Mohamed A. Salim; Adela Tripe

Idempotents and the multiplicative group of some totally bounded rings

Czechoslovak Mathematical Journal, Vol. 61 (2011), No. 2, 509–519

Persistent URL: http://dml.cz/dmlcz/141549

Czechoslovak Mathematical Journal, 61 (136) (2011), 509–519

IDEMPOTENTS AND THE MULTIPLICATIVE GROUP OF SOME TOTALLY BOUNDED RINGS

Mohamed A. Salim, Al Ain, Adela Tripe, Oradea

(Received March 10, 2010)

Abstract. In this paper, we extend some results of D. Dolzan on finite rings to profinite rings, a complete classification of profinite commutative rings with a monothetic group of units is given. We also prove the metrizability of commutative profinite rings with monothetic group of units and without nonzero Boolean ideals. Using a property of Mersenne numbers, we construct a family of power $2^{\aleph_0}$ commutative non-isomorphic profinite semiprimitive rings with monothetic group of units.

Keywords: compact ring, group of units, Jacobson radical, left linearly compact ring, Mersenne number, monothetic group, primary ring, summable set, totally bounded ring

MSC 2010: 16W80, 16U60, 22C05, 22D05

1. Introduction

The class of profinite rings can be viewed as a natural generalization of the class of finite rings. Some results about finite rings can be generalized in a natural form to compact ones. The well-known Kaplansky's theorem (see [8]) on the structure of compact semiprimitive rings can be considered a natural extension of Wedderburn-Artin theorem about the structure of semiprimitive artinian rings to compact rings. Moreover, the proofs of some results which are easy for finite rings need highly non-trivial arguments of algebraic and topological nature in the compact case. For instance, in [13] it has been proved that every compact nil ring has a finite nilindex.

As well as finite rings, compact rings usually have many idempotents. Recently, in [4], Dolzan has proved that some multiplicative properties of idempotents of finite rings imply that these rings are products of local rings. In Section 3, we extend these results to the class of compact rings, countably compact rings and linearly compact rings.

By [6], [7] and [11], a classification of finite rings with identity whose group of units is cyclic has been given. In Section 4, we do the following:

(i) classify compact rings with 1 that have a monothetic group of units;

(ii) show that compact rings with a *monothetic* group of units without nonzero closed Boolean ideals are metrizable;

(iii) using properties of *Mersenne numbers*, we construct a set of cardinality of continuum of compact commutative rings with 1 having a monothetic group of units; and

(iv) derive some results about commutative linearly compact rings with 1 whose groups of units are topologically finitely generated.

2. Notation and conventions

All topological rings are assumed to be associative, Hausdorff and with 1. By the *radical* of a ring R we mean its Jacobson radical, denoted by $J(R)$, or briefly by J. By $R(\cdot)$ we denote the multiplicative semigroup of R. A ring R is called *semiprimitive* if $J(R) = 0$, and is called *radical* if R coincides with its radical (i.e. $J(R) = R$). Sometimes we use the term a profinite ring instead of a totally disconnected compact ring. By a *profinite ring* we mean an inverse limit of finite rings. Following [3] we say that a compact group is said to be *monothetic* if it contains a dense cyclic subgroup. To [13] we refer for the notions of *monocompact* and *primary* rings: a topological ring R is said to be *monocompact* if every element of R is contained in a compact subring. By a *primary* profinite ring we mean a ring R for which $R/J(R)$ is a finite simple ring. Under the last condition, R is a matrix ring over a profinite local ring. We define (see [9]) a *left linearly compact ring* to be a topological ring having a fundamental system of neighborhoods of zero consisting of left ideals in which the intersection of every filter basis consisting of closed cosets with respect to left ideals is non-empty. For two idempotents of a ring R, we write $e \leqslant e'$ if $ee' = e'e = e$. A non-zero idempotent e is said to be *minimal* in R if there is no non-zero idempotent $e_1 \neq e$ such that $e_1 \leqslant e$. From [10] we recall that a ring R with 1 is said to be *clean* provided that every element in R is the sum of an idempotent and a unit.

The *closure* of a subset A of a topological space X will be denoted by $\mathrm{cl}(A)$. We refer to [1] for the notion and properties of *summable sets* in topological Abelian groups.

An ideal I of a ring R is called *cofinite* if the subgroup I is of finite index. The fact that I is a *left ideal* or a 2-sided ideal of a ring R is denoted by $I_l \trianglelefteq R$ or $I \trianglelefteq R$, respectively. We recall that a topological ring $\langle R, \mathscr{T}\rangle$ is *totally bounded* provided its completion $\langle c(R), c(\mathscr{T})\rangle$ is compact (see [13]).

3. Idempotents of compact rings

Lemma 1. *If R is a compact ring with identity, then for every $a \in R$ there exists an idempotent e such that $eR = \bigcap_{n\in\mathbb{N}} a^n R$.*

P r o o f. It is well-known that every compact semigroup contains an idempotent (see [13]). Let $a \in R$ and let $e \in \mathrm{cl}\{a^i \colon i \in \mathbb{N}\}$ be an idempotent. For a fixed $n \in \mathbb{N}$ and for any open ideal V of R there exist $k \in \mathbb{N}$ and $v \in V$ such that $e = a^k + v$. Since V is an ideal of R, we may assume that $k \geqslant n$ and then $e = a^n a^{k-n} + v \in a^n R + V$. It follows that $e \in a^n R$ and hence $eR \subset \bigcap_{n\in\mathbb{N}} a^n R$. Conversely, let V be an open ideal of R. Then there exist $k \in \mathbb{N}$ and $v \in V$ such that $a^k = e + v$. Then $a^k R \subset eR + V$ and hence $\bigcap_{n\in\mathbb{N}} a^n R \subset eR + V$. Since V is arbitrary, we have $\bigcap_{n\in\mathbb{N}} a^n R \subset eR$. □

Lemma 2. *Let R be a ring with identity 1 and let $I = aR = Rb$ be an ideal of R which is a left and right principal ideal. Then $I^n = a^n R = Rb^n$ for every $n \in \mathbb{N}$.*

P r o o f. Induction on n. The lemma is obviously true for $n = 1$. If $I^k = a^k R = Rb^k$, then $I^{k+1} = aRa^k R$. Since $a^k R$ is an ideal, $aRa^k R \subset aa^k R = a^{k+1} R \subset I^{k+1}$, and hence $I^{k+1} = a^{k+1} R$. In an analogous way, $I^{k+1} = Rb^{k+1}$. □

Theorem 1. *Let R be a profinite ring with 1 in which every open ideal is left and right principal. Then R is a product of profinite primary rings.*

P r o o f. By Kaplansky's theorem (see [8]), $R/J(R) \cong_{top} \prod_{\alpha<\tau} R_\alpha$ where each R_α is a finite simple ring with identity g_α and τ is a cardinal. We identify $R/J(R)$ with $\prod_{\alpha<\tau} R_\alpha$ and denote by π the canonical homomorphism of R onto $R/J(R)$. By [13], there exists an idempotent $e_\alpha \in R$ such that $\pi(e_\alpha) = g_\alpha$, $\alpha < \tau$. If $A_\alpha = \pi^{-1}(R_\alpha)$, then A_α is open and hence there exist $a, b \in R$ such that $A_\alpha = aR = Rb$. By Lemma 2, $A_\alpha^n = a^n R = Rb^n$ for every $n \in \mathbb{N}$. Set $B_\alpha = \bigcap_{n\in\mathbb{N}} A_\alpha^n$. Then, by Lemma 1, B_α is a topological direct summand with identity h_α. By compactness of R, we have $\pi(B_\alpha) = \bigcap_{n\in\mathbb{N}} \pi(A_\alpha^n)$. Obviously, $\pi(h_\alpha) = g_\alpha$ and $\pi(Rh_\alpha) = R_\alpha$, which means that Rh_α is a primary ring. We have constructed a family $\{h_\alpha\}_{\alpha<\tau}$ of central idempotents such that

(i) $\pi(h_\alpha) = g_\alpha$, $\alpha < \beta$; and

(ii) Rh_α is a primary ring for $\alpha < \beta$.

We claim that the idempotents h_α, $\alpha < \tau$, are orthogonal. Indeed, $h_\alpha h_\beta \in J(R)$ for $\alpha \neq \beta$, which implies that $h_\alpha h_\beta = 0$. The set $\{h_\alpha \colon \alpha \in \Omega\}$ is summable. If $h = \sum_{\alpha<\tau} h_\alpha$, then $h - 1 \in J(R)$, and hence $h = 1$. By standard arguments, the topological ring R is the product of rings Rh_α, $\alpha < \tau$. □

Remark 1. Let R be a ring and $I \trianglelefteq_l R$ a left ideal. For any $x \in R$, the left coset $x + I$ is a subsemigroup of the multiplicative semigroup $R(\cdot)$ of R if and only if $Ix \subset I$ and $x^2 - x \in I$.

Obviously, $x^2 - x \in I$. If $i \in I$, then there exists $i_1 \in I$ such that $(x+i)(x+i) = x + i_1$, which implies that $ix = x - x^2 + i_1 - xi - i^2 \in I$.

Conversely, let $i, i_1 \in I$; then $(x+i)(x+i_1) = x + x^2 - x + xi_1 + ix + ii_1 \in x + I$, i.e. $x + I$ is a subsemigroup of $R(\cdot)$.

The following result is a generalization of a theorem of Eckstein on $I = J(R)$ (see [5]).

Theorem 2. *Let R be a left linearly compact ring and I a closed 2-sided ideal of R such that $x + I$ is an idempotent of the factor ring R/I. Then the set $x + I$ contains an idempotent.*

P r o o f. Let $\mathfrak{M} = \{y + H\colon \operatorname{cl}(H) = H \trianglelefteq_l R\}$, where $y + H$ is a subsemigroup of $R(\cdot)$. For any chain $\mathfrak{N}$ of subsemigroups in $\mathfrak{M}$, its intersection satisfies $\bigcap \mathfrak{N} \in \mathfrak{M}$. Also, by Zorn's Lemma, $\mathfrak{M}$ has a minimal element $S = s + K$. Then $SsSs \subset Ss \subset S$ and $Ss = s^2 + Ks$ where Ks is a closed left ideal of R, as R is left linearly compact, and hence $Ss \in \mathfrak{M}$. By minimality of S we obtain that $Ss = S$, hence there exists $s_0 \in S$ such that $s_0 s = s$, $s_0^2 s = s_0 s$ and so $(s_0^2 - s_0)s = 0$. Set $L = \{x \in K\colon xs = 0\}$ and let $s_0 = s + k \in s + K = S$; then $s_0^2 - s_0 = s^2 - s + sk + ks + k^2 - k \in K$. Hence $s_0^2 - s_0 \in L$ and $Ls_0 = L(s+k) \subset Ls + Lk \subset Ks + Kk \subset K$. Moreover, $Ls_0 s = Ls = 0$ implies that $Ls_0 \subset L$. By minimality of S, we have $s_0 + L = s + K$, which implies that $K = L$. Then $(s^2 - s)s = 0$ implies that $s^3 = s^2$; i.e. $s^4 = s^3 = s^2$and hence $e = s^2 \in S$ is an idempotent. $\square$

A similar technique and argument can be used to prove the following result.

Theorem 3. *Let R be a left linearly compact ring and $I \nsubseteq J(R)$ a 2-sided ideal (not necessarily closed) of R. Then I contains a non-zero idempotent.*

Open question. Let R be a left linearly compact ring with 1 and $I \trianglelefteq_l R$, $I \nsubseteq J(R)$. Is it true that I contains a non-zero idempotent?

We note here that this assertion is true for compact rings.

Lemma 3. *Every set $\{e_\alpha\colon \alpha \in \Omega\}$ of central orthogonal idempotents of a left linearly compact ring with identity is summable.*

P r o o f. By the *Cauchy Criterion* (see [1]), it suffices to check that the set $\Omega_0 = \{\alpha \in \Omega\colon e_\alpha \notin V\} \subset \Omega$ is finite for every open left ideal V of R. On the contrary, assume that there exists an open left ideal V of R for which the set Ω_0 is infinite. If $\alpha_1,\dots,\alpha_n \in \Omega$, $r_1,\dots,r_n \in R$ such that $(r_1e_{\alpha_1}+V)+\dots+(r_ne_{\alpha_n}+V)=V$, then $r_ie_{\alpha_i}\in V$ for $i=1,\dots,n$. This shows that $\sum\limits_{\alpha\in\Omega}((Re_\alpha+V)/V)=\bigoplus\limits_{\alpha\in\Omega}((Re_\alpha+V)/V)$. A contradiction, since the R-module R/V is finite-dimensional in the sense of Goldie. $\square$

Theorem 4. *Let R be a linearly compact ring with 1. Then every idempotent of R is central if and only if R is a topological product of local rings.*

Proof. Obviously, if R is a product of local rings, then every idempotent of R is central (see [13]). Now, if every idempotent of R is central, it is well-known that $J(R)$ is closed. It follows from Theorem 2 that every idempotent of $R/J(R)$ is central. By Leptin's theorem (see [9]), the factor ring $R/J(R)$ is isomorphic to a product $\prod\limits_{\alpha\in\Omega}\Delta_\alpha$, where each factor Δ_α is the ring of endomorphisms rings of a vector space over a division ring. Since idempotents of $R/J(R)$ are central, each factor Δ_α is a division ring. Consider the set $\{e'_\alpha\colon\ \alpha\in\Omega\}$, where e'_α is the identity of Δ_α, $\alpha\in\Omega$. By Theorem 2, for each $\alpha\in\Omega$ there exists an idempotent e_α of R such that $e_\alpha+J(R)=e'_\alpha$. By Lemma 3, the set $\{e_\alpha\colon\ \alpha\in\Omega\}$ is summable. Obviously, $Re_\alpha/J(Re_\alpha)$ is isomorphic to Δ_α. As $1-\sum\limits_{\alpha\in\Omega}e_\alpha\in J(R)$, we have $1=\sum\limits_{\alpha\in\Omega}e_\alpha$ and hence the ring R is isomorphic to $\prod\limits_{\alpha\in\Omega}Re_\alpha$. $\square$

Lemma 4. *A monocompact subring with 1 of a compact local ring is local.*

Proof. Let S be a monocompact subring with 1 of a compact local ring R. Since $S/S\cap J(R)\cong S+J(R)/J(R)\subset R/J(R)$ is a field, we have $J(S)\subset S\cap J(R)$. As the subring $S\cap J(R)$ consists of topologically nilpotent elements, we have $S\cap J(R)\subset J(S)$ and hence $J(S)=S\cap J(R)$. $\square$

Theorem 5. *A countably compact ring R with 1 is local if and only if its completion $c(R)$ is local.*

Proof. On the contrary, assume that R is local but not $c(R)$. Then $c(R)$ can be mapped continuously on a finite ring S which has an idempotent $e'\notin\{0,1\}$. Let $f\colon R\to S$ be a continuous surjective homomorphism. Then there exists an idempotent $e\in R$ such that $f(e)=e'$; obviously, $e\notin\{0,1\}$, a contradiction.

The converse follows from Lemma 4. $\square$

Lemma 5. *An idempotent e of a countably compact ring R with 1 is minimal if and only if the subring eRe is local.*

P r o o f. On the contrary, assume that 1 is minimal in R but eRe is not local. Since eRe is countably compact, then (by Theorem 5) its completion $c(eRe)$ is not local. Therefore there exists a continuous surjective homomorphism $f\colon \operatorname{cl}(eRe) \to S$, where S has an idempotent $e' \notin \{0,1\}$. Since $f(eRe) = S$, the ring eRe contains an idempotent $e \notin \{0,1\}$, a contradiction.

The converse is obvious. $\square$

Corollary 1. *Let R and R' be countably compact rings with* 1 *and let $f\colon R \to R'$ be a surjective continuous ring homomorphism. If $e \in R$ is a minimal idempotent of R, then $f(e)$ is a minimal idempotent of R' or $f(e) = 0$.*

A topological ring R is a *subdirect product* of rings $R_\alpha, \alpha \in \Omega$, if there exists a topological isomorphism on its image $f\colon R \to \prod\limits_{\alpha\in\Omega} R_\alpha$ such that the composition $\mathrm{pr}_\alpha \circ f$ is surjective and open for every $\alpha \in \Omega$.

Theorem 6. *Let R be a totally bounded monocompact ring with* 1 *in which all idempotents are central. Then R is a subdirect product of finite local rings.*

P r o o f. The completion $c(R)$ of R is compact. We claim that every idempotent of $c(R)$ is central. If V is an open ideal of $c(R)$, then $p_V(c(R)) = p_V(R)$, where p_V is the canonical homomorphism of $c(R)$ onto $c(R)/V$. Let e be an idempotent of R. Since p_V is surjective and $p_V(e)$ is an idempotent of $c(R)/V$, there exists an idempotent $e' \in R$ such that $p_V(e') = p_V(e)$. This implies that e is a central idempotent of $c(R)$. The ring $c(R) = \prod\limits_{\alpha\in\Omega} R_\alpha$ is a product of compact local rings. Let $0 \neq x \in R$; then there exists $\alpha \in \Omega$ such that $\mathrm{pr}_\alpha(x) \neq 0$. Then by Lemma 4, $\mathrm{pr}_\alpha(R)$ is a local ring. Let W be an open ideal of $\mathrm{pr}_\alpha(R)$ such that $\mathrm{pr}_\alpha(x) \notin W$. Then $V = \mathrm{pr}_\alpha^{-1}(W) \cap R$ is an open ideal of R, the ring R/V is local and $x \notin V$. $\square$

Corollary 2. *A countably compact ring with* 1 *whose all idempotents are central is a subdirect product of finite local rings.*

Theorem 7. *Every left linearly compact ring with* 1 *and with bounded factor ring $R/J(R)$ is a clean ring.*

P r o o f. By Leptin's Theorem (see [9]), $R/J(R)$ is a direct product of discrete matrix rings over division rings. By [10], every matrix ring a division ring is clean. Then, obviously, $R/J(R)$ is a clean ring which implies that R is a clean ring. $\square$

The next theorem needs the following three basic results.

Lemma 6. *Let $f\colon R \to R'$ be a continuous homomorphism of compact rings. If e' in $f(R)$ is an idempotent, then there exists an idempotent e in R such that $f(e) = e'$.*

Corollary 3. *Let $f\colon R \to R'$ be a contiuous surjective homomorphism of compact rings. If T and T' are the sets of all idempotents of R and R', respectively, then $f(T) = T'$.*

Corollary 4. *Let $f\colon R \to R'$ be a contiuous surjective homomorphism of compact rings and let T and T' be the sets of all idempotents of R and R', respectively. If T is a subsemigroup of the semigroup $R(\cdot)$, then T' is a subsemigroup of the semigroup $R'(\cdot)$.*

Theorem 8. *If R is a compact ring with 1 and T is the set of all idempotents of R, then T is a subsemigroup of the multiplicative semigroup $R(\cdot)$ of R if and only if R is a product of compact local rings.*

Proof. Suppose that T is a subsemigroup of $R(\cdot)$. Then, by Corollary 4, the set of all idempotents of $R/J(R)$ is a subsemigroup of its multiplicative semigroup. Thus, by Kaplansky's Theorem (see [8]), the ring $R/J(R)$ is a product of matrix rings over finite fields, hence it is a product of finite fields. We claim that each idempotent e of R is central. It suffices to show that e commutes with every idempotent f of R. Since $ef(1-fe)$ is an idempotent in $J(R)$, we have $ef(1-fe) = 0$ and hence $ef = efe$. Similarly, $fe = efe$ and therefore every idempotent of R is central. As every idempotent of a compact ring is central, hence R is a product of local rings. $\square$

We omit the proof of the following result:

Remark 2. The set of all idempotents of a compact ring (not necessarily with 1) is a semigroup if and only if the ring is a product of a connected ring (with trivial multiplication) and compact local rings.

Theorem 9. *Let R be a totally bounded monocompact ring with 1 for which the set T of idempotents is a subsemigroup of $R(\cdot)$. Then R is a subdirect product of finite local rings.*

Proof. The completion $c(R)$ of R is a compact ring. Let $x \in R \setminus V$, $x \neq 0$, for a fixed open ideal V of $c(R)$. If p is the canonical homomorphism of $c(R)$ onto $c(R)/V$, then $p(R) = c(R)/V$ since R is dense in $c(R)$. We claim that the set T' of idempotents in $c(R)/V$ is a subsemigroup of $(c(R)/V)(\cdot)$. Since R is monocompact, the idempotents of $c(R)/V$ can be lifted in R. This implies that T' is a subsemigroup of $c(R)/V$. By Theorem 8, $c(R)/V$ is a direct product $P_1 \times P_2 \times \ldots \times P_n$ of local rings and there exists i, $1 \leqslant i \leqslant n$, such that $p(x) \neq 0$. $\square$

Corollary 5. *Let R be a countably compact ring with 1 for which the set T of idempotents is a subsemigroup of $R(\cdot)$. Then R is a subdirect product of finite local rings.*

Theorem 10. *Let R be a compact ring with 1 and let $\mathscr{M}$ be the set of all minimal idempotents of R. Then $\mathscr{M} \cup \{0\}$ is a subsemigroup of $R(\cdot)$ if and only if R is a product of compact local rings.*

Proof. Consider the ring $R/J(R)$ and the canonical homomorphism $\varphi\colon R \to R/J(R)$. Let e' be a minimal idempotent of $R/J(R)$. Then, by Lemma 5 we obtain that $e'(R/J(R))e'$ is a field. If $e \in \varphi^{-1}(e')$ is an idempotent of R, then $\varphi(eRe) = e'(R/J(R))e'$ is a field and $\ker(\varphi \restriction_{eRe}) = eRe \cap J(R)$, which is equal to $J(eRe)$. This implies that eRe is a local ring. Thus, by Lemma 5, e is a minimal idempotent of R, and hence $\mathscr{M}' \cup \{0\}$ is a subsemigroup of $R/J(R)$, where $\mathscr{M}'$ is the set of all minimal idempotents of $R/J(R)$. This implies that $R/J(R)$ is a product $\prod\limits_{\alpha\in\Omega} F_\alpha$ of fields (see [4]).

For each $\alpha \in \Omega$, let us fix an idempotent e_α in $\varphi^{-1}(e'_\alpha)$. Then each e_α is minimal in R. If $\alpha \neq \beta$, $\alpha, \beta \in \Omega$, then $e_\alpha e_\beta$ is either 0 or an idempotent. In fact, $e_\alpha e_\beta = 0$ as it belongs to $J(R)$. Therefore there exists $e \in R$ which is equal to the sum $\sum\limits_{\alpha\in\Omega} e_\alpha$. But $e = 1$ since $1 - e \in J(R)$. By a standard argument, we can prove that $R = \prod\limits_{\alpha\in\Omega} e_\alpha R e_\alpha$, where each $e_\alpha R e_\alpha$ is a local ring. □

We note that Theorem 8 and Theorem 10 are closely related to Theorem 5.5 and Corollary 5.6 of [4].

4. Compact rings with monothetic group of units

In [7], Gilmer has characterized commutative rings with 1 having a cyclic multiplicative group. Another proof can be found in [11].

Recall that a topological ring R is called *left linear* provided it has a basis at zero consisting of left ideals. It is well known that the group $U(R)$ of units of a compact ring R with 1 is closed and is a topological group. Below $\mathbb{Z}_p$, p being a prime number, denotes the compact ring of p-adic integers.

Remark 3. If $f\colon R \to R'$ is a surjective homomorphism of local rings, then $f(U(R)) = U(R')$.

Indeed, $f(1) = 1$ and $f(U(R)) \subset U(R')$. If $x' = f(x) \in U(R')$, then $x \in U(R)$, otherwise $x \in J(R)$ would imply $x' \in J(R')$, a contradiction.

Lemma 7. *Every commutative artinian ring with identity whose group of units is finitely generated, is finite.*

Proof. Since every commutative artinian ring is a product of finite number of artinian local rings, we can assume without loss of generality that R is a local commutative artinian ring. Then the field $R/J(R)$ is finitely generated as a ring. Then, by Hilbert's Nullstellensatz, the ring $R/J(R)$ is finite. Since $J(R)$ is nilpotent, we obtain that R has a finite characteristic. The subset $1+J(R)$ is a subgroup of $U(R)$, therefore it is finitely generated. Let $a_1,\dots,a_n$ be the generators of $1+J(R)$ and $b_1,\dots,b_n$ their quasiinverses. Then for every $x\in J(R)$ there exist non-negative integers $k_1,\dots,k_{2n}$ such that $1+x=(1+a_1)^{k_1}\dots(1+b_n)^{k_{2n}}$. Expanding this application, we obtain that $x\in\langle a_1,\dots,b_n\rangle$. We proved that $J(R)=\langle a_1,\dots,b_n\rangle$. Since $J(R)$ is a nilpotent ring of finite characteristic, it is finite and so R is finite. $\square$

We call a topological Abelian group *polythetic* if it has a dense finitely generated subgroup.

Theorem 11. *Every commutative linearly compact ring R with polythetic group of units is compact.*

Proof. It is well-known (see [2]) that R is a product of local linearly compact rings. According to Theorem of Tykhonov, we may assume that R is a local ring. The ring R is an inverse system of local rings whose group of units is monothetic. Therefore, without loss of generality, we may assume that R is a discrete linearly compact ring with polythetic group of units. Since R is countable, it is artinian. Then, by Lemma 7, R is finite. $\square$

Corollary 6. *Every commutative linearly compact ring R with monothetic group of units is compact.*

Theorem 12. *An infinite compact local ring R has a monothetic $U(R)$ if R is isomorphic to $\mathbb{Z}_p$ for an odd prime number p.*

Proof. Let V be a proper open ideal of R. According to Remark 3, the group of units of the ring R/V is cyclic. By Gilmer's Theorem (see [11]), the factor ring R/V is isomorphic to one of the following rings: $GF(p^m)$, p any prime and $m\geqslant 1$; $\mathbb{Z}/(p^m)$, p an odd prime and $m\geqslant 2$; $F[X]/(X^2)$, where F is a finite prime field of finite order; $\mathbb{Z}/(4)$; $F[X]/(X^3)$, where $F=GF(2)$, $\mathbb{Z}[X]/(4,\ 2X,\ X^2-2)$, or the ring of all upper triangular 2×2 matrices over $GF(2)$. Since R is infinite, there exists an open ideal V_0 such that R/V is isomorphic to $\mathbb{Z}/(p^m)$, p an odd prime, and fixed for every open ideal $V\subset V_0$. This implies that $R=\langle 1\rangle+V$ for every open ideal $V\subset V_0$. We obtain that $R=\mathrm{cl}\langle 1\rangle$. This implies that $R\cong\mathbb{Z}_p$. $\square$

Theorem 13. *The group $U(R)$ of units of a compact commutative ring R is monothetic if and only if R is isomorphic to $\prod\limits_{i\in\omega} R_i$ where no more than one ring R_i is isomorphic to $\mathbb{Z}_p$ for an odd prime number p and $|U(R_i)|$ are relatively prime to p and to each $|U(R_j)|$ for a finite R_j, $j\neq i$.*

P r o o f. If the group of units $U(R)$ is monothetic, then the assertion follows directly from Theorem 8. Conversely, if $R = \prod\limits_{i \in \omega} R_i$ satisfies the theorem condition, then (θ_i) generates $U(R)$ for every generator $\theta_i, i \in \omega$. $\square$

The following fact from the theory of numbers was communicated kindly by M. Juras, M. Bachraoui and M. Ursul. Recall that a *Mersenne number* M_n, $n \in \mathbb{N}$, is $2^n - 1$.

Proposition 1. *For all relatively prime numbers m, n the Mersenne numbers M_m and M_n are relatively prime.*

P r o o f. On the contrary, assume that there exist a pair (p, q) of relatively prime numbers such that $(M_p, M_q) = d > 1$. Without loss of generality, we may assume that p is the minimal natural number for which there exists a natural number $q < p$ such that $(M_p, M_q) = d > 1$. But $M_n = 2^n - 1 = 2 \cdot 2^{n-1} - 1 = 2(2^{n-1} - 1) + 1 = 2M_{n-1} + 1$. By recursion, $M_n = 2^i M_{n-i} + M_i$ for every $i \in [1, n-1]$. Then $M_p = 2^{p-q} M_q + M_{p-q}$. This implies $(M_p, M_q) = (M_{p-q}, M_q)$, a contradiction. $\square$

Remark 4. Let $\{A_n\}_{n \in \mathbb{N}}$ be a family of groups each of which is a finite cyclic group or a group of p-adic numbers such that $(a_n, a_m) = 1$ for $n, m \in \mathbb{N}$, $n \neq m$, where

$$a_i = \begin{cases} |A_i| & \text{if } \ A_i \text{ is finite,} \\ p & \text{if } \ A_i = \mathbb{Z}_p, \end{cases}$$

$i \in \mathbb{N}$. Then the compact group $\prod\limits_{n \in \mathbb{N}} A_n$ is monothetic.

Let $\mathbb{P}$ be the set of all prime numbers. The next result follows directly from Proposition 1 and Remark 4.

Corollary 7. *Let $P_0 \subset \mathbb{P}$. Then $\prod\limits_{p \in P_0} \mathbb{F}_{2^p}$ is a compact semiprimitive ring with a monothetic group of units.*

Corollary 8. *There exists a family of cardinality 2^ω of non-isomorphic commutative compact semiprimitive rings with monothetic group of units.*

Example 1. The group $U(R)$ of units of the ring $R = \mathbb{Z}_3 \times \prod\limits_{p \in P_0} \mathbb{F}_{2^p}$ is monothetic. Indeed, it is well-known (see, for example [12], Proposition 7, Proposition 8) that $U(\mathbb{Z}_3) \cong (\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}_3$. By Remark 4, it suffices to show that $\gcd(2^p - 1, 3) = 1$ for every prime $p > 5$. But, as $p = 2t + 1$, $t \in \mathbb{N}$, hence $2^p - 1 = (2^2)^t \cdot 2 - 1 = 1$ (mod 3).

Acknowledgement. Thanks to our friend Prof. M. Ursul (Univ. of Oradea, Romania) for great effort in making our collaboration possible.

References

[1] *N. Bourbaki*: Elemente der Mathematik. Allgemaine Topologie. Topologische Gruppen. Zahlen und die mit ihnen zusammenhängenden Gruppen und Räume (Russian). Nauka, Moskau, 1969.
[2] *N. Bourbaki*: Elements de mathematique. Algebre commutative (Russian). Mir, Moskau, 1971.
[3] *D. Van Dantzig*: Zur topologischen Algebra. Mathematische Annalen *107* (1933), 591.
[4] *D. Dolžan*: Multiplicative sets of idempotents in finite ring. J. Algebra *304* (2006), 271–277.
[5] *F. Eckstein*: Semigroup methods in ring theory. J. Algebra *12* (1969), 177–190.
[6] *K. E. Eldridge, I. Fischer*: DCC rings with a cyclic group of units. Duke Math. J. *34* (1967), 243–248.
[7] *R. W. Gilmer, jun.*: Finite rings having a cyclic multiplicative group of units. Am. J. Math. *85* (1963), 447–452.
[8] *I. Kaplansky*: Topological rings. Am. J. Math. *69* (1947), 153–183.
[9] *H. Leptin*: Linear kompakte Moduln und Ringe. Math. Z. *62* (1955), 241–267.
[10] *W. K. Nicholson, Y. Zhou*: Clean general rings. J. Algebra *291* (2005), 297–311.
[11] *R. Raghavendran*: A class of finite rings. Compos. Math. *22* (1970), 49–57.
[12] *J.-P. Serre*: Cours d'aritmetique. Le mathematicien (French). Presses Universitaires de France, Paris, 1970.
[13] *M. Ursul*: Topological Rings Satisfying Compactness Conditions. Mathematics and its Applications. Vol. 549. Kluwer Academic Publishers, Dordrecht, 2002.

Authors' addresses: Mohamed A. Salim, Dept. of Math. Sci., UAEU, POBox 17551, Al Ain, UAE, e-mail: `msalim@uaeu.ac.ae`; Adela Tripe, Dept. of Math., University of Oradea, St. Armatei Romane 3, Oradea, Romania, e-mail: `tadela@uoradea.ro`.