that the idempotents are permutable, we may conclude that $(R, \cdot)$ is a semilattice of $t$-archimedean semigroups. Then, $(R, \cdot)$ is strongly reversible, by [3, Proposizione 8]. In addition, since a power of each element of $R$ lies in a group, $N$ turns out to be an ideal of $R,$ by Theorem 8 of [9]. Now, it remains to prove that $R/N$ is the direct sum of two fields. In fact, since $E = \{0, 1, e, 1 - e\}$ by Theorem 2.1, $(R, \cdot)$ is a semilattice of four $t$-archimedean semigroups $T_0 = N, T_1, T_{-e}, T_{1-e}$ with idempotent; then, making use of Lemma 2.7, we may easily see that $(R/N, \cdot)$ is a semilattice of four groups $G_0 = 0, G_1, G_{-e}, G_{1-e}.$ At this point, partially repeating the proof of Theorem 2.2, we find that $R/N$ is the direct sum of two division rings, which turn out to be fields by periodicity.

Conversely, suppose that $R$ satisfies conditions i), ii), iii) and iv) of the statement. First, $R$ is periodic: in fact, for every $x \in R$ there exist some positive integers $h, r$ such that $(N + x)^h = (N + x)^{h+r},$ whence $x^h - x^{h+r} \in N.$ Thus the periodicity of $R$ follows from Proposition 2 of [2]. Moreover, since $(R, \cdot)$ is strongly reversible, the idempotents of $R$ commute, which implies $E \subseteq Z.$ To complete the proof it will suffice to prove that $R$ has four idempotents, one of which is the identity of $E$ (Theorem 2.1). To this end, we observe that $(R, \cdot),$ being strongly reversible, is a semilattice of $t$-archimedean semigroups with idempotent, by [3, Proposizione 8]; consequently, $(R/N, \cdot)$ is a semilattice of four groups, by Lemma 2.7 and the fact that a direct sum of two fields has exactly four idempotents. At this point, it is obvious that $|E| \geq 4.$ On the other hand, if $e \in E, N + e$ turns out to be an idempotent of $R/N.$ Let $e, f$ be two distinct idempotents of $R,$ and suppose $N + e = = N + f.$ Then $e - f \in N,$ whence $e - ef \in N$ and $ef - f \in N.$ But $(e - ef)^2 = = e - ef, (ef - f)^2 = ef - f,$ consequently $e = ef = f,$ a contradiction. Thus it must be $|E| \leq 4,$ and therefore $|E| = 4.$ Finally, let $u$ be the idempotent of $R$ such that $N + u$ is the identity of $R/N.$ Then, for every $e \in E,$ we have $N + ue = = (N + u)(N + e) = N + ue.$ Since $ue \in E,$ we may conclude as above that $ue = e,$ so $e$ is the identity of $E.$

462
Example 1. Let $R$ be the ring of integers modulo $p^\alpha q^\beta$ (where $p$, $q$ are distinct primes and $\alpha$, $\beta$ positive integers. $R$ has exactly four idempotents $0, 1, e, 1 - e$ (see e.g. [10], Theorem 2.1), so it is a non-trivial $E_2$-ring satisfying condition i) of Theorem 2.1. Moreover, if $\alpha + \beta > 2$, $R$ contains some nilpotent, so it provides an example of non regular $E_2$-ring.

Example 2. Let $p$ an odd prime. The ring $R$ of all matrices of order two over the field $\mathbb{Z}_p$, of the form
\[
\begin{bmatrix}
x \\
y
\end{bmatrix},
\]
has exactly $p + 1$ idempotents, namely
\[
\begin{bmatrix}
0 & 0 \\
0 & 0
\end{bmatrix}
\quad \text{and} \quad
\begin{bmatrix}
1 & 0 \\
y & 0
\end{bmatrix}
\]
with $y = 0, 1, \ldots, p - 1$. It is immediately verified that the non zero idempotents of $R$ form a left zero semigroup. Moreover, every non zero idempotent may be written in the form
\[
\begin{bmatrix}
1 & 0 \\
y & 0
\end{bmatrix} = \begin{bmatrix}
1 & 0 \\
0 & 0
\end{bmatrix} + y \begin{bmatrix}
0 & 0 \\
1 & 0
\end{bmatrix},
\]
so $R$ is an example of non-trivial $E_2$-ring satisfying condition ii) of Theorem 2.1.

References


Authors’ address: Dipartimento di Matematica, Politecnico di Milano, 20133, Milano, Italia.