Bull. Aust. Math. Soc. **99** (2019), 403–412
doi:10.1017/S0004972719000017

FINITE UNITARY RINGS IN WHICH ALL SYLOW SUBGROUPS OF THE GROUP OF UNITS ARE CYCLIC

M. AMIRI and M. ARIANNEJAD✉

(Received 2 August 2018; accepted 10 December 2018; first published online 13 February 2019)

Abstract

We characterise finite unitary rings R such that all Sylow subgroups of the group of units R^* are cyclic. To be precise, we show that, up to isomorphism, R is one of the three types of rings in $\{O, E, O \oplus E\}$, where $O \in \{GF(q), \mathbb{Z}_{p^\alpha}\}$ is a ring of odd cardinality and E is a ring of cardinality 2^n which is one of seven explicitly described types.

2010 *Mathematics subject classification*: primary 16U60; secondary 16P10.

Keywords and phrases: finite ring, group of units, Sylow subgroup.

1. Introduction

In this paper, we examine the properties of finite rings in which every Sylow subgroup of the group of units is cyclic. In 1966, Erickson [3] showed that the order of a finite noncommutative ring (without unity) is squarefree. In 1968, Eldridge [2] extended this result and proved that if R is a finite ring with unity of order m such that m is cubefree, then R is a commutative ring. In 1989, Groza [5] showed that if R is a finite ring and at most one simple component of the semi-simple ring $R/J(R)$ is a field of order 2, then R^* (the group of units of R) is a nilpotent group if and only if R is a direct sum of two-sided ideals that are homomorphic images of group algebras of type SP, where S is a particular commutative finite ring and P is a finite p-group for a prime number p. More recently, in 2009, Dolzan [1] improved this result and described the structure of finite rings in which the group of units is nilpotent. Here we characterise the structure of all finite unitary rings R, in which every Sylow subgroup of the group of units R^* is cyclic. Let F be a field and let $M_n(F)$ and $T_n(F)$ be respectively the set of all $n \times n$ square and upper triangle matrices over F. Also, let $GF(q)$ be the Galois field of finite order q. The main result of this paper is the following theorem.

This work has been partially supported by Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) of the Ministry of Education of Brazil.

Theorem 1.1. *Let R be a unitary ring of finite cardinality $2^n m$, where n is a positive integer and m is a positive odd number. If all Sylow subgroups of R^* are cyclic, then, up to isomorphism, R is one of the three types of rings in $\{O, E, O \oplus E\}$, where $O \in \{GF(q), \mathbb{Z}_{p^\alpha} : p$ a prime number$\}$ is a ring of cardinality m and E is a ring of cardinality 2^n which is one of the following seven explicitly described types:*

$$E \in \Big\{M_2(GF(2)), T_2(GF(2)), T_2(GF(2) \bigoplus_{i=1}^{k} GF(2^{n_i})), \\ \mathbb{Z}_4, \mathbb{Z}_4 \bigoplus_{i=1}^{k} GF(2^{n_i}), \bigoplus_{i=1}^{k} GF(2^{n_i})\Big\},$$

where $\gcd(n_i, n_j) = 1$ *for* $1 \le i, j \le k$ *and* $i \neq j$, *or*

$$E \cong M_2(GF(2)) \bigoplus_{i=1}^{k} GF(2^{n_i}),$$

where $\gcd(n_i, n_j) = 1 = \gcd(2, n_i)$ *for* $1 \le i, j \le k$ *and* $i \neq j$. *Furthermore, if* $R = O \oplus E$, *then* $\gcd(|O^*|, |E^*|) = 1$.

In the proof of the theorem, we use the following concepts and notations. Let R be a ring with identity $1 \neq 0$. We denote by $\mathrm{char}(R)$ the characteristic of R, by $J(R)$ the Jacobson radical of R, by R^* the set of all unit elements of R (or the group of units of R), and by R_0 the prime subring of R (the subring generated by the identity element 1). The cardinality of a set X is denoted by $|X|$. For a given prime number p, the set of all Sylow p-subgroups of R^* is denoted by $\mathrm{Syl}_p(R^*)$. For $g \in R^*$, the smallest positive integer m such that $g^m = 1$ is called the order of g in R^* and is denoted by $o(g)$. The subgroup generated by g in R^* is denoted by $\langle g \rangle$. For a subset S of R, we denote by $R_0[S]$ the subring generated by $\{S \cup R_0\}$ or equivalently by $\{S \cup \{1\}\}$. The ring of all $n \times n$ matrices over R is denoted by $M_n(R)$ and the ring of integers modulo m is denoted by Z_m. For a pair of elements $a, b \in R$, the Lie bracket of a and b is $[a, b] = ab - ba$. Finally, $GF(p^m)$ denotes the unique finite field of characteristic p and order p^m.

2. Proof of Theorem 1.1

We begin with two elementary lemmas.

Lemma 2.1. *Let R be a ring and I an ideal of R such that $I \subseteq J(R)$. If all Sylow subgroups of R^* are cyclic, then all Sylow subgroups of $(R/I)^*$ are cyclic. In addition, $(R/I)^* = (R^* + I)/I$.*

Proof. The canonical epimorphism $f : R^* \longrightarrow (R/I)^*$ defined by $f(a) = a + H$ shows that every Sylow subgroup of $(R/I)^*$ is cyclic. Clearly, $(R^* + I)/I \subseteq (R/I)^*$. For the reverse inclusion, let $x + I \in (R/I)^*$. Then there exists $y + I \in (R/I)^*$ such that $xy + I = 1 + I$. It follows that $xy - 1 \in I$. Since $I \subseteq J(R)$, we have $xy = xy - 1 + 1 \in R^*$, so $x \in R^*$ and $x + I \in (R^* + I)/I$. □

https://doi.org/10.1017/S0004972719000017 Published online by Cambridge University Press

Lemma 2.2. *Suppose that R is a unitary finite local ring with a nontrivial minimal ideal I and $J(R)$ is commutative. Then $J(R) = \mathrm{Ann}_R(I)$.*

Proof. By [4, Theorem 2.4], there is an integer m such that $J(R)^m = 0$. Suppose $I^n = 0$ and $I^{n-1} \neq 0$, where $2 \leq n \leq m$. It is clear that $I^{n-1} = I$. Since $2n - 2 \geq n$, we see that $I^2 = (I^{n-1})^2 = 0$. Therefore $n = 2$. Let $u \in I$ and $h \in J(R)$. If $hu \neq 0$, then $RhuR = I = RuR$ and $u = \sum_{\text{finite}} rhus$, for some $r, s \in R$. By commutativity of $J(R)$,

$$u = \sum_{\text{finite}} (rh)(us) = \sum_{\text{finite}} (us)(rh) = \sum_{\text{finite}} u(srh) = \sum_{\text{finite}} srhu,$$

and hence $u(\sum_{\text{finite}} srh - 1) = 0$. Since $(\sum_{\text{finite}} srh) - 1 \in R^*$, clearly $u = 0$, which is a contradiction. Consequently $hu = 0$ for all $h \in J(R)$, that is, $J(R) = (I)$. □

Remark 2.3. Let $R = A \oplus B$ be a finite ring, where A and B are two ideals of R. Then $R^* = A^* \oplus B^*$ and $1 = 1_A + 1_B$, where 1_A and 1_B are the identity elements of A and B, respectively. It is also clear that $A^* + 1_B \leq R^*$ and $A^* + 1_B \cong A^*$. In addition, if $p \mid \gcd(|A^*|, |B^*|)$ for some prime number p, then by Cauchy's Theorem, R^* has two elements $a + 1_B$ and $1_A + b$ with the same order p. Clearly, $\langle a + 1_B \rangle \neq \langle 1_A + b \rangle$, and this implies that the Sylow p-subgroups of R^* are not cyclic. This idea can be generalised for any similar finite decomposition of R.

We need the following lemma, which is a direct consequence of [5, Lemma 1.1].

Lemma 2.4. *If R is a finite unitary ring of odd cardinality, then $R = R_0[R^*]$.*

The first step in the proof of the theorem is to characterise all finite unitary rings R of odd cardinality with a specific assumption.

Proposition 2.5. *Let R be a unitary ring of finite odd cardinality m. If every Sylow subgroup of R^* is cyclic, then, up to isomorphism, R is either a finite field or $\mathbb{Z}_{p^t}$, for a positive integer t.*

Proof. Let $|R| = m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ be the canonical prime factorisation. Then

$$R = R_1 \oplus R_2 \oplus \cdots \oplus R_k,$$

where each R_i is an ideal of order $p_i^{\alpha_i}$. If $k > 1$, then Remark 2.3 shows that 2-Sylow subgroups of R^* are not cyclic. Hence either $k = 1$ or $|R| = p^\alpha$, for a prime number p and positive integer α. We continue the proof by induction on α. First suppose that $|R| = p^2$. From [2], every unitary ring of order p^α with $\alpha < 3$ is commutative. Hence R is either a field of order p^2 or one of the rings $\mathbb{Z}_{p^2}$ and $\mathbb{Z}_p \oplus \mathbb{Z}_p$. Again, Remark 2.3 removes the case $\mathbb{Z}_p \oplus \mathbb{Z}_p$ and the ring R is as desired. Now let $|R| = p^\alpha$, where $\alpha > 2$ and consider the following two cases depending on the Jacobson radical: $J(R) = 0$ or $J(R) \neq 0$.

Case 1. If $J(R) = 0$, then R is a semi-simple Artinian ring and by the structure theorem of Artin–Wedderburn $R \cong \bigoplus_{i=1}^t M_{n_i}(D_i)$, where all D_i are finite fields (see [6, page 33] and [7]). By Remark 2.3 we may consider $t = 1$ or $R \cong M_n(D)$, where D is a finite

https://doi.org/10.1017/S0004972719000017 Published online by Cambridge University Press

field and n is a positive integer. If $n = 1$, then $R = D$ is a finite field, as desired. So suppose that $n > 1$. Since R has odd cardinality, $\mathrm{char}(D) \neq 2$, and hence $-1 \neq 1$ and the two diagonal matrices $\mathrm{diag}(-1, 1, \ldots, 1)$ and $\mathrm{diag}(-1, -1, \ldots, -1)$ belong to the same Sylow 2-subgroup of $GL_n(D)$ (the general linear group). This shows that the Sylow 2-subgroups of $GL_n(D)$ are not cyclic, which is a contradiction.

Case 2. Suppose $J(R) \neq 0$. An induction argument guarantees that every proper subring of R is commutative. Suppose that R is noncommutative.

If R^* is a nilpotent group, then it is a direct product of its Sylow subgroups which are all cyclic, so R^* is an abelian group. Therefore, by Lemma 2.4, R is commutative, which contradicts our assumption. Hence R^* is not a nilpotent group.

Let H be an ideal of R with $0 \neq H \subseteq J(R)$. By Lemma 2.1, every Sylow subgroup of $(R/H)^*$ is cyclic. By induction, the ring R/H is commutative and the additive commutator subgroup of R is contained in H, that is, $[R, R] \subseteq H$. Let M be a maximal ideal of R. Then R/M is a simple commutative ring and so is a finite field. By [5, Lemma 1.2], $1 + J(R)$ is a p-group and $o(-1) = 2$. Therefore $\mathrm{Syl}_p(R^*)$ and $\mathrm{Syl}_2(R^*)$ are nonempty. Let $\{M_1, \ldots, M_k\}$ be the set of all maximal ideals of R. Then $R/J(R) = R/(M_1 \cap \cdots \cap M_k) \cong R/M_1 \times \cdots \times R/M_k$, from which $(R/J(R))^* \cong (R/M_1)^* \times \cdots \times (R/M_k)^*$. Lemma 2.1 and Remark 2.3 guarantee that $k = 1$ and so R is a local ring. Let $|R/M_1| = p^\gamma$ with $\gamma \leq \alpha$. Clearly $J(R) = M_1$. So $(R/J(R))^* = \langle x + J(R)\rangle = p^\gamma - 1$. Since $|R| = p^\gamma |J(R)|$, we have $|R| = (p^\gamma - 1 + 1)|J(R)|$ and then $|R| - |J(R)| = |R^*| = (p^\gamma - 1)|J(R)| = o(x + J(R))|J(R)|$. Also, since $\gcd(p^\gamma - 1, p) = 1$ and $1 + J(R)$ is a normal p-subgroup of R^*,

$$|J(R)| = |1 + J(R)| \leq |P| \leq |J(R)|.$$

Thus $1 + J(R) = P$. Since $|\langle x\rangle P| = |\langle x\rangle||P|/|\langle x\rangle \cap P| = |R^*|$, we have $R^* = \langle x\rangle P$. Since $R = R_0[R^*]$ and R is not commutative, the equality $R^* = \langle x\rangle P$ shows that $x \notin Z(R^*)$. Since $J(R)$ is commutative and $R/J(R)$ is a finite field, $J(R)$ is not a central ideal (otherwise R would be a commutative ring, which is a contradiction). So there exists $w \in J(R)$ such that $wx \neq xw$. Consequently, $R = R_0[w, x]$. Let I be a minimal ideal of R. We consider two subcases: $Z(R) \cap I \neq 0$ or $Z(R) \cap I = 0$.

Subcase 1. Suppose $0 \neq a \in Z(R) \cap I$. By Lemma 2.2, $J(R) = \mathrm{Ann}_R(I)$. It follows that $I = Ra = (R^* \cup J(R))a = \{\sum_{\text{finite}} n_i a : n_i \in R^*\}$. Let $y \in R^*$. Then $y + J(R) = x^i + J(R)$ for some integer i with $0 \leq i \leq p^\gamma - 1$, that is, $y = x^i + s$ for some element $s \in J(R)$. Hence $ya = x^i a + sa = x^i a$ and so $I = \{0, xa, \ldots, x^{p^\gamma - 1}a\} \subseteq J(R)$. Since $xx^i a = x^i ax$, $w(x^i a) = (x^i a)w$ and $R = R_0[x, w]$, we have $x^i a \in Z(R)$, and so $I \subseteq Z(R)$. Also, for all $u, v \in R^*$, we have $uv - vu \in I$ and so $uvu^{-1}v^{-1} - 1 \in I \subseteq Z(R)$. Therefore $uvu^{-1}v^{-1} \in Z(R^*)$ and the multiplicative derived subgroup of R^* is a central subgroup of R^*. It follows that R^* is nilpotent and so abelian, which implies that R is commutative and contradicts our assumption.

Subcase 2. Let $Z(R) \cap I = 0$. If $0 \neq b \in I$, then $bw = wb$ and $[b, x] \neq 0$. Hence $R = R_0[b, x]$ and we may consider $w = b \in I$. Let $m_1, m_2 \in J(R)$. Since $J(R)$ is a

https://doi.org/10.1017/S0004972719000017 Published online by Cambridge University Press

commutative ring and $xm_1, m_2x \in J(R)$,

$$(xm_1)m_2 = m_2(xm_1) = (m_2x)m_1 = m_1m_2x.$$

Since $R = R_0[w, x]$, we conclude that $m_1m_2 \in Z(R)$ and so $J(R)^2 \subseteq Z(R)$. If $J(R)^2 \neq 0$, then by the induction hypothesis $R/J(R)^2$ is a commutative ring, and so $0 \neq [R, R] \subseteq J(R)^2 \cap I$. Since I is a minimal ideal and $J(R)^2$ is an ideal, $I \subseteq J(R)^2 \subseteq Z(R)$, which is a contradiction.

Hence $J(R)^2 = 0$. By considering R as a local ring, for all $s \in J(R)$, we find $\mathrm{Ann}_R(s) = J(R)$. We claim that $I = J(R)$. Otherwise consider $l \in J(R) \setminus I$. Since $R = R_0[w, x]$, we have $l = (\sum_{\text{finite}} n_i x^i) + c$, where $c \in I$ and $n_i \in R_0$. Since $l - c \in J(R)$, we have $a = \sum_{\text{finite}} n_i x^i \in J(R)$. Then $aw = wa$ and $ax = xa$. It follows that $a \in Z(R) \cap J(R)$. Let $H = Ra$. Since $\mathrm{Ann}_R(a) = J(R)$,

$$H = Ra = (R^* \cup J(R))a = \left\{ \sum_{\text{finite}} n_i a : \; n_i \in R^* \right\} = \{0, xa, \ldots, x^{p^{\gamma}-1}a\} \subseteq J(R).$$

If $H \neq 0$, we reach a contradiction by an argument similar to that in Subcase 1. If $H = 0$, then $l = c \in I$, which is again a contradiction. Therefore $I = J(R)$. Since $R/J(R)$ is a finite field, we deduce that $\mathrm{char}(R/J(R)) = p \neq 0$. Hence $p + J(R) = J(R)$ and $p \in J(R)$. Let $L = pR$. If $L \neq 0$, then $J(R) = L$ and $p \in Z(R) \cap J(R)$, which is a contradiction. Therefore $L = pR = 0$, so $\mathrm{char}(R) = p$. Let $h \in J(R)$. Since $(1 + h)^p = 1^p + h^p = 1$, we see that $P = 1 + J(R)$ is an elementary abelian p-group and since P is a cyclic group, we have $|P| = p$. Thus $|J(R)| = |P| = p$. Since $|J(R)| = |\{0, w, xw, \ldots, x^{p-1}w\}| \leq p$, there exists an integer i such that $1 \leq i \leq p - 1$ and $x^i w = x^p w$. Since $w \neq 0$, we have $x^{p-i} - 1 \in J(R) \setminus \{0\}$. Since $J(R)$ is a commutative ideal, we have $(x^{p-i} - 1)w = w(x^{p-i} - 1)$. Also, $(x^{p-i} - 1)x = x(x^{p-i} - 1)$, and so $x^{p-i} - 1 \in Z(R) \cap J(R) = 0$. Hence $o(x + J(R)) \leq p - 1$ and $|(R/J(R))^*| = p - 1$. Therefore $|R| = |J(R)|p = p^2$. This contradicts our first assumption that $|R| \notin \{p, p^2\}$.

To sum up, the two subcases show that R is a commutative ring. Now, let I be the minimal ideal contained in $J(R)$ with $\mathrm{char}(I) = p^i$. If $i > 1$, then Ip is a nontrivial ideal of R, so $I = Ip$. Let $s \in I$. Then $s = \sum vp$ for some $v \in I$. It follows that $sp^{i-1} = \sum vp^i = 0$, and so $\mathrm{char}(I) = p^{i-1}$, which is a contradiction. Therefore $\mathrm{char}(I) = p$. Clearly, $I^2 = 0$. For all $s \in I$, we have $(1 + s)^p = 1$. Therefore $1 + I$ is an elementary abelian p-group. Since Sylow p-subgroups of R^* are cyclic, we have $|1 + I| = |I| = p$. Therefore $I = \{0, a, 2a, 3a, \ldots, (p - 1)a\}$ for any nonzero element $a \in I$. By the first part of the proof of Case 2, R is a local ring. By the induction hypothesis, R/I is a finite field or $R/I \cong \mathbb{Z}_{p^v}$ where v is a positive integer.

First, suppose R/I is a finite field. Then $I = J(R)$ and $|R/I| = p^v$ for some positive integer v $(v \leq t)$. Therefore $(R/I)^*$ is a cyclic group. Let w be a generator for this group. A similar argument to that given in the first part of this case shows that $I = \{0, a, wa, \ldots, w^{p^v-1}a\}$ where $p^v - 1 = o(w + I)$. If $w^i a = w^j a$ for $i < j \leq p^v - 1$, then $w^{j-i} - 1 \in \mathrm{Ann}_R(a) = I$. Then $w^{j-i} + I = 1 + I$ and so $o(w + I) \leq j - i < p^v - 1$, which is a contradiction. If $v > 1$, then $|I| > p$, which is a contradiction. If $v = 1$, then $|R| = p^2$, which is again a contradiction. Now, let $R/I \cong \mathbb{Z}_{p^v}$. If $v = 1$, then

https://doi.org/10.1017/S0004972719000017 Published online by Cambridge University Press

$|R| = p^2$, a contradiction. Hence $v > 1$. Clearly, either $\mathrm{char}(R) = p^{v+1}$ or $\mathrm{char}(R) = p^v$. If $\mathrm{char}(R) = p^{v+1}$, then $R \cong \mathbb{Z}_{p^{v+1}}$, as desired. So suppose that $\mathrm{char}(R) = p^v$. Since $o(1 + p^{v-1}) = p$, we deduce that $I = Rp^{v-1} = \{jp^{v-1} : j = 0, 1, \ldots, p-1\}$. Let $o(x + I) = p^{v-1}$ for some $x \in R$. Since $R/I \cong Z_{p^v}$ and $o(x + I) = p^{v-1}$, we have $x - j \in J(R)$ for some integer j. Since $o(1 + p^{v-1}(x - j)) = p$, we have $p^{v-1}(x - j) \in I$. So there is an integer $1 \le f \le p-1$ such that $p^{v-1}(x - j) = p^{v-1} f$. Therefore $p^{v-1}(x - j - f) = 0$. If $x - j - f \in J(R)$, then $f \in J(R)$, which is a contradiction. If $x - j - f \in R^*$, then $p^{v-1} = 0$, which is also a contradiction. □

In the following three propositions, we characterise the rings of order 2^n, all of whose Sylow subgroups are cyclic. Since in this case $2 \mid |R|$, Proposition 2.5 may no longer be true. As an example, let R be the set of all 2×2 matrices over the finite field $GF(2)$. Then $R^* \cong S_3$, where S_3 is the symmetric group of order 6 and all its Sylow subgroups are cyclic, but R is noncommutative, is not a finite field and is not isomorphic with Z_{p^t} for any integer t. For simplicity, we denote by Δ the set of all rings R with $R \cong M_2(GF(2))$ or $R \cong M_2(GF(2)) \bigoplus_{i=1}^{k} GF(2^{n_i})$, where $\gcd(n_i, n_j) = 1 = \gcd(2, n_i)$ for all i, j with $1 \le i, j \le k$ and $i \ne j$.

Proposition 2.6. *Let R be a unitary ring of finite cardinality 2^n, such that $R = R_0[R^*]$. If every Sylow subgroup of R^* is cyclic, then either R is commutative or $R \in \Delta$.*

Proof. Let R be a noncommutative ring with minimal cardinality satisfying the assumptions stated in the proposition. We aim to show that $R \in \Delta$. We consider two cases depending on the Jacobson radical: either $J(R) = 0$ or $J(R) \ne 0$.

Case 1. If $J(R) = 0$, then R is a semi-simple Artinian ring and by the Artin–Wedderburn structure theorem, $R \cong \bigoplus_{i=1}^{t} M_{n_i}(D_i)$, where all the D_i are finite fields. If $t = 1$, the only possible case is $R \cong M_2(GF(2)) \in \Delta$. Let $t > 1$. If $n_i = 1$ for all i, then R is a commutative ring, a contradiction. It follows that there is some n_i with $n_i > 1$ and, as above, this implies that $n_i = 2$ and $D_i = GF(2)$. If there are two distinct indices i and j such that $n_i > 1$ and $n_j > 1$, then $M_{n_i}(D_i) \cong M_{n_j}(D_i) \cong M_2(GF(2))$ and the Sylow 2−subgroups of R^* are not cyclic, a contradiction. Therefore $n_j = 1$ for all $j \ne i$ and $\gcd(|D_j^*|, |D_s^*|) = 1$ for $1 \le j \ne s \le t$, that is, $R \in \Delta$, as desired.

Case 2. Suppose $J(R) \ne 0$. We show that this case always leads to a contradiction.

Let I be a minimal ideal of R with $0 \ne I \subseteq J(R)$. Arguing as in the proof of Proposition 2.5, $\mathrm{char}(I) = 2$, $I^2 = 0$ and I is an elementary abelian 2-group. Since a Sylow 2-subgroup of R^* is cyclic, $|I| = 2$ or $I = \{0, a\}$ for the unique nonzero element $a \in I$. Since $1 + I \lhd R^*$, we have $1 + I \le Z(R^*)$ and, from $R = R_0[R^*]$, it follows that $\mathrm{Ann}_R(I)$ is a two-sided ideal. By Lemma 2.2, $(R/I)^* = (R^* + I)/I$. Moreover every Sylow subgroup of $(R/I)^*$ is cyclic. By the minimality of R, either R/I is a commutative ring or $R/I \in \Delta$.

First, suppose R/I is a commutative ring. Then $[R, R] \subseteq I$. Since $R = R_0[R^*]$ and R is noncommutative, there are two elements $x, y \in R^*$, such that $xy \ne yx$, and at least one of them, say x, has odd order. Then $xyx^{-1}y^{-1} + I = 1 + I = 1 + \{0, a\}$ and

https://doi.org/10.1017/S0004972719000017 Published online by Cambridge University Press

$x^2yx^{-2}y^{-1} + I = 1 + I = 1 + \{0, a\}$, so $xyx^{-1}y^{-1} = 1 + a = x^2yx^{-2}y^{-1}$, which implies $yx = xy$, a contradiction. Now suppose that $R/I \in \Delta$. Either $R/I \cong M_2(GF(2))$ or $R/I \cong M_2(GF(2)) \bigoplus_{i=1}^{k} GF(2^{n_i})$, where $\gcd(n_i, n_j) = 1 = \gcd(2, n_i)$ for $1 \leq i, j \leq k$ and $i \neq j$. Let A be an ideal of R containing I such that $R/A \cong M_2(GF(2))$ and let $z + A \in (R/A)^*$ with $o(z + A) > 1$. Then $az \in I = \{0, a\}$, so $az = a$ and $z - 1 \in \mathrm{Ann}_R(I)$. Since R/A is a simple ring and $\mathrm{Ann}_R(I) = Ra = aR$ is a two-sided ideal, it follows that $\mathrm{Ann}_R(I) \subseteq A$, from which $z - 1 \in A$ and $o(z + A) = 1$, a contradiction. □

Let Γ be the set of all finite rings R such that $R \cong \mathbb{Z}_{2^v}$ or $R \cong \bigoplus_{i=1}^{k} GF(2^{n_i})$ or $R \cong \mathbb{Z}_{2^v} \bigoplus_{i=1}^{k} GF(2^{n_i})$, where $\gcd(n_i, n_j) = 1$ for $i \neq j$ and $v = 1, 2$. Let m be a positive integer and let C_m be a cyclic group of order m. We recall that for $v \geq 3$ the group $(\mathbb{Z}_{2^v})^* \cong C_{2^{v-2}} \times C_2$ is not cyclic.

Proposition 2.7. *Let R be a unitary commutative ring of finite cardinality 2^n, such that $R = R_0[R^*]$. If every Sylow subgroup of R^* is cyclic, then $R \in \Gamma$.*

Proof. We proceed by induction on n. The case $|R| = 2^2$ has already been discussed. Let $n > 2$. We consider two cases depending on the Jacobson radical: $J(R) = 0$ or $J(R) \neq 0$.

Case 1. Let $J(R) = 0$. Then R is a semi-simple ring and by the Wedderburn structure theorem, $R \cong \bigoplus_{i=1}^{k} R_i$ is a direct product of matrix rings over division rings. Since R is a commutative ring, all the R_i are finite fields and, by Remark 2.3, $\gcd(|(R_i)^*|, |(R_j)^*|) = 1$ for $1 \leq i \neq j \leq k$. Consequently, $R \in \Gamma$.

Case 2. Suppose $J(R) \neq 0$ and let $I \subseteq J(R)$ be a minimal ideal of R. Arguing as in the proof of Proposition 2.5, $\mathrm{char}(I) = 2$, $I^2 = 0$ and I is an elementary abelian 2-group. Since a Sylow 2-subgroup of R^* is cyclic, $|I| = 2$ or $I = \{0, a\}$, for a unique nonzero element $a \in I$. Let $y \in R \setminus \mathrm{Ann}_R(a)$. Since $ya \in I$, we have $(y - 1)a = 0$ and $y - 1 \in \mathrm{Ann}_R(a)$. Hence the group index $[(R, +) : (\mathrm{Ann}_R(a), +)] = 2$. By induction, $R/I \cong \mathbb{Z}_{2^v}$ or $R/I \cong \bigoplus_{i=1}^{k} GF(2^{n_i})$ or $R/I \cong \mathbb{Z}_{2^v} \bigoplus_{i=1}^{k} GF(2^{n_i})$, where $\gcd(n_i, n_j) = 1$ for $i \neq j$ and $v = 1, 2$.

If $R/I \cong \mathbb{Z}_{2^v}$, we claim that $R \cong \mathbb{Z}_{2^c}$, where $c = 1, 2$. Let $\mathrm{char}(R) = 2^r$. First suppose that $r = v$. If $2^r = 0$, then $(1 + 2^{r-1})^2 = 1$ and $2^{r-1} = a \in I$, a contradiction (because $R/I \cong \mathbb{Z}_{2^r}$). Hence $\mathrm{char}(R) = 2^{v+1}$ and $R \cong Z_{2^{v+1}}$, where $v + 1 = 2, 3$. If $v = 2$, then $R^* \cong C_2 \times C_2$, which is impossible. Hence $R/I \ncong \mathbb{Z}_{2^v}$. Now, suppose that $R/I \cong GF(2^v)$. By the earlier arguments, we may consider $v > 1$. Let $(R/I)^* = \langle z + I \rangle$. Then there exists $y \in R$ such that $y(z - 1) + I = 1 + I$. Since $z \notin \mathrm{Ann}_R(a)$, we have $z - 1 \in \mathrm{Ann}_R(a)$. But then $y(z - 1) - 1 \in I \subseteq \mathrm{Ann}_R(a)$ and $-1 \in \mathrm{Ann}_R(a)$, a contradiction. Therefore $R/I \ncong GF(2^v)$ and $R/I \ncong \mathbb{Z}_{2^v}$. It follows that either $R/I \cong \bigoplus_{i=1}^{k} GF(2^{n_i})$ or $R/I \cong \mathbb{Z}_{2^v} \bigoplus_{i=1}^{k-1} GF(2^{n_i})$, where $k > 1$, $v = 1, 2$ and $\gcd(n_i, n_j) = 1$ for $i \neq j$. Clearly $|J(R)| \leq 4$. Let $\{M_1, \ldots, M_k\}$ be the set of all maximal ideals of R. By the previous arguments, we may consider $k > 1$. We may assume that $M_1 = \mathrm{Ann}_R(a)$. Then $f : R/M_1 \oplus R/M_2 \oplus \cdots \oplus R/M_k \cong R/J(R)$. Let $f((1 + M_1, M_2, M_3, \ldots, M_k)) = x + J(R)$. It is clear that $|(\mathrm{Ann}_R(x) + J(R))/J(R)| = |R|/2|J(R)|$, so $|Rx| = |R/\mathrm{Ann}_R(x)| = 2|J(R)|$.

Since $ax \neq 0$, we have $a \notin \mathrm{Ann}_R(x)$. Since I is the unique minimal ideal of R and $a \notin \mathrm{Ann}_R(x)$, we have $\mathrm{Ann}_R(x) \cap J(R) = 0$. If $I = J(R)$, then clearly $I \subseteq Rx$. So suppose that $I \neq J(R)$. Then $J(R) = \{0, b, b^2 = a, b^3\}$. Since $J(R) \cap \mathrm{Ann}_R(x) = 0$, we have $bx \neq 0$. Then $J(R)x \subseteq Rx$. If $J(R)x \neq J(R)$, then $xb^i = 0$ for some positive integer i and so $xb^{2i} = xa = 0$, a contradiction. It follows that $J(R) \subseteq Rx$ and so $R = \mathrm{Ann}_R(x) \oplus Rx$. By the induction hypothesis, $\mathrm{Ann}_R(x)$ and Rx belong to the set Γ. Clearly $\gcd(|(\mathrm{Ann}_R(x))^*|, |(Rx)^*|) = 1$ and so $R \in \Gamma$, as desired. □

PROPOSITION 2.8. *Let R be a unitary ring of finite cardinality 2^n and $H = R_0[R^*]$ and suppose that every Sylow subgroup of R^* is a cyclic group. If H is a commutative ring and R is noncommutative, then either $R \cong T_2(GF(2))$ or $R \cong T_2(GF(2)) \oplus A$ where $A \in \Gamma$ and* $\gcd(|A^*|, 2) = 1$.

PROOF. Let R be a finite noncommutative ring with minimal cardinality 2^n, such that every Sylow subgroup of R is cyclic. Let $I \subseteq J(R)$ be a minimal ideal of R. From [3], every unitary noncommutative ring of order 8 is isomorphic to $T_2(GF(2))$, so we may assume that $|R| > 8$. By the minimality of R, either R/I is a commutative ring or $R/I \cong T_2(GF(2))$ or $R/I \cong T_2(GF(2)) \oplus A$ where $A \in \Gamma$ and $\gcd(|A^*|, 2) = 1$.

First suppose that R/I is noncommutative. Suppose that $f : R/I \cong T_2(GF(2)) \oplus A$. Let T/I be a subring of R/I, such that $T/I \cong T_2(GF(2))/I$. It is clear that $T_o[T^*] \neq T$ and $|J(T)| = 4$. By induction $T = T_2(GF(2))$ or $T_2(GF(2)) \oplus B$ where $B \in \Gamma$ and $\gcd(|B^*|, 2) = 1$. Hence $|J(T)| = 2$, a contradiction. Therefore $R/I \cong T_2(GF(2))$, $|R| = 16$, $\mathrm{char}(R) \leq 4$, R is a local ring and $J(R) = \{0, a, b, a + b\}$ where $a \in I \setminus \{0\}$. If $b^2 = 0$, then $o(1 + b) = 2$, and so a Sylow 2-subgroup of R^* is not cyclic, a contradiction. If $b^2 \neq 0$, then $ab = a(a + b) = 0$ and $b(a + b) = b^2 = (a + b)b$, so $J(R)$ is a commutative ideal. Choose $z \in R$ with $f(z + I) = 1$. Then $z - 1 \in J(R)$, since $f(z - 1 + I) \in J(T_2(GF(2)))$. Therefore $z \in C_R(J(R))$. Since the ring generated by z and $J(R)$ is R, it follows that R is a commutative ring, a contradiction.

Now suppose that R/I is commutative. Let $\{M_1, \ldots, M_k\}$ be the set of all maximal ideals of R and let $a \in I \setminus \{0\}$. If $k = 1$, then $J(R) = M_1 = \mathrm{Ann}_R(a)$, because R/I is commutative. Since $[R : \mathrm{Ann}_R(a)] = 2$, we have $R = R_0[(1 + J(R))] = R_0[R^*]$, a contradiction. So $k > 1$ and we may assume that $M_1 = \mathrm{Ann}_R(a)$. We have $f : R/M_1 \oplus R/M_2 \oplus \cdots \oplus R/M_k \cong R/J(R)$. Let $f((1 + M_1, M_2, M_3, \ldots, M_k)) = x + J(R)$ where $x \in R$. It is clear that $\mathrm{Ann}_R(x) \cong R/M_2 \oplus \cdots \oplus R/M_k \in \Gamma$ is a commutative ring, so $|(\mathrm{Ann}_R(x) + J(R))/J(R)| = |R|/2|J(R)|$. Since $ax \neq 0$, we have $a \notin \mathrm{Ann}_R(x)$. Since I is the unique minimal ideal of R and $a \notin \mathrm{Ann}_R(x)$, we have $\mathrm{Ann}_R(x) \cap J(R) = 0$. Then $|Rx| = |R/\mathrm{Ann}_R(x)| = 2|J(R)|$. If $I = J(R)$, then $I \subseteq Rx$. So suppose that $I \neq J(R)$. Then $J(R) = \{0, b, b^2 = a, b^3\}$. Since $J(R) \cap \mathrm{Ann}_R(x) = 0$, we have $bx \neq 0$ and $J(R)x \subseteq Rx$. If $J(R)x \neq J(R)$, then $xb^i = 0$ for some positive integer i and so $xb^{2i} = xa = 0$, a contradiction. It follows that $J(R) \subseteq Rx$, and hence that $R = \mathrm{Ann}_R(x) \oplus Rx$. Since R is not commutative, neither is Rx. By the induction hypothesis, either $Rx \cong T_2(GF(2))$ or $Rx \cong T_2(GF(2)) \oplus B$ where $B \in \Gamma$ and $\gcd(|B^*|, 2) = 1$. Hence either

https://doi.org/10.1017/S0004972719000017 Published online by Cambridge University Press

$R \cong \mathrm{Ann}_R(x) \oplus T_2(GF(2))$ or $R \cong \mathrm{Ann}_R(x) \oplus T_2(GF(2)) \oplus B$ for some positive integer k, where $\gcd(|B^*|, 2) = 1$. Clearly, $\mathrm{Ann}_R(x) \oplus B = A \in \Gamma$. □

Proof of Theorem 1.1. Let $|R| = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ be the canonical factorisation of $|R|$ into prime powers. Then $R = R_1 \oplus R_2 \oplus \cdots \oplus R_k$, where each R_i is an ideal of order $p_i^{\alpha_i}$ containing 1_{R_i}. We may assume that p_1 is a the smallest prime divisor of $|R|$. Let $E = 1$ and $O = R$ if $p_1 > 2$, and $E = R_1$ and $O = R_2 \oplus \cdots \oplus R_t$ if $p_1 = 2$. By Proposition 2.5, O is either a finite field or $\mathbb{Z}_{p^t}$, for a positive integer t.

First suppose that E is noncommutative. If $E = E_0[E^*]$, then by Proposition 2.6, $E \in \Delta$. If $E \neq E_0[E^*]$, then by Proposition 2.8, $E \in \Gamma$.

Now suppose that E is a commutative ring. If $J(E) = 0$, then by the Wedderburn structure theorem $E \in \Gamma$. Therefore suppose that $J(E) \neq 0$. Let I be a minimal ideal of E contained in $J(E)$ and $T = E_0[E^*]$. By Proposition 2.7, $T \cong \mathbb{Z}_{2^2}$ or $T \cong \mathbb{Z}_{2^2} \bigoplus_{i=1}^{s} GF(2^{n_i})$, where $\gcd(n_i, n_j) = 1$ for $i \neq j$. If $T = E$, then clearly, $E \in \Gamma$. Suppose that $T \neq E$. Then $2 \nmid |(E/I)^*| = |(T^* + I)/I|$ and $J(E) = I$. Let $\{M_1, \ldots, M_q\}$ be the set of all maximal ideals of E and let $a \in I \setminus \{0\}$. If $q = 1$, then $J(E) = M_1 = \mathrm{Ann}_E(a)$. Since $[E : \mathrm{Ann}_E(a)] = 2$, we have $E = E_0[(1 + J(E))] = E_0[E^*] = T$, a contradiction. So $q > 1$. We may assume that $M_1 = \mathrm{Ann}_E(a)$. Then $f : E/M_1 \oplus E/M_2 \oplus \cdots \oplus E/M_q \cong E/J(E)$. Let $f((1 + M_1, M_2, M_3, \ldots, M_q)) = x + J(E)$, where $x \in E$. By a similar argument to that in Proposition 2.8, $E = \mathrm{Ann}_E(x) \oplus Ex$ and $J(E) \subseteq Ex$. Clearly $\gcd((\mathrm{Ann}_E(x))^*, 2) = 1$, because $\mathrm{Ann}_E(x) \cap J(E) = 0$. Since $J(E) \subseteq Ex$ and $|Ex| = 4$, we have $Ex \cong \mathbb{Z}_{2^2}$ and it follows that $E \in \Gamma$. The rest of the proof is clear. □

Acknowledgement

The authors would like to thank the referees for careful reading and useful comments which improved the paper.

References

[1] D. Dolzan, 'Nilpotency of the group of units of a finite ring', *Bull. Aust. Math. Soc.* **79** (2009), 177–182.
[2] K. E. Eldridge, 'Orders for finite noncommutative rings with unity', *Amer. Math. Monthly* **75** (1968), 512–514.
[3] D. B. Erickson, 'Orders for finite noncommutative rings', *Amer. Math. Monthly* **73** (1966), 376–377.
[4] B. Farb and R. Keith Dennis, *Noncommutative Algebra*, Graduate Texts in Mathematics, 144 (Springer, New York, 1993).
[5] G. Groza, 'Artinian rings having a nilpotent group of units', *J. Algebra* **121** (1989), 253–262.
[6] T. Y. Lam, *A First Course in Noncommutative Rings*, Graduate Texts in Mathematics, 2nd edn (Springer, New York, 2001).
[7] J. H. M. Wedderburn, 'A theorem on finite algebra', *Trans. Amer. Math. Soc.* **6** (1905), 349–352; 1996.

M. AMIRI, Departamento de Matemática-ICE-UFAM,
69080-900, Manaus-AM, Brazil
e-mail: mohsen@ufam.edu.br

M. ARIANNEJAD, Department of Mathematics,
University of Zanjan, Zanjan, Iran
e-mail: arian@znu.ac.ir