Research Article

Classification of Finite Rings of Order p^6 by Generators and Relations

P. Karimi Beiranvand,¹ R. Beyranvand,² and M. Gholami³

¹ Department of Mathematics, Islamic Azad University, Khorramabad Branch, Khorramabad 68178-16645, Iran

² Department of Mathematics, Lorestan University, P.O. Box 465, Khorramabad 68137-17133, Iran

³ Department of Mathematical Sciences, Shahrekord University, P.O. Box 115, Shahrekord 88186-34141, Iran

Correspondence should be addressed to R. Beyranvand, beyranvand.r@lu.ac.ir

Received 26 September 2012; Accepted 10 December 2012

Academic Editor: Liwei Zhang

Copyright © 2013 P. Karimi Beiranvand et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

For any finite abelian group $(R, +)$, we define a binary operation or “multiplication” on R and give necessary and sufficient conditions on this multiplication for R to extend to a ring. Then we show when two rings made on the same group are isomorphic. In particular, it is shown that there are $n + 1$ rings of order p^n with characteristic p^n , where p is a prime number. Also, all finite rings of order p^6 are described by generators and relations. Finally, we give an algorithm for the computation of all finite rings based on their additive group.

1. Introduction

The problem of determining and classifying up to isomorphism finite rings has received considerable attention, both old and new, see [1–4]. It is well known that if R is a finite ring (with identity), then the additive group of R splits as the direct of its p -primary components $R(p)$, where p is a prime number, and these are pairwise orthogonal ideals. Thus R is the direct sum of the rings $R(p)$. We provide a new proof of this fact in the paper.

Now let p be a prime number. It is easy to see that there are two rings of order p , $\mathbb{Z}_p$ and the null ring of order p . In [5], Raghavendran (1969) proved that there exist eleven rings of order p^2 , only four of these rings have identity. Also in [6], Gilmer and Mott (1973) showed that there exist $4p + 48$ rings of order p^3 ($p \neq 2$), only twelve of these rings have identity, and 59 rings of order 8, only eleven of these rings have identity. For p^4 , a comprehensive list of noncommutative rings was first only drawn up in [7]. Commutative rings of order p^4 have been characterized by Wilson [4]. Finally, Corbas and Williams (2000) in [1, 8], determined

all rings of order p^5 . The rings of upper order are not still characterized.

Throughout the paper, all rings are associative (not necessarily commutative or with identity). For a set X , $|X|$ denotes the cardinal of X . For two integers a, b and positive integer n , we denote $a \equiv_n b$ in case a and b are congruent modulo n , and $a \mid b$ in case a divides b . Also, for two integers a and b , $\gcd(a, b)$ denotes the greatest common divisor of a and b . In [9], the authors introduced a multiplication (similar to Theorem 3) on a finitely generated S -module to extend to an S -algebra, where S is a commutative ring. Also a number of necessary and sufficient conditions for any S -module to extend to an S -algebra, where S is a commutative ring, is given by Behboodi et al. [9]. Here instead of modules over a commutative ring, we focus our attention to the $\mathbb{Z}$ -modules. In Section 2, by using the method in [9], we define a binary operation or “multiplication” on a finite abelian group and extend to a ring. In particular, we prove that there are $n + 1$ rings (up to isomorphism) of order p^n whose abelian group is cyclic. Also, all rings of order p^6 whose abelian group is $\mathbb{Z}_p \oplus \mathbb{Z}_{p^5}$ are determined. In Section 3, an algorithm for the

computation of all finite rings based on their additive group is given.

2. A Representation of Finite Rings and Fundamental Theorems

We begin the paper with the following well known fact and give a new proof of this fact.

Theorem 1. *Let R be a ring of order $p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$, where the p_i are distinct primes and the n_i are positive integers. Then R is expressible, in a unique manner, as the direct sum of rings R_i , where $|R_i| = p_i^{n_i}$, $i = 1, 2, \dots, k$.*

Proof. We know that the additive group R is expressible, in a unique manner, as the direct sum of groups R_i , where $|R_i| = p_i^{n_i}$, $i = 1, 2, \dots, k$. We claim that R_i is an ideal of R , for $i = 1, \dots, k$. Suppose that $a_i, b_i \in R_i$ and $a_i b_i = x_1 + x_2 + \cdots + x_k$ where $x_j \in R_j$, for $1 \leq j \leq k$. Then $a_i b_i - x_i = x_1 + \cdots + x_{i-1} + x_{i+1} + \cdots + x_k$. Since $p_1^{n_1} \cdots p_{i-1}^{n_{i-1}} p_{i+1}^{n_{i+1}} \cdots p_k^{n_k} (x_1 + \cdots + x_{i-1} + x_{i+1} + \cdots + x_k) = 0$, $p_1^{n_1} \cdots p_{i-1}^{n_{i-1}} p_{i+1}^{n_{i+1}} \cdots p_k^{n_k} (a_i b_i - x_i) = 0$. If $a_i b_i - x_i \neq 0$, then we must have $p_i \mid p_1^{n_1} \cdots p_{i-1}^{n_{i-1}} p_{i+1}^{n_{i+1}} \cdots p_k^{n_k}$, a contradiction. Thus $a_i b_i - x_i = 0$ and so $a_i b_i \in R_i$. Now suppose that $a_i \in R_i$ and $a_j \in R_j$ where $i \neq j$ and $1 \leq i, j \leq k$. We show that $a_i a_j = 0$. Let $a_i a_j = x_1 + x_2 + \cdots + x_k$, where $x_t \in R_t$, for $1 \leq t \leq k$. Then $p_i^{n_i} a_i a_j = (p_i^{n_i} a_i) a_j = 0$ implies that $p_i^{n_i} (x_1 + x_2 + \cdots + x_k) = 0$ and hence $p_i^{n_i} x_t = 0$ for $1 \leq t \leq k$. Now for any $t \neq i$, if $x_t \neq 0$, then $p_t \mid p_i^{n_i}$, a contradiction. Thus for all $t \neq i$, $x_t = 0$. On the other hand, since $p_j^{n_j} a_i a_j = a_i (p_j^{n_j} a_j) = 0$, by a similar argument, we conclude that for all $t \neq j$, $x_t = 0$. Thus $x_1 = x_2 = \cdots = x_k = 0$ and so for all $1 \leq i \leq k$, R_i is an ideal of R , and the proof is complete. $\square$

Remark 2. 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 $a_1, a_2, \dots, a_n$ of orders $m_1, m_2, \dots, m_n$. Then the ring structure is determined by the n^2 products

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

and thus by the n^3 structure constants w_{ijk} . As [6] we introduce a convenient notation, motivated by group theory, for giving the structure of a finite ring. A *presentation* for a finite ring R consists of a set of generators $a_1, a_2, \dots, a_n$ of the additive group of R together with relations. The relations are of two types:

- (i) $m_i a_i = 0$ for $i = 1, \dots, n$;
- (ii) $a_i a_j = \sum_{k=1}^n w_{ijk} a_k$ with $w_{ijk} \in \mathbb{Z}$ for $i, j = 1, \dots, n$.

If the ring R has the presentation above we write

R

$$= \left\langle a_1, \dots, a_n : m_i a_i = 0, a_i a_j = \sum_{k=1}^n w_{ijk} a_k, i, j = 1, \dots, n \right\rangle. \quad (2)$$

Theorem 3. *Let R be a finite ring with additive group $\oplus_{i=1}^n A_i$, where $A_i = \langle a_i \rangle$ ($1 \leq i \leq n$) are cyclic subgroups of orders m_i , respectively. Assume $w_{ijk} \in \mathbb{Z}$, $\lambda_{ij} = (m_i, m_j)$, where $1 \leq i, j, k \leq n$, and “ $\cdot$ ” is the following operation*

$$\cdot : R \times R \longrightarrow R$$

$$\left(\sum_{i=1}^n s_i a_i, \sum_{j=1}^n t_j a_j \right) \longrightarrow \sum_{k=1}^n \left(\sum_{i,j=1}^n s_i t_j w_{ijk} \right) a_k. \quad (3)$$

Then

- (1) “ $\cdot$ ” is well-defined if and only if

$$m_k \mid \lambda_{ij} w_{ijk} \quad \forall 1 \leq i, j, k \leq n; \quad (*)$$

- (2) “ $\cdot$ ” is always distributive, in the case when “ $\cdot$ ” is well-defined;

- (3) “ $\cdot$ ” is associative if and only if

$$\sum_{\alpha=1}^n w_{i\alpha} w_{\alpha k} \equiv_{m_k} \sum_{\alpha=1}^n w_{j\alpha} w_{\alpha k} \quad \forall 1 \leq i, j, k, l \leq n. \quad (**)$$

Consequently,

$$\left\langle a_1, \dots, a_n : m_i a_i = 0, a_i a_j = \sum_{k=1}^n w_{ijk} a_k, i, j = 1, \dots, n \right\rangle \quad (4)$$

is a ring if and only if (*) and (**) above hold.

Proof. (1) $(\Rightarrow)$. Assume “ $\cdot$ ” is well-defined and fix i, j where $1 \leq i, j \leq n$. Let $x \in m_i \mathbb{Z}$. Then by definition of “ $\cdot$ ”, we have

$$\sum_{k=1}^n x w_{ijk} a_k = (x a_i) \cdot (a_j) = (0) \cdot (a_j) = 0. \quad (5)$$

Thus for each $k = 1, \dots, n$, we deduce $x w_{ijk} a_k = 0$ that is, $m_i w_{ijk} \mathbb{Z} \subseteq m_k \mathbb{Z}$, for $k = 1, \dots, n$. Similarly, $m_j w_{ijk} \mathbb{Z} \subseteq m_k \mathbb{Z}$, for $k = 1, \dots, n$. Therefore,

$$[m_i \mathbb{Z} + m_j \mathbb{Z}] w_{ijk} \subseteq m_k \mathbb{Z} \quad \forall 1 \leq i, j, k \leq n. \quad (6)$$

Now one can easily check that the last relation holds if and only if (*) holds.

- (1) $(\Leftarrow)$. Assume

$$\sum_{i=1}^n s_i a_i = \sum_{i=1}^n u_i a_i, \quad \sum_{j=1}^n t_j a_j = \sum_{j=1}^n v_j a_j, \quad (7)$$

where $s_i, u_i, t_j, v_j \in \mathbb{Z}$. Then $s_i a_i = u_i a_i$ and $t_j a_j = v_j a_j$ for all i, j . Let $x_i = u_i - s_i$ and $y_j = v_j - t_j$. Then $u_i = x_i + s_i$, $v_j = y_j + t_j$, $x_i \in m_i \mathbb{Z}$ and $y_j \in m_j \mathbb{Z}$. Hence

$$\begin{aligned} u_i v_j - s_i t_j &= s_i y_j + x_i t_j + x_i y_j \\ &= x_i t_j + (s_i + x_i) y_j \in [m_i \mathbb{Z} + m_j \mathbb{Z}] \end{aligned} \quad (8)$$

and so

$$(u_i v_j - s_i t_j) w_{ijk} \in [m_i \mathbb{Z} + m_j \mathbb{Z}] w_{ijk} \quad \forall k \quad (1 \leq k \leq n). \quad (9)$$

Now by condition (*) we have

$$(u_i v_j - s_i t_j) w_{ijk} a_k = 0 \quad \forall k \quad (1 \leq k \leq n). \quad (10)$$

It follows that

$$\sum_{k=1}^n \left(\sum_{i,j=1}^n s_i t_j w_{ijk} \right) a_k = \sum_{k=1}^n \left(\sum_{i,j=1}^n u_i v_j w_{ijk} \right) a_k, \quad (11)$$

that is,

$$\sum_{i=1}^n s_i a_i \cdot \sum_{j=1}^n t_j a_j = \sum_{i=1}^n u_i a_i \cdot \sum_{j=1}^n v_j a_j. \quad (12)$$

Thus the operation “.” is well-defined.

(2) Suppose the operation “.” is well-defined. Then

$$\begin{aligned} & \left(\sum_{i=1}^n s_i a_i + \sum_{i=1}^n u_i a_i \right) \cdot \left(\sum_{j=1}^n t_j a_j \right) \\ &= \left(\sum_{i=1}^n (s_i + u_i) a_i \right) \cdot \sum_{j=1}^n t_j a_j \\ &= \sum_{k=1}^n \left(\sum_{i,j=1}^n (s_i + u_i) t_j w_{ijk} \right) a_k \\ &= \sum_{k=1}^n \left(\sum_{i,j=1}^n s_i t_j w_{ijk} \right) a_k + \sum_{k=1}^n \left(\sum_{i,j=1}^n u_i t_j w_{ijk} \right) a_k \\ &= \left(\sum_{i=1}^n s_i a_i \right) \cdot \left(\sum_{j=1}^n t_j a_j \right) + \left(\sum_{i=1}^n u_i a_i \right) \cdot \left(\sum_{j=1}^n t_j a_j \right). \end{aligned} \quad (13)$$

On the other hand

$$\begin{aligned} & \left(\sum_{i=1}^n s_i a_i \right) \cdot \left(\sum_{j=1}^n t_j a_j + \sum_{j=1}^n v_j a_j \right) \\ &= \left(\sum_{i=1}^n s_i a_i \right) \cdot \left(\sum_{j=1}^n (t_j + v_j) a_j \right) \\ &= \sum_{k=1}^n \left(\sum_{i,j=1}^n s_i (t_j + v_j) w_{ijk} \right) a_k \\ &= \sum_{k=1}^n \left(\sum_{i,j=1}^n s_i t_j w_{ijk} \right) a_k + \sum_{k=1}^n \left(\sum_{i,j=1}^n s_i v_j w_{ijk} \right) a_k \\ &= \left(\sum_{i=1}^n s_i a_i \right) \cdot \left(\sum_{j=1}^n t_j a_j \right) + \left(\sum_{i=1}^n s_i a_i \right) \cdot \left(\sum_{j=1}^n v_j a_j \right). \end{aligned} \quad (14)$$

Thus “.” is a distributive operation.

(3) By definition of “.”, we have

$$a_i \cdot a_j = \sum_{k=1}^n w_{ijk} a_k \quad \forall 1 \leq i, j \leq n \quad (15)$$

and so

$$(a_i \cdot a_j) \cdot a_l = \left(\sum_{\alpha=1}^n w_{ij\alpha} a_\alpha \right) \cdot a_l = \sum_{k=1}^n \left(\sum_{\alpha=1}^n w_{ij\alpha} w_{\alpha lk} \right) a_k \quad (16)$$

and also

$$a_i \cdot (a_j \cdot a_l) = a_i \cdot \left(\sum_{\alpha=1}^n w_{jl\alpha} a_\alpha \right) = \sum_{k=1}^n \left(\sum_{\alpha=1}^n w_{jl\alpha} w_{i\alpha k} \right) a_k. \quad (17)$$

Now, it is clear that “.” is associative if and only if $(a_i \cdot a_j) \cdot a_l = a_i \cdot (a_j \cdot a_l)$ for all $1 \leq i, j, l \leq n$, if and only if

$$\sum_{\alpha=1}^n w_{ij\alpha} w_{\alpha lk} \equiv_{m_k} \sum_{\alpha=1}^n w_{jl\alpha} w_{i\alpha k} \quad \forall 1 \leq i, j, k, l \leq n. \quad (18)$$

□

Theorem 4. For $n \in \mathbb{N}$, let

$$\begin{aligned} R_1 &= \left\langle a_1, \dots, a_n : m_i a_i = 0, a_i a_j = \sum_{k=1}^n w_{ijk} a_k, i, j = 1, \dots, n \right\rangle, \\ R_2 &= \left\langle a_1, \dots, a_n : m_i a_i = 0, a_i a_j = \sum_{k=1}^n z_{ijk} a_k, i, j = 1, \dots, n \right\rangle \end{aligned} \quad (19)$$

be two presentations with suitable $w_{ijk}, z_{ijk} \in \mathbb{Z}$, $(1 \leq i, j, k \leq n)$. Assume $p_{ij} \in \mathbb{Z}$ where $1 \leq i, j \leq n$ and f is the following map:

$$f : R_1 \longrightarrow R_2,$$

$$f \left(\sum_{i=1}^n s_i a_i \right) = \sum_{j=1}^n \left(\sum_{i=1}^n s_i p_{ij} \right) b_j. \quad (20)$$

Then

(1) f is well-defined if and only if for $1 \leq i, j \leq n$,

$$m_j \mid m_i p_{ij}. \quad (21)$$

(2) If f is well-defined, then

- (a) f is an $\mathbb{Z}$ -module homomorphism,
- (b) f is one to one if and only if for each $s_1, s_2, \dots, s_n \in \mathbb{Z}$, $m_j \mid \sum_{i=1}^n s_i p_{ij}$ implies that $m_j \mid s_j$ for all $1 \leq j \leq n$, and
- (c) f is a ring homomorphism if and only if for $1 \leq i, j, k \leq n$,

$$\sum_{\alpha, \beta=1}^n p_{i\alpha} p_{j\beta} w_{\alpha\beta k} \equiv_{m_k} \sum_{l=1}^n z_{ijl} p_{lk}. \quad (22)$$

Proof. (1) $(\Rightarrow)$. Assume $s \in m_i\mathbb{Z}$, where $1 \leq i \leq n$. Then by definition f we have

$$\sum_{j=1}^n s p_{ij} b_j = f(sa_i) = f(0) = 0. \quad (23)$$

It follows that $s p_{ij} b_j = 0$ for all $1 \leq j \leq n$. Therefore, $m_i p_{ij} \mathbb{Z} \subseteq m_j \mathbb{Z}$, for all $1 \leq j \leq n$ and so for $1 \leq i, j \leq n$,

$$m_j \mid m_i p_{ij}. \quad (24)$$

(1) $(\Leftarrow)$. Suppose $\sum_{i=1}^n s_i a_i = \sum_{i=1}^n t_i a_i$ where $s_i, t_i \in \mathbb{Z}$. Then $s_i - t_i \in m_i \mathbb{Z}$ for all i ($1 \leq i \leq n$) and so $(s_i - t_i) p_{ij} \in m_i p_{ij} \mathbb{Z}$. Now by our hypothesis $m_j \mid (s_i - t_i) p_{ij}$ that is, $s_i p_{ij} b_j = t_i p_{ij} b_j$ for all $1 \leq i, j \leq n$. Therefore,

$$\sum_{j=1}^n \left(\sum_{i=1}^n s_i p_{ij} \right) b_j = \sum_{j=1}^n \left(\sum_{i=1}^n t_i p_{ij} \right) b_j. \quad (25)$$

This means that

$$f\left(\sum_{i=1}^n s_i a_i\right) = f\left(\sum_{i=1}^n t_i a_i\right) \quad (26)$$

and hence f is well-defined.

(2) (a) Assume $r, s_i, t_i \in \mathbb{Z}$, for $i = 1, \dots, n$. Clearly,

$$\begin{aligned} & f\left(r \sum_{i=1}^n s_i a_i + \sum_{i=1}^n t_i a_i\right) \\ &= f\left(\sum_{i=1}^n (rs_i + t_i) a_i\right) \\ &= \sum_{j=1}^n \left(\sum_{i=1}^n (rs_i + t_i) p_{ij}\right) b_j \\ &= \sum_{j=1}^n \left(\sum_{i=1}^n r s_i p_{ij}\right) b_j + \sum_{j=1}^n \left(\sum_{i=1}^n t_i p_{ij}\right) b_j \\ &= r f\left(\sum_{i=1}^n s_i a_i\right) + f\left(\sum_{i=1}^n t_i a_i\right). \end{aligned} \quad (27)$$

Thus f is an $\mathbb{Z}$ -module homomorphism.

(2) (b) By definition f , (b) is clear.

(2) (c) By (2) (a), f is always a group homomorphism. Thus it is sufficient to show that $f(a_i a_j) = f(a_i) f(a_j)$ for each i, j ($1 \leq i, j \leq n$). However by multiplications of R_1, R_2 and definition of f we have

$$f(a_i a_j) = f\left(\sum_{l=1}^n w_{ijl} a_l\right) = \sum_{k=1}^n \left(\sum_{l=1}^n w_{ijl} p_{lk}\right) b_k \quad (28)$$

and also

$$\begin{aligned} f(a_i) f(a_j) &= \left(\sum_{s=1}^n p_{is} b_s\right) \left(\sum_{t=1}^n p_{jt} b_t\right) \\ &= \sum_{k=1}^n \left(\sum_{s,t=1}^n p_{is} p_{jt} z_{stk}\right) b_k. \end{aligned} \quad (29)$$

Thus f is a ring homomorphism if and only if for all $1 \leq i, j, k \leq n$,

$$\sum_{\alpha, \beta=1}^n p_{i\alpha} p_{j\beta} w_{\alpha\beta k} \equiv_{m_k} \sum_{l=1}^n z_{ijl} p_{lk}. \quad (30)$$

□

Corollary 5. Let n be a positive integer and let $A_i = \langle a_i \rangle$ ($1 \leq i \leq n$) be cyclic additive groups of orders m_i , respectively. If

$$R_1 = \left\langle a_1, \dots, a_n : m_i a_i = 0, a_i a_j = \sum_{k=1}^n w_{ijk} a_k, i, j = 1, \dots, n \right\rangle,$$

$$R_2 = \left\langle a_1, \dots, a_n : m_i a_i = 0, a_i a_j = \sum_{k=1}^n z_{ijk} a_k, i, j = 1, \dots, n \right\rangle \quad (31)$$

are two presentations with suitable $w_{ijk}, z_{ijk} \in \mathbb{Z}$ ($1 \leq i, j, k \leq n$), then $R_1 \cong R_2$ if and only if there exist $p_{ij} \in \mathbb{Z}$ ($1 \leq i, j \leq n$) such that

- (1) $m_j \mid m_i p_{ij}$, for $1 \leq i, j \leq n$;
- (2) for all $s_i \in \mathbb{Z}$ and $1 \leq j \leq n$, $m_j \mid \sum_{i=1}^m s_i p_{ij}$ implies that $m_j \mid s_j$ for all $1 \leq j \leq n$, and
- (3) $\sum_{\alpha, \beta=1}^n p_{i\alpha} p_{j\beta} w_{\alpha\beta k} \equiv_{m_k} \sum_{l=1}^n z_{ijl} p_{lk}$, for $1 \leq i, j, k \leq n$.

Proof. It is clear by Theorem 4. □

3. Finite Rings of Order p^6 with Characteristic p^6 and p^5

In this section, we first classify all finite rings of order p^6 with characteristic p^6 . Then this classification is extended to the rings order p^n with characteristic p^n .

Proposition 6. (i) Let $R = \langle a \rangle$ be an additive cyclic group of order p^6 and $w \in \mathbb{Z}$. Then $R = \langle a : p^6 a = 0, a^2 = wa \rangle$ is always a ring.

(ii) Let $R_1 = \langle a : p^6 a = 0, a^2 = wa \rangle$ and $R_2 = \langle a : p^6 a = 0, a^2 = za \rangle$ be two presentations with $w, z \in \mathbb{Z}$. Assume $q \in \mathbb{Z}$ and f is the following map:

$$\begin{aligned} f : R_1 &\longrightarrow R_2, \\ f(ra) &= rqa. \end{aligned} \quad (32)$$

Then

- (1) f is well-defined;
- (2) f is a ring homomorphism if and only if for $wq \equiv_{p^6} zq^2$;
- (3) f is one to one if and only if for each $r \in \mathbb{Z}$, $p^6 \mid rq$ implies that $p^6 \mid r$.

Proof. (i) It is straightforward by relations (*) and (**) in Theorem 3.

(ii) The proof is obtained by simplification of the relations in Theorem 4. $\square$

Since the function introduced in preceding proposition is multiplication by some $q \in \mathbb{Z}$, and is always well-defined, we have the following corollary.

Corollary 7. Let $R_1 = \langle a : p^6 a = 0, a^2 = wa \rangle$ and $R_2 = \langle a : p^6 a = 0, a^2 = za \rangle$ be two presentations with $w, z \in \mathbb{Z}$. Then $R_1 \cong R_2$ if and only if there exists $q \in \mathbb{Z}$ such that

- (1) $wq \equiv_{p^6} zq^2$;
- (2) for each $r \in \mathbb{Z}$, $p^6 \mid rq$ implies that $p^6 \mid r$.

Proof. It is clear by Proposition 6. $\square$

Theorem 8. For any prime number p , there are exactly seven rings of order p^6 whose additive group is cyclic, only one of these rings have identity. However all of these are commutative.

Proof. Let $R_1 = \langle a : p^6 a = 0, a^2 = wa \rangle$ and $R_2 = \langle a : p^6 a = 0, a^2 = za \rangle$ be two presentations with $w, z \in \mathbb{Z}$. The relation (2) in Corollary 7 implies that p is relatively prime to q and so by the relation (1) in Corollary 7, we deduce that $w \equiv_{p^6} zq$. Since the relation $w \equiv_{p^6} zx$ has a solution, $\gcd(p^6, z) \mid w$. Now we proceed by cases.

Case 1. $\gcd(p, w) = 1$, that is, w is relatively prime to p . Since $\gcd(p^6, z) \mid w$, z is also relatively prime to p . Thus $R_1 \cong R_2$ where both w and z are relatively prime to p .

Case 2. $\gcd(p^2, w) = p$. Then the relation $(p^6, z) \mid w$ shows that either $\gcd(z, p) = 1$ or $z \in \{p, 2p, 3p, \dots, (p-1)p\}$. But the relation $w \equiv_{p^6} zq$ follows that $w \equiv_p zq$ and hence $p \mid zq$ because $\gcd(p^2, w) = p$. Since $\gcd(p, q) = 1$, $p \mid z$. Therefore we obtain that $z \in \{p, 2p, 3p, \dots, (p-1)p\}$ and so $\gcd(p^2, z) = p$. Thus $R_1 \cong R_2$ where both $\gcd(p^2, w) = p$ and $\gcd(p^2, z) = p$.

Case 3. $\gcd(p^3, w) = p^2$. Then the relation $\gcd(p^6, z) \mid w$ shows that either $\gcd(z, p) = 1$ or $z \in \{p, 2p, 3p, \dots, (p-1)p, p^2, 2p^2, 3p^2, \dots, (p-1)p^2\}$. But the relation $w \equiv_{p^6} zq$ follows that $w \equiv_{p^2} zq$ and hence $p^2 \mid zq$ because $\gcd(p^2, w) = p$. Since $\gcd(p, q) = 1$, $p^2 \mid z$. Therefore we obtain that $z \in \{p^2, 2p^2, 3p^2, \dots, (p-1)p^2\}$ and so $\gcd(p^3, z) = p^2$. Thus $R_1 \cong R_2$ where both $\gcd(p^3, w) = p^2$ and $\gcd(p^3, z) = p^2$.

Case 4. $\gcd(p^4, w) = p^3$. Then the relation $\gcd(p^6, z) \mid w$ shows that either $\gcd(z, p) = 1$ or

$$z \in \{p, 2p, 3p, \dots, (p-1)p, p^2, 2p^2, 3p^2, \dots, (p-1)p^2, p^3, 2p^3, 3p^3, \dots, (p-1)p^3\}. \quad (33)$$

But the relation $w \equiv_{p^6} zq$ follows that $w \equiv_{p^3} zq$ and hence $p^3 \mid zq$ because $\gcd(p^4, w) = p^3$. Since $\gcd(p, q) = 1$, $p^3 \mid z$. Therefore we obtain that $z \in \{p^3, 2p^3, 3p^3, \dots, (p-1)p^3\}$ and so $\gcd(p^4, z) = p^3$. Thus $R_1 \cong R_2$ where both $\gcd(p^4, w) = p^3$ and $\gcd(p^4, z) = p^3$.

Case 5. $\gcd(p^5, w) = p^4$. By a similar argument, we deduce $R_1 \cong R_2$ where both $\gcd(p^5, w) = p^4$ and $\gcd(p^5, z) = p^4$.

Case 6. $\gcd(p^6, w) = p^5$. By a similar argument, we deduce $R_1 \cong R_2$ where both $\gcd(p^6, w) = p^5$ and $\gcd(p^6, z) = p^5$.

Case 7. $\gcd(p^6, w) = p^6$. By a similar argument, we deduce $R_1 \cong R_2$ where both $\gcd(p^6, w) = p^6$ and $\gcd(p^6, z) = p^6$. $\square$

An analysis similar to that in the proof of Theorem 8 shows that there are exactly $n + 1$ rings of order p^n with characteristic p^n . These rings are

$$\langle a : p^n a = 0, a^2 = wa \rangle, \quad (34)$$

$$w \in \{1, p, p^2, \dots, p^n\}$$

We can obtain the following result by applying relations (*) and (**) in Theorem 3, for the rings of order p^6 with characteristic p^5 . Also, this manner may be used for obtaining all finite rings of order p^6 with characteristic p^k , where $1 \leq k \leq 4$.

Corollary 9. Let $R = A_1 \oplus A_2$ where $A_1 = \langle a_1 \rangle$ and $A_2 = \langle a_2 \rangle$ be cyclic groups of order p and p^5 , respectively. Assume $w_{ijk} \in \mathbb{Z}$ where $1 \leq i, j, k \leq 2$. Then $R = \langle a_1, a_2 : pa_1 = p^5 a_2 = 0, a_i a_j = \sum_{k=1}^2 w_{ijk} a_k, i, j = 1, 2 \rangle$ is a ring if and only if the following hold.

- (1) $p^4 \mid w_{112}, p^4 \mid w_{122}$ and $p^4 \mid w_{212}$;
- (2) $w_{111}w_{122} \equiv_{p^5} w_{121}w_{112}$;
- (3) $w_{211}w_{212} \equiv_{p^5} w_{121}w_{122} \equiv_{p^5} w_{221}w_{112}$;
- (4) $w_{211}w_{112} \equiv_{p^5} w_{111}w_{212} + w_{112}w_{222}$;
- (5) $w_{211}w_{122} + w_{212}w_{222} \equiv_{p^5} w_{121}w_{212} + w_{122}w_{222}$;
- (6) $w_{221}w_{122} \equiv_{p^5} w_{212}w_{221}$.

Application and simplification of the relations (1), (2), and (3) in Corollary 5, for the rings of order p^6 with characteristic p^5 , give us the following result.

Corollary 10. *Let*

$$R = \left\langle a_1, a_2 : pa_1 = p^5 a_2 = 0, a_i a_j = \sum_{k=1}^2 w_{ijk} a_k, i, j = 1, 2 \right\rangle,$$

$$S = \left\langle a_1, a_2 : pa_1 = p^5 a_2 = 0, a_i a_j = \sum_{k=1}^2 z_{ijk} a_k, i, j = 1, 2 \right\rangle \quad (35)$$

be two rings with suitable integers w_{ijk} and z_{ijk} satisfied in Theorem 3, for $1 \leq i, j, k \leq 2$. Then $R \cong S$ if and only if there exist $p_{ij} \in \mathbb{Z}$ such that the following hold.

- (1) $p^4 \mid p_{12}$;
- (2) If $p \mid s_1 p_{11} + s_2 p_{21}$ and $p^5 \mid s_1 p_{12} + s_2 p_{22}$, then $p \mid s_1$ and $p^5 \mid s_2$;
- (3) $p_{11}^2 \equiv_p z_{111}(p_{11} + p_{21})$;
- (4) $p_{11} p_{21} w_{111} + p_{11} p_{22} w_{121} \equiv_p z_{121}(p_{11} + p_{21})$;
- (5) $p_{21}^2 w_{111} + p_{22} p_{21} w_{211} + p_{22}^2 w_{221} \equiv_p z_{221}(p_{11} + p_{21})$;
- (6) $p_{11}^2 w_{112} \equiv_p z_{112} p_{22}$;
- (7) $p_{21} p_{11} w_{112} + p_{22} p_{11} w_{212} + p_{22} p_{12} w_{222} \equiv_p z_{212} p_{22}$;
- (8) $p_{11} p_{21} w_{112} + p_{11} p_{22} w_{122} + p_{12} p_{22} w_{222} \equiv_p z_{122} p_{22}$;
- (9) $p_{21}^2 w_{112} + p_{22} p_{21} (w_{212} + w_{122}) + p_{22}^2 w_{222} \equiv_p z_{222} (p_{12} + p_{22})$.

In the following, one gives an algorithm for computing the finite rings whose abelian group is isomorphic to $\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \dots \oplus \mathbb{Z}_{m_n}$. We represent the algorithm in the form of two sub-algorithms. In Algorithm 11, one lets $(m_1, m_2, \dots, m_n)$ be the input and A be the set of all sequences (w_{ijk}) that satisfy the condition $0 \leq w_{ijk} \leq m_k - 1$, for any $1 \leq i, j, k \leq n$. Then one has the sequences (w_{ijk}) that satisfy the conditions (*) and (**) in Theorem 3 as the outputs of the algorithm. In fact, any sequence (w_{ijk}) that is an output of this algorithm shows a ring as the following:

$$\left\langle a_1, a_2, \dots, a_n : m_i a_i = 0, a_i a_j = \sum_{k=1}^n w_{ijk} a_k, i, j = 1, \dots, n \right\rangle. \quad (36)$$

In Algorithm 12, one represents the conditions required for the isomorphism of two rings based upon Theorem 4. In fact, one verifies the two sequences (w_{ijk}) and (z_{ijk}) obtained from Algorithm 11, under isomorphic conditions in Theorem 4. Therefore under Algorithms 11 and 12, one computes all the rings whose abelian group is isomorphic to $\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \dots \oplus \mathbb{Z}_{m_n}$ and are not isomorphic. We have implemented Algorithms 11 and 12 in C^{++} and presents a sample of its responses for the rings whose abelian group is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_{32}$ in the following example.

Algorithm 11. (1) Input $(m_1, m_2, \dots, m_n)$
 (2) Let $N =: \{1, 2, \dots, n\}$

- (3) For all $(i, j) \in N^2$, let $\lambda_{ij} =: \gcd(m_i, m_j)$
- (4) Let $A =: \{w = (w_{ijk})_{(i,j,k) \in N^3} ; \text{ for all } (i, j, k) \in N^3, 0 \leq w_{ijk} \leq m_k - 1\}$
- (5) $B =: \{\}$
- (6) If $A = B$, then go to end
- (7) Choose $w = (w_{ijk})_{(i,j,k) \in N^3} \in A \setminus B$
- (8) Let $B =: B \cup \{w\}$
- (9) If there is $(i, j, k) \in N^3$ such that $\lambda_{ij} w_{ijk} \not\equiv_{m_k} 0$, then go to step 6
- (10) If there is $(i, j, k, l) \in N^4$ such that $\sum_{\alpha=1}^n w_{i\alpha} w_{\alpha l k} \not\equiv_{m_k} \sum_{\alpha=1}^n w_{j\alpha} w_{\alpha l k}$, then go to step 6
- (11) Print $w = (w_{ijk})_{(i,j,k) \in N^3}$
- (12) End

Algorithm 12. (1) Input $(m_1, m_2, \dots, m_n)$

- (2) Let $N =: \{1, 2, \dots, n\}$
- (3) For all $(i, j) \in N^2$, let $\lambda_{ij} =: \gcd(m_i, m_j)$
- (4) Input $w = (w_{ijk})_{(i,j,k) \in N^3}$ and $z = (z_{ijk})_{(i,j,k) \in N^3}$ satisfied in Algorithm 11
- (5) Let $A =: \{P = (p_{ij})_{(i,j) \in N^2} ; \text{ for all } (i, j) \in N^2, 0 \leq p_{ij} \leq m_j - 1\}$
- (6) $B =: \{\}$
- (7) If $A = B$, then go to end
- (8) Choose $P = (p_{ij})_{(i,j) \in N^2} \in A \setminus B$
- (9) Let $B =: B \cup \{P\}$
- (10) If there is $(i, j) \in N^2$ such that $m_i p_{ij} \not\equiv_{m_j} 0$, then go to step 7
- (11) Let $C =: \{\}$
- (12) Let $D =: \{r = (r_j)_{j \in N} ; \text{ for all } j \in N, 0 \leq r_j \leq m_j - 1, \sum_{i=1}^n r_i p_{ij} \equiv_{m_j} 0\}$
- (13) Choose $r \in D$
- (14) Let $C =: C \cup \{r\}$
- (15) If there is $i \in N$ such that $r_i \not\equiv_{m_i} 0$, then go to step 7
- (16) If there is $(i, j, k) \in N^3$ such that $\sum_{\alpha, \beta=1}^n p_{i\alpha} p_{j\beta} w_{\alpha\beta k} \not\equiv_{m_k} \sum_{l=1}^n z_{ijl} p_{lk}$, then go to step 7
- (17) Print two rings R and S with representations $w = (w_{ijk})_{(i,j,k) \in N^3}$ and $z = (z_{ijk})_{(i,j,k) \in N^3}$, respectively, are isomorphic
- (18) End

Example 13. We compute the presentations of all finite rings of order 2^6 , whose abelian group is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_{32}$. Let R be a such ring. Then we write the following presentation for $R = \langle a_1, a_2 : 2a_1 = 2^5 a_2 = 0, a_i a_j = w_{ij1} a_1 + w_{ij2} a_2, i, j = 1, 2 \rangle$:

$$R = \left[\begin{array}{c} w_{111} \\ w_{112} \\ w_{121} \\ w_{122} \\ w_{211} \\ w_{212} \\ w_{221} \\ w_{222} \end{array} \right]. \quad (37)$$

The outputs of these algorithms for the rings of order 2^6 whose abelian group is $\mathbb{Z}_2 \oplus \mathbb{Z}_{32}$ are listed below.

$$\begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 2 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 4 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 8 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 16 \end{bmatrix},$$

$$\begin{bmatrix} 0 \\ 0 \\ 0 \\ 16 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 16 \\ 0 \\ 0 \\ 2 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 16 \\ 0 \\ 0 \\ 4 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 16 \\ 0 \\ 0 \\ 8 \end{bmatrix},$$

$$\begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 16 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 16 \\ 2 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 16 \\ 4 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 16 \\ 8 \end{bmatrix},$$

$$\begin{bmatrix} 0 \\ 0 \\ 0 \\ 16 \\ 0 \\ 16 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 16 \\ 0 \\ 16 \\ 2 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 16 \\ 0 \\ 16 \\ 4 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 16 \\ 0 \\ 16 \\ 8 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 16 \\ 0 \\ 16 \\ 16 \end{bmatrix},$$

$$\begin{bmatrix} 0 \\ 16 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 16 \\ 0 \\ 0 \\ 0 \\ 0 \\ 2 \end{bmatrix}, \begin{bmatrix} 0 \\ 16 \\ 0 \\ 0 \\ 0 \\ 0 \\ 4 \end{bmatrix}, \begin{bmatrix} 0 \\ 16 \\ 0 \\ 0 \\ 0 \\ 0 \\ 8 \end{bmatrix}, \begin{bmatrix} 0 \\ 16 \\ 0 \\ 0 \\ 0 \\ 0 \\ 16 \end{bmatrix},$$

$$\begin{bmatrix} 0 \\ 16 \\ 0 \\ 16 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 16 \\ 0 \\ 16 \\ 0 \\ 0 \\ 2 \end{bmatrix}, \begin{bmatrix} 0 \\ 16 \\ 0 \\ 16 \\ 0 \\ 0 \\ 4 \end{bmatrix}, \begin{bmatrix} 0 \\ 16 \\ 0 \\ 16 \\ 0 \\ 0 \\ 8 \end{bmatrix}, \begin{bmatrix} 0 \\ 16 \\ 0 \\ 16 \\ 0 \\ 0 \\ 16 \end{bmatrix},$$

$$\begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 2 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 4 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 8 \end{bmatrix},$$

$$\begin{bmatrix} 0 \\ 0 \\ 0 \\ 16 \\ 0 \\ 16 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 16 \\ 0 \\ 16 \\ 2 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 16 \\ 0 \\ 16 \\ 4 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 16 \\ 0 \\ 16 \\ 8 \end{bmatrix},$$

$$\begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 16 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix},$$

$$\begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 2 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 4 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 8 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 16 \end{bmatrix}.$$

(38)

Thus there exist 47 rings of order 2^6 with characteristic 2^5 .

Acknowledgment

This research was supported by Islamic Azad University, Khorramabad Branch.

References

- [1] B. Corbas and G. D. Williams, "Rings of order p^5 . I. Nonlocal rings," *Journal of Algebra*, vol. 231, no. 2, pp. 677–690, 2000.
- [2] K. E. Eldridge, "Orders for finite noncommutative rings with unity," *The American Mathematical Monthly*, vol. 75, pp. 512–514, 1968.
- [3] B. Fine, "Classification of finite rings of order p^2 ," *Mathematics Magazine*, vol. 66, no. 4, pp. 248–252, 1993.
- [4] R. S. Wilson, "Representations of finite rings," *Pacific Journal of Mathematics*, vol. 53, no. 2, pp. 643–649, 1974.
- [5] R. Raghavendran, "A class of finite rings," *Compositio Mathematica*, vol. 21, pp. 195–229, 1969.
- [6] R. Gilmer and J. Mott, "Associative rings of order p^3 ," *Proceedings of the Japan Academy*, vol. 49, pp. 795–799, 1973.

- [7] J. B. Derr, G. F. Orr, and P. S. Peck, “Noncommutative rings of order p^4 ,” *Journal of Pure and Applied Algebra*, vol. 97, no. 2, pp. 109–116, 1994.
- [8] B. Corbas and G. D. Williams, “Rings of order p^5 . II. Local rings,” *Journal of Algebra*, vol. 231, no. 2, pp. 691–704, 2000.
- [9] M. Behboodi, R. Beyranvand, A. Hashemi, and H. Khabazian, “Classification of finite rings: theory and algorithm,” In press.