EUROPEAN JOURNAL OF PURE AND APPLIED MATHEMATICS
Vol. 7, No. 1, 2014, 109-113
ISSN 1307-5543 – www.ejpam.com

On Distinguishing Local Finite Rings from Finite Rings Only by Counting Elements and Zero Divisors

Marcos J. González

Departamento de Matemáticas, Universidad Simón Bolívar, Caracas 1080-A, Venezuela

Abstract. The purpose of this short communication is to prove the following: *Let* R *be a finite associative ring with unit. Then* R *is local if and only if* $|R| = p^n$ *and* $|Z(R)| = p^m$ *for some prime number* p *and integers* $1 \leq m < n$. For the commutative case, this have been recently discovered by Behboodi and Beyranvand [1, Theorem 3]. We will also present yet another proof for the commutative case.

2010 Mathematics Subject Classifications: 16B99, 13A99, 68R10

Key Words and Phrases: Finite ring, Zero-divisor, Local rings

1. Introduction

The purpose of this paper is to prove the following:

Theorem 1. *Let* R *be a finite associative ring with unit. Then* R *is local if and only if* $|R| = p^m$ *and* $|Z(R)| = p^n$ *for some prime number* p *and integers* $1 \leq n < m$.

This allows us to recognize local rings out of finite rings only by counting the number of elements in the ring and the number of zero divisors. This result is inspired by the corresponding result Behboodi and Beyranvand [1, Theorem 3, pp. 306–307] where R is assumed to be commutative.

More precisely, they proved the following:

Theorem 2. *Let* R *be a finite commutative ring with unit. Then* R *is local if and only if* $|R| = p^m$ *and* $|Z(R)| = p^n$ *for some prime number* p *and integers* $1 \leq n < m$.

We will also provide another proof for this theorem which differs both from the proof of Theorem 1 and the original proof presented in [1].

Email address: mago@usb.ve

2. Preliminaries

Almost all the facts we require for the both proofs can be found in McDonald's monograph [4]. We use a different notation though, similar to the one used in [1].

The letter R always denotes a finite associative ring with identity. An element $r \in R$ is said to be *invertible* is there exists $s \in R$ such that $rs = sr = 1$. The set of all invertible elements of R forms a group denoted by $R^\times$. An element $r \in R$ is said to be a *left (right, resp.) zero divisor* if there exists $s \in R$ such that $sr = 0$ ($rs = 0$, resp.) and r is said to be a *two-sided zero divisor* if it is both a left and a right zero divisor. The set of all zero divisors is denoted by $Z(R)$. For R a finite ring with identity, any zero divisor is a two-sided zero divisor and every element that is not a zero divisor is invertible (see Ganesan [2, Theorem 5, p.245]). Consequently,

(i) $|R^\times| = |R| - |Z(R)|$, and

(ii) If $R = R_1 \oplus \cdots \oplus R_t$ is a direct sum of rings, then $R^\times = R_1^\times \oplus \cdots \oplus R_t^\times$.

The symbol $J(R)$ denotes *the Jacobson radical*, or briefly *the radical*, of R, which can be equivalently defined as:

(a) the intersection of all left maximal ideals of R, or

(b) the intersection of all right maximal ideals of R, or

(c) the set of all elements $r \in R$ such that $1 + sr$ is invertible for every $s \in R$.

Consequently, $1 + J(R)$ is a subgroup of the group $R^\times$ of invertible element in R. A finite ring R is *semi-simple* if and only if $J(R) = \{0\}$. For any finite ring R, the quotient ring $R/J(R)$ is semi-simple. A finite ring R is local if and only if $R/J(R)$ is a finite field, called *the residue field*. Notice that a semi-simple ring is local if and only if it is a field. Finite fields are denoted by $\mathbb{F}_q$, where $q = |\mathbb{F}_q|$ is a power of some prime. If $\mathbb{F}_q$ is the residue field of some finite local ring having p^n elements, then $q = p^r$, for some $1 \leq r \leq n$.

In 1969, Raghavendra [5] proved the following:

Proposition 1. *Let R be a finite ring with multiplicative identity $1 \neq 0$ and suppose that the set of zero divisors $Z(R)$ forms an additive group. Then*

(i) *$Z(R)$ is the Jacobson radical of R;*

(ii) *$|R| = p^{nr}$, and $|J| = p^{(n-1)r}$ for some prime number p, and some positive integers n, r;*

(iii) *$Z(R)^n = \{0\}$;*

(iv) *the characteristic of the ring R is p^k for some integer k with $1 \leq k \leq n$, where p is the same prime number as in (ii); and*

(v) *if the characteristic of the ring R is p^n (i.e., the largest possible choice of p^k in (iv)), then R is commutative.*

We also refer to Gilmer [3] where alternative proofs for some of these results can be found, as well as examples showing that all possible values of n, r and k in the above proposition already appear in the commutative case.

3. Proof of Theorem 1

In this section, we shall provide a proof for Theorem 1. This also provides a new proof for Theorem 2. Our idea is to reduce the statement to the case in which R is semi-simple. It is natural to replace R by $R/J(R)$ and the next lemma tells us that, if we do so, the hypotheses still hold for $R/J(R)$.

Lemma 1. *Let p be a prime number, and let R be a finite ring with identity such that $|R| = p^m$ and $|Z(R)| = p^n$, for some $0 \leq n < m$, and let $S := R/J(R)$. Then, $|S| = p^{m-k}$ and $|Z(S)| = p^{n-k}$, where $0 \leq k \leq n$ is the integer determined by $|J(R)| = p^k$.*

Let $\pi\colon R \to S = R/J(R)$ be the quotient map. Then the restriction $\pi|_{R^\times} : R^\times \to S^\times$ is a surjective group homomorphism. Since $\ker \pi|_{R^\times} = 1 + J(R)$, we have that $R^\times/(1+J(R)) \cong S^\times$. Consequently,

$$|S^\times| = \frac{|R^\times|}{|1+J(R)|} = \frac{|R|-|Z(R)|}{|J(R)|} = \frac{|R|}{|J(R)|} - \frac{|Z(R)|}{|J(R)|} = p^{m-k} - p^{n-k},$$

which implies that $|Z(S)| = |S| - |S^\times| = p^{n-k}$. This concludes the proof of the lemma.

Now we can prove Theorem 1. The forward direction follows from Proposition 1, *(ii)*. For the converse, let R be such that $|R| = p^m$ and $|Z(R)| = p^n$. Suppose first that $J(R) = \{0\}$. In this case, R is semi-simple and the Wedderburn-Artin theorem (cf. [4, Theorem VIII.4, pp.128–130]) asserts that R is a direct sum of full matrix rings over fields. More precisely, there exist finite fields $\mathbb{F}_{q_1}, \ldots, \mathbb{F}_{q_t}$ having $q_s = p^{d_s}$ elements, for every $s = 1, \ldots, t$ and positive integers $n_1, \ldots, n_t$, such that

$$R = M_{n_1}\left(\mathbb{F}_{q_1}\right) \oplus \cdots \oplus M_{n_t}\left(\mathbb{F}_{q_t}\right) = R_{n_1,q_1} \oplus \cdots \oplus R_{n_t,q_s}, \tag{1}$$

where $R_{n,q} := M_n(\mathbb{F}_q)$. Now clearly $|M_n(\mathbb{F}_q)| = q^{n^2}$ and the group of invertible elements in $M_n(\mathbb{F}_q)$ is the general linear group $GL_n(\mathbb{F}_q)$ which has

$$(q^n - 1)(q^n - q)\ldots(q^n - q^{n-1}) = q^{n(n-1)/2}\prod_{k=1}^{n}(q^k - 1)$$

elements (cf. [4, Theorem VIII.19, p.156]). Since $|R| = p^m$, we have that $q_s = p^{d_s}$, for every $s = 1, \ldots, t$ (that is, all the q_s's are powers of the same prime) and the numbers d_s satisfy the equation $m = \sum_{s=1}^{t} n_s^2 d_s$. Since $R^\times = R^\times_{n_1,q_1} \oplus \cdots \oplus R^\times_{n_t,q_t}$, we have that

$$\begin{aligned}
|Z(R)| =& |R| - |R^\times| = |R| - |R^\times_{n_1,q_1}| \times \cdots \times |R^\times_{n_t,q_t}| \\
=& p^m - \prod_{s=1}^{t}\left(q_s^{n_s(n_s-1)/2}\prod_{k=1}^{n_s}(q_s^k - 1)\right) \\
=& \prod_{s=1}^{t} q_s^{n_s^2} - \left(\prod_{s=1}^{t} q_s^{n_s(n_s-1)/2}\right)\left(\prod_{s=1}^{t}\prod_{k=1}^{n_s}(q_s^k - 1)\right)
\end{aligned}$$

$$= \prod_{s=1}^{t} q_s^{n_s(n_s-1)/2} \left(\prod_{s=1}^{t} q_s^{n_s(n_s+1)/2} - \prod_{s=1}^{t} \prod_{k=1}^{n_s} (q_s^k - 1) \right),$$

and hence $|Z(R)|$ is a power of p if and only if $\Delta := \prod_{s=1}^{t} q_s^{n_s(n_s+1)/2} - \prod_{s=1}^{t} \prod_{k=1}^{n_s} (q_s^k - 1)$ is a power of p. Since $\Delta \equiv \pm 1 \bmod p$, and $\Delta \neq 1$ unless $n_1 = \cdots = n_t = 1$, and $t = 1$, we conclude that $|Z(R)|$ is a power of p if and only if $R = \mathbb{F}_{q_1}$. For the general case, we have that $S = R/J(R)$ is semi-simple and, according to Lemma 1, both $|S|$ and $Z(S)$ are powers of p. Consequently, by applying the first part of the proof, S is a field and hence R is a local ring. □

4. New Proof of Theorem 2

In this section, we shall provide a new proof for Theorem 2 based on the fact that, for the case in which R is a finite commutative ring, the Jacobson radical $J(R)$ coincides with the ideal of all the nilpotent elements of the ring R.

Let R be finite commutative ring with identity of order $|R| = p^m$ and having $|Z(R)| = p^n$ zero divisors. We want to prove that R is local, for which it is enough to prove that $Z(R) = J(R)$. Moreover, since $J(R) \subset Z(R)$, it is enough to prove that $|J(R)| = |Z(R)|$. Since $|R^\times| = |R| - |Z(R)| = (p^{m-n} - 1)p^n$, and the integers $p^{m-n} - 1$ and p^n are relatively prime, there exists a Sylow p-subgroup of $|R^\times|$, say G, having order p^n (cf. Wielandt [6]). We claim that $G \subset 1 + J(R)$. Indeed, the characteristic of R is a power of p, and in particular p is nilpotent, so $p \in J(R)$. We have that $(a + b)^p = a^p + b^p + c$, where c is nilpotent, whence $c \in J(R)$. Let $g \in G$ be an arbitrary element. Then $g^{p^n} = 1$ (because p^n is the order of G). Hence we can conclude that $(g - 1)^{p^n} = g^{p^n} - 1 + d = d \in J(R)$ (even for the case $p = 2$ because $1 = -1 + p$) and so $g - 1 \in J(R)$ (because, if some power of $a \in R$ belongs to $J(R)$, then $a \in J(R)$). We have proved that $g \in 1 + J(R)$, for every $g \in G$, that is, $G \subset 1 + J(R)$, as claimed. Finally, $p^n = |G| \leq |1 + J(R)| = |J(R)| \leq |Z(R)| = p^n$ and hence $|J(R)| = p^n = |Z(R)|$, whence $J(R) = Z(R)$. □

5. Final Remarks

Concerning the proof of Theorem 1, the present version of Wedderburn-Artin Theorem given by [4, Theorem VIII.4, pp.128–130], asserts that there exist finite fields $\mathbb{F}_{q_1}, \ldots, \mathbb{F}_{q_t}$ and some positive integers $n_1, \ldots, n_t$ such that

$$R = M_{n_1}\left(\mathbb{F}_{q_1}\right) \oplus \cdots \oplus M_{n_t}\left(\mathbb{F}_{q_t}\right). \tag{2}$$

The fact that $\mathbb{F}_{q_s}$ has $q_s = p^{d_s}$ elements, for every $s = 1, \ldots, t$, is a consequence of two facts:

(i) $\left|M_{n_s}\left(\mathbb{F}_{q_s}\right)\right|$ divides $|R|$ for every $s = 1, \ldots, t$, and

(ii) the assumption that $|R| = p^m$.

Finally, we have that

$$p^m = |R| = \left|M_{n_1}\left(\mathbb{F}_{q_1}\right)\right| \times \cdots \times \left|M_{n_t}\left(\mathbb{F}_{q_t}\right)\right| = \prod_{s=1}^{t} p^{n_s^2 d_s}$$

and hence we obtain the condition $m = \sum_{s=1}^{t} n_s^2 d_s$.

ACKNOWLEDGEMENTS The author is indebted to Professor Marek Wójtowicz for making many important observations regarding the composition of this paper.

References

[1] M. Behboodi and R. Beyranvand. On the Structure of Commutative Rings with $p_1^{k_1} \cdots p_n^{k_n}$ ($1 \leq k \leq 7$) zero divisors. *European Journal of Pure and Applied Mathematics*, 3(2):303–316, 2010.

[2] N. Ganesan. Properties of rings with a finite number of zero-divisors II. *Mathematische Annale*, 161:241–246, 1965.

[3] R. Gilmer. Zero-divisors in commutative rings. *The American Mathematical Monthly*, 93(5):382–387, 1986.

[4] B. R. McDonald. *Finite Rings with Identity*. Marcel Dekker, New York, 1974.

[5] R. Raghavendran. Finite associative rings. *Compositio Mathematica*, 21:195–229, 1969.

[6] H. Wielandt. Ein Beweis für die Existenz der Sylowgruppen. *Archiv der Mathematik*, 10(1):401–402, 1959.