ЧЕБЫШЕВСКИЙ СБОРНИК
Том 20. Выпуск 3.

УДК 512.552.7+519.725 DOI 10.22405/2226-8383-2019-20-3-107-123

Структура конечной групповой алгебры одного полупрямого произведения абелевых групп и её приложения

К. В. Веденёв, В. М. Деундяк

Веденёв Кирилл Владимирович — Южный федеральный университет (г. Ростов-на-Дону).
e-mail: vedenev@sfedu.ru
Деундяк Владимир Михайлович — кандидат физико-математических наук, доцент, Южный федеральный университет, ФГАНУ НИИ «Спецвузавтоматика» (г. Ростов-на-Дону).
e-mail: vl.deundyak@gmail.com

Аннотация

В 1978 году Р. Мак-Элисом построена первая асимметричная кодовая криптосистема, основанная на применении помехоустойчивых кодов Гоппы, при этом эффективные атаки на секретный ключ этой криптосистемы до сих пор не найдены. К настоящему времени известно много криптосистем, основанных на теории помехоустойчивого кодирования. Одним из способов построения таких криптосистем является модификация криптосистемы Мак-Элиса с помощью замены кодов Гоппы на другие классы кодов. Однако, известно что криптографическая стойкость многих таких модификаций уступает стойкости классической криптосистемы Мак-Элиса.

В связи с развитием квантовых вычислений кодовые криптосистемы, наряду с криптосистемамми на решётках, рассматриваются как альтернатива теоретико-числовым. Поэтому актуальна задача поиска перспективных классов кодов, применимых в криптографии. Представляется, что для этого можно использовать некоммутативные групповые коды, т. е. левые идеалы в конечных некоммутативных групповых алгебрах.

Для исследования некоммутативных групповых кодов полезной является теорема Веддерберна, доказывающая существование изоморфизма групповой алгебры на прямую сумму матричных алгебр. Однако конкретный вид слагаемых и конструкция изоморфизма этой теоремой не определены, и поэтому для каждой группы стоит задача конструктивного описания разложения Веддерберна. Это разложение позволяет легко получить все левые идеалы групповой алгебры, т.е. групповые коды.

В работе рассматривается полупрямое произведение $Q_{m,n} = (\mathbb{Z}_m \times \mathbb{Z}_n) \leftthreetimes (\mathbb{Z}_2 \times \mathbb{Z}_2)$ абелевых групп и конечная групповая алгебра $\mathbb{F}_q Q_{m,n}$ этой группы. Для этой алгебры при условиях $n \mid q-1$ и НОД$(2mn, q) = 1$ построено разложение Веддербёрна. В случае поля чётной характеристики, когда эта групповая алгебра не является полупростой, также получена сходная структурная теорема. Описаны все неразложимые центральные идемпотенты этой групповой алгебры. Полученные результаты используются для алгебраического описания всех групповых кодов над $Q_{m,n}$.

Ключевые слова: групповая алгебра, полупрямое произведение, конечное поле, разложение Веддербёрна, левые идеалы, групповые коды.

Библиография: 21 названий.

Для цитирования:
К. В. Веденёв, В. М. Деундяк. Структура конечной групповой алгебры одного полупрямого произведения абелевых групп и её приложения // Чебышевский сборник. 2019. Т. 20, вып. 3, с. 107–123.

CHEBYSHEVSKII SBORNIK

Vol. 20. No. 3.

UDC 512.552.7+519.725 DOI 10.22405/2226-8383-2019-20-3-107-123

The structure of finite group algebra of a semidirect product of abelian groups and its applications

K. V. Vedenev, V. M. Deundyak

Vedenev Kirill Vladimirovich — Southern Federal University (Rostov-on-Don).
e-mail: vedenev@sfedu.ru

Deundyak Vladimir Mikhailovich — candidate of physical and mathematical Sciences, associate Professor, Southern Federal University, Research Institute "Specvuzavtomatika" (Rostov-on-Don).
e-mail: vl.deundyak@gmail.com

Abstract

In 1978 R. McEliece developed the first assymetric cryptosystem based on the use of Goppa's error–correctring codes and no effective key attacks has been described yet. Now there are many code–based cryptosystems known. One way to build them is to modify the McEliece cryptosystem by replacing Goppa's codes with other codes. But many variants of this modification were proven to be less secure.

In connection with the development of quantum computing code cryptosystems along with lattice-based cryptosystems are considered as an alternative to number-theoretical ones. Therefore, it is relevant to find promising classes of codes that are applicable in cryptography. It seems that for this non–commutative group codes, i.e. left ideals in finite non–commutative group algebras, could be used.

The Wedderburn theorem is useful to study non–commutative group codes. It implies the existence of an isomorphism of a semisimple group algebra onto a direct sum of matrix algebras. However, the specific form of the summands and the isomorphism construction are not explicitly defined by this theorem. Hence for each semisimple group algebra there is a task to explicitly construct its Wedderburn decomposition. This decomposition allows us to easily describe all left ideals of group algebra, i.e. group codes.

In this paper we consider one semidirect product $Q_{m,n} = (\mathbb{Z}_m \times \mathbb{Z}_n) \leftthreetimes (\mathbb{Z}_2 \times \mathbb{Z}_2)$ of abelian groups and the group algebra $\mathbb{F}_q Q_{m,n}$. In the case when $n \mid q-1$ and $\gcd(2mn, q) = 1$, the Wedderburn decomposition of this algebra is constructed. In the case when field is of characteristic 2, i.e. when this group algebra is not semisimple, a similar structure theorem is also obtained. Further in the paper, the primitive central idempotents of this group algebra are described. The obtained results are used to algebraically describe the group codes over $Q_{m,n}$.

Keywords: group algebra, semidirect product, finite field, Wedderburn decomposition, left ideals, group codes.

Bibliography: 21 titles.

For citation:
K. V. Vedenev, V. M. Deundyak, 2019, "The structure of finite group algebra of a semidirect product of abelian groups and its applications" , *Chebyshevskii sbornik*, vol. 20, no. 3, pp. 107–123.

Introduction

Let G be a finite group with the identity e, written multiplicatively, let R be a ring with the identity 1_R and $\mathbb{F}_q$ be a Galois field of order q. Recall, the group ring RG is a set of all formal linear combinations $\alpha = \sum_{g\in G} a_g g$, $a_g \in R$, equipped with operations of addition and (left and right) multiplication by elements of R defined componentwise and multiplication defined as follows:

$$\sum_{g\in G} \alpha_g g \sum_{g\in G} \beta_g g = \sum_{g\in G} \left(\sum_{h\in H} \alpha_{gh^{-1}} \beta_h \right) g.$$

(see [1]). In the case when R is commutative, RG is also called group algebra of G over R ([2], [1]). Note that, the correspondences $g \mapsto 1_R g$, $g \in G$, and $r \mapsto re$, $r \in R$, define natural embeddings of the group G and the ring R into RG.

Any left ideal $I \subset \mathbb{F}_q G$ is called a group code over G (see [3], [4]). This algebraic approach to codding theory was introduced by S.D. Berman [5]. In this approach, all elements of the field $\mathbb{F}_q$ are the encoding alphabet and the order of the group G is the length of codewords. Note that the dimension of a code $C \subset \mathbb{F}_q$ is its dimension as an $\mathbb{F}_q$-subspace in $\mathbb{F}_q G$. Many classical codes can be realized as (left) ideals in group algebras (see survey [3]), including Reed-Solomon codes ([4], [6]) and Reed–Muller codes ([4], [5], [7]). Algebraic approach to error–correcting codes gives some benefits, i.e. additional algebraic structure helps to study more efficient encoding and decoding algorithms for known codes (see for example [8]) and to discover new classes of codes in group algebras ([9], [10], [11]).

Another motivation to study codes in non–commutative group algebras is that this codes could be useful in cryptography. R. McEliece developed an asymmetric cryptosystem based on the use of binary Goppa codes in 1978 and no effective key attacks has been described yet. Code cryptosystems are considered as a potential replacement to number-theoretical ones in the connection with the development of quantum computing (see NIST-PQC competition [12]). The main disadvantage of the original McEliece cryptosystem is that the private and public keys are very large matrices. To reduce the key size there have been attempts to replace Goppa codes with other classes of error–correcting codes. Variants of the McEliece cryptosystem based on the use of well-known Reed–Solomon codes and Reed–Muller codes, which can be realized as two–sided ideals in some abelian group algebras, were proven to be less secure ([13], [14], [15]). So, non–commutative codes, which are one–sided (left) ideals in non–commutative group algebras, could be a good option to build new resistant and convenient in use cryptosystems.

The Wedderburn theorem implies that if $\mathbb{F}_q G$ is semisimple then $\mathbb{F}_q G$ is isomorphic to a direct sum of matrix algebras over some extensions of the field $\mathbb{F}_q$. This theorem is a very powerful tool to study the structure of non-commutative codes, but it gives no information about the summands and the isomorphism. So, for an arbitary group algebra $\mathbb{F}_q G$ there is a problem of constructing its Wedderburn decomposition. There are several results on how to construct the Wedderburn decomposition and central primitive idempotents known (see [16], [17]). In [18] the Wedderburn decomposition of finite dihedral group algebra was described and in [11] this decomposition was used to study the dihedral codes.

Let $m, n \in \mathbb{N}$ and let $Q_{m,n}$ be a group with the following presentation:

$$\langle a_1, a_2, b, c \mid a_1^m, a_2^n, b^2, c^2, a_1^c = a_1^{-1}, a_2^b = a_2^{-1}, a_1 a_2 = a_2 a_1, bc = cb, ba_1 = a_1 b, ca_2 = a_2 c \rangle, \qquad (1)$$

hereinafter $\hat{g}^g = g^{-1}\hat{g}g$. We will call $Q_{m,n}$ the (m, n)–bidihedral group. In this paper we consider the bidihedral group and its group algebra $\mathbb{F}_q Q_{m,n}$. Under certain conditions, we obtain its Wedderburn decomposition in the semisimple case. Also we prove the similar structure theorem in the non–semisimple case. Then we explicitly describe the primitive central idempotents of this algebra. Finally, the obtained results are applied to algebraic codding theory.

The paper is organized as follows. In section 1 we introduce some preliminaries about the bidihedral group $Q_{m,n}$, its group algebra and polynomials over finite fields. In section 2 we prove the general structure theorem for this group algebra and then we obtain the Wedderburn decomposition of $\mathbb{F}_q Q_{m,n}$. In section 3 we construct the inverse of isomorphisms described in the previous section and then explicitly describe primitive central idempotents. In section 4 we apply this results to codding theory, i.e. we obtain the explicit description of the group codes over $Q_{m,n}$.

1. Preliminaries

Let G be a group and $S \subset G$. Bellow, by $\langle S \rangle$ we denote the subgroup of G generated by S. Let D_{2n} be a dihedral of order $2n$, i.e. D_{2n} has the presentation (see [19], p. 6):

$$D_{2n} = \langle x, y \mid x^n, y^2, x^y = x^{-1} \rangle.$$

Consider the group $Q_{m,n}$ defined in (1). Hereinafter a_1, a_2, b, c are from (1).

Lemma 1. *Let $G_1 = \langle a_1, c \rangle$ and $G_2 = \langle a_2, b \rangle$. Then*
(i) $G_1 \simeq D_{2m}$ and $G_2 \simeq D_{2n}$
(ii) $Q_{m,n}$ decomposes into a direct product of G_1 and G_2.

Доказательство. We obviously have

$$G_1 = \langle a_1, c \mid a_1^m, c^2, a_1^c = a_1^{-1} \rangle, \quad G_2 = \langle a_2, b \mid a_2^n, b^2, a_2^b = a_2^{-1} \rangle$$

are presentations of G_1 and G_2. It follows that $G_1 \simeq D_{2m}$ and $G_2 \simeq D_{2n}$.

Since [19], p. 3, it follows that a direct product of G_1 and G_2 has a presentation of the form (1), hence $Q_{m,n}$ decomposes into a direct product of G_1 and G_2. □

From previous lemma we obtain the following result.

Lemma 2. *Let $N = \langle a_1, a_2 \rangle$ and $H = \langle b, c \rangle$; then*
(i) $N \simeq \mathbb{Z}_m \times \mathbb{Z}_n$ is normal;
(ii) $H \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$;
(iii) $Q_{m,n}$ is a semidirect product of N by H ($Q_{m,n} = N \leftthreetimes H$).

Let R be a ring (field); by $\mathbb{M}_n(R)$ we denote the ring (algebra) of $(n \times n)$–matrices over R.

Lemma 3. *The group $Q_{m,n}$ is isomorphic to the matrix group*

$$T_{m,n} := \left\{ \begin{pmatrix} \epsilon_1 & nz_1 & mz_2 \\ 0 & \epsilon_2 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in \mathbb{M}_3(\mathbb{Z}_{mn}) \;\middle|\; \epsilon_i = \pm 1, z_1, z_2 \in \mathbb{Z}_{mn} \right\}$$

Доказательство. Let

$$\hat{a}_1 = \begin{pmatrix} 1 & n & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \widehat{a}_2 = \begin{pmatrix} 1 & 0 & m \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \widehat{b} = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \widehat{c} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Observe that

$$\widehat{b}^t \widehat{c}^k \widehat{a}_1^i \widehat{a}_2^j = \begin{pmatrix} (-1)^t & (-1)^t ni & (-1)^t mj \\ 0 & (-1)^{k+t} & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

It follows that $\widehat{a}_1, \widehat{a}_2, \widehat{b}, \widehat{c}$ are the generators of $T_{m,n}$. It is easy to check that

$$\widehat{a}_1^m = \widehat{a}_2^n = \widehat{b}^2 = \widehat{c}^2 = \widehat{a}_1^0, \quad \widehat{a}_1^{\widehat{c}} = \widehat{a}_1^{-1}, \quad \widehat{a}_2^{\widehat{b}} = \widehat{a}_2^{-1},$$

$$\widehat{a}_1\widehat{a}_2 = \widehat{a}_2\widehat{a}_1, \quad \widehat{b}\widehat{c} = \widehat{c}\widehat{b}, \quad \widehat{b}\widehat{a}_1 = \widehat{a}_1\widehat{b}, \quad \widehat{c}\widehat{a}_2 = \widehat{a}_2\widehat{c}.$$

Hence we can define epimorphism (see [20], p. 15) $\varphi : Q_{m,n} \to T_{m,n}$ by the generators of $Q_{m,n}$:

$$\varphi : \quad a_1 \mapsto \widehat{a}_1, \quad a_2 \mapsto \widehat{a}_2, \quad b \mapsto \widehat{b}, \quad c \mapsto \widehat{c}.$$

Since $|Q_{m,n}| = 4mn$ and $|T_{mn}| = 4mn$, it follows that φ is an isomorphism. $\square$

Consider the group algebra $\mathbb{F}_q Q_{m,n}$. Any $u \in \mathbb{F}_q Q_{m,n}$ can be written as

$$u = P_0(a_1, a_2) + bP_1(a_1, a_2) + cP_2(a_1, a_2) + bcP_3(a_1, a_2), \tag{2}$$

where $P_k(x_1, x_2) \in \mathbb{F}_q[x_1, x_2]$ has degree in x_1 less than m and degree in x_2 less than n, i.e. $\deg_{x_1}(P_k) < m$, $\deg_{x_2}(P_k) < n$.

Throughout this paper we will assume that $\gcd(mn, q) = 1$ *and* $n \mid q - 1$.

Bellow we will use the following results on polynomials over finite fields. For every polynomial $g(x) \in \mathbb{F}_q[x]$ with $g(0) \neq 0$, $g^*(x)$ denotes its reciprocal polynomial, i.e., $g^*(x) = x^{\deg(g)} g(x^{-1})$. We say that a polinomial $g(x)$ is auto-reciprocal if $g(x)$ and $g^*(x)$ differ by a multiplicative constant.

Define

$$\xi(n) := \begin{cases} 1, & n \text{ is odd}, \\ 2, & n \text{ is even}. \end{cases}$$

The polynomials $x^m - 1 \in \mathbb{F}_q[x]$ and $x^n - 1 \in \mathbb{F}_q[x]$ split into monic irreducible factors as

$$x^m - 1 = (f_1 \dots f_{r_1})(f_{r_1+1} f_{r_1+1}^* f_{r_1+2} f_{r_1+2}^* \cdots f_{r_1+s_1} f_{r_1+s_1}^*), \tag{3}$$

$$x^n - 1 = (g_1 \dots g_{r_2})(g_{r_2+1} g_{r_2+1}^* g_{r_2+2} g_{r_2+2}^* \cdots g_{r_2+s_2} g_{r_2+s_2}^*), \tag{4}$$

where $f_1 = g_1 = x - 1$, $f_j^* = f_j$ for $1 < j \leq r_1$, $g_j^* = g_j$ for $1 < j \leq r_2$; and $f_2 = x + 1$ if m is even, $g_2 = x + 1$ if n is even. Here r_1, r_2 denote the numbers of auto-reciprocal factors in these factorizations and $2s_1, 2s_2$ denote the numbers of non-auto-reciprocal factors.

Since $\mathbb{F}_q^* \simeq \mathbb{Z}_{q-1}$ and $n \mid q-1$, it follows that there exist a multiplicative subgroup of $\mathbb{F}_q^*$ of order n, hence the factors in (4) are of degree 1. And since $x - 1$ and $x + 1$ are the only auto–reciprocal polynomials of degree 1, it follows that $r_2 = \xi(n)$ and $s_2 = \frac{n - \xi(n)}{2}$.

Let $h \in \mathbb{F}_q[x]$ be irreducible, $\deg(h) = k$ and let α be a root of h in an extension of $\mathbb{F}_q$. By $\mathbb{F}_q[\alpha]$ we denote the extension of $\mathbb{F}_q$ with α. It is well known that $\mathbb{F}_q[\alpha] = \mathbb{F}_q[\alpha^{-1}]$ and $\mathbb{F}_q[\alpha] \simeq F_{q^{\deg(h)}}$. Any element $t \in \mathbb{F}_q[\alpha]$ can be written as $v(\alpha)$ or $w(\alpha^{-1})$, $v, w \in \mathbb{F}_q[x]$ and $\deg(v) < k$, $\deg(u) < k$. Polynomials $v(x)$ and $w(x)$ are called polynomial representations of t with α and α^{-1}.

By α_i we denote a root of the polynomial f_j in an extension of $\mathbb{F}_q$ and by β_j we denote a root of the polynomial g_j.

2. The Wedderburn decomposition of $\mathbb{F}_q Q_{m,n}$

Bellow, by $\langle h \rangle_k$ we denote the cyclic group of order k with a generator h.

Let G be a group and R be a $\mathbb{F}_q$–algebra, then we can extend multiplication by the elements of $\mathbb{F}_q$ to RG. Note that, RG equipped with this operation is a $\mathbb{F}_q$–algebra.

For each $i \in \{1, \dots, r_1 + s_1\}$ and $j \in \{1, \dots, r_2 + s_2\}$ let $\nu_{i,j}$ be the $\mathbb{F}_q$–algebras homomorphism of $\mathbb{F}_q Q_{m,n}$ defined by the generators of $Q_{m,n}$ as follows:

1. $1 \le i \le \xi(m)$ and $1 \le j \le r_2$:

$$\nu_{i,j} : \mathbb{F}_q Q_{m,n} \to \mathbb{F}_q(\langle h_1\rangle_2 \times \langle h_2\rangle_2)$$

$$\nu_{i,j}(a_1) = \alpha_i, \quad \nu_{i,j}(a_2) = \beta_j, \quad \nu_{i,j}(b) = h_1, \quad \nu_{i,j}(c) = h_2.$$

2. $\xi(m) + 1 \le i \le r_1 + s_1$ and $1 \le j \le r_2$:

$$\nu_{i,j} : \mathbb{F}_q Q_{m,n} \to \mathbb{M}_2(\mathbb{F}_q[\alpha_i])\langle h\rangle_2$$

$$\nu_{i,j}(a_1) = \begin{pmatrix} \alpha_i & 0 \\ 0 & \alpha_i^{-1} \end{pmatrix}, \quad \nu_{i,j}(a_2) = \begin{pmatrix} \beta_j & 0 \\ 0 & \beta_j \end{pmatrix}, \quad \nu_{i,j}(b) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} h, \quad \nu_{i,j}(c) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

3. $1 \le i \le \xi(m)$ and $r_2 + 1 \le j \le r_2 + s_2$:

$$\nu_{i,j} : \mathbb{F}_q Q_{m,n} \to \mathbb{M}_2(\mathbb{F}_q)\langle h\rangle_2$$

$$\nu_{i,j}(a_1) = \begin{pmatrix} \alpha_i & 0 \\ 0 & \alpha_i \end{pmatrix}, \quad \nu_{i,j}(a_2) = \begin{pmatrix} \beta_j & 0 \\ 0 & \beta_j^{-1} \end{pmatrix}, \quad \nu_{i,j}(b) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \nu_{i,j}(c) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} h.$$

4. $\xi(m) + 1 \le i \le r_1 + s_1$ and $r_2 + 1 \le j \le r_2 + s_2$:

$$\nu_{i,j} : \mathbb{F}_q Q_{m,n} \to M_4(\mathbb{F}_q[\alpha_i])$$

$$\nu_{i,j}(a_1) = \begin{pmatrix} \alpha_i & 0 & 0 & 0 \\ 0 & \alpha_i & 0 & 0 \\ 0 & 0 & \alpha_i^{-1} & 0 \\ 0 & 0 & 0 & \alpha_i^{-1} \end{pmatrix}, \quad \nu_{i,j}(a_2) = \begin{pmatrix} \beta_j & 0 & 0 & 0 \\ 0 & \beta_j^{-1} & 0 & 0 \\ 0 & 0 & \beta_j & 0 \\ 0 & 0 & 0 & \beta_j^{-1} \end{pmatrix},$$

$$\nu_{i,j}(b) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad \nu_{i,j}(c) = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

For each $\xi(m) + 1 \le i \le r_1$ define

$$Z_i := \begin{pmatrix} 1 & -\alpha_i \\ 1 & -\alpha_i^{-1} \end{pmatrix}, \quad \hat{Z}_i := \begin{pmatrix} 1 & 0 & -\alpha_i & 0 \\ 0 & 1 & 0 & -\alpha_i \\ 1 & 0 & -\alpha_i^{-1} & 0 \\ 0 & 1 & 0 & -\alpha_i^{-1} \end{pmatrix}$$

and automorphisms

$$\sigma_i : \mathbb{M}_2(\mathbb{F}_q[\alpha_i])\langle h\rangle_2 \to \mathbb{M}_2(\mathbb{F}_q[\alpha_i])\langle h\rangle_2, \quad \sigma_i(X) = Z_i^{-1} X Z_i;$$

$$\hat{\sigma}_i : \mathbb{M}_4(\mathbb{F}_q[\alpha_i]) \to \mathbb{M}_4(\mathbb{F}_q[\alpha_i]), \quad \hat{\sigma}_i(X) = \hat{Z}_i^{-1} X \hat{Z}_i.$$

LEMMA 4. *(i) Let* $\xi(m) + 1 \le i \le r_1$ *and* $1 \le j \le r_2$*; then* $\operatorname{im}(\sigma_i \nu_{i,j}) \subset \mathbb{M}_2(\mathbb{F}_q[\alpha_i + \alpha_i^{-1}])\langle h\rangle_2$.
(ii) Let $\xi(m) + 1 \le i \le r_1$ *and* $r_2 + 1 \le j \le r_2 + s_2$*; then* $\operatorname{im}(\hat{\sigma}_i \nu_{i,j}) \subset \mathbb{M}_4(\mathbb{F}_q[\alpha_i + \alpha_i^{-1}])$.

Доказательство. In the case $\xi(m)+1 \le i \le r_1+s_1$ and $1 \le j \le r_2$ we have

$$(\sigma_i\nu_{i,j})(a_1) = \begin{pmatrix} 0 & 1 \\ -1 & \alpha_i+\alpha_i^{-1} \end{pmatrix}, \quad (\sigma_i\nu_{i,j})(a_2) = \begin{pmatrix} \beta_j & 0 \\ 0 & \beta_j \end{pmatrix}, \quad (\sigma_i\nu_{i,j})(b) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} h,$$

$$(\sigma_i\nu_{i,j})(c) = \begin{pmatrix} 1 & -(\alpha_i+\alpha_i^{-1}) \\ 0 & -1 \end{pmatrix}.$$

Hence $\mathrm{im}(\sigma_i\nu_{i,j}) \subset \mathbb{M}_2(\mathbb{F}_q[\alpha_i+\alpha_i^{-1}])\langle h\rangle_2$.

Similar computations shows that in the case $\xi(m)+1 \le i \le r_1+s_1$ and $r_2+1 \le j \le r_2+s_2$ we have $\mathrm{im}(\hat{\sigma}_i\nu_{i,j}) \subset \mathbb{M}_4(\mathbb{F}_q[\alpha_i+\alpha_i^{-1}])$. $\square$

Замечание 1. *Observe that if t is a root of the polynomial $g \in \mathbb{F}_q[x]$, then t^{-1} is a root of g^*. When $g \in \mathbb{F}_q[x]$ is auto-reciprocal and irreducible and $g(1) \neq 0$, $g(-1) \neq 0$, there exists a polynomial $h \in \mathbb{F}_q[x]$, such that $h(t+t^{-1}) = 0$ and $\deg(h) = \frac{\deg(g)}{2}$ (see [18], remark 3.2). It follows that*

$$\dim_{\mathbb{F}_q}(\mathbb{F}_q[t+t^{-1}]) = \frac{\deg(g)}{2}. \tag{5}$$

Finally, let us define the map

$$\rho := \bigoplus_{i=1}^{r_1+s_1} \bigoplus_{j=1}^{r_2+s_2} \rho_{i,j}, \quad \rho_{i,j} := \begin{cases} \sigma_j\nu_{i,j}, & (\xi(m)+1 \le i \le r_1) \wedge (1 \le j \le r_2) \\ \hat{\sigma}_j\nu_{i,j}, & (\xi(m)+1 \le i \le r_1) \wedge (r_2+1 \le j \le r_2+s_2) \\ \nu_{i,j}, & \textit{otherwise} \end{cases}. \tag{6}$$

Теорема 1. *Let $\gcd(mn,q)=1$ and $n \mid q-1$; then the map*

$$\rho : \mathbb{F}_qQ_{m,n} \to \bigoplus_{i=1}^{r_1+s_1} \bigoplus_{j=1}^{r_2+s_2} \mathcal{B}_{i,j},$$

$$\mathcal{B}_{i,j} = \begin{cases} \mathbb{F}_q(\langle h_1\rangle_2 \times \langle h_2\rangle_2), & (1 \le i \le \xi(m)) \wedge (1 \le j \le r_2) \\ \mathbb{M}_2(\mathbb{F}_q[\alpha_i+\alpha_i^{-1}])\langle h\rangle_2, & (\xi(m)+1 \le i \le r_1) \wedge (1 \le j \le r_2) \\ \mathbb{M}_2(\mathbb{F}_q[\alpha_i])\langle h\rangle_2, & (r_1+1 \le i \le r_1+s_1) \wedge (1 \le j \le r_2) \\ \mathbb{M}_2(\mathbb{F}_q)\langle h\rangle_2, & (1 \le i \le \xi(m)) \wedge (r_2+1 \le j \le r_2+s_2) \\ \mathbb{M}_4(\mathbb{F}_q[\alpha_i+\alpha_i^{-1}]), & (\xi(m)+1 \le i \le r_1) \wedge (r_2+1 \le j \le r_2+s_2) \\ \mathbb{M}_4(\mathbb{F}_q[\alpha_i]), & (r_1+1 \le i \le r_1+s_1) \wedge (r_2+1 \le j \le r_2+s_2) \end{cases}$$

is an isomorphism.

Доказательство. First we show that ρ is injective, i.e. if $\rho(u)=0$ then $u=0$.

Now let $u \in \mathbb{F}_qQ_{m,n}$ be of the form (2) then

1) in the case $(1 \le i \le \xi(m))$ and $(1 \le j \le r_2)$ we have

$$\nu_{i,j}(u) = P_0(\alpha_i,\beta_j) + P_1(\alpha_i,\beta_j)h_1 + P_2(\alpha_i,\beta_j)h_2 + P_3(\alpha_i,\beta_j)h_1h_2; \tag{7}$$

2) in the case $\xi(m)+1 \le i \le r_1+s_1$ and $1 \le j \le r_2$ we have

$$\nu_{i,j}(u) = \begin{pmatrix} P_0(\alpha_i,\beta_j) & P_2(\alpha_i^{-1},\beta_j) \\ P_2(\alpha_i,\beta_j) & P_0(\alpha_i^{-1},\beta_j) \end{pmatrix} + \begin{pmatrix} P_1(\alpha_i,\beta_j) & P_3(\alpha_i^{-1},\beta_j) \\ P_3(\alpha_i,\beta_j) & P_1(\alpha_i^{-1},\beta_j) \end{pmatrix} h; \tag{8}$$

3) in the case $1 \le i \le \xi(m)$ and $r_2+1 \le j \le r_2+s_2$ we have

$$\nu_{i,j}(u) = \begin{pmatrix} P_0(\alpha_i,\beta_j) & P_1(\alpha_i,\beta_j^{-1}) \\ P_1(\alpha_i,\beta_j) & P_0(\alpha_i,\beta_j^{-1}) \end{pmatrix} + \begin{pmatrix} P_2(\alpha_i,\beta_j) & P_3(\alpha_i,\beta_j^{-1}) \\ P_3(\alpha_i,\beta_j) & P_2(\alpha_i,\beta_j^{-1}) \end{pmatrix} h; \tag{9}$$

4) in the case $\xi(m)+1 \le i \le r_1+s_1$ and $r_2+1 \le j \le r_2+s_2$ we have

$$\nu_{i,j}(u) = \begin{pmatrix} P_0(\alpha_i,\beta_j) & P_1(\alpha_i,\beta_j^{-1}) & P_2(\alpha_i^{-1},\beta_j) & P_3(\alpha_i^{-1},\beta_j^{-1}) \\ P_1(\alpha_i,\beta_j) & P_0(\alpha_i,\beta_j^{-1}) & P_3(\alpha_i^{-1},\beta_j) & P_2(\alpha_i^{-1},\beta_j^{-1}) \\ P_2(\alpha_i,\beta_j) & P_3(\alpha_i,\beta_j^{-1}) & P_0(\alpha_i^{-1},\beta_j) & P_1(\alpha_i^{-1},\beta_j^{-1}) \\ P_3(\alpha_i,\beta_j) & P_2(\alpha_i,\beta_j^{-1}) & P_1(\alpha_i^{-1},\beta_j) & P_0(\alpha_i^{-1},\beta_j^{-1}) \end{pmatrix}. \tag{10}$$

Note that, since $\alpha_i \in \mathbb{F}_q[\alpha_i]$ and $\beta_j \in \mathbb{F}_q$, it follows that $P_k(\alpha_i,\beta_j^{\pm 1}), P_k(\alpha_i^{-1},\beta_j^{\pm 1}) \in \mathbb{F}_q[\alpha_i]$.

Since $\rho(u)=0$ we see that $\nu_{i,j}(u)=0$. It follows that

$$P_k(\alpha_i,\beta_j) = P_k(\alpha_i,\beta_j^{-1}) = P_i(\alpha_i^{-1},\beta_j) = P_i(\alpha_i^{-1},\beta_j^{-1}) = 0 \quad (k=0..3) \tag{11}$$

for all $1 \le i \le r_1+s_1$, $1 \le j \le r_2+s_2$. Since $\deg_{x_1} P_k(x_1,x_2) < m$ and $\deg_{x_2} P_k(x_1,x_2) < n$, it follows that

$$P_k(x_1,x_2) = \sum_{i=0}^{m-1}\sum_{j=0}^{n-1} c_{i,j}x_1^i x_2^j = \sum_{i=0}^{m-1} x_1^i \left(\sum_{j=0}^{n-1} c_{i,j}x_2^j\right) = \sum_{i=0}^{m-1} x_1^i P_{ki}(x_2), \quad \deg P_{ki}(x) < n.$$

Using (11) and (3), we obtain $P_k(x,\beta_j) \in \mathbb{F}_q[x]$ and $P_k(x,\beta_j^{-1}) \in \mathbb{F}_q[x]$ are divisible by the polynomial x^m-1 for all $j \in \{1,\dots,r_2+s_2\}$. Since $\deg_{x_1} P_k(x_1,x_2) < m$, we conclude that $P_k(x,\beta_j)$ and $P_k(x,\beta_j^{-1})$ are null polynomials, hence

$$P_{ki}(\beta_j) = P_{ki}(\beta_j^{-1}) = 0.$$

It follows that polynomials $P_{ki}(x)$ are divisible by x^n-1 and we immediately conclude that $P_{ki}(x)$ are also null polynomials. Therefore, we have $P_k(x_1,x_2) \equiv 0$. Injectivity is proved.

Finally, it remains to show that

$$\dim_{\mathbb{F}_q} \mathbb{F}_q Q_{m,n} = \dim_{\mathbb{F}_q} \left(\bigoplus_{i=1}^{r_1+s_1} \bigoplus_{j=1}^{r_2+s_2} \mathcal{B}_{i,j} \right).$$

Using (5), we obtain $\dim_{\mathbb{F}_q}\left(\bigoplus_{i=1}^{r_1+s_1}\bigoplus_{j=1}^{r_2+s_2}\mathcal{B}_{i,j}\right) =$

$$= r_2\left(4\xi(m) + 2\sum_{i=\xi(m)+1}^{r_1} \dim_{\mathbb{F}_q}\left(\mathbb{M}_2(\mathbb{F}_q[\alpha_i+\alpha_i^{-1}])\right) + 2\sum_{i=r_1+1}^{r_1+s_1} \dim_{\mathbb{F}_q}\left(\mathbb{M}_2(\mathbb{F}_q[\alpha_i])\right)\right) +$$

$$+s_2\left(2\xi(m)\dim_{\mathbb{F}_q}\mathbb{M}_2(\mathbb{F}_q) + \sum_{i=r_1+1}^{r_1+s_1} \dim_{\mathbb{F}_q}\left(\mathbb{M}_4(\mathbb{F}_q[\alpha_i+\alpha_i^{-1}]\right) + \sum_{i=r_1+1}^{r_1+s_1} \dim_{\mathbb{F}_q}\left(\mathbb{M}_4(\mathbb{F}_q[\alpha_i])\right)\right) =$$

$$= (n-2s_2)\left(4\xi(m) + 4\sum_{i=\xi(m)+1}^{r_1} \deg f_j + 8\sum_{i=r_1+1}^{r_1+s_1} \deg f_j\right) +$$

$$+s_2\left(8\xi(m) + 8\sum_{i=\xi(m)+1}^{r_1} \deg f_j + 16\sum_{i=r_1+1}^{r_1+s_1} \deg f_j\right) = 4(n-2s_2)m + 8s_2m = 4mn =$$

$$= \dim_{\mathbb{F}_q} \mathbb{F}_q Q_{m,n}.$$

Hence ρ is an isomorphism. □

LEMMA 5. *Let R be an algebra with identity 1_R and $(1_R + 1_R)$ has an inverse element in R; then $R\langle h\rangle_2 \simeq R \oplus R$ and $R(\langle h_1\rangle_2 \times \langle h_2\rangle_2) \simeq R \oplus R \oplus R \oplus R$.*

ДОКАЗАТЕЛЬСТВО. Indeed, the map $\varphi : R\langle h\rangle_2 \to R \oplus R$ such that

$$\varphi(r_1 + r_2 h) = (r_1 + r_2, r_1 - r_2)$$

is an isomorphism and

$$\varphi^{-1}(r_1, r_2) = \frac{r_1 + r_2}{(1_R + 1_R)} + \frac{r_1 - r_2}{(1_R + 1_R)} h.$$

Since $R(\langle h_1\rangle_2 \times \langle h_2\rangle_2) \simeq (R\langle h_1\rangle_2)\langle h_2\rangle_2$ it follows that

$$R(\langle h_1\rangle_2 \times \langle h_2\rangle_2) \simeq R\langle h\rangle_2 \oplus R\langle h\rangle_2 \simeq R \oplus R \oplus R \oplus R.$$

□

Now we can establish the Wedderburn decomposition of $\mathbb{F}_q Q_{m,n}$ in the case $\gcd(2mn, q) = 1$ and $n \mid q - 1$.

ТЕОРЕМА 2. *Let* $\gcd(2mn, q) = 1$ *and* $n \mid q-1$*; then* $\mathbb{F}_q Q_{m,n}$ *has the Wedderburn decomposition of the form:*

$$d : \mathbb{F}_q Q_{m,n} \to \bigoplus_{i=1}^{r_1+s_1} \bigoplus_{j=1}^{r_2+s_2} \mathcal{A}_{i,j}, \tag{12}$$

$$\mathcal{A}_{i,j} = \begin{cases} \mathbb{F}_q \oplus \mathbb{F}_q \oplus \mathbb{F}_q \oplus \mathbb{F}_q, & (1 \le i \le \xi(m)) \wedge (1 \le j \le r_2) \\ \mathbb{M}_2(\mathbb{F}_q[\alpha_i + \alpha_i^{-1}]) \oplus \mathbb{M}_2(\mathbb{F}_q[\alpha_i + \alpha_i^{-1}]), & (\xi(m) + 1 \le i \le r_1) \wedge (1 \le j \le r_2) \\ \mathbb{M}_2(\mathbb{F}_q[\alpha_i]) \oplus \mathbb{M}_2(\mathbb{F}_q[\alpha_i]), & (r_1 + 1 \le i \le r_1 + s_1) \wedge (1 \le j \le r_2) \\ \mathbb{M}_2(\mathbb{F}_q) \oplus \mathbb{M}_2(\mathbb{F}_q), & (1 \le i \le \xi(m)) \wedge (r_2 + 1 \le j \le r_2 + s_2) \\ \mathbb{M}_4(\mathbb{F}_q[\alpha_i + \alpha_i^{-1}]), & (\xi(m) + 1 \le i \le r_1) \wedge (r_2 + 1 \le j \le r_2 + s_2) \\ \mathbb{M}_4(\mathbb{F}_q[\alpha_i]), & (r_1 + 1 \le i \le r_1 + s_1) \wedge (r_2 + 1 \le j \le r_2 + s_2) \end{cases}$$

ДОКАЗАТЕЛЬСТВО. Let us define the maps $\tau_{i,j}$

1. for $1 \le i \le \xi(m)$ and $1 \le j \le r_2$:

$$\tau_{i,j} : \mathbb{F}_q(\langle h_1\rangle_2 \times \langle h_2\rangle_2) \to \mathbb{F}_q^4$$

$$\tau_{i,j}(X_0 + X_1 h_1 + X_2 h_2 + X_3 h_1 h_2) = \begin{array}{l} (P_0 + P_1 + P_2 + P_3,\ P_0 + P_1 - P_2 - P_3, \\ P_0 - P_1 + P_2 - P_3,\ P_0 - P_1 - P_2 + P_3); \end{array}$$

2. for $\xi(m) + 1 \le i \le r_1$ and $1 \le j \le r_2$:

$$\tau_{i,j} : M_2(\mathbb{F}_q[\alpha_i + \alpha_i^{-1}])\langle h\rangle_2 \to M_2(\mathbb{F}_q[\alpha_i + \alpha_i^{-1}]) \oplus M_2(\mathbb{F}_q[\alpha_i + \alpha_i^{-1}]),$$

$$\tau_{i,j}(X_0 + X_1 h) = (X_0 + X_1, X_0 - X_1);$$

3. for $r_1 + 1 \le i \le r_1 + s_1$ and $1 \le j \le r_2$:

$$\tau_{i,j} : M_2(\mathbb{F}_q[\alpha_i])\langle h\rangle_2 \to M_2(\mathbb{F}_q[\alpha_i]) \oplus M_2(\mathbb{F}_q[\alpha_i]), \quad \tau_{i,j}(X_0 + X_1 h) = (X_0 + X_1, X_0 - X_1);$$

4. for $1 \le i \le \xi(m)$ and $r_2 + 1 \le j \le r_2 + s_2$

$$\tau_{i,j} : M_2(\mathbb{F}_q)\langle h\rangle_2 \to M_2(\mathbb{F}_q) \oplus M_2(\mathbb{F}_q), \quad \tau_{i,j}(X_0 + X_1 h) = (X_0 + X_1, X_0 - X_1);$$

Using lemma 5 we conclude that $\tau_{i,j}$ are $\mathbb{F}_q$–algebras isomorphisms. Now let

$$d = \bigoplus_{i=1}^{r_1+s_1} \bigoplus_{j=1}^{r_2+s_2} d_{i,j}, \quad d_{i,j} := \begin{cases} \tau_{i,j}\nu_{i,j}, & (1 \le i \le \xi(m)) \wedge (1 \le j \le r_2) \\ \tau_{i,j}\sigma_i\nu_{i,j}, & (\xi(m)+1 \le i \le r_1) \wedge (1 \le j \le r_2) \\ \tau_{i,j}\nu_{i,j}, & (r_1+1 \le i \le r_1+s_1) \wedge (1 \le j \le r_2) \\ \tau_{i,j}\nu_{i,j}, & (1 \le i \le \xi(m)) \wedge (r_2+1 \le j \le r_2+s_2) \\ \widehat{\sigma}_i\nu_{i,j}, & (\xi(m)+1 \le i \le r_1) \wedge (r_2+1 \le j \le r_2+s_2) \\ \nu_{i,j}, & (r_1+1 \le i \le r_1+s_1) \wedge (r_2+1 \le j \le r_2+s_2) \end{cases}$$

Therefore, using theorem 1 we see that d is an isomorphism. □

Замечание 2. *Since $Q_{m,n} \simeq Q_{n,m}$, we can also use these theorems in the case $n \nmid q-1$ but $m \mid q-1$.*

3. Primitive central idempotents of $\mathbb{F}_q Q_{m,n}$

Let R be a ring. Recall, $i \in R$ is an idempotent if $i^2 = i$. Two idempotents $i_1, i_2 \in R$ are called orthogonal if $i_1 i_2 = i_2 i_1 = 0$. An idempotent i is called central if $ri = ir$ for all $r \in R$. An (central) idempotent i is said to be primitive (central) idempotent if i cannot be written as $i = i' + i''$ where i' and i'' are such (central) idempotents that $i', i'' \neq 0$ and $i'i'' = 0$.

In this section, firstly, we consider the set of idempotents of cyclic group algebra. This set allows us to explicitly construct ρ^{-1} and d^{-1}, where isomorphisms ρ and d are defined in the section 3. Then we use d^{-1} to describe the primitive central idempotents of $\mathbb{F}Q_{m,n}$ in the case $\gcd(2mn, q) = 1$, $n \mid q-1$. Note that the maps ρ^{-1} and d^{-1} could also be useful to study the algebraic structure of group codes over $Q_{m,n}$.

Let $\gcd(k, q) = 1$. Let $\mathcal{R}_k := \mathbb{F}_q[x]/(x^k - 1)$, where $(x^k - 1)$ denotes the principal ideal of $F_q[x]$ generated by $x^k - 1$. It is known (see [18], lemma 2.1) that for monic polynomial $g(x) \mid x^k - 1$ an element

$$e_g^k(x) := -\frac{[(g(x)^*)']^*}{k} \cdot \frac{x^k - 1}{g(x)}, \tag{13}$$

is the principal idempotent of the ideal $\mathcal{R}_k \lceil \frac{x^k-1}{g(x)} \rceil$, where $\lceil g(x) \rceil \in \mathcal{R}_k$ is the equivalence class of $g(x)$.

Lemma 6. *Let $g(x)$ be a monic irreducible divisor of $x^k - 1$ and α be a root of g; then*
(i) $e_g^k(\alpha) = 1$;
(ii) $e_g^k(\beta) = 0$ for any root β of the polynomial $\frac{x^k-1}{g(x)}$.

Доказательство. The definition (13) yields *(ii)*. The Chinese reminder theorem implies that the map

$$\varphi : \mathcal{R}_k \to \frac{\mathbb{F}_q[x]}{(g(x))} \oplus \frac{\mathbb{F}_q[x]}{((x^k-1)/g(x))}, \quad P(x) \mapsto \left(P(x) \bmod g(x), P(x) \bmod \frac{x^k-1}{g(x)} \right)$$

is an isomorphism. Since $e_g^k(x)$ is an idempotent and $\frac{\mathbb{F}_q[x]}{(g(x))}$ is a field, it follows that

$$e_g^k(x) \bmod g(x) = 1.$$

Hence $e_g^k(\alpha) = 1$. □ It is well known that $\mathbb{F}_q\langle h \rangle_k \simeq \mathcal{R}_k$, hence for any $g(x) \mid (x^k - 1)$ we have $e_g^k(h) \in \mathbb{F}_q\langle h \rangle_k$ is an idempotent.

Let S be a set. By id_S we denote the identity map on S.

LEMMA 7. *Let* $\gcd(q, mn) = 1$, $1 \le i \le \xi(m)$ *and* $1 \le j \le r_2$. *Let*

$$\mu_{i,j} : \mathbb{F}_q(\langle h_1\rangle_2 \times \langle h_2\rangle_2) \to \mathbb{F}_q Q_{m,n}$$

be a map defined by

$$\mu_{i,j}(p_0 + p_1h_1 + p_2h_2 + p_3h_1h_2) := (p_0 + p_1b + p_2c + p_3bc)\, e^m_{f_i}(a_1)e^n_{g_j}(a_2).$$

Then $\nu_{i,j}\mu_{i,j} = \mathrm{id}_{\mathrm{im}(\nu_{i,j})}$ *and* $\nu_{i'j'}\mu_{i,j} = 0$ *if* $i' \ne i$ *or* $j' \ne j$.

Доказательство. Lemma 6 implies that $\nu_{i'j'}\mu_{i,j} = 0$ if $i' \ne i$ or $j' \ne j$. We have

$$\nu_{i,j}\left((p_0 + p_1b + p_2c + p_3bc)\, e^m_{f_i}(a_1)e^n_{g_j}(a_2)\right) = p_0 + p_1h_1 + p_2h_2 + p_3h_3.$$

Hence $\nu_{i,j}\mu_{i,j} = \mathrm{id}_{\mathrm{im}(\nu_{i,j})}$. □

Lemmas 8–12 are proved in the same way. Recall, the maps $\nu_{i,j}$ are $\mathbb{F}_q$–algebras homomorphism and their images in fact were described in (7)—(10).

LEMMA 8. *Let* $\xi(m) + 1 \le i \le r_1$ *and* $1 \le j \le r_2$. *Let*

$$\mu_{i,j} : \mathrm{im}(\nu_{i,j}) \to \mathbb{F}_q Q_{m,n},$$

$$\mu_{i,j} : \begin{pmatrix} p_0(\alpha_i) & p_1(\alpha_i^{-1}) \\ p_1(\alpha_i) & p_0(\alpha_i^{-1}) \end{pmatrix} + \begin{pmatrix} p_2(\alpha_i) & p_3(\alpha_i^{-1}) \\ p_3(\alpha_i) & p_2(\alpha_i^{-1}) \end{pmatrix} h \mapsto \Big[p_0(a_1) + bp_2(a_1) + cp_1(a_1) + bcp_3(a_1)\Big] e^m_{f_i}(a_1)e^n_{g_j}(a_2).$$

Then $\nu_{i,j}\mu_{i,j} = \mathrm{id}_{\mathrm{im}(\nu_{i,j})}$ *and* $\nu_{i'j'}\mu_{i,j} = 0$ *if* $i' \ne i$ *or* $j' \ne j$.

LEMMA 9. *Let* $r_1 + 1 \le i \le r_1 + s_1$ *and* $1 \le j \le r_2$. *Let*

$$\mu_{i,j} : \mathrm{im}(\nu_{i,j}) \to \mathbb{F}_q Q_{m,n},$$

$$\mu_{i,j} : \begin{pmatrix} p_0(\alpha_i) & p_2(\alpha_i^{-1}) \\ p_1(\alpha_i) & p_3(\alpha_i^{-1}) \end{pmatrix} + \begin{pmatrix} p_4(\alpha_i) & p_6(\alpha_i^{-1}) \\ p_5(\alpha_i) & p_7(\alpha_i^{-1}) \end{pmatrix} h \mapsto \Big[p_0(a_1) + bp_4(a_1) + cp_1(a_1) + bcp_5(a_1)\Big] e^m_{f_i}(a_1)e^n_{g_j}(a_2) + \Big[p_2(a_1) + bp_6(a_1) + cp_3(a_1) + bcp_7(a_1)\Big] e^m_{f^*_i}(a_1)e^n_{g_j}(a_2).$$

Then $\nu_{i,j}\mu_{i,j} = \mathrm{id}_{\mathrm{im}(\nu_{i,j})}$ *and* $\nu_{i'j'}\mu_{i,j} = 0$ *if* $i' \ne i$ *or* $j' \ne j$.

LEMMA 10. *Let* $1 \le i \le \xi(m)$ *and* $r_2 + 1 \le j \le r_2 + s_2$. *Let*

$$\mu_{i,j} : \mathrm{im}(\nu_{i,j}) \to \mathbb{F}_q Q_{m,n},$$

$$\mu_{i,j} : \begin{pmatrix} p_0 & p_2 \\ p_1 & p_3 \end{pmatrix} + \begin{pmatrix} p_4 & p_6 \\ p_5 & p_7 \end{pmatrix} h \mapsto \Big[p_0 + bp_1 + cp_4 + bcp_5\Big] e^m_{f_i}(a_1)e^n_{g_j}(a_2) + \Big[p_2 + bp_3 + cp_6 + bcp_7\Big] e^m_{f_i}(a_1)e^n_{g^*_j}(a_2).$$

Then $\nu_{i,j}\mu_{i,j} = \mathrm{id}_{\mathrm{im}(\nu_{i,j})}$ *and* $\nu_{i'j'}\mu_{i,j} = 0$ *if* $i' \ne i$ *or* $j' \ne j$.

LEMMA 11. *Let* $\xi(m)+1 \le i \le r_1$ *and* $r_2+1 \le j \le r_2+s_2$. *Let*

$$\mu_{i,j} : \operatorname{im}(\nu_{i,j}) \to \mathbb{F}_q Q_{m,n},$$

$$\mu_{i,j} : \begin{pmatrix} p_0(\alpha_i) & p_4(\alpha_i) & p_2(\alpha_i^{-1}) & p_6(\alpha_i^{-1}) \\ p_1(\alpha_i) & p_5(\alpha_i) & p_3(\alpha_i^{-1}) & p_7(\alpha_i^{-1}) \\ p_2(\alpha_i) & p_6(\alpha_i) & p_0(\alpha_i^{-1}) & p_4(\alpha_i^{-1}) \\ p_3(\alpha_i) & p_7(\alpha_i) & p_1(\alpha_i^{-1}) & p_5(\alpha_i^{-1}) \end{pmatrix} \mapsto$$

$$\mapsto \Big[p_0(a_1)+bp_1(a_1)+cp_2(a_1)+bcp_3(a_1)\Big] e_{f_i}^m(a_1) e_{g_j}^n(a_2) +$$

$$+\Big[p_5(a_1)+bp_4(a_1)+cp_7(a_1)+bcp_6(a_1)\Big] e_{f_i}^m(a_1) e_{g_j^*}^n(a_2).$$

Then $\nu_{i,j}\mu_{i,j} = \mathrm{id}_{\operatorname{im}(\nu_{i,j})}$ *and* $\nu_{i'j'}\mu_{i,j} = 0$ *if* $i' \ne i$ *or* $j' \ne j$.

LEMMA 12. *Let* $r_1+1 \le i \le r_1+s_1$ *and* $r_2+1 \le j \le r_2+s_2$. *Let*

$$\mu_{i,j} : \operatorname{im}(\nu_{i,j}) \to \mathbb{F}_q Q_{m,n},$$

$$\mu_{i,j} : \begin{pmatrix} p_0(\alpha_i) & p_4(\alpha_i) & p_8(\alpha_i^{-1}) & p_{12}(\alpha_i^{-1}) \\ p_1(\alpha_i) & p_5(\alpha_i) & p_9(\alpha_i^{-1}) & p_{13}(\alpha_i^{-1}) \\ p_2(\alpha_i) & p_6(\alpha_i) & p_{10}(\alpha_i^{-1}) & p_{14}(\alpha_i^{-1}) \\ p_3(\alpha_i) & p_7(\alpha_i) & p_{11}(\alpha_i^{-1}) & p_{15}(\alpha_i^{-1}) \end{pmatrix} \mapsto$$

$$\mapsto \Big[p_0(a_1)+bp_1(a_1)+cp_2(a_1)+bcp_3(a_1)\Big] e_{f_i}^m(a_1) e_{g_j}^n(a_2) +$$

$$+\Big[p_5(a_1)+bp_4(a_1)+cp_7(a_1)+bcp_6(a_1)\Big] e_{f_i}^m(a_1) e_{g_j^*}^n(a_2) +$$

$$+\Big[p_{10}(a_1)+bp_{11}(a_1)+cp_8(a_1)+p_9(a_1)\Big] e_{f_i^*}^m(a_1) e_{g_j}^n(a_2) +$$

$$+\Big[p_{15}(a_1)+bp_{14}(a_1)+cp_{13}(a_1)+bcp_{12}(a_1)\Big] e_{f_i^*}^m(a_1) e_{g_j^*}^n(a_2).$$

Then $\nu_{i,j}\tau_{i,j} = \mathrm{id}_{\operatorname{im}(\nu_{i,j})}$ *and* $\nu_{i'j'}\mu_{i,j} = 0$ *if* $i' \ne i$ *or* $j' \ne j$.

In the following theorem by the use of these lemmas we describe ρ^{-1} and d^{-1}.

TEOPEMA 3. *(i) Let* $\gcd(mn,q)=1$ *and let*

$$\bar\rho := \sum_{i=1}^{r_1+s_1}\sum_{j=1}^{r_2+s_2} \bar\rho_{i,j} : \quad \bigoplus_{i=1}^{r_1+s_1}\bigoplus_{j=1}^{r_2+s_2} \mathcal{B}_{i,j} \to \mathbb{F}_q Q_{m,n}$$

$$\bar\rho_{i,j} := \begin{cases} \mu_{i,j}\sigma_j^{-1}, & (\xi(m)+1 \le i \le r_1) \wedge (1 \le j \le r_2) \\ \mu_{i,j}\hat\sigma_j^{-1}, & (\xi(m)+1 \le i \le r_1) \wedge (r_2+1 \le j \le r_2+s_2) \\ \mu_{i,j}, & \textit{otherwise} \end{cases}.$$

Then $\rho^{-1} = \bar\rho$.

(ii) Let $\gcd(2mn,q)=1$ *and let*

$$\bar d = \sum_{i=1}^{r_1+s_1}\sum_{j=1}^{r_2+s_2} \bar d_{i,j} : \quad \bigoplus_{i=1}^{r_1+s_1}\bigoplus_{j=1}^{r_2+s_2} \mathcal{A}_{i,j} \to \mathbb{F}_q Q_{m,n}$$

$$\bar{d}_{i,j} := \begin{cases} \mu_{i,j}\tau_{i,j}^{-1}, & (1 \le i \le \xi(m)) \wedge (1 \le j \le r_2) \\ \mu_{i,j}\sigma_i^{-1}\tau_{i,j}^{-1}, & (\xi(m)+1 \le i \le r_1) \wedge (1 \le j \le r_2) \\ \mu_{i,j}\tau_{i,j}^{-1}, & (r_1+1 \le i \le r_1+s_1) \wedge (1 \le j \le r_2) \\ \mu_{i,j}\tau_{i,j}^{-1}, & (1 \le i \le \xi(m)) \wedge (r_2+1 \le j \le r_2+s_2) \\ \mu_{i,j}\widehat{\sigma}_i^{-1}, & (\xi(m)+1 \le i \le r_1) \wedge (r_2+1 \le j \le r_2+s_2) \\ \mu_{i,j}, & (r_1+1 \le i \le r_1+s_1) \wedge (r_2+1 \le j \le r_2+s_2) \end{cases}$$

Then $d^{-1} = \bar{d}$.

Доказательство. Since ρ is of the form (6), directly computing from lemmas 8–12 we obtain

$$\rho\bar{\rho} = \bigoplus_{i=1}^{r_1+s_1} \bigoplus_{j=1}^{r_2+s_2} \sum_{i'=1}^{r_1+s_1} \sum_{j'=1}^{r_2+s_2} \rho_{i,j}\bar{\rho}_{i'j'} = \bigoplus_{i=1}^{r_1+s_1} \bigoplus_{j=1}^{r_2+s_2} \rho_{i,j}\bar{\rho}_{i,j} = \bigoplus_{i=1}^{r_1+s_1} \bigoplus_{j=1}^{r_2+s_2} \mathrm{id}_{\mathcal{B}_{i,j}}$$

Since ρ is an isomorphism (see theorem 1), it follows that $\rho^{-1} = \bar{\rho}$. This is also true in the case (ii). □

Now we can describe the primitive central idempotents in $F_qQ_{m,n}$ in the case $\gcd(2mn, q) = 1$ and $n \mid q-1$.

Теорема 4. *Let* $\gcd(2mn, q) = 1$ *and* $n \mid q-1$*; then* $\mathbb{F}_qQ_{m,n}$ *has*

1) $4\xi(m)r_2$ *primitive central idempotents of the form*

$$\frac{e+b+c+bc}{4}e_{f_i}^m(a_1)e_{g_j}^n(a_2), \quad \frac{e+b-c-bc}{4}e_{f_i}^m(a_1)e_{g_j}^n(a_2),$$

$$\frac{e-b+c-bc}{4}e_{f_i}^m(a_1)e_{g_j}^n(a_2), \frac{e-b-c+bc}{4}e_{f_i}^m(a_1)e_{g_j}^n(a_2),$$

where $1 \le i \le \xi(m)$ *and* $1 \le j \le r_2$*;*

2) $2(r_1 - \xi(m))r_2$ *primitive central idempotents of the form:*

$$\frac{e-b}{2}e_{f_i}^m(a_1)e_{g_j}^n(a_2), \quad \frac{e+b}{2}e_{f_i}^m(a_1)e_{g_j}^n(a_2),$$

where $\xi(m)+1 \le i \le r_1$ *and* $1 \le j \le r_2$*;*

3) $2s_1r_2$ *primitive central idempotents of the form:*

$$\frac{e-b}{2}\left(e_{f_i}^m(a_1) + e_{f_i^*}^m(a_1)\right)e_{g_j}^n(a_2), \quad \frac{e+b}{2}\left(e_{f_i}^m(a_1) + e_{f_i^*}^m(a_1)\right)e_{g_j}^n(a_2),$$

where $r_1+1 \le i \le r_1+s_1$ *and* $1 \le j \le r_2$*;*

4) $2\xi(m)s_2$ *primitive central idempotents of the form:*

$$\frac{e-c}{2}e_{f_i}^m(a_1)\left(e_{g_j}^n(a_2) + e_{g_j^*}^n(a_2)\right), \quad \frac{e+c}{2}e_{f_i}^m(a_1)\left(e_{g_j}^n(a_2) + e_{g_j^*}^n(a_2)\right),$$

where $1 \le i \le \xi(m)$ *and* $r_2+1 \le j \le r_2+s_2$*;*

5) $(r_1 - \xi(m))s_2$ *primitive central idempotents of the form:*

$$e_{f_i}^m(a_1)\left(e_{g_j}^n(a_2) + e_{g_j^*}^n(a_2)\right),$$

where $\xi(m)+1 \le i \le r_1$ *and* $r_2+1 \le j \le r_2+s_2$*;*

6) $s_1 s_2$ primitive central idempotents of the form:

$$\left(e^m_{f_i}(a_1) + e^m_{f_i^*}(a_1)\right)\left(e^n_{g_j}(a_2) + e^n_{g_j^*}(a_2)\right),$$

where $r_1 + 1 \le i \le r_1 + s_1$ and $r_2 + 1 \le j \le r_2 + s_2$.

Доказательство. Let R be a semisimple ring and let

$$\varphi : R \to R_1 \oplus R_2 \oplus \cdots \oplus R_l,$$

where R_i are matrix rings over division rings, be the Wedderburn decomposition of R. It is well-known (see [1], 2.6) that R has l primitive central idempotents, and each one is of the form

$$e_i = \varphi^{-1}(0 \oplus \cdots \oplus 0 \oplus I_i \oplus 0 \oplus \cdots \oplus 0),$$

where $I_i \in R_i$ is the identity element.

Therefore, using theorems 2 and 3, we obtain 1)–6). Indeed, consider for example 1) in the case $i = 1$ and $j = 1$. Using theorem 3 we get

$$d^{-1}\left((1,0,0,0) \oplus 0 \oplus 0 \cdots \oplus 0\right) = \mu_{1,1}\tau^{-1}_{1,1}(1,0,0,0).$$

By definitions of $\tau_{1,1}$ from theorem 2 and $\mu_{1,1}$ from theorem 3 we obtain

$$\mu_{1,1}\tau^{-1}_{1,1}(1,0,0,0) = \mu_{1,1}\left(\frac{1 + h_1 + h_2 + h_1h_2}{4}\right) = \frac{e + b + c + bc}{4} e^m_{f_1}(a_1)e^n_{g_1}(a_2).$$

Similarly we can evaluate

$$d^{-1}\left((0,1,0,0) \oplus 0 \oplus 0 \cdots \oplus 0\right) \ldots d^{-1}\left((0,0,0,1) \oplus 0 \oplus 0 \cdots \oplus 0\right)$$

and remaining primitive central idempotents for $1 \le i \le \xi(m)$ and $1 \le j \le r_2$.

Now let's consider 2). In the case $\xi(m) + 1 \le i \le r_1$ and $1 \le j \le r_2$ using definitions of d and $\mu_{i,j}$ from theorem 3 and $\tau_{i,j}$ from theorem 2 we get

$$d^{-1}(0 \oplus \cdots \oplus 0 \oplus (E \oplus 0) \oplus 0 \oplus \cdots \oplus 0) = \mu_{i,j}\sigma^{-1}_{i,j}\tau^{-1}_{i,j}(E \oplus 0) = \mu_{i,j}(E + 0h) = \frac{e - b}{2} e^m_{f_i}(a_1)e^n_{g_j}(a_2)$$

and

$$d^{-1}(0 \oplus \cdots \oplus 0 \oplus (0 \oplus E) \oplus 0 \oplus \cdots \oplus 0) = \mu_{i,j}\sigma^{-1}_{i,j}\tau^{-1}_{i,j}(0 \oplus E) = \mu_{i,j}(0 + Eh) = \frac{e + b}{2} e^m_{f_i}(a_1)e^n_{g_j}(a_2),$$

here E denotes the identity matrix and $(0 \oplus E), (E \oplus 0) \in \mathcal{A}_{i,j}$.

The remaining cases 3)–6) are proved in the same way. For example, let's consider 6). In the case $r_1 + 1 \le i \le r_1 + s_1$ and $r_2 + 1 \le j \le r_2 + s_2$ we have

$$d^{-1}(0 \oplus \cdots \oplus 0 \oplus E \oplus 0 \oplus \cdots \oplus 0) = \mu_{i,j}(E) = \left(e^m_{f_i}(a_1) + e^m_{f_i^*}(a_1)\right)\left(e^n_{g_j}(a_2) + e^n_{g_j^*}(a_2)\right),$$

here $E \in \mathcal{A}_{i,j}$ is identity matrix. □

Замечание 3. *Note that, $\mathbb{F}_q Q_{m,n}$ splits into internal direct sum of minimal two–sided ideals $I_k \subset \mathbb{F}_q Q_{m,n}$. Each I_k is isomorphic to one of the simple direct summands in (12) and generated by an idempotent from theorem 4.*

4. An application to algebraic codding theory

Now we can establish the structure of the group codes over $Q_{m,n}$. First, let us introduce the notation. Define

$$M(i,j) := \begin{cases} 1, & (1 \le i \le \xi(m)) \wedge (1 \le j \le r_2), \\ 4, & (r_1+1 \le i \le r_1+s_1) \wedge (r_2+1 \le j \le r_2+s_2), \\ 2 & \text{otherwise} \end{cases}$$

and

$$F_i := \begin{cases} \mathbb{F}_q, & 1 \le i \le \xi(n), \\ \mathbb{F}_q[\alpha_i + \alpha_i^{-1}], & \xi(n)+1 \le i \le r, \\ \mathbb{F}_q[\alpha_i], & r+1 \le i \le r+s. \end{cases}$$

Let $k \in \mathbb{N}$, let $\mathbb{F}$ be a field and V be a subspace of $\mathbb{F}^k$; by $\mathcal{I}(\mathbb{F}, k, V)$ we denote the set of all matrices $K \in \mathbb{M}_k(\mathbb{F})$ such that $K\bar{v} = 0$ for all $\bar{v} \in V$.

In [21], p. 93, it was proved that any left ideal of $\mathbb{M}_k(\mathbb{F})$ is of the form $\mathcal{I}(\mathbb{F}, k, V)$ and there is one–to–one correspondence between the left ideals of $\mathbb{M}_k(\mathbb{F})$ and the linear subspaces of $\mathbb{F}^k$.

Теорема 5. *Let* $\gcd(2mn, q) = 1$ *and* $n \mid (q-1)$. *For any group code* $C \subset \mathbb{F}_q Q_{m,n}$ *there exist subspaces* $V_{i,j,k} \subset F_i^{M(i,j)}$ *such that*

$$d(C) = \bigoplus_{i=1}^{r_1+s_1} \bigoplus_{j=1}^{r_2+s_2} \mathcal{C}_{i,j}, \quad \mathcal{C}_{i,j} = \tag{14}$$

$$= \begin{cases} \bigoplus_{k=1}^{4} \mathcal{I}(F_i, 1, V_{i,j,k}), & (1 \le i \le \xi(m)) \wedge (1 \le j \le r_2) \\ \mathcal{I}(F_i, 2, V_{i,j,1}) \oplus \mathcal{I}(F_i, 2, V_{i,j,2}), & (\xi(m)+1 \le i \le r_1) \wedge (1 \le j \le r_2) \\ \mathcal{I}(F_i, 2, V_{i,j,1}) \oplus \mathcal{I}(F_i, 2, V_{i,j,2}), & (r_1+1 \le i \le r_1+s_1) \wedge (1 \le j \le r_2) \\ \mathcal{I}(F_i, 2, V_{i,j,1}) \oplus \mathcal{I}(F_i, 2, V_{i,j,2}), & (1 \le i \le \xi(m)) \wedge (r_2+1 \le j \le r_2+s_2) \\ \mathcal{I}(F_i, 4, V_{i,j,1}), & (\xi(m)+1 \le i \le r_1) \wedge (r_2+1 \le j \le r_2+s_2) \\ \mathcal{I}(F_i, 4, V_{i,j,1}), & (r_1+1 \le i \le r_1+s_1) \wedge (r_2+1 \le j \le r_2+s_2) \end{cases} \tag{15}$$

Contrariwise, for any subspaces $V_{i,j,k} \subset F_i^{M(i,j)}$ *the set*

$$d^{-1}(\bigoplus_{i,j=1}^{r+s} \mathcal{C}_{i,j}),$$

with $\mathcal{C}_{i,j}$ *defined in (15), is a group code in* $\mathbb{F}_q Q_{m,n}$.

Доказательство. Consider (12) from theorem 2. Let

$$\Delta = \bigoplus_{i=1}^{r_1+s_1} \bigoplus_{j=1}^{r_2+s_2} \mathcal{A}_{i,j}.$$

Since $d : \mathbb{F}_q Q_{m,n} \to \Delta$ is an isomorphism, it follows that there is one–to–one correspondence between the codes in $\mathbb{F}_q Q_{m,n}$ and the left ideals of Δ. It is well–known that any left ideal of a direct sum of algebras is a direct sum of left ideals of summands. It is established that the ideals of summands are of the form $\mathcal{I}(F_i, t, V_{i,j,k})$. Hence the theorem is entirely proved. □

Consider a group code $C \subset \mathbb{F}_q Q_{m,n}$. We obliviously have the length of C equals to $4mn$ and the dimension can be evaluated by following formula:

$$\dim(C) = \sum_{i=1}^{r_1+s_1} \sum_{j=1}^{r_2+s_2} \dim(\mathcal{C}_{i,j}).$$

5. Conclusion

In the paper we considered the bidihedral group $Q_{m,n}$ and its group algebra $\mathbb{F}_q Q_{m,n}$. In the case $\gcd(mn, q) = 1$ and $n \mid q - 1$ we obtained the structural theorem for $\mathbb{F}_q Q_{m,n}$. Then we used it to explicitly describe the Wedderburn decomposition of $\mathbb{F}_q Q_{m,n}$ in the case $\gcd(2mn, q) = 1$. Moreover, we constructed inverse isomorphisms ρ^{-1} and d^{-1}, which helped us to describe the central primitive idempotents of $\mathbb{F}_q Q_{m,n}$.

Finally, we used the Wedderburn decomposition d and d^{-1} to algebraically describe all codes in $\mathbb{F}_q Q_{m,n}$ in the case $\gcd(2mn, q) = 1$ and $n \mid (q - 1)$. In addition, it is easy to find their length and dimension.

Further research is needed to find among these codes promising classes of error–correcting codes with good parameters and to construct decoders.

REFERENCES

1. Milies, C. P. & Sehgal, S. K. 2002, *An inroduction to Group Rings*, Kluwer Academic Publishers, Boston.

2. Lang, S., 2002, *Algebra*, Springer-Verlag, New York.

3. Kelarev, A. V. & Solé, P. 2001, "Error correcting codes as ideals in group rings", Contemp. Math., vol. 273, pp. 11–18.

4. Kouselo, E., Gonsales, S., Markov, V. T., Martines, K. & Nechaev, A. A. 2012, "Ideal representations of Reed-Solomon and Reed-Muller codes", *Algebra Logic*, vol. 51, no. 3, pp. 195–212.

5. Berman, S. D. 1967, "On the theory of group codes", *Cybernetics*, vol. 3, pp. 25–31.

6. Charpin, P. 1983, "The Extended Reed-Solomon Codes Considered as Ideals or a Modular Algebra" *North-Holland Mathematics Studies*, vol. 75, pp. 171–176.

7. Tumaykin, I. N. 2018, "Group Ring Ideals Related to Reed–Muller Codes", *J Math Sci*, vol. 233, pp. 745–748.

8. Zimmermann, K.-H. 1994, *Beitrage zur algebraischen Codierungstheorie mittels modularer Darstellungstheorie*, Bayreuther Mathematische Schriften Vol. 48, University of Bayreuth.

9. Assuena, S. & Milies, C. P 2019, "Good codes from metacyclic groups", Contemp. Math., vol. 727, pp. 39–49.

10. Olteanu, G. & Van Gelder, I. 2015, "Construction of minimal non-abelian left group codes", Des. Codes Cryptogr., vol. 75, no. 3, pp. 359–373.

11. Vedenev, K. V. & Deundyak, V. M 2018, "Codes in Dihedral Group Algebra" (in Russian), Modeling and Analysis of Information Systems, vol. 25, no. 2, pp. 232–245.

12. https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization Last visited 1.07.2019.

13. Minder, L. & Shokrollahi, A. 2007, "Cryptanalysis of the Sidelnikov cryptosystem", Lecture Notes in Computer Science, vol. 4515, pp. 347–360.

14. Chizhov, I. I. & Borodin, M. A. 2014, "Effective attack on the McEliece cryptosystem based on Reed-Muller codes", Discrete Mathematics and Applications, vol. 24, issue 5, pp. 273–280.

15. Sidelnikov, V. M., & Shestakov, S. O. 1992, "On an encoding system constructed on the basis of generalized Reed–Solomon codes",Discrete Mathematics and Applications, vol. 2, issue 4, pp. 439–444.

16. Broche, O. & Del RiO, A. 2007, "Wedderburn decomposition of finite group algebras", Finite Fields and Their Applications, vol. 13(1), pp. 71–79.

17. Bakshi, G. K., Gupta, S., & Passi, I. B. S. 2013, "The structure of finite semisimple metacyclic group algebras", J. Ramanujan Math. Soc, vol. 28(2), pp. 141–158.

18. Martinez, F. B. 2015, "Structure of finite dihedral group algebra", Finite Fields and Their Applications, vol. 35, pp. 204–214.

19. Coxeter, H. S., & Moser, W. O. 2013, *Generators and relations for discrete groups*, Springer Science & Business Media.

20. Magnus, W., Karrass, A., & Solitar, D. 2004, *Combinatorial group theory: Presentations of groups in terms of generators and relations*, Courier Corporation.

21. Jacobson, N. 1956, *Structure of rings*, Vol. 37, American Mathematical Soc.

Получено 7.08.2019 г.
Принято в печать 12.11.2019 г.