Classification of finite rings: Theory and algorithm

Article *in* Czechoslovak Mathematical Journal · January 2013

DOI: 10.1007/s10587-014-0124-7

CITATIONS
3

READS
393

4 authors, including:

Mahmood Behboodi
Isfahan University of Technology
72 PUBLICATIONS **790** CITATIONS

SEE PROFILE

Amir Hashemi
Institute for Research in Fundamental Sciences (IPM)
79 PUBLICATIONS **272** CITATIONS

SEE PROFILE

Hossain Khabazian
Isfahan University of Technology
20 PUBLICATIONS **28** CITATIONS

SEE PROFILE

Czechoslovak Mathematical Journal

Mahmood Behboodi; Reza Beyranvand; Amir Hashemi; Hossein Khabazian
Classification of finite rings: theory and algorithm

Czechoslovak Mathematical Journal, Vol. 64 (2014), No. 3, 641–658

Persistent URL: http://dml.cz/dmlcz/144050

Czechoslovak Mathematical Journal, 64 (139) (2014), 641–658

CLASSIFICATION OF FINITE RINGS: THEORY AND ALGORITHM

Mahmood Behboodi, Esfahan, Reza Beyranvand, Khoramabad,
Amir Hashemi, Hossein Khabazian, Esfahan

(Received February 13, 2013)

Abstract. An interesting topic in the ring theory is the classification of finite rings. Although rings of certain orders have already been classified, a full description of all rings of a given order remains unknown. The purpose of this paper is to classify all finite rings (up to isomorphism) of a given order. In doing so, we introduce a new concept of *quasi basis* for certain type of modules, which is a useful computational tool for dealing with finite rings. Then, using this concept, we give structure and isomorphism theorems for finite rings and state our main result to classify (up to isomorphism) the finite rings of a given order. Finally, based on these results, we describe an algorithm to calculate the structure of all such rings. We have implemented our new algorithm in `Maple`, and we apply it to an example.

Keywords: classification of finite ring; finite abelian group; quasi base

MSC 2010: 16P10, 16Z05, 68W30

1. Introduction

Classification of finite groups and finite rings are well-known problems which have been studied by many researchers. The oldest result on finite abelian groups has its origin in the works of German mathematician Gauss on quadratic forms. This result was explicitly proved by Kronecker and Stickelberger which is nowadays known as the fundamental theorem for finite abelian groups: *A finite abelian group is a direct sum of primary cyclic groups.* This may be considered as the cornerstone of many classification theorems in algebra and specially it may be used for the *classification of finite rings.*

The research of the first and third authors was in part supported by a grant from IPM (No. 91130413 and 92550420). The research of the first and third authors is partially carried out in the IPM-Isfahan Branch.

The problem of determining and classifying (up to isomorphism) the finite rings has attracted the attention of many mathematicians. To explain the existing results in this direction, let R be a finite ring of order m. It is well-known that every finite ring can be decomposed into a direct sum of p-rings, see [12]. Recall that a p-ring is a finite ring whose order is a power of a prime p, i.e., its additive structure is a p-primary abelian group. So, the decomposition of the additive structure $(R,+)$ of R into p-primary subgroups leads to the ring decomposition $R = R_1 \oplus \ldots \oplus R_n$ where $m = p_1^{k_1} \ldots p_n^{k_n}$ and R_i is a finite ring of order $p_i^{k_i}$. Thus, in order to classify the finite rings, it would suffice to deal only with p-rings. So, let p be a prime number. It is easy to see that there are merely two rings of order p; $\mathbb{Z}_p$ and the null ring of order p. In 1969, Raghavendran [10] proved that there exist eleven rings of order p^2 only four of which have the identity element. Also, in 1973, Gilmer and Mott [8] showed that there exist $4p + 48$ rings of order p^3 for $p \neq 2$ and only twelve of these rings have the identity element. Moreover, for $p = 2$, they found 59 rings of order 2^3. Only eleven of these have the identity. For p^4, a comprehensive list of non-commutative rings was first drawn up by Derr et al. in [5]. Commutative rings of order p^4 were characterized by Wilson [16]. In 2000, Corbas and Williams [3], [4] determined all rings of order p^5. The characterization of rings of higher orders remains still open. For more details on finite rings, we refer to the papers [1], [2], [6], [7], [9], [11], [12], [13], [14], [15] and also to the book [9], pages 133–141.

The aim of this paper is to classify all finite rings (up to isomorphism) of a given order m. For this purpose, we first calculate all decompositions $[p_1^{k_1}, \ldots, p_n^{k_n}]$ where $m = p_1^{k_1} \ldots p_n^{k_n}$, $p_1^{k_1} \leqslant \ldots \leqslant p_n^{k_n}$ and the p_i's are (not necessarily distinct) prime numbers. It is well-known that to find all finite rings (up to isomorphism) of order m, it suffices to calculate all finite rings of the form $R_1 \oplus \ldots \oplus R_n$ (corresponding to $[m_1, \ldots, m_n]$) such that the order of R_i is m_i and $[m_1, \ldots, m_n]$ is a decomposition of m (note that such a ring has a ring structure over the abelian group $\mathbb{Z}_{m_1} \oplus \ldots \oplus \mathbb{Z}_{m_n}$). In doing so, we introduce a new concept of *quasi basis* for certain type of modules. Based on this concept, we give new structure and isomorphism theorems for finite rings and state our main result to classify (up to isomorphism) the finite rings corresponding to a decomposition $[m_1, \ldots, m_n]$. Finally, based on these results, we describe an algorithm for calculating the structure of all finite rings of a given order. We have implemented our new algorithm in `Maple`, and apply it to compute all finite rings of order 12.

The paper is organized as follows. In Section 2, we introduce the concept of quasi basis for modules, and use it to define a multiplication on a class of modules. Then, we provide sufficient conditions for such a multiplication to yield an algebra. Furthermore, we obtain criteria to decide whether or not two such algebras over a given finite module are isomorphic (Theorem 2.1). Section 3 aims to describe

the structure of all finite rings over a given (finite) abelian group (Theorem 3.1). Moreover, we present a number of necessary and sufficient conditions to check if two finite rings (given by their structures) over an abelian group are isomorphic or not (Theorem 3.2). This concludes a classification (up to isomorphism) of all finite rings corresponding to a given decomposition. In Section 4, we propose an algorithm for the computation of the structures of all finite rings (up to isomorphism) of a given order.

2. Quasi bases and their applications

In this section, we first introduce the new concept of the quasi basis for modules in order to define a multiplication on a class of modules. We present then sufficient conditions for such a multiplication to provide an algebra. Finally, we give criteria to decide whether or not two such algebras over a given finite module are isomorphic (Theorem 2.1).

Let us start with some notation that we use throughout the paper. We denote by S an associative commutative ring with identity. All S-modules are considered to be unitary left S-modules.

Definition 2.1. Let M be a left S-module. A subset $A \subseteq M$ is called *quasi S-linear independent* if for any distinct elements $a_1, a_2, \ldots, a_n \in A$ and $s_1, s_2, \ldots, s_n \in S$, $\sum_{i=1}^{n} s_i a_i = 0$ implies that $s_i a_i = 0$ for all i. A generating set A of M is called a *quasi S-basis* for M if A is quasi S-linear independent.

Clearly every free S-module F possesses a quasi S-basis. Furthermore, every semi-simple left S-module has a quasi S-basis. The following result (which follows immediately from Definition 2.1) characterizes the modules having quasi S-bases.

Proposition 2.1. *An S-module has a quasi S-basis if and only if it is the internal direct sum of a family of cyclic S-modules.*

Corollary 2.1. *If M is a finitely generated $\mathbb{Z}$-module, then it has a quasi $\mathbb{Z}$-basis.*

P r o o f. Since every finitely generated $\mathbb{Z}$-module is a finite direct product of cyclic groups, M has a quasi $\mathbb{Z}$-basis (Proposition 2.1). □

Let M be an associative S-algebra with a finite quasi basis $\{a_1, a_2, \ldots, a_n\}$. Then the algebraic structure of $(M, +, \cdot)$ can be displayed by n^2 products

$$a_i a_j = \sum_{k=1}^{n} w_{ijk} a_k$$

with $w_{ijk} \in S$ and thus by n^3 constants w_{ijk} for $1 \leqslant i, j, k \leqslant n$. Using this notation, the multiplication on M is performed by

$$\Big(\sum_{i=1}^{n} s_i a_i\Big)\Big(\sum_{j=1}^{n} t_j a_j\Big) = \sum_{k=1}^{n}\Big(\sum_{i,j=1}^{n} s_i t_j w_{ijk}\Big)a_k.$$

For the sake of simplification, we introduce a convenient notion of *presentation* to describe the structure of an associative S-algebra with a finite quasi basis.

Definition 2.2 (Presentation)**.** Let M be an S-algebra with a quasi basis $\{a_1, a_2, \ldots, a_n\}$ so that $a_i a_j = \sum\limits_{k=1}^{n} w_{ijk} a_k$ for all i, j. Then we write

$$M = \Big\langle a_1, \ldots, a_n;\ a_i a_j = \sum_{k=1}^{n} w_{ijk} a_k, \quad i, j = 1, \ldots, n \Big\rangle$$

and we call it a *presentation* for M.

Below, we will provide some necessary and sufficient conditions for the above multiplication on an S-module (with a finite quasi S-basis) to yield an S-algebra. Recall that the *left annihilator* of an element $a \in S$ is the ideal $\operatorname{ann}_\ell(a) = \{s \in S;\ sa = 0\}$.

Lemma 2.1. *Let S be a commutative ring with identity, M an S-module and $M = \Big\langle a_1, \ldots, a_n;\ a_i a_j = \sum\limits_{k=1}^{n} w_{ijk} a_k \Big\rangle$. Consider the following multiplication on M:*

$$\begin{aligned} \cdot\colon M \times M &\to M \\ \Big(\sum_{i=1}^{n} s_i a_i, \sum_{j=1}^{n} t_j a_j\Big) &\mapsto \sum_{k=1}^{n}\Big(\sum_{i,j=1}^{n} s_i t_j w_{ijk}\Big)a_k. \end{aligned}$$

Then, the following assertions hold.

(1) *"$\cdot$" is well-defined iff* $[\operatorname{ann}_\ell(a_i) + \operatorname{ann}_\ell(a_j)]w_{ijk} \subseteq \operatorname{ann}_\ell(a_k)$ *for all i, j, k.*

(2) *"$\cdot$" is distributive, if "$\cdot$" is well-defined.*

(3) *"$\cdot$" is associative iff* $\sum\limits_{\alpha=1}^{n} (w_{ij\alpha} w_{\alpha lk} - w_{jl\alpha} w_{i\alpha k}) \in \operatorname{ann}_\ell(a_k)$ *for all i, j, k.*

Moreover, $(M, +, \cdot)$ is an S-algebra if and only if (1) *and* (3) *are satisfied.*

P r o o f. (1) Assume that "$\cdot$" is well-defined and fix i, j where $1 \leqslant i, j \leqslant n$. Let $x \in \operatorname{ann}_\ell(a_i)$. Then, by definition of "$\cdot$", we have

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

Since $\{a_1, a_2, \ldots, a_n\}$ is a quasi S-basis for M, $xw_{ijk}a_k = 0$ for each k and therefore $\mathrm{ann}_\ell(a_i)w_{ijk} \subseteq \mathrm{ann}_\ell(a_k)$ for all k. Similarly $\mathrm{ann}_\ell(a_j)w_{ijk} \subseteq \mathrm{ann}_\ell(a_k)$ for any k. Thus, $[\mathrm{ann}_\ell(a_i) + \mathrm{ann}_\ell(a_j)]w_{ijk} \subseteq \mathrm{ann}_\ell(a_k)$ for all i, j, k. Conversely, assume that

$$\sum_{i=1}^{n} s_i a_i = \sum_{i=1}^{n} u_i a_i \quad \text{and} \quad \sum_{j=1}^{n} t_j a_j = \sum_{j=1}^{n} v_j a_j$$

where $s_i, u_i, t_j, v_j \in S$. Hence it follows that $s_i a_i = u_i a_i$ and $t_j a_j = v_j a_j$ for all i, j. Set $x_i = u_i - s_i$ and $y_j = v_j - t_j$. Then $u_i = x_i + s_i$, $v_j = y_j + t_j$, $x_i \in \mathrm{ann}_\ell(a_i)$ and $y_j \in \mathrm{ann}_\ell(a_j)$. Hence, we can write

$$u_i v_j - s_i t_j = s_i y_j + x_i t_j + x_i y_j = x_i t_j + (s_i + x_i) y_j \in [\mathrm{ann}_\ell(a_i) + \mathrm{ann}_\ell(a_j)]$$

and so $(u_i v_j - s_i t_j) w_{ijk} \in [\mathrm{ann}_\ell(a_i) + \mathrm{ann}_\ell(a_j)]w_{ijk}$ for all k. From the hypothesis, one obtains $(u_i v_j - s_i t_j) w_{ijk} a_k = 0$ for all k. It follows that

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

and therefore

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

(2) Suppose that "$\cdot$" is well-defined. We prove the right distributivity of "$\cdot$"; the other side is proved similarly. We have

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

(3) For all i, j, l, let us consider the multiplications:

$$\begin{aligned}
(a_i \cdot a_j) \cdot a_l &= \Big(\sum_{\alpha=1}^{n} w_{ij\alpha} a_\alpha \Big) \cdot a_l = \sum_{k=1}^{n} \Big(\sum_{\alpha=1}^{n} w_{ij\alpha} w_{\alpha lk} \Big) a_k, \\
a_i \cdot (a_j \cdot a_l) &= a_i \cdot \Big(\sum_{\alpha=1}^{n} w_{jl\alpha} a_\alpha \Big) = \sum_{k=1}^{n} \Big(\sum_{\alpha=1}^{n} w_{jl\alpha} w_{i\alpha k} \Big) a_k.
\end{aligned}$$

Thus, we have $(a_i \cdot a_j) \cdot a_l = a_i \cdot (a_j \cdot a_l)$ if and only if $\sum_{\alpha=1}^{n} (w_{ij\alpha} w_{\alpha lk} - w_{jl\alpha} w_{i\alpha k}) \in \operatorname{ann}_\ell(a_k)$ for all i, j, k, which ends the proof. □

Corollary 2.2. *With notation as in Lemma* 2.1, *let M be a finitely generated free S-module with the basis $A = \{a_1, a_2, \ldots, a_n\}$. Then $(M, +, \cdot)$ is an associative S-algebra if and only if for each i, j, k we have*

$$\sum_{\alpha=1}^{n} (w_{ij\alpha} w_{\alpha lk} - w_{jl\alpha} w_{i\alpha k}) = 0.$$

P r o o f. Since M is a free S-module and A is its basis, hence $\operatorname{ann}_\ell(a_k) = 0$ for all k and thus "$\cdot$" is well-defined by the first item of Lemma 2.1. Thereby, $(M, +, \cdot)$ is an S-algebra if and only if $\sum_{\alpha=1}^{n} (w_{ij\alpha} w_{\alpha lk} - w_{jl\alpha} w_{i\alpha k}) = 0$. □

So far, we have provided sufficient conditions to define the structure of an associative algebra over a given module with a presentation. Below, we want to give criteria to decide whether or not two algebras (defined as above) are isomorphic (see Theorem 2.1).

Lemma 2.2. *Let S be a commutative ring with identity and M, N two S-modules with quasi bases $A = \{a_1, a_2, \ldots, a_n\}$ and $B = \{b_1, b_2, \ldots, b_n\}$, respectively. Assume that $p_{ij} \in S$ for all $1 \leqslant i, j \leqslant n$ and $f\colon M \to N$ is the map defined by*

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

Then the following statements hold:

(1) *f is well-defined iff $\operatorname{ann}_\ell(a_i) p_{ij} \subseteq \operatorname{ann}_\ell(b_j)$ for all $i, j = 1, \ldots, n$.*
(2) *If f is well-defined, then*
   (a) *f is an S-module homomorphism.*
   (b) *f is one-to-one iff for each $s_1, s_2, \ldots, s_n \in S$ such that $\sum_{i=1}^{n} s_i p_{ij} \in \operatorname{ann}_\ell(b_j)$ for all j, we have $s_i \in \operatorname{ann}_\ell(a_i)$ for all i.*
   (c) *if*

$$M = \Big\langle a_1, \ldots, a_n;\ a_i a_j = \sum_{k=1}^{n} w_{ijk} a_k,\ i, j = 1, \ldots, n \Big\rangle,$$
$$N = \Big\langle b_1, \ldots, b_n;\ b_i b_j = \sum_{k=1}^{n} z_{ijk} b_k,\ i, j = 1, \ldots, n \Big\rangle$$

are two S-algebras, then f is an S-algebra homomorphism iff for all i, j, k we have

$$\sum_{s,t=1}^{n} p_{is}p_{jt}w_{stk} - \sum_{l=1}^{n} z_{ijl}p_{lk} \in \operatorname{ann}_\ell(b_k).$$

P r o o f. (1) Suppose that f is well-defined. We consider $s \in \operatorname{ann}_\ell(a_i)$ for an integer $1 \leqslant i \leqslant n$. Then by definition of f we have

$$\sum_{j=1}^{n} sp_{ij}b_j = f(sa_i) = f(0) = 0.$$

Since B is a quasi basis for N, $sp_{ij}b_j = 0$ for all $1 \leqslant j \leqslant n$. Therefore, $\operatorname{ann}_\ell(a_i)p_{ij} \subseteq \operatorname{ann}_\ell(b_j)$ for all j. Conversely, suppose that $\sum\limits_{i=1}^{n} s_ia_i = \sum\limits_{i=1}^{n} t_ia_i$ where $s_i, t_i \in S$. Since A is a quasi basis for M, $s_i - t_i \in \operatorname{ann}_\ell(a_i)$ for all i. From the hypothesis, $(s_i - t_i)p_{ij} \in \operatorname{ann}_\ell(b_j)$ for all i, j. It follows that $s_ip_{ij}b_j = t_ip_{ij}b_j$ for all i, j and

$$\sum_{j=1}^{n}\Big(\sum_{i=1}^{n} s_ip_{ij}\Big)b_j = \sum_{j=1}^{n}\Big(\sum_{i=1}^{n} t_ip_{ij}\Big)b_j.$$

Therefore $f\Big(\sum\limits_{i=1}^{n} s_ia_i\Big) = f\Big(\sum\limits_{i=1}^{n} t_ia_i\Big)$ and hence f is well-defined.

(2) (a) Assume that $r, s_i, t_i \in S$ for $i = 1, \ldots, n$. So, we can write

$$\begin{aligned} f\Big(r\sum_{i=1}^{n} s_ia_i + \sum_{i=1}^{n} t_ia_i\Big) &= f\Big(\sum_{i=1}^{n}(rs_i + t_i)a_i\Big) \\ &= \sum_{j=1}^{n}\Big(\sum_{i=1}^{n}(rs_i + t_i)p_{ij}\Big)b_j \\ &= \sum_{j=1}^{n}\Big(\sum_{i=1}^{n} rs_ip_{ij}\Big)b_j + \sum_{j=1}^{n}\Big(\sum_{i=1}^{n} t_ip_{ij}\Big)b_j \\ &= rf\Big(\sum_{i=1}^{n} s_ia_i\Big) + f\Big(\sum_{i=1}^{n} t_ia_i\Big). \end{aligned}$$

Thus f is an S-module homomorphism.

(b) The assertion follows immediately from the fact that A and B are quasi S-bases for M and N, respectively.

(c) By (2) (a), f is always a group homomorphism. Thus, it suffices to show that $f(a_ia_j) = f(a_i)f(a_j)$ for each i, j. However, by multiplications defined in

S-algebras M, N and also by the definition of f we have

$$f(a_i a_j) = f\Big(\sum_{l=1}^{n} w_{ijl} a_l\Big) = \sum_{k=1}^{n}\Big(\sum_{l=1}^{n} w_{ijl} p_{lk}\Big) b_k.$$

On the other hand,

$$f(a_i)f(a_j) = \Big(\sum_{s=1}^{n} p_{is} b_s\Big)\Big(\sum_{t=1}^{n} p_{jt} b_t\Big) = \sum_{k=1}^{n}\Big(\sum_{s,t=1}^{n} p_{is} p_{jt} z_{stk}\Big) b_k.$$

Since B is a quasi basis for N, we conclude that f is an S-algebras homomorphism if and only if $\sum\limits_{s,t=1}^{n} p_{is}p_{jt}z_{stk} - \sum\limits_{l=1}^{n} w_{ijl}p_{lk} \in \operatorname{ann}_\ell(b_k)$ for all i, j, k. □

Corollary 2.3. *Let the notation and hypotheses be as in Lemma* 2.2*, and suppose that M and N are two free S-modules and $p_{ij} \in S$ for all $1 \leqslant i, j \leqslant n$. Then*

(1) *f is well-defined.*
(2) *f is an S-module homomorphism.*
(3) *f is one-to-one iff for each $s_1, s_2, \ldots, s_n \in S$ s.t. $\sum\limits_{i=1}^{n} s_i p_{ij} = 0$ for all j, we have $s_i = 0$ for all i.*
(4) *If*

$$M = \Big\langle a_1, \ldots, a_n;\ a_i a_j = \sum_{k=1}^{n} w_{ijk} a_k,\ i, j = 1, \ldots, n \Big\rangle,$$
$$N = \Big\langle b_1, \ldots, b_n;\ b_i b_j = \sum_{k=1}^{n} z_{ijk} b_k,\ i, j = 1, \ldots, n \Big\rangle$$

are S-algebras, then f is an S-algebra homomorphism iff for all i, j, k

$$\sum_{s,t=1}^{n} p_{is}p_{jt}w_{stk} - \sum_{l=1}^{n} z_{ijl}p_{lk} = 0.$$

P r o o f. Since A and B are bases for the free modules M and N, respectively, hence $\operatorname{ann}_\ell(a_i) = \operatorname{ann}_\ell(b_i) = 0$ for all $a_i \in A$ and $b_i \in B$. Thus, by Lemma 2.2 all the above assertions are correct. □

For a finite set X, we denote by $|X|$ the size of X.

Theorem 2.1. *Let S be a commutative ring with identity and let*

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

$$N = \left\langle b_1, \dots, b_n;\ b_i b_j = \sum_{k=1}^{n} z_{ijk} b_k,\ i, j = 1, \dots, n \right\rangle$$

be two finite S-algebras with $|M| = |N|$. Then $M \cong N$ as S-algebras iff there exist $p_{ij} \in S$ $(1 \leqslant i, j \leqslant n)$ such that

- ▷ $\operatorname{ann}_\ell(a_i) p_{ij} \subseteq \operatorname{ann}_\ell(b_j)$ *for all* $i, j = 1, \dots, n$,
- ▷ *for each* $s_1, s_2, \dots, s_n \in S$ *such that* $\sum_{i=1}^{n} s_i p_{ij} \in \operatorname{ann}_\ell(b_j)$ *for all* j, *we have* $s_i \in \operatorname{ann}_\ell(a_i)$ *for all* i,
- ▷ $\sum_{s,t=1}^{n} p_{is} p_{jt} w_{stk} - \sum_{l=1}^{n} z_{ijl} p_{lk} \in \operatorname{ann}_\ell(b_k)$ *for all* i, j, k.

P r o o f. Since M and N are finite S-algebras and $|M| = |N|$, a map $f\colon M \to N$ is one-to-one if and only it f is surjective. So, the assertions follow from Lemma 2.2. □

3. Structure and isomorphism theorems

In this section, we use the results of the previous section to state a structure theorem describing the structure of all finite rings over the same additive structure (Theorem 3.1). Moreover, we give an isomorphism theorem to test whether or not two such structures are isomorphic (Theorem 3.2).

Let us denote by R an associative ring (not necessarily commutative or with identity). It is clear that R is a $\mathbb{Z}$-algebra. Also, by Corollary 2.1, every finitely generated $\mathbb{Z}$-module has a quasi $\mathbb{Z}$-basis. So, if R is a finite ring then its additive group is a finite abelian group and is thus a direct sum of cyclic groups. Suppose that $a_1, a_2, \dots, a_n$ of orders $m_1, m_2, \dots, m_n$, respectively, form a set of generators for the abelian group of R. This implies that $A = \{a_1, a_2, \dots, a_n\}$ is a quasi $\mathbb{Z}$-basis for R and hence, its ring structure can be determined by n^2 products $a_i a_j = \sum_{k=1}^{n} w_{ijk} a_k$ with $w_{ijk} \in \mathbb{Z}_{m_k}$ and thus by n^3 constants w_{ijk}. Analogously to [7], we introduce a convenient notation, motivated by group theory, to state our structure theorem for finite rings. A *presentation* for a finite ring R consists of a set of generators $a_1, a_2, \dots, a_n$ for the additive group of R together with *relations*: The relations are of two types:

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

Therefore, if R is a finite ring with the above properties, to simplify the notation, we write

$$R = \Big\langle a_1, \dots, a_n;\ m_i a_i = 0,\ a_i a_j = \sum_{k=1}^{n} w_{ijk} a_k,\ i, j = 1, \dots, n \Big\rangle.$$

Theorem 3.1 (Structure theorem)**.** *Let n be a positive integer, and for each $i = 1, \dots, n$, let $A_i = \langle a_i \rangle$ be the cyclic subgroup of order m_i. Then there exists a ring R with additive group $\bigoplus_{i=1}^{n} A_i$ and multiplication relations $a_i a_j = \sum_{k=1}^{n} w_{ijk} a_k$ for each i, j and $w_{ijk} \in \mathbb{Z}$ if and only if (w_{ijk}) satisfies the following conditions:*

(1) $m_k \mid \lambda_{ij} w_{ijk}$ *where* $\lambda_{ij} = \gcd(m_i, m_j)$ *for all* $1 \leqslant i, j, k \leqslant n$,

(2) $\sum_{\alpha=1}^{n} w_{ij\alpha} w_{\alpha lk} \equiv \sum_{\alpha=1}^{n} w_{jl\alpha} w_{i\alpha k} \bmod m_k$ *for all* $1 \leqslant i, j, k, l \leqslant n$.

P r o o f. Suppose that there exists a ring R such that $a_i a_j = \sum_{k=1}^{n} w_{ijk} a_k$. We show that the conditions (1) and (2) hold for (w_{ijk}). By Corollary 2.1, $\{a_1, a_2, \dots, a_n\}$ is a quasi $\mathbb{Z}$-basis for $(R, +)$. Since for each i, $\operatorname{ann}_\ell(a_i) = m_i \mathbb{Z}$, by Lemma 2.1 we have $[m_i \mathbb{Z} + m_j \mathbb{Z}] w_{ijk} \subseteq m_k \mathbb{Z}$ for all i, j, k, and $\sum_{\alpha=1}^{n} (w_{ij\alpha} w_{\alpha lk} - w_{jl\alpha} w_{i\alpha k}) \in m_k \mathbb{Z}$. Hence it follows that

(1) $m_k \mid \lambda_{ij} w_{ijk}$, for all $1 \leqslant i, j, k \leqslant n$,

(2) $\sum_{\alpha=1}^{n} w_{ij\alpha} w_{\alpha lk} \equiv \sum_{\alpha=1}^{n} w_{jl\alpha} w_{i\alpha k} \bmod m_k$ for all $1 \leqslant i, j, k, l \leqslant n$.

The converse is obvious. □

Theorem 3.2 (Isomorphism theorem)**.** *Let*

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

$$R_2 = \Big\langle a_1, \dots, a_n;\ m_i a_i = 0, a_i a_j = \sum_{k=1}^{n} z_{ijk} a_k,\ i, j = 1, \dots, n \Big\rangle$$

be two presentations. Then $R_1 \cong R_2$ iff there exist $p_{jk} \in \{0, \dots, m_k - 1\}$ for $1 \leqslant j, k \leqslant n$ such that the following conditions hold:

(1) $m_k \mid m_j p_{jk}$ *for* $1 \leqslant j, k \leqslant n$,

(2) *for each* $s_1, \dots, s_n \in \mathbb{Z}$, *if* $m_k \mid \sum_{j=1}^{m} s_j p_{jk}$ *for all* $1 \leqslant k \leqslant n$, *then* $m_i \mid s_i$ *for all* i,

(3) $\sum_{\alpha,\beta=1}^{n} p_{i\alpha} p_{j\beta} w_{\alpha\beta k} \equiv \sum_{l=1}^{n} z_{ijl} p_{lk} \bmod m_k$ *for* $1 \leqslant k \leqslant n$.

P r o o f. By Corollary 2.1, $\{a_1, a_2, \ldots, a_n\}$ is a quasi $\mathbb{Z}$-basis for both R_1 and R_2. On the other hand, for each i, $\mathrm{ann}_\ell(a_i) = m_i\mathbb{Z}$. Thus by Lemma 2.2, $R_1 \cong R_2$ if and only if there exist $p_{jk} \in \mathbb{Z}$ such that

(1) $\mathrm{ann}_\ell(a_j)p_{jk} \subseteq \mathrm{ann}_\ell(a_k)$ for $1 \leqslant j, k \leqslant n$,

(2) for each $s_1, \ldots, s_n \in \mathbb{Z}$, $\sum\limits_{j=1}^{m} s_j p_{jk} \in \mathrm{ann}_\ell(a_k)$ for each k implies that $s_i \in \mathrm{ann}_\ell(a_i)$ for all i,

(3) $\sum\limits_{\alpha,\beta=1}^{n} p_{i\alpha}p_{j\beta}w_{\alpha\beta k} - \sum\limits_{l=1}^{m} z_{ijl}p_{lk} \in \mathrm{ann}_\ell(a_k)$ for $1 \leqslant k \leqslant n$.

These conditions are trivially equivalent to those given in the theorem. □

Now, we will present an application of these theorems to prove a classical result in the ring theory. It is well-known that every finite ring R can be uniquely (up to isomorphism) decomposed into a direct sum of rings of prime power order (see [12] for example). Below, we give a simple proof for this result (Proposition 3.1).

Lemma 3.1. *Let R be a finite ring with the additive group $\bigoplus\limits_{i=1}^{n} A_i$ where $A_i = \langle a_i \rangle$ for each i is a cyclic additive subgroup of R of order m_i. With no loss of generality, we can arrange the A_i's so that there exists $\varrho \in \{1, 2, \ldots, n\}$ with $\gcd(m_i, m_j) = 1$ for all $1 \leqslant i \leqslant \varrho$ and $\varrho < j \leqslant n$. Then $I = \bigoplus\limits_{i=1}^{\varrho} A_i$ and $J = \bigoplus\limits_{i=\varrho+1}^{n} A_i$ are ideals of R.*

P r o o f. Let $R = \left\langle a_1, \ldots, a_n;\ m_i a_i = 0, a_i a_j = \sum\limits_{k=1}^{n} w_{ijk}a_k,\ i, j = 1, \ldots, n \right\rangle$ be a presentation of R and $\lambda_{ij} = \gcd(m_i, m_j)$ for all i, j. Let i and j be two integers with $1 \leqslant i \leqslant \varrho$ and $\varrho < j \leqslant n$. By Theorem 3.1, we can conclude that $m_k \mid \lambda_{ij}w_{ijk}$ for all $1 \leqslant k \leqslant n$. Thus, for any k, we have $m_k \mid w_{ijk}$ and hence $w_{ijk}a_k = 0$. This implies that $a_i a_j = 0$ and so $IJ = 0$. Now, assume that $1 \leqslant i, j \leqslant \varrho$. From the hypothesis, for any $\varrho < k \leqslant n$, $\gcd(m_k, \lambda_{ij}) = 1$ and hence $m_k \mid w_{ijk}$. Thus $w_{ijk}a_k = 0$ and $a_i a_j \in I$. Therefore $I^2 \subseteq I$. Similarly, one can show that $J^2 = J$ and $JI = 0$. □

As a corollary of this lemma, the classification of finite rings quickly reduces to the study of rings whose additive groups are p-primary.

Proposition 3.1. *Every finite ring R can be uniquely (up to isomorphism) decomposed into a direct sum of rings of prime power order. Consequently, the order of any indecomposable finite ring is a power of a prime number.*

4. Description of the new algorithm

In this section, we show how to design an algorithm (based on Theorems 3.1 and 3.2) for computing the presentations of all finite rings (up to isomorphism) of a given order. At the end of this section, we present an example to show the performance of the algorithm for computing the presentations of all finite rings (up to isomorphism) of order 12.

Let R be a finite ring (not necessarily commutative or with identity) of order m. As we proved in the previous section, every finite ring can be decomposed into a direct sum of indecomposable rings (p-rings). Recall that a p-ring is a finite ring whose order is a power of a prime p, i.e., its additive structure is a p-primary abelian group. So, the decomposition of the additive structure $(R,+)$ of R into p-primary subgroups leads to the ring decomposition

$$R = R_1 \oplus \ldots \oplus R_n$$

where R_i is a finite ring of order $p_i^{k_i}$, $m = p_1^{k_1} \ldots p_n^{k_n}$ and the p_i's are not necessarily distinct. On the other hand, using Theorem 3.1, one can find the structure of all finite rings with the additive group $\mathbb{Z}_{p_1^{k_1}} \oplus \ldots \oplus \mathbb{Z}_{p_n^{k_n}}$. In order to establish a connection between this result and finding the presentation of all finite rings of a given order, it is helpful to introduce the following definition.

Definition 4.1. We call $[p_1^{k_1}, \ldots, p_n^{k_n}]$ a *prime decomposition* (p-decomposition) of a positive integer m if $m = p_1^{k_1} \ldots p_n^{k_n}$, $p_1^{k_1} \leqslant \ldots \leqslant p_n^{k_n}$ and the p_i's are (not necessarily distinct) prime numbers.

For example, $[3,4]$ and $[2,2,3]$ are all p-decompositions of 12. Thus, to find all the presentations of all finite rings of order m, we must first find all the p-decompositions of m. Then for each p-decomposition $[m_1, \ldots, m_n]$ we calculate all finite rings $R_1 \oplus \ldots \oplus R_n$ such that the order of R_i is m_i. Thus, it is enough to design an algorithm for computing all the presentations of all finite rings (up to isomorphism) corresponding to a given p-decomposition $[m_1, \ldots, m_n]$. It is worth noting that the additive group of all these rings is $\mathbb{Z}_{m_1} \oplus \ldots \oplus \mathbb{Z}_{m_n}$. In this direction, based on Theorem 3.1, we describe first Structure algorithm to compute the set of all presentations of all finite rings corresponding to a given p-decompositions $[m_1, \ldots, m_n]$.

Proposition 4.1. *The* Structure *algorithm terminates and outputs the set of all presentations of all finite rings corresponding to M.*

Proof. The termination of the algorithm is guaranteed by the termination of the **for**-loops. To prove its correctness, we observe that $\mathcal{A}$ contains all the presen-

Algorithm STRUCTURE

Input: $M = [m_1, \ldots, m_n]$ a p-decomposition

Output: $\mathcal{W}$, the set of all presentations of all finite rings corresponding to M

1: $N := \{1, \ldots, n\}$;
2: **for** $(i, j) \in N^2$ **do**
3: $\quad \lambda_{ij} := \gcd(m_i, m_j)$;
4: **end for**
5: let $\mathcal{A}$ be the set of all $W = (w_{ijk})_{i,j,k \in N}$ with the following property:
6: **for** $(i, j, k) \in N^3$ **do**
7: $\quad w_{ijk} \in \{(m_k / \gcd(m_k, \lambda_{ij}))l \bmod m_k;\ l = 0, \ldots, m_k - 1\}$
8: **end for**
9: $\mathcal{W} := \{\}$;
10: **for** $W = (w_{ijk})_{i,j,k \in N} \in \mathcal{A}$ **do**
11: $\quad$ **if** $\forall (i, j, k, l) \in N^4$ we have $\sum_{\alpha=1}^{n} w_{ij\alpha} w_{\alpha lk} \equiv \sum_{\alpha=1}^{n} w_{jl\alpha} w_{i\alpha k} \bmod m_k$ **then**
12: $\quad\quad \mathcal{W} := \mathcal{W} \cup \{W\}$;
13: $\quad$ **end if**
14: **end for**
15: **Return** $(\mathcal{W})$

tations satisfying only the first condition of Theorem 3.1. Indeed, by this condition, we must have $m_k \mid \lambda_{ij} w_{ijk}$. This implies that $\gcd(m_k, \lambda_{ij})$ must divide w_{ijk}. On the other hand, w_{ijk} is multiplied by a_k for all i, j. Thus, $0 \leqslant w_{ijk} \leqslant m_k - 1$, and it should belong to

$$\Big\{ \frac{m_k}{\gcd(m_k, \lambda_{ij})} l \bmod m_k;\ l = 0, \ldots, m_k - 1 \Big\}.$$

It follows that for each $(w_{ijk}) \in \mathcal{A}$ we have $m_k \mid \lambda_{ij} w_{ijk}$. Furthermore, by the last **for**-loop, we check if each element of $\mathcal{A}$ satisfies the second item of Theorem 3.1, then we add it to $\mathcal{W}$. Therefore, $\mathcal{W}$ contains all presentations of all finite rings of order M. □

Once the set of all finite rings corresponding to a given p-decomposition is computed (by STRUCTURE algorithm), then from this set we must remove any ring which is isomorphic to another one. For this purpose, based on Theorem 3.2, we propose ISOMORPHIC algorithm to test whether or not two given finite rings are isomorphic. The input of this algorithm are a p-decomposition M, two presentations W, Z and $\mathcal{P}$ where $\mathcal{P}$ is a set of the elements of the form $P = (p_{ij})$ where the p_{ij}'s satisfy the first and second conditions of Theorem 3.2 for a given p-decomposition M. It is worth

noting that $\mathcal{P}$ depends only on the given p-decomposition, and thus it is enough to compute it once in the main algorithm for a given p-decomposition.

Algorithm ISOMORPHIC

Input: $\begin{cases} M = [m_1, \ldots, m_n]\colon \text{ a } p\text{-decomposition} \\ W = (w_{ijk}), Z = (z_{ijk})\colon \text{ two presentations of two finite rings} \\ \mathcal{P}\colon \text{ a finite set of the elements } P = (p_{ij}) \end{cases}$

Output: true if two presentations W and Z are isomorphic, and false otherwise

1: $N := \{1, \ldots, n\}$;
2: **for** $P \in \mathcal{P}$ **do**
3: **if** $\forall (i,j,k) \in N^3$ we have $\sum_{\alpha,\beta=1}^{n} p_{i\alpha}p_{j\beta}w_{\alpha\beta k} \equiv \sum_{l=1}^{n} z_{ijl}p_{lk} \bmod m_k$ **then**
4: **Return** (true)
5: **else**
6: **Return** (false)
7: **end if**
8: **end for**

Proposition 4.2. *The* ISOMORPHIC *algorithm terminates and returns true if two presentations W and Z are isomorphic, and false otherwise.*

P r o o f. The termination of the algorithm follows immediately from the termination of the **for**-loops. We prove now its correctness. We note that each $P \in \mathcal{P}$ satisfies the first and second conditions of Theorem 3.2 for M. Therefore, it suffices to look for a $P \in \mathcal{P}$ such that the third condition of Theorem 3.2 is satisfied. On the other hand, by the structure of the algorithm, if it finds such a P, it returns true, and false otherwise. □

Finally, we present the main algorithm for computing all the presentations of all finite rings (up to isomorphism) corresponding to a given p-decomposition. Thus, one can use this algorithm to compute the presentations of all finite rings of a given order m. In doing so, we first compute the set of all p-decompositions of m. Then, for each p-decomposition M, we compute the set of all non-isomorphic finite rings corresponding to M, and the union of all these sets forms the set of the presentations of all finite rings (up to isomorphism) of order m.

Theorem 4.1. *The* CLASSIFICATION *algorithm terminates and computes the presentations of all finite rings (up to isomorphism) corresponding to M.*

P r o o f. The termination of the algorithm is trivial as all the **for**-loops in the algorithm terminate in finitely many steps. We deal now with its correctness. In

Algorithm CLASSIFICATION

Input: $M = [m_1, \ldots, m_n]$, a p-decomposition

Output: $\mathcal{R}$, the presentations of all non-isomorphic finite rings corresponding to M

```
N := {1, ..., n};
let A be the set of all P = (p_ij)_{i,j∈N} with the following property:
for (j, k) ∈ N^2 do
    p_jk ∈ {(m_k/ gcd(m_k, m_j))l mod m_k ; l = 0, ..., m_k − 1}
end for
P := {};
for P = (p_ij)_{i,j∈N} ∈ A do
    flag1 := true;
    for (s_1, ..., s_n) ∈ {1, ..., m_n}^n while flag1 do
        flag2 := true;
        for k ∈ {1, ..., n} while flag2 do
            if Σ_{j=1}^{n} s_j p_jk ≢ 0 mod m_k then
                flag2 := false;
            end if
        end for
        flag3 := true if m_i | s_i for all i, and false otherwise;
        if flag2 and not flag3 then
            flag1 := false;
        end if
    end for
    if flag1=true then
        P := P ∪ {P};
    end if
end for
W := STRUCTURE(M);
R := {the first element of W} (we remove this element from W);
for W ∈ W do
    flag := false;
    for R ∈ R while not flag do
        flag := ISOMORPHIC(M, W, R, P);
    end for
    if not flag then
        R := R ∪ {W};
    end if
end for
Return (R)
```

the first step of the algorithm, we compute the set $\mathcal{P}$ of all $P = (p_{ij})$ satisfying two first conditions of Theorem 3.2. In doing so, we first construct the set $\mathcal{A}$ containing all $P = (p_{ij})$ meeting the first condition of Theorem 3.2. Next, in the second **for**-loop, we verify the second condition of this theorem for each $P \in \mathcal{A}$. Note that we must check the relation $\sum_{j=1}^{n} s_j p_{jk} \not\equiv 0 \bmod m_k$ for all $s_j \in \mathbb{Z}$. On the other hand, the maximum order of the additive subgroups of the rings corresponding to the p-decomposition M is m_n. Thus, it is enough to check the required relation only for $s_j \in \{1, \ldots, m_n\}$. After constructing the set $\mathcal{P}$, we calculate the set $\mathcal{W}$ of all presentations of all finite rings corresponding to M, and we save one of them in $\mathcal{R}$; the output of the algorithm. Now, for each $W \in \mathcal{W}$, if it is not isomorphic to any element of $\mathcal{R}$ (see ISOMORPHIC algorithm) then we add it to $\mathcal{R}$. Therefore, at the end, $\mathcal{R}$ will be the set of all presentations of all finite rings (up to isomorphism) corresponding to M. □

In the next theorem, we discuss the arithmetic complexity of this algorithm.

Theorem 4.2. *Let $M = [m_1, \ldots, m_n]$ be a p-decomposition, and $m = m_n$. The arithmetic complexity of the* CLASSIFICATION *algorithm to compute the presentations of all finite rings (up to isomorphism) corresponding to M is $m^{O(n^3)}$.*

P r o o f. In the second **for**-loop in the algorithm, we have, in the worst case, m^{n^2} choices for $P \in \mathcal{A}$. On the other hand, for each P we may perform $m_n^n \times n$ operations. Since $n \leqslant m^n$ and $m_n = m$, the maximum number of operations that we carry out in this **for**-loop is of the order of $m^{O(n^2)}$. At the second step, we compute the set $\mathcal{W} = \text{STRUCTURE}(M)$. In doing so, we construct a set $\mathcal{A}$ with at most m^{n^3} elements and for each member of this set we do n^4 checks. Thus, at this stage, the arithmetic complexity is $m^{O(n^3)}$, and the size of $\mathcal{W}$ would be of this order. Finally, for each element of $\mathcal{W}$, we perform $|\mathcal{P}| \times |\mathcal{R}| \times n^3$ tests. However, $|\mathcal{R}| \leqslant |\mathcal{W}|$ and $|\mathcal{P}|$ is of the order of $m^{O(n^2)}$. This implies that the complexity of this step of the algorithm is $m^{O(n^3)}$, and this completes the proof. □

We have implemented CLASSIFICATION algorithm in `Maple` 12.[1] Finally, we end this section by giving an example where we compute all presentations of all finite rings (up to isomorphism) of order 12. It should be noted that, as far as our knowledge is concerned, there is no contribution dealing with algorithmic aspects of classifying finite rings. Thereby, we have not compared our results with other methods.

Example 4.1. In this example, we calculate the presentations of all finite rings (up to isomorphism) of order 12. Recall that $[3, 4]$ and $[2, 2, 3]$ are all p-decompositions

[1] The `Maple` codes of our program are available at `http://amirhashemi.iut.ac.ir/software.html`

of 12. The outputs of CLASSIFICATION algorithm for $[3,4]$ and $[2,2,3]$ are listed below, where each row is a sequence of the form $(w_{111}, w_{112}, \ldots, w_{11n}, w_{121}, \ldots, w_{nnn})$ showing a presentation corresponding to a finite ring.

(0 0 0 0 0 0 0 0)
(0 0 0 0 0 0 0 1)
(0 0 0 0 0 0 0 2)
(1 0 0 0 0 0 0 0)
(1 0 0 0 0 0 0 1)
(1 0 0 0 0 0 0 2)
(0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0)
(0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1)
(0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0)
(0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1)
(0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0)
(0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1)
(0 0 0 1 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0)
(0 0 0 1 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1)
(0 0 0 0 0 0 0 0 1 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0)
(0 0 0 0 0 0 0 0 1 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1)
(0 0 0 1 0 0 0 0 0 1 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0)
(0 0 0 1 0 0 0 0 0 1 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1)
(0 1 0 1 1 0 0 0 0 1 1 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0)
(0 1 0 1 1 0 0 0 0 1 1 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1)
(1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0)
(1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1)

For example, if we consider the second row, it is a presentation of a ring over the additive group $\mathbb{Z}_3 \oplus \mathbb{Z}_4$. If we denote the elements $(1,0)$ and $(0,1)$ of this ring by a_1 and a_2, respectively, then the structure of this ring is as follows: $a_1 \cdot a_1 = 0$, $a_1 \cdot a_2 = 0$, $a_2 \cdot a_1 = 0$ and $a_2 \cdot a_2 = a_2$. We can see that there are 22 finite rings of order 12. For more details on the classification of finite rings of some classical orders, we refer to the web site `http://home.wlu.edu/~dresdeng/smallrings/`.

Acknowledgment. The authors would like to thank Dr. M. Gholami for helpful conversations. Further, they would like to thank the anonymous referee for valuable comments on the submitted manuscript. The third author extends his appreciation to the IPM-Isfahan Branch for supporting this work.

References

[1] *C. J. Chikunji*: On a class of finite rings. Commun. Algebra *27* (1999), 5049–5081.
[2] *C. J. Chikunji*: On a class of rings of order p^5. Math. J. Okayama Univ. *45* (2003), 59–71.
[3] *B. Corbas, G. D. Williams*: Rings of order p^5 I: Nonlocal rings. J. Algebra *231* (2000), 677–690.
[4] *B. Corbas, G. D. Williams*: Rings of order p^5 II: Local rings. J. Algebra *231* (2000), 691–704.
[5] *J. B. Derr, G. F. Orr, P. S. Peck*: Noncommutative rings of order p^4. J. Pure Appl. Algebra *97* (1994), 109–116.
[6] *K. E. Eldridge*: Orders for finite noncommutative rings with unity. Am. Math. Mon. *75* (1968), 512–514.
[7] *B. Fine*: Classification of finite rings of order p^2. Math. Mag. *66* (1993), 248–252.
[8] *R. Gilmer, J. Mott*: Associative rings of order p^3. Proc. Japan Acad. *49* (1973), 795–799.
[9] *R. Lidl, J. Wiesenbauer*: Ring Theory and Applications. Foundations and Examples of Application in Coding Theory and in Genetics. Textbooks for Mathematics, Akademische Verlagsgesellschaft, Wiesbaden, 1980. (In German.)
[10] *R. Raghavendran*: A class of finite rings. Compos. Math. *22* (1970), 49–57.
[11] *R. Raghavendran*: Finite associative rings. Compos. Math. *21* (1969), 195–229.
[12] *K. Shoda*: Über die Einheitengruppe eines endlichen Ringes. Math. Ann. *102* (1929), 273–282. (In German.)
[13] *J. Wiesenbauer*: Über die endlichen Ringe mit gegebener additiver Gruppe. Monatsh. Math. *78* (1974), 164–173. (In German.)
[14] *R. S. Wilson*: On the structure of finite rings. Compos. Math. *26* (1973), 79–93.
[15] *R. S. Wilson*: On the structure of finite rings II. Pac. J. Math. *51* (1974), 317–325.
[16] *R. S. Wilson*: Representations of finite rings. Pac. J. Math. *53* (1974), 643–649.

Authors' addresses: Mahmood Behboodi, Department of Mathematical Sciences, Isfahan University of Technology, Isfahan, 84156-83111, Iran and School of Mathematics, Institute for Research in Fundamental Sciences (IPM), Tehran, 19395-5746, Iran, e-mail: `mbehbood@cc.iut.ac.ir`; Reza Beyranvand, Department of Mathematics, Lorestan University, Khorramabad, Iran, e-mail: `beyranvand.r@lu.ac.ir`; Amir Hashemi, Department of Mathematical Sciences, Isfahan University of Technology, Isfahan, 84156-83111, Iran and School of Mathematics, Institute for Research in Fundamental Sciences (IPM), Tehran, 19395-5746, Iran, e-mail: `amir.hashemi@cc.iut.ac.ir`; Hossein Khabazian, Department of Mathematical Sciences, Isfahan University of Technology, Isfahan, 84156-83111, Iran, e-mail: `khabaz@cc.iut.ac.ir`.