EUROPEAN JOURNAL OF PURE AND APPLIED MATHEMATICS
Vol. 3, No. 2, 2010, 303-316
ISSN 1307-5543 – www.ejpam.com

On the Structure of Commutative Rings with ${p_1}^{k_1} \cdots {p_n}^{k_n}$ $(1 \leq k_i \leq 7)$ Zero-Divisors

M. Behboodi[1,2]* and R. Beyranvand[1]

[1] *Department of Mathematical Science, Isfahan University of Technology, Isfahan, Iran*
[2] *School of Mathematics, Institute for Research in Fundamental Sciences (IPM), Tehran, Iran*

Abstract. Let R be a finite commutative ring with identity and $Z(R)$ denote the set of all zero-divisors of R. Note that R is uniquely expressible as a direct sum of local rings R_i $(1 \leq i \leq m)$ for some $m \geq 1$. In this paper, we investigate the relationship between the prime factorizations $|Z(R)| = {p_1}^{k_1} \cdots {p_n}^{k_n}$ and the summands R_i. It is shown that for each i, $|Z(R_i)| = {p_j}^{t_j}$ for some $1 \leq j \leq n$ and $0 \leq t_j \leq k_j$. In particular, rings R with $|Z(R)| = p^k$ where $1 \leq k \leq 7$, are characterized. Moreover, the structure and classification up to isomorphism all commutative rings R with $|Z(R)| = {p_1}^{k_1} \ldots {p_n}^{k_n}$, where $n \in \mathbb{N}$, p_i's are distinct prime numbers, $1 \leq k_i \leq 3$ and nonlocal commutative rings R with $|Z(R)| = p^k$ where $k = 4$ or 5, are determined.

2000 Mathematics Subject Classifications: 16B99; 13A99; 68R10

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

---

1. Introduction

Throughout the paper R always denotes a commutative ring with identity, $J(R)$ is the Jacobson radical of R and $Z(R)$ denotes the set of all zero-divisors of R. We denote F_q for the finite field of order q and for any finite subset Y of R, we denote $|Y|$ for the cardinality of Y.

The zero-divisor graph of R, denoted by $\Gamma(R)$, is the graph whose vertices are the nonzero zero-divisors of R with two distinct vertices a and b joined by an edge if and only if $ab = 0$. One might ask which graphs on n vertices can be realized as the zero-divisor graph of a commutative ring? This question has been partially answered. [1] determines, up to isomorphism, all such rings for which $\Gamma(R)$ is a graphs on $n = 1, 2, 3,$ or 4 vertices. This list was extended to $n = 5$ vertices in [10], and to $n = 6, 7, \ldots, 14$ vertices in [11]. The aim of the paper is to develop this list to a wider class of numbers n. In fact, this observation motivates us the

*Corresponding author.

Email addresses: `mbehbood@cc.iut.ac.ir` (M. Behboodi), `r_beyranvand@math.iut.ac.ir` (R. Beyranvand)

following fundamental question:

Question. If R is a finite commutative ring, can we find the relationship between the prime factorizations $|Z(R)| = {p_1}^{k_1} \cdots {p_n}^{k_n}$ and the summands R_i, where $R = R_1 \times R_2 \times \ldots \times R_m$ ($m \geq 1$) and $R_i^{,}s$ are local rings?

Then we will give an answer to this question. We show that the answer is "yes" and a preliminary answer is given in Theorem 1 of Section 2; which shows that if R is a finite commutative ring, then either R is a reduced ring or there are positive integers s, m, $t_1, \ldots, t_s$, prime numbers $p_1, p_2, \ldots, p_s$ and a non-negative integer t such that $|Z(R)| = {p_1}^{t_1}{p_2}^{t_2}\ldots{p_s}^{t_s}m$ and $R \cong R_1 \times \ldots \times R_s \times F_{q_1} \times \ldots \times F_{q_t}$ with $|Z(R_i)| = p_i^{t_i}$. Therefore, in classifying commutative rings with ${p_1}^{k_1}\ldots{p_n}^{k_n}$ zero-divisors it suffices to deal with local rings with ${p_i}^{t_i}$ zero-divisors where that $1 \leq i \leq n$ and $0 \leq t_i \leq k_i$, and henceforth we focus on rings R with $|Z(R)| = p^k$ where p is a prime number and $k \geq 1$. It is shown that a finite commutative ring R is local if and only if $|Z(R)| = p^k$ and $|R| = p^n$ for some prime number p and $n > k \geq 0$ (Theorem 3). In Section 3, first we characterize commutative rings R with $|Z(R)| = p^k$ where $1 \leq k \leq 7$. Then the structure and classification up to isomorphism all commutative rings R with $|Z(R)| = {p_1}^{k_1}\ldots{p_n}^{k_n}$, where $n \in \mathbb{N}$, $p_i^{,}s$ are distinct prime numbers and $1 \leq k_i \leq 3$, are determined. Finally, we determine the structure of nonlocal rings R with $|Z(R)| = p^k$ where $k = 4$ or 5.

2. On Rings with p^k Zero-Divisors

Recall that an Artinian commutative ring R is called *completely primary* if $R/J(R)$ is a field. One can easily see that an Artinian commutative ring R is completely primary if and only if $Z(R)$ is an ideal of R, if and only if R is a local ring. Moreover, we have the following lemma which is essentially Theorem 2 of [9].

Lemma 1. *[9, Theorem 2] Let R be a finite completely primary ring. Then*

(i) $Z(R) = J(R)$;

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

(iii) $Z(R)^n = (0)$;

(iv) $char(R) = p^k$ *for some integer k with* $1 \leq k \leq n$;

(v) $R/J(R) \cong F_q$, *where* $q = p^r$.

Let R_i ($1 \leq i \leq s$) be a finite commutative ring with m_i elements and n_i zero-divisors. Let $R = R_1 \times \ldots \times R_s$. Then by [6, Theorem 2], $|Z(R)| = m_1 m_2 \ldots m_s - (m_1 - n_1)(m_2 - n_2)\ldots(m_s - n_s)$. Thus by using this fact, Lemma 1 and the fact that every finite commutative ring is uniquely expressible as a direct sum of completely primary (local) rings (see for example [8, p.95]), we have the following evident result.

Lemma 2. *Let R be a finite commutative ring. Then $R \cong R_1 \times \ldots \times R_s$ where $s \in \mathbb{N}$ and R_i's are local rings with $|R_i| = p_i^{k_i}$, $|Z(R_i)| = p_i^{t_i}$ for some prime numbers $p_1, p_2, \ldots, p_s$ and $k_i \geq 1$, $t_i \geq 0$. Consequently,*

$$|Z(R)| = \prod_{i=1}^{s} p_i^{t_i} (\prod_{i=1}^{s} p_i^{k_i - t_i} - \prod_{i=1}^{s} (p_i^{k_i - t_i} - 1)).$$

Now we are in position to prove the following two theorems which are crucial in our investigation.

Theorem 1. *Let R be a finite commutative ring. Then*

(i) if R is reduced, then there are finite fields $F_{q_1}, \ldots, F_{q_t}$ $(t \geq 1)$ such that $R \cong F_{q_1} \times \ldots \times F_{q_t}$ with $|Z(R)| = q_1 q_2 \ldots q_t - (q_1 - 1)(q_2 - 1) \ldots (q_t - 1)$.

(ii) if R is not reduced, then there are a positive integer s, a non-negative integer t, prime numbers $p_1, p_2, \ldots, p_s$ and positive integers $k_1, \ldots, k_s$ such that

$$|Z(R)| = \prod_{i=1}^{s} p_i^{t_i} [q_1 \ldots q_t \prod_{i=1}^{s} p_i^{k_i - t_i} - (q_1 - 1) \ldots (q_t - 1) \prod_{i=1}^{s} (p_i^{k_i - t_i} - 1)] \quad (1)$$

and $R \cong R_1 \times \ldots \times R_s \times F_{q_1} \times \ldots \times F_{q_t}$ where each F_{q_i} is a finite field and each R_i is a finite local ring such that $|Z(R_i)| = p_i^{t_i}$ for some $1 \leq t_i \leq k_i$.

Consequently, for each $i = 1, \ldots, s$, $|Z(R_i)|$ is a divisor of $|Z(R)|$.

Proof. The proof is clear by Lemma 1 and Lemma 2.

Theorem 2. *Let R be a commutative ring such that $|Z(R)| = p^k$ for some prime number p and a positive number k. Then either*

(i) R is local,

(ii) R is reduced, or

(iii) $k \geq 3$ and $R \cong R_1 \times \ldots \times R_s \times F_{q_1} \times \ldots \times F_{q_t}$ where s and t are positive integers, each F_{q_i} is a field, and where each R_i is a commutative finite local ring with $|Z(R_i)| = p^{t_i}$, $|R_i| = p^{k_i}$ for some positive integers k_i and t_i with $1 \leq \sum_{i=1}^{s} t_i \leq \sum_{i=1}^{s} k_i - s \leq k - s - 1$ such that

$$p^{k - \Sigma_{i=1}^{s} t_i} = q_1 \ldots q_t p^{\Sigma_{i=1}^{s} (k_i - t_i)} - (q_1 - 1) \ldots (q_t - 1) \Pi_{i=1}^{s} (p^{k_i - t_i} - 1). \quad (2)$$

Consequently, in the latter case, $t_i \leq k - 2$ for each $i = 1, \ldots, s$ and $q_j \equiv 1 \ (p)$ for some j. Moreover, if $t_i = k - 2$ for some i, then $s = t = 1$, i.e., $R \cong R_1 \times F_q$ where $|Z(R_1)| = p^{k-2}$ and so $p^2 = p + q - 1$.

Proof. Suppose R is not local. Then $R \cong R_1 \times \ldots \times R_n$, where $n \geq 2$ and each R_i is a local ring. If for each i $(1 \leq i \leq n)$ R_i is not field, then $|Z(R_i)| = p^{t_i}$ and $|R_i| = p^{k_i}$ for some $1 \leq t_i < k_i \leq k$. By the relation (1) of Theorem 1, we have

$$p^k = p^{\sum_{i=1}^{s} t_i}[p^{\sum_{i=1}^{s}(k_i - t_i)} - \prod_{i=1}^{s}(p^{k_i - t_i} - 1)]$$

and hence

$$p^{k - \sum_{i=1}^{s} t_i} = p^{\sum_{i=1}^{s}(k_i - t_i)} - \prod_{i=1}^{s}(p^{k_i - t_i} - 1).$$

This implies that $0 \equiv 1(p)$ or $0 \equiv -1(p)$, a contradiction. Thus R_j is field for some $1 \leq j \leq n$. If each R_i is field, then R is a reduced ring. Suppose R is non-reduced. Without loss of generality we can assume that

$$R \cong R_1 \times \ldots \times R_s \times F_{q_1} \times \ldots \times F_{q_t}$$

where $s, t \geq 1$ and each R_i is a commutative finite local ring with $|Z(R_i)| = p^{t_i}$ and $|R_i| = p^{k_i}$ for some $1 \leq t_i < k_i \leq k$. Since $t \geq 1$, it is easy to check that

$$p^k = |Z(R)| > \prod_{i=1}^{s} |R_i| = p^{\sum_{i=1}^{s} k_i} \geq p^{\sum_{i=1}^{s}(t_i + 1)} = p^{(\sum_{i=1}^{s} t_i) + s}.$$

Consequently we have $1 \leq \sum_{i=1}^{s} t_i \leq \sum_{i=1}^{s} k_i - s \leq k - s - 1$ and hence we obtain relation (2). Now since $k - \sum_{i=1}^{s} t_i$ and $\sum_{i=1}^{s}(k_i - t_i)$ are positive, the relation (2) shows that $q_i \equiv 1(p)$ for some i. Also, since $s \geq 1$, $t_i \leq k - 2$ for each $i = 1, \ldots, s$. If $t_j = k - 2$ for some $j \in \{1, \ldots, s\}$, then $s = 1$. Thus $R \cong R_1 \times F_{q_1} \times \ldots \times F_{q_t}$, where R_1 is a local ring with $|Z(R_1)| = p^{k-2}$. Since $|Z(R)| = p^k$ and $t \geq 1$, by Theorem 1, $|R_1| = p^{k-1}$. Also by the relation (2) we have

$$p^2 = pq_1q_2 \ldots q_t - (p-1)(q_1 - 1)(q_2 - 1) \ldots (q_t - 1).$$

Since $q_i \equiv 1 \ (p)$ for some i, we can assume that $q_1 \equiv 1 \ (p)$ and so $q_1 > p$. Now if $t \geq 2$, then $|Z(R)| \geq |R_1|q_1 > p^{k-1}p = p^k$, a contradiction. Thus $t = 1$ and $p^2 = pq_1 - (p-1)(q_1 - 1)$, i.e., $p^2 = p + q_1 - 1$.

Obviously for every finite local ring R we have $|R| = p^n$ for some prime number p and $n \geq 0$. In general, the converse is not true (the nonlocal ring $F_2 \times F_2$ has 4 elements). Here we show that a finite ring R is local if and only if $|Z(R)| = p^m$ and $|R| = p^n$ for some prime number p and $n > m \geq 0$.

Theorem 3. *Let R be a commutative ring. Then R is a finite local ring if and only if $|Z(R)| = p^k$ and $|R| = p^n$ for some prime number p and $n > k \geq 0$.*

Proof. For one direction, the proof is clear by Lemma 1. For the other direction, suppose that $|Z(R)| = p^k$ and $|R| = p^n$ for some prime number p and $n > k \geq 0$. If R is not a local ring, then by Theorem 2, either $R \cong F_{q_1} \times \ldots \times F_{q_t}$ (when R is reduced) or $R \cong R_1 \times \ldots \times R_s \times F_{q_1} \times \ldots \times F_{q_t}$ where s and t are positive integers and each R_i is a commutative finite local ring that is not a field, and where each F_{q_i} is a field. Since $|R| = p^n$, each q_i is a divisor of p^n and since q_i is a prime power, $q_i \equiv 0$ (p) for each i $(1 \le i \le t)$. If R is reduced, then we have $p^k = q_1 \dots q_t - (q_1 - 1)\dots(q_t - 1)$ and if R is not reduced, then we have

$$p^{k-\Sigma_{i=1}^s t_i} = q_1 \dots q_t p^{\Sigma_{i=1}^s (k_i - t_i)} - (q_1 - 1)\dots(q_t - 1)\Pi_{i=1}^s (p^{k_i - t_i} - 1).$$

Thus in any case $0 \equiv 1(p)$ or $0 \equiv -1(p)$, which is impossible. Thus R is a local ring.

3. On Commutative Rings with ${p_1}^{k_1} \dots {p_n}^{k_n} (1 \le k_i \le 7)$ Zero-Divisors

By Lemma 1, for each finite local ring R we have $|Z(R)| = p^k$ for some prime number p and $k \ge 0$, but the converse is not true in general. For example, the nonlocal ring $\mathbb{Z}_8 \times F_7$ has 32 zero-divisors. In this section, we will characterize rings with p^k zero-divisors where k is a positive integer $1 \le k \le 7$.

Theorem 4. *Let R be a commutative ring with $|Z(R)| = p^k$ where p is a prime number and $1 \le k \le 6$. Then either*

(i) R is a local ring;

(ii) R is a reduced ring and so $R \cong F_{q_1} \times \dots \times F_{q_t}$, where each F_{q_i} $(1 \le i \le t)$ is a finite field and $p^k = q_1 q_2 \dots q_t - (q_1 - 1)(q_2 - 1)\dots(q_t - 1)$;

(iii) $R \cong R_1 \times F_{q_1} \times \dots \times F_{q_t}$, where each F_{q_i} $(1 \le i \le t)$ is a finite field and R_1 is a local ring with $|Z(R_1)| = p^m$, $|R_1| = p^n$ such that $0 < m < n \le k - 1$ and $p^k = p^n q_1 q_2 \dots q_t - (p^n - p^m)(q_1 - 1)(q_2 - 1)\dots(q_t - 1)$; or

(iv) $R \cong R_1 \times R_2 \times F_5$ where each R_i is isomorphic to $\mathbb{Z}_4$ or $\mathbb{Z}_2[x]/(x^2)$.

Proof. Suppose $|Z(R)| = p^k$ and R is not a local ring. If R is reduced, then we are done. Now let R is not a reduced ring. Then by Theorem 2, we can assume that $R \cong R_1 \times \dots \times R_s \times F_{q_1} \times \dots \times F_{q_t}$, where $s,\ t \ge 1$ and each R_i is a local ring with $|Z(R_i)| = p^{t_i}$, $|R_i| = p^{k_i}$ for some $t_i,\ k_i \ge 1$ such that

$$1 \le \sum_{i=1}^{s} t_i \le \sum_{i=1}^{s} k_i - s \le k - s - 1 \le 6 - 1 - 1 = 4.$$

It follows that $s \le 4$. If $s = 3$ or 4, then since $t \ge 1$, $p^k = |Z(R)| > |R_1||R_2||R_3| \ge p^6$, this is a contradiction. Hence $s \le 2$. If $s = 1$, then by Theorem 2, we are done. Thus we can assume that $s = 2$, i.e., $R \cong R_1 \times R_2 \times F_{q_1} \times \dots \times F_{q_t}$, where R_1 and R_2 are local rings with $|Z(R_i)| = p^{t_i}$. Clearly $|R_i| \ge p^{t_i+1}$ for $i = 1,\ 2$ and since $t \ge 1$, $|Z(R)| > |R_1||R_2|$. If $t_i \ge 3$ for some i or $t_1 = t_2 = 2$, then $|Z(R)| > |R_1||R_2| = p^{t_1+t_2+2} \ge p^6$, a contradiction. Thus without loss of generality we can assume that either $t_1 = 2$, $t_2 = 1$ or $t_1 = t_2 = 1$.

- Case 1: $t_1 = 2$, $t_2 = 1$ i.e., $|Z(R_1)| = p^2$ and $|Z(R_2)| = p$. Then by Lemma 1, we conclude that $|R_1| = p^3$ or $|R_1| = p^4$ and $|R_2| = p^2$. If $|R_1| = p^4$, then $|Z(R)| > p^6$, a contradiction. Thus $|R_1| = p^3$ and $|R_2| = p^2$ and so $|Z(R)| > |R_1||R_2| \geq p^5$ i.e., $k = 6$. We claim that $t = 1$, for if not, since $q_i > p$ for some i (see Theorem 2), $|Z(R)| \geq |R_1||R_2||F_{q_i}| > p^6$, a contradiction. Thus $t = 1$ and hence by using the relation (2) we have

$$p^3 = p^2 q_1 - (p-1)^2(q_1 - 1).$$

This implies that $q_1(2p-1) = p^3 - p^2 + 2p - 1$ and so $(2p-1)$ is a divisor of $p^2(p-1)$. But since $(2p-1, p^2) = 1$, $2p-1$ is a divisor of $p-1$, a contradiction.

- Case 2: $t_1 = t_2 = 1$ i.e., $|Z(R_1)| = |Z(R_2)| = p$. Then $|Z(R)| > |R_1||R_2| \geq p^4$, i.e., $k \geq 5$. If $t \geq 3$, then by the relation (2), p^2 is a divisor of $(q_i - 1)(q_j - 1)$ for some $1 \leq i, j \leq t$. It follows that $q_i q_j > p^2$ and hence $|Z(R)| > |R_1||R_2|q_i q_j > p^4 p^2 = p^6$, a contradiction. Therefore $t \leq 2$. We claim that $t = 1$. If $t = 2$, then by the relation (2) we have

$$p^{k-2} = p^2 q_1 q_2 - (p-1)^2(q_1 - 1)(q_2 - 1). \tag{3}$$

Since $k \geq 5$, p^2 is a divisor of $(q_1 - 1)(q_2 - 1)$. If p^2 is a divisor of $q_i - 1$, then $q_i > p^2$ and so $|Z(R)| > p^6$, a contradiction. Thus p is a divisor of both $q_1 - 1$ and $q_2 - 1$. Hence $q_1 - 1 = k_1 p$ and $q_2 - 1 = k_2 p$ for some positive integers k_1 and k_2. Then one obtains from (3),

$$p^{k-4} = (k_1 p + 1)(k_2 p + 1) - (p-1)^2 k_1 k_2,$$

and hence

$$p^{k-4} - (k_1 + k_2 + 2k_1 k_2)p + k_1 k_2 - 1 = 0.$$

If $k = 5$, then $p = \frac{k_1 k_2 - 1}{k_1 + k_2 + 2k_1 k_2 - 1}$, a contradiction. Thus we can assume that $k = 6$ and hence

$$p^2 - (k_1 + k_2 + 2k_1 k_2)p + k_1 k_2 - 1 = 0. \tag{4}$$

Thus the equation (4) shows that the integer p is a solution of

$$X^2 - (k_1 + k_2 + 2k_1 k_2)X + k_1 k_2 - 1 = 0. \tag{5}$$

Now let μ be another solution of (5). Clearly $\mu \neq 1$, $p\mu = k_1 k_2 - 1 > 0$ and $p + \mu = k_1 + k_2 + 2k_1 k_2$. It follows that μ is an integer≥ 2 and hence $p\mu \geq p + \mu$, i.e., $k_1 k_2 - 1 > k_1 + k_2 + 2k_1 k_2$, a contradiction (since k_1, $k_2 \geq 1$). Thus $t = 1$ and since $|Z(R_1)| = |Z(R_2)| = p$, we have

$$p^4 = p^2 q_1 - (p-1)^2(q_1 - 1)$$

and so $q_1(2p-1) = p^4 - p^2 + 2p - 1$. Thus $2p - 1$ is a divisor of $p^2 - 1$, i.e., $p^2 - 1 = (2p-1)a$ for some positive integer a. Then the equation $p^2 - 2ap + a - 1 = 0$ implies that p is a divisor of $a - 1$, i.e., $a - 1 = p\lambda$ for some non-negative integer λ. It follows that p and λ are solutions of $x^2 - 2ax + a - 1 = 0$ and so $p + \lambda = 2a$. If $\lambda = 1$, then $p = a - 1$ and $p + 1 = 2a$ and hence $a = 0$, a contradiction. Also, if $\lambda > 1$, then $p\lambda \geq p + \lambda$ and so $a \leq -1$, a contradiction.

Finally, if $\lambda = 0$, then $p = 2$, which yields $q_1 = 5$, i.e., $R \cong R_1 \times R_2 \times F_5$ where R_1 and R_2 are local rings of order 4 with 2 zero-divisors. Now by [2, page 687], each R_i is isomorphic to $\mathbb{Z}_4$ or $\mathbb{Z}_2[x]/(x^2)$.

Corollary 1. *Let R be a commutative ring with $|Z(R)| = p$, where p is a prime number. Then R is isomorphic to one of the rings $\mathbb{Z}_{p^2}$, $\mathbb{Z}_p[x]/(x^2)$ or $F_{q_1} \times \ldots \times F_{q_t}$ where $p = q_1q_2\ldots q_t - (q_1 - 1)(q_2 - 1)\ldots(q_t - 1)$.*

Proof. If R is a local ring, then by Lemma 1, $|R| = p^2$ and hence by [2, page 687], R is isomorphic to $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p[x]/(x^2)$. If R is not local, then by Theorem 4, $R \cong F_{q_1} \times \ldots \times F_{q_t}$ where $t \geq 2$ and $p = q_1q_2\ldots q_t - (q_1 - 1)(q_2 - 1)\ldots(q_t - 1)$.

In [5], it was shown that any commutative ring R with m zero-divisors has m^2 or fewer elements. It was proved in [7] that if $|Z(R)| = m$ and $|R| = m^2$, then $m = p^r$ for some integer $r \geq 1$ and some prime p. These rings were categorized in [4] by the use of two constructions. When the ring R is commutative with 1, then there are only two such rings (up to isomorphism) for $m = p^r$: $F_{p^r}[x]/(x^2)$ and $\mathbb{Z}_{p^2}[x]/(f(x))$, where $f(x)$ is an irreducible polynomial of degree r over F_p. The rings from the second construction in [4] are shown by Raghavendran [9] to all be isomorphic to the ring $\mathbb{Z}_{p^2}[x]/(f(x))$ given above, which is called the Galois Ring of order p^{2r} and characteristic p^2, denoted $GR(p^{2r}, p^2)$.

Let p be a prime number. We write Σ_m for a set of coset representatives of $(F_p^*)^m$ in F_p^*, and $\Sigma_m^0 = \Sigma_m \cup \{0\}$. Since F_p^* is cyclic, $|\Sigma_m| = (m, p-1)$.

Corollary 2. *Let R be a commutative ring with $|Z(R)| = p^2$, where p is a prime number. Then R is isomorphic to one of the rings $\mathbb{Z}_{p^3}$, $F_p[x,y]/(x,y)^2$, $F_p[x]/(x^3)$, $\mathbb{Z}_{p^2}[x]/(px, x^2 - \varepsilon p)$ where $\varepsilon \in \Sigma_2^0$, $F_{p^2}[x]/(x^2)$, the Galois ring $GR(p^4, p^2)$ or $F_{q_1} \times \ldots \times F_{q_t}$ where $t \geq 2$ and $p^2 = q_1q_2\ldots q_t - (q_1 - 1)(q_2 - 1)\ldots(q_t - 1)$.*

Proof. Suppose that R is a local ring with $|Z(R)| = p^2$. Then by Lemma 1, $|R| = p^3$ or p^4. If $|R| = p^3$, then by [2, p.687], R is isomorphic to one of the rings $\mathbb{Z}_{p^3}$, $F_p[x,y]/(x,y)^2$, $F_p[x]/(x^3)$, $\mathbb{Z}_{p^2}[x]/(px, x^2 - \varepsilon p)$ where $\varepsilon \in \Sigma_2^0$. If $|R| = p^4$, then by [9, Theorem 12], R is isomorphic to the Galois ring $GR(p^4, p^2)$ or $F_{p^2}[x]/(x^2)$. Now suppose that R is not a local ring. Then by Theorem 2, $R \cong F_{q_1} \times \ldots \times F_{q_t}$ with $p^2 = q_1q_2\ldots q_t - (q_1 - 1)(q_2 - 1)\ldots(q_t - 1)$.

If R is a finite ring then its additive group is a finite abelian group and is thus a direct product of cyclic groups. Suppose these have generators a_1,...,a_n of orders m_1,...,m_n. Then the ring structure is determined by the n^2 products

$$a_i a_j = \sum_{k=1}^{n} w_{ijk} a_k \text{ with } w_{ijk} \in \mathbb{Z}_{m_k}$$

and thus by the n^3 structure constants w_{ijk} for $1 \leq i, j, k \leq n$.

Thus we introduce a convenient notation, for giving the structure of a finite ring. A *presentation* for a finite ring R consists of a set of generators $a_1, a_2, \ldots, a_n$ of the additive group of R together with *relations*. The relations are of two types:

(i) $m_i a_i = 0$ for $i = 1, ..., n$ indicating the additive order of a_i, and

(ii) $a_i a_j = \sum_{k=1}^{n} w_{ijk} a_k$ with $w_{ijk} \in \mathbb{Z}_{m_k}$ for $1 \leq i, j \leq n$.

If the ring R has the presentation above we write

$$R = \left\langle a_1, \ldots, a_n; m_i a_i = 0,\ a_i a_j = \sum_{k=1}^{n} w_{ijk} a_k, \text{ for } i, j = 1, \ldots, n \right\rangle.$$

Corollary 3. *Let R be a commutative ring with $|Z(R)| = p^3$, where p is a prime number. Then R is isomorphic to one of the rings $\mathbb{Z}_{p^2} \times F_q$, $\mathbb{Z}_p[x]/(x^2) \times F_q$ where $p^2 = p + q - 1$, $F_{q_1} \times \ldots \times F_{q_t}$ where $p^3 = q_1 q_2 \ldots q_t - (q_1 - 1)(q_2 - 1)\ldots(q_t - 1)$, the Galois ring $GR(p^6, p^2)$, $F_{p^3}[x]/(x^2)$, $F_p[x]/(x^4)$, $\mathbb{Z}_{p^2}[x]/(px, x^3)$, $\mathbb{Z}_{p^2}[x]/(x^2)$, $\mathbb{Z}_{p^2}[x]/(px, x^3 - ap)$ where $a \in \Sigma_3$, $\mathbb{Z}_{p^2}[x]/(x^2 - bp)$ where $b \in \Sigma_2$ and $p \neq 2$, $\mathbb{Z}_4[x]/(x^2 - 2)$, $\mathbb{Z}_4[x]/(x^2 - 2x - 2)$, $\mathbb{Z}_{p^2}[x, y]/(p, x, y)^2$, $F_p[x, y, z]/(x, y, z)^2$, $\mathbb{Z}_{p^3}[x]/(px, x^2 - cp^2)$ where $c \in \Sigma_2^0$, $\mathbb{Z}_4[x]/(x^2 - 2x)$, $\mathbb{Z}_{p^4}$,*

$$R_1 := \langle 1, x_1, x_2, y; p1 = 0, {x_1}^2 = y, {x_2}^2 = 0, x_i x_j = x_i y = y x_i = y^2 = 0, i \neq j \rangle,$$
$$R_2 := \langle 1, x_1, x_2, y; p1 = 0, {x_1}^2 = y, {x_2}^2 = y, x_i x_j = x_i y = y x_i = y^2 = 0, i \neq j \rangle,$$
$$R_3 := \langle 1, x_1, x_2, y; p1 = 0, {x_1}^2 = y, {x_2}^2 = \xi y, x_i x_j = x_i y = y x_i = y^2 = 0, i \neq j \rangle,$$
$$R_4 := \langle 1, x_1, x_2; p^2 1 = p x_1 = p x_2 = 0, {x_1}^2 = p, {x_2}^2 = 0, x_1 x_2 = x_2 x_1 = 0 \rangle,$$
$$R_5 := \langle 1, x_1, x_2; p^2 1 = p x_1 = p x_2 = 0, {x_1}^2 = \xi p, {x_2}^2 = 0, x_1 x_2 = x_2 x_1 = 0 \rangle,$$
$$R_6 := \langle 1, x_1, x_2; p^2 1 = p x_1 = p x_2 = 0, {x_1}^2 = p, {x_2}^2 = p, x_1 x_2 = x_2 x_1 = 0 \rangle,$$
$$R_7 := \langle 1, x_1, x_2; p^2 1 = p x_1 = p x_2 = 0, {x_1}^2 = p, {x_2}^2 = \xi p, x_1 x_2 = 0 \rangle,$$

where ξ is a non-square in F_p and if $p = 2$ then instead of R_3, R_5 and R_7, R is isomorphic to R_3' or R_5' where

$$R_3' := \langle 1, x_1, x_2; 4.1 = 2x_1 = 2x_2 = 0, {x_1}^2 = 0, {x_2}^2 = 0, x_1 x_2 = x_2 x_1 = 2 \rangle \text{ or}$$
$$R_5' := \langle 1, x_1, x_2, y; 2.1 = 0, x_1 x_2 = x_2 x_1 = y, {x_1}^2 = {x_2}^2 = x_i y = y x_i = y^2 = 0 \rangle.$$

Proof. If R is a local ring with $|Z(R)| = p^3$, then by Lemma 1, either $|R| = p^4$ or $|R| = p^6$. If $|R| = p^6$, then by [9, Theorem 12], R is isomorphic to $F_{p^3}[x]/(x^2)$ or the Galois ring $GR(p^6, p^2)$. If $|R| = p^4$, then since $|Z(R)| = p^3$, by using [2, p.687-690], one can easily see that R is isomorphic to one of the local rings in above list. Now suppose that R is not local. Then by Theorem 2, R is isomorphic to one of the rings $\mathbb{Z}_{p^2} \times F_q$, $\mathbb{Z}_p[x]/(x^2) \times F_q$ where $p^2 = p + q - 1$ or $F_{q_1} \times \ldots \times F_{q_t}$ where $p^3 = q_1 q_2 \ldots q_t - (q_1 - 1)(q_2 - 1)\ldots(q_t - 1)$. This completes the proof.

Now we are in position to determine the structure of commutative rings R with $|Z(R)| = p_1^{k_1} p_2^{k_2} \ldots p_n^{k_n}$, where $n \geq 1$, $1 \leq k_i \leq 3$ and p_i's are distinct prime numbers.

Theorem 5. *Let R be a commutative ring with $|Z(R)| = p_1^{k_1} p_2^{k_2} \ldots p_n^{k_n}$, where $n \geq 1$, $1 \leq k_i \leq 3$ and p_i's are distinct prime numbers. Then there exist $0 \leq s \leq \Sigma_{i=1}^{n} k_i$ and $t \geq 0$ such that*

$$R \cong R_1 \times \ldots \times R_s \times F_{q_1} \times \ldots \times F_{q_t}$$

where F_{q_i}'s are finite fields and each R_i is local ring with $|Z(R_i)| = p_j^{t_j}$ for some p_j $(1 \leq j \leq n)$ and $1 \leq t_j \leq k_j$. Consequently, each R_i is isomorphic to one of the local rings described in Corollaries 1, 2 or 3.

Proof. We put

$$R \cong R_1 \times \ldots \times R_s \times F_{q_1} \times \ldots \times F_{q_t},$$

where $F_{q_1}, \ldots, F_{q_t}$ are finite fields and each R_i is a commutative finite local ring that is not a field. If $s = 0$, then there is nothing to prove. Thus we can assume that $s \geq 1$ and so by Theorem 1, for each i, $|Z(R_i)| = p^k$ for some prime number p and $k \geq 1$ such that p^k is a divisor of $|Z(R)|$ and also $0 \leq s \leq \Sigma_{i=1}^{n} k_i$. Thus $|Z(R_i)| = p_j^{t_j}$ where $1 \leq t_j \leq k_j$, $1 \leq j \leq n$ and $1 \leq i \leq s$. Thus for each $1 \leq i \leq s$, $t_i = 1, 2$ or 3 and so each R_i is isomorphic to one of the local rings described in Corollaries 1, 2 or 3

Next, we determine the structure of commutative nonlocal rings R with $|Z(R)| = p^4$ or p^5 where p is a prime number.

Proposition 1. *Let R be a commutative nonlocal ring with $|Z(R)| = p^4$ where p is a prime number. Then $R \cong F_{q_1} \times \ldots \times F_{q_t}$ with $p^4 = q_1q_2 \ldots q_t - (q_1 - 1)(q_2 - 1) \ldots (q_t - 1)$, $R \cong R_1 \times F_{q_1} \times \ldots \times F_{q_t}$ where $R_1 \cong \mathbb{Z}_{p^2}$ or $\mathbb{Z}_p[x]/(x^2)$ with $p^3 = pq_1q_2 \ldots q_t - (p-1)(q_1 - 1)(q_2 - 1) \ldots (q_t - 1)$ or $R \cong R_1 \times F_q$ where and $p^2 = p + q - 1$ and R_1 is isomorphic to one of the local rings of order p^3 described in Corollary 2.*

Proof. By Theorem 4, either R is reduced or $R \cong R_1 \times F_{q_1} \times \ldots \times F_{q_t}$, where R_1 is a local ring with $|Z(R_1)| = p$ or p^2 and $t \geq 1$. Now we proceed by cases.

- Case 1: R is reduced. Then $R \cong F_{q_1} \times \ldots \times F_{q_t}$ with

$$p^4 = q_1q_2 \ldots q_t - (q_1 - 1)(q_2 - 1) \ldots (q_t - 1).$$

- Case 2: R is not reduced and $|Z(R_1)| = p$. Then by Corollary 1, R_1 is isomorphic to $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p[x]/(x^2)$ and $p^3 = pq_1q_2 \ldots q_t - (p-1)(q_1 - 1)(q_2 - 1) \ldots (q_t - 1)$.
- Case 3: R is not reduced and $|Z(R_1)| = p^2$. Then by Lemma 1, either $|R_1| = p^3$ or $|R_1| = p^4$. Since $t \geq 1$, $p^4 = |Z(R)| > |R_1|$ and hence $|R_1| = p^3$. Thus by Corollary 2, R_1 is isomorphic to one of the rings $F_p[x, y]/(x, y)^2$, $F_p[x]/(x^3)$, $\mathbb{Z}_{p^3}$ or $\mathbb{Z}_{p^2}[x]/(px, x^2 - \varepsilon p)$ where $\varepsilon \in \Sigma_2^0$ with $p^2 = p + q - 1$.

Proposition 2. *Let R be a commutative nonlocal ring with $|Z(R)| = p^5$ where p is a prime number. Then*

(i) $R \cong F_{q_1} \times \ldots \times F_{q_t}$ *with* $p^5 = q_1q_2 \ldots q_t - (q_1 - 1)(q_2 - 1) \ldots (q_t - 1)$,

(ii) $R \cong R_1 \times F_{q_1} \times \ldots \times F_{q_t}$ *where* $R_1 \cong \mathbb{Z}_{p^2}$ *or* $\mathbb{Z}_p[x]/(x^2)$ *with* $p^4 = pq_1q_2 \ldots q_t - (p - 1)(q_1 - 1)(q_2 - 1) \ldots (q_t - 1)$,

(iii) *$R \cong R_1 \times F_{q_1} \times \ldots \times F_{q_t}$ where R_1 is isomorphic to one of the rings $\mathbb{Z}_{p^3}$, $F_p[x,y]/(x,y)^2$, $F_p[x]/(x^3)$, or $\mathbb{Z}_{p^2}[x]/(px, x^2-\varepsilon p)$ where $\varepsilon \in \Sigma_2^0$ and $p^3 = pq_1q_2\ldots q_t - (p-1)(q_1-1)(q_2-1)\ldots(q_t-1)$,*

(iv) *$R \cong R_1 \times F_q$ where $R_1 \cong F_{p^2}[x]/(x^2)$ or $GR(p^4, p^2)$ with $p^3 = p^2+q-1$, or*

(v) *$R \cong R_1 \times F_q$ and $p^2 = p+q-1$ where R_1 is isomorphic to one of the local rings of order p^4 described in Corollary 3.*

Proof. By Theorem 4, either R is reduced or $R \cong R_1 \times F_{q_1} \times \ldots \times F_{q_t}$, where R_1 is a local ring with $|Z(R_1)| = p$, p^2 or p^3 and $t \geq 1$. Now we proceed by cases.

- Case 1: R is reduced. Then $R \cong F_{q_1} \times \ldots \times F_{q_t}$ with

$$p^5 = q_1q_2\ldots q_t - (q_1-1)(q_2-1)\ldots(q_t-1)$$

- Case 2: R is not reduced and $|Z(R_1)| = p$. Then by Corollary 1, R_1 is isomorphic to $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p[x]/(x^2)$ and $p^4 = pq_1q_2\ldots q_t - (p-1)(q_1-1)(q_2-1)\ldots(q_t-1)$.

- Case 3: R is not reduced and $|Z(R_1)| = p^2$. Then by Lemma 1, $|R_1| = p^3$ or p^4. If $|R_1| = p^3$, then by Corollary 2, R_1 is isomorphic to one of the ring $\mathbb{Z}_{p^3}$, $F_p[x,y]/(x,y)^2$, $F_p[x]/(x^3)$, or $\mathbb{Z}_{p^2}[x]/(px, x^2-\varepsilon p)$ where $\varepsilon \in \Sigma_2^0$ and $p^3 = pq_1q_2\ldots q_t - (p-1)(q_1-1)(q_2-1)\ldots(q_t-1)$. If $|R_1| = p^4$, then $t = 1$, for if not, then by Theorem 2, $q_i > p$ for some i and hence $|Z(R)| > |R_1|q_i > p^5$, a contradiction. Thus $t = 1$ and so $R \cong R_1 \times F_q$ with $p^3 = p^2+q-1$. Moreover, since $|Z(R_1)| = p^2$ and $|R_1| = p^4$, by [9, Theorem 12], R_1 is isomorphic to $F_{p^2}[x]/(x^2)$ or $GR(p^4, p^2)$.

- Case 4: R is not reduced and $|Z(R_1)| = p^3$. Then by Lemma 1, $|R_1| = p^4$ or p^6. If $|R_1| = p^6$, then $|Z(R)| \geq p^6$, a contradiction (we note that $t \geq 1$). Thus $|R_1| = p^4$ and so by Theorem 2, $t = 1$, i.e., $R \cong R_1 \times F_q$ with $p^2 = p+q-1$. Now since $|R_1| = p^4$ and $|Z(R_1)| = p^3$, R_1 is isomorphic to one of the local rings of order p^4 described in Corollary 3.

The next theorem characterizes commutative rings with p^7 zero-divisors.

Theorem 6. *Let R be a commutative ring with $|Z(R)| = p^7$ where p is a prime number. Then either*

(i) *R is a local ring with $|R| = p^8$ or p^{14};*

(ii) *R is a reduced ring and so $R \cong F_{q_1} \times \ldots \times F_{q_t}$, where each F_{q_i} $(1 \leq i \leq t)$ is a finite field and $p^7 = q_1q_2\ldots q_t - (q_1-1)(q_2-1)\ldots(q_t-1)$;*

(iii) *$R \cong R_1 \times F_{q_1} \times \ldots \times F_{q_t}$, where each F_{q_i} $(1 \leq i \leq t)$ is a finite field and R_1 is a local ring with $|Z(R_1)| = p^m$, $|R_1| = p^n$ such that $0 < m < n \leq 6$ and*

$$p^7 = p^nq_1q_2\ldots q_t - (p^n - p^m)(q_1-1)(q_2-1)\ldots(q_t-1);$$

(iv) $R \cong R_1 \times R_2 \times F_{q_1} \times \ldots \times F_{q_t}$, *where each* F_{q_i} *(*$1 \leq i \leq t$*) is a finite field, each* R_i *is isomorphic to* $\mathbb{Z}_{p^2}$ *or* $\mathbb{Z}_p[x]/(x^2)$ *and*

$$p^5 = p^2 q_1 q_2 \ldots q_t - (p-1)^2(q_1-1)(q_2-1)\ldots(q_t-1); \text{ or}$$

(v) $R \cong R_1 \times R_2 \times F_5$ *where* R_1 *is isomorphic to one of the rings* $\mathbb{Z}_4$ *or* $\mathbb{Z}_2[x]/(x^2)$ *and* R_2 *is isomorphic to one of the rings* $\mathbb{Z}_8$, $\mathbb{Z}_2[x,y]/(x,y)^2$, $\mathbb{Z}_2[x]/(x^3)$, *or* $\mathbb{Z}_4[x]/(2x, x^2-2\varepsilon)$ *where* $\varepsilon \in \Sigma_2^0$.

Proof. Suppose $|Z(R)| = p^7$ and R is not a local ring. If R is reduced, then we are done. Now suppose R is not a reduced ring. Then by Theorem 2, we can assume that $R \cong R_1 \times \ldots \times R_s \times F_{q_1} \times \ldots \times F_{q_t}$, where $s,\ t \geq 1$ and each R_i is a local ring with $|Z(R_i)| = p^{t_i}$, $|R_i| = p^{k_i}$ for some $t_i,\ k_i \geq 1$ such that

$$1 \leq \sum_{i=1}^{s} t_i \leq \sum_{i=1}^{s} k_i - s \leq 7 - s - 1 \leq 7 - 1 - 1 = 5.$$

It follows that $s \leq 5$. We claim that $s = 1$ or 2, for if not either $s \geq 4$ or $s = 3$. If $s \geq 4$, then $|Z(R)| > p^8$ (because $|R_i| \geq p^2$ for all i), a contradiction. Now let $s = 3$. If $|Z(R_i)| = p^{t_i}$ with $t_i \geq 2$ for some i, then $|Z(R)| > p^7$, a contradiction. Thus $|Z(R_i)| = p$ for $i = 1,2,3$. Now by the relation (1) of Theorem 1, we have

$$p^7 = p^6 q_1 q_2 \ldots q_t - (p^2-p)^3(q_1-1)(q_2-1)\ldots(q_t-1).$$

Thus $p^4 = p^3 q_1 q_2 \ldots q_t - (p-1)^3(q_1-1)(q_2-1)\ldots(q_t-1)$ and so p is a divisor of (q_i-1) for some i (so $q_i > p$). Now if $t \geq 2$, then $|Z(R)| \geq |R_1||R_2||R_3|q_i > p^7$, this is a contradiction. Thus $t = 1$ and so the relation $p^4 = p^3 q_1 - (p-1)^3(q_1-1)$ implies that p^3 is a divisor of (q_1-1). Hence $q_1 > p^3$ and so $|Z(R)| \geq |Z(R_1)||R_2||R_3|q_1 > p^7$, a contradiction. Thus $s \leq 2$.

Suppose $s = 1$, i.e., $R \cong R_1 \times F_{q_1} \times \ldots \times F_{q_t}$. Then by Theorem 2, either R_1 is a local ring with $|Z(R_1)| = p^{t_1}$ where $t_1 = 1,2,3$ or 4 such that

$$p^7 = |R_1| q_1 \times \ldots \times q_t - (|R_1| - p^k)(q_1-1) \times \ldots (q_t-1)$$

or $R \cong R_1 \times F_{q_1}$ where $|R_1| = p^6$, $|Z(R_1)| = p^5$ and $p^2 - p - q_1 + 1 = 0$.

Now suppose $s = 2$. The proof now proceeds by cases.

- Case 1: $t_1 \geq 3$ or $t_2 \geq 3$. Without loss of generality we can assume that $t_1 \geq 3$. Then $|R_1| = p^{k_1}$, and $|R_2| = p^{k_2}$ where $k_1 \geq 4$ and $k_2 \geq 2$. If $k_1 \geq 5$ or $k_2 \geq 3$, then $|Z(R)| > |R_1||R_2| \geq p^7$, a contradiction. Now let $k_1 = 4$ and $k_2 = 2$. By Theorem 2, $q_i > p$ for some $1 \leq i \leq t$. If $t \geq 2$, then $|Z(R)| > |R_1||R_2|q_i \geq p^7$, a contradiction. Thus $t = 1$ and so $p^7 = p^6 q_1 - (p^4 - p^3)(p^2 - p)(q_1 - 1)$. It follows that p^2 is a divisor of $q_1 - 1$ and so $q_1 > p^2$. Hence $|Z(R)| > |Z(R_1)||R_2||F_{q_1}| > p^7$, a contradiction.

- Case 2: $t_1 = t_2 = 2$ i.e., $|Z(R_1)| = |Z(R_2)| = p^2$. Then by Lemma 1, $|R_1| = p^{k_1}$ and $|R_2| = p^{k_2}$ where $3 \leq k_1, k_2 \leq 4$. If $k_1 = 4$ or $k_2 = 4$, then $|Z(R)| > |R_1||R_2| \geq p^7$, a contradiction. Now let $k_1 = k_2 = 3$. By Theorem 2, $q_i > p$ for some $1 \leq i \leq t$. If $t \geq 2$, then $|Z(R)| > |R_1||R_2|q_i \geq p^7$, a contradiction. Thus $t = 1$ and so $p^7 = p^6 q_1 - (p^3 - p^2)^2(q_1 - 1)$. It follows that p^2 is a divisor of $q_1 - 1$ and so $q_1 > p^2$. Hence $|Z(R)| > |Z(R_1)||R_2||F_{q_1}| > p^7$, a contradiction.

- Case 3: $t_1 = 2$ and $t_2 = 1$ or $t_1 = 1$ and $t_2 = 2$. Without loss of generality we can assume that $t_1 = 2$ and $t_2 = 1$. By Lemma 1, either $|R_1| = p^3$ or $|R_1| = p^4$ and $|R_2| = p^2$. By the proof in Case 1, $|R_1| \neq p^4$. Thus $|R_1| = p^3$ and $|R_2| = p^2$ and hence by the relation (2) of Theorem 2 we have

$$p^4 = p^2 q_1 q_2 \dots q_t - (p-1)^2(q_1 - 1)(q_2 - 1)\dots(q_t - 1). \tag{6}$$

  It follows that p^2 is a divisor of $(q_1 - 1)(q_2 - 1)\dots(q_t - 1)$. Without loss of generality we may assume that p^2 is a divisor of $(q_1 - 1)$ or p is a divisor of $(q_1 - 1)$ and $(q_2 - 1)$. If $t > 2$, then $|Z(R)| > |R_1||R_2||F_{q_1}||F_{q_2}| \geq p^7$, a contradiction. Thus $t \leq 2$ and so the proof now proceeds by subcases.

  - Subcase 1: $t = 1$ i.e., $R \cong R_1 \times R_2 \times F_{q_1}$. Then by (6), we have

$$p^4 = p^2 q_1 - (p-1)^2(q_1 - 1). \tag{7}$$

    This implies that p^2 is a divisor of $(q_1 - 1)$. Thus $q_1 - 1 = p^2 k$ for some positive integer k and so by using (7) we obtain $p^2 - 2pk + k - 1 = 0$. This equation implies that p is a divisor of $k - 1$, i.e., $k - 1 = p\lambda$ for some non-negative integer λ. It follows that p and λ are solutions of $x^2 - 2kx + k - 1 = 0$ and so $p + \lambda = 2k$. If $\lambda = 1$, then $p = k - 1$ and $p + 1 = 2k$ and hence $k = 0$, a contradiction. Also, if $\lambda > 1$, then $p\lambda \geq p + \lambda$ and so $k \leq -1$, a contradiction. Finally, if $\lambda = 0$, then $p = 2$ which yields $q_1 = 5$, i.e., $R \cong R_1 \times R_2 \times F_5$ where R_1 and R_2 are local rings with $|R_1| = 8$ and $|R_2| = 4$. Since $|Z(R_1)| = 4$, by [2, p.687], R_1 is isomorphic to one of the rings $\mathbb{Z}_8$, $\mathbb{Z}_2[x,y]/(x,y)^2$, $\mathbb{Z}_2[x]/(x^3)$, or $\mathbb{Z}_4[x]/(2x, x^2 - 2\varepsilon)$ where $\varepsilon \in \Sigma_2^0$. Also, R_2 is isomorphic to $\mathbb{Z}_4$ or $\mathbb{Z}_2[x]/(x^2)$.
  - Subcase 2: $t = 2$ i.e., $R \cong R_1 \times R_2 \times F_{q_1} \times F_{q_2}$. Then by (6), we have

$$p^4 = p^2 q_1 q_2 - (p-1)^2(q_1 - 1)(q_2 - 1).$$

    Thus p^2 is a divisor of $(q_1 - 1)(q_2 - 1)$. If p^2 is a divisor of $q_1 - 1$ (or $q_2 - 1$), then $q_1 > p^2$ (or $q_2 > p^2$) and so $|Z(R)| > |R_1||R_2||F_{q_i}| > p^7$ where $i = 1$ or 2, this is a contradiction. Thus p is a divisor of both $q_1 - 1$ and $q_2 - 1$. Hence $q_1 - 1 = k_1 p$ and $q_2 - 1 = k_2 p$ for some positive integers k_1 and k_2. Then one obtains from (6),

$$p^2 = (k_1 p + 1)(k_2 p + 1) - (p-1)^2 k_1 k_2,$$

    and hence

$$p^2 - (k_1 + k_2 + 2k_1 k_2)p + k_1 k_2 - 1 = 0. \tag{8}$$

Now the equation (8) shows that the integer p is a solution of

$$X^2 - (k_1 + k_2 + 2k_1k_2)X + k_1k_2 - 1 = 0. \tag{9}$$

Now let μ be another solution of (9). Clearly $\mu \neq 1$, $p\mu = k_1k_2 - 1 > 0$ and $p + \mu = k_1 + k_2 + 2k_1k_2$. It follows that μ is an integer≥ 2 and hence $p\mu \geq p + \mu$, i.e., $k_1k_2 - 1 > k_1 + k_2 + 2k_1k_2$, a contradiction (since k_1, $k_2 \geq 1$).

- Case 4: $t_1 = t_2 = 1$ i.e., $|Z(R_1)| = |Z(R_2)| = p$ and $R \cong R_1 \times R_2 \times F_{q_1} \times \ldots \times F_{q_t}$ with $p^5 = p^2 q_1 q_2 \ldots q_t - (p-1)(q_1 - 1)(q_2 - 1)\ldots(q_t - 1)$. On the other hand by by [2, p.687], R_1 is isomorphic to $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p[x]/(x^2)$.

Finally, we conclude the article with the next remark which is a good justification for the classification up to isomorphism commutative rings with ${p_1}^{k_1} \ldots {p_n}^{k_n}$ zero-divisors, where $1 \leq k_i \leq 5$.

Remark 1. *We remark that by Propositions 1 and 2, for classifying up to isomorphism commutative rings with ${p_1}^{k_1} \ldots {p_n}^{k_n}$ zero-divisors, where $1 \leq k_i \leq 5$, it suffices to find local rings with $|R| = p^6$, $|Z(R)| = p^4$ and $|R| = p^6$, $|Z(R)| = p^5$. In fact, if R is a local ring with $|Z(R)| = p^4$, then by Lemma 1, $|R| = p^5$, p^6 or p^8. The local rings of order p^5 is determined in [3]. Also, if $|R| = p^8$, then by [9, Theorem 12], R is isomorphic to the Galois ring $GR(p^8, p^2)$ or $F_{p^4}[x]/(x^2)$. On the other hand, if R is a local ring with $|Z(R)| = p^5$, then by Lemma 1, $|R| = p^6$ or p^{10}. If $|R| = p^{10}$, then by [9, Theorem 12], R is isomorphic to the Galois ring $GR(p^{10}, p^2)$ or $F_{p^5}[x]/(x^2)$.*

ACKNOWLEDGEMENTS This work was partially supported by IUT (CEAMA). The research of the first author was in part supported by a grant from IPM (No. 87160026).

References

[1] D.F. Anderson, A. Farzier, A. Lauve, and P.S. Livingston, The zero-divisor graph of a commutative ring, II, Lecture notes in pure and appl. Math. 202 (2001), 61-72, Marcel Dekker, New York.

[2] B. Corbas and G.D. Williams, Rings of order p^5 Part I. Nonlocal rings, J. Algebra, 231 (2000), 677-690.

[3] B. Corbas and G.D. Williams, Rings of order p^5 Part II. Local rings, J. Algebra, 231 (2000), 691-704.

[4] B. Corbas, Rings with few zero-divisors, Math. Ann. 181 (1) (1969), 1Ű7.

[5] N. Ganesan, Properties of rings with a finite number of zero-divisors, Math. Ann. 157 (1964), 215Ű218.

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

[7] K. Koh, On properties of rings with a finite number of zero-divisors, Math. Ann. 171 (1967), 79-80.

[8] B.R. McDonald, Finite rings with identity (Marcell Dekker, New York, 1974).

[9] R. Raghavendran, Finite associative rings, Compositio Math. 21 (1969), 195-229.

[10] S.P. Redmond, An ideal-based zero-divisor graph of a commutative ring, Comm. Algebra 31 (2003), 4425-4443.

[11] S.P. Redmond, On zero-divisor graphs of small finite commutative rings. Discrete Math. 307 (2007), 1155-1166.