ГОДИШНИК НА СОФИЙСКИЯ УНИВЕРСИТЕТ „СВ. КЛИМЕНТ ОХРИДСКИ“
ФАКУЛТЕТ ПО МАТЕМАТИКА И ИНФОРМАТИКА
Том 104

ANNUAL OF SOFIA UNIVERSITY „ST. KLIMENT OHRIDSKI“
FACULTY OF MATHEMATICS AND INFORMATICS
Volume 104

ON THE REPRESENTATION OF MODULES OVER FINITE CHAIN RINGS

NEVYANA GEORGIEVA, IVAN LANDJEV

We define a standard form for matrices over finite chain rings and describe some basic operations on modules over such rings. These results are used as a tool for the investigation of network codes over finite chain rings and spreads in projective Hjelmslev geometries.

Keywords: finite chain rings, modules over finite chain rings, standard form of a matrix over a finite chain ring.

2000 Math. Subject Classification: 16D10,16P10 (Primary); 51C05,94B05 (Secondary).

1. INTRODUCTION

The aim of this paper is to define a standard representation for modules over finite chain rings and demonstrate its application to certain basic operations over modules. The problem of defining a standard representation arises in connection with various problems. These include the problem of the construction of spreads of projective Hjelmslev spaces by subspaces of various shapes, the problem of the construction of R-analogues of designs, as well as the construction of network codes over finite chain rings.

The paper is structured as follows. In section 2 we summarize some basic facts about the structure of finite chain rings. We introduce a linear order on the ring elements which is used in the definition of the standard form. In section 3 we

present structure results about modules over finite chain rings as well as a counting formula for the number of submodules of given shape contained in a fixed module. In section 4 we introduce the standard form of a matrix over a finite chain ring. We prove one of our central results that for every module ${}_RM \leq {}_RR^n$ there exists a unique matrix in standard form whose rows generate ${}_RM$. In section 5 we obtain the standard form of the matrix whose rows generate the right orthogonal $M_R^{\perp}$ of a given left module ${}_RM$. In section 6 we discuss how to generate all submodules of a given module spanned by the rows of a matrix in standard form.

2. FINITE CHAIN RINGS

In this section, we give some facts about finite chain rings. An associative ring with identity is called a left (right) chain ring if the lattice of its left (right) ideals is a chain. The general structure of finite chain rings is given in the following theorem.

Theorem 1. *For a finite chain ring R the following conditions are equivalent*

(i) R is a left chain ring;

(ii) the principal left ideals of R form a chain;

(iii) R is a local ring and $\operatorname{Rad} R = R\theta$ for any $\theta \in \operatorname{Rad} R/(\operatorname{Rad} R)^2$;

(iv) R is a right chain ring.

If R satisfies the above conditions then every proper left(right) ideal of R has the form $(\operatorname{Rad} R)^i = R\theta^i = \theta^i R$ for some positive integer i.

It is well-known that the factor-ring $R/\operatorname{Rad} R$ is a field. We denote its cardinality by $q = p^r$. The smallest positive integer m for which $(\operatorname{Rad} R)^m = (0)$ is called the length of R. Furthermore, for each $i = 0, \ldots, m-1$, $(\operatorname{Rad} R)^i/(\operatorname{Rad} R)^{i+1}$ is a vector space of dimension 1 over $R/\operatorname{Rad} R$, and we have $|(\operatorname{Rad} R)^i/(\operatorname{Rad} R)^{i+1}| = q$. This implies that $|R| = q^m$. The characteristic of R is $\operatorname{char} R = p^s$ for some positive integer s.

Let $\Gamma = \{\gamma_0 = 0, \gamma_1 = 1, \gamma_2, \ldots, \gamma_{q-1}\}$ be a set of elements of R with $\gamma_i \not\equiv \gamma_j \pmod{\operatorname{Rad} R}$ for all i, j with $0 \leq i < j \leq q-1$. Let us fix a generator θ of R. Every element a from R can be written in a unique way as

$$a = a_0 + a_1\theta + \cdots + a_{m-1}\theta^{m-1},$$

for some $a_i \in \Gamma$. We fix the following linear order on Γ:

$$\gamma_0 \prec \gamma_1 \prec \cdots \prec \gamma_{m-1}.$$

This order is extended to the elements of R as follows. For the elements $a = a_0 + a_1\theta + \cdots + a_{m-1}\theta^{m-1}$ and $b = b_0 + b_1\theta + \cdots + b_{m-1}\theta^{m-1}$, $a_i, b_i \in \Gamma$, we write $a \prec b$ if and only if

$$a_{m-1} = b_{m-1}, \ldots, a_{j+1} = b_{j+1}, a_j \prec b_j,$$

for some $0 \leq j \leq m-1$. We can define a bijection $\varphi : R \to \{0, 1, \ldots, q^m - 1\}$ which is consistent with the linear order of the elements of R given above. Set $\varphi(\gamma_i) = i$. Further for $a = a_0 + a_1\theta + \cdots + a_{m-1}\theta^{m-1}$, $a_i \in \Gamma$, we let $\varphi(a) = \sum_{i=0}^{m-1} \varphi(a_i)q^i$. The following lemma contains some straightforward properties of φ.

Lemma 1. *(1) $a \in \Gamma$ if and only if $\varphi(a) < q$; more generally, the elements a with $\varphi(a) < q^i$ form a system of distinct representatives modulo $(\operatorname{Rad} R)^i$;*

(2) for each $i \in \mathbb{N}$, $a \in (\operatorname{Rad} R)^i$, i.e. $a = b\theta^i$, $b \in R^*$, if and only if $\varphi(a)$ divides q^i;

(3) if q^i divides $\varphi(b)$ then $b = a\theta^i$ with $a = \varphi^{-1}\left(\frac{\varphi(b)}{q^i}\right)$.

Throughout the paper, the letters $\theta, \Gamma, p, q, m, r, s$ will have the meaning fixed above. For a more detailed study of finite chain rings we refer to [2,3,4,5,7,8].

3. MODULES OVER FINITE CHAIN RINGS

Let ${}_RM$ be a finitely generated left R-module. We say that the element $x \in {}_RM$ has period θ^i if $i \geq 0$ is the smallest integer with $\theta^i x = 0$. The element $x \in {}_RM$ is said to have height j if j is the largest integer with $x = \theta^j y$ for some $y \in M$. We set

$$M^* = \{x \in M \mid x \text{ has period } \theta^m\}.$$

An integer partition of the positive integer N is a sequence $\lambda = (\lambda_1, \lambda_2, \ldots)$ with $\lambda_i \in \mathbb{Z}$, $\lambda_1 \geq \lambda_2 \geq \cdots$, $\lambda_i = 0$ for all but finitely many i, and $N = \lambda_1 + \lambda_2 + \cdots$. We write this as $\lambda \vdash N$. Sometimes it is convenient to suppress the trailing zeros in the sequence λ. Partitions can be written multiplicatively as $\lambda = 1^{s_1}2^{s_2}3^{s_3}\ldots$ where s_i is the number of λ_j's equal to i. Denote by λ'_j the number of parts greater or equal to j. Then $\lambda' = (\lambda'_1, \lambda'_2, \ldots)$ is again a partition of N and it is called the conjugate partition of λ.

The following theorem describes the structure of finite R-modules.

Theorem 2. *Let R be a finite chain ring. For every finite module ${}_RM$ there exists a uniquely determined partition $\lambda = (\lambda_1, \ldots, \lambda_k) \vdash \log_R |M|$ into parts $1 \leq \lambda_i \leq m$ such that*

$${}_RM \cong R/(\operatorname{Rad} R)^{\lambda_1} \oplus \cdots \oplus R/(\operatorname{Rad} R)^{\lambda_k}.$$

The parts of the conjugate partition $\lambda' = (\lambda'_1, \lambda'_2, \ldots) \vdash \log_q |M|$ are the Ulm-Kaplansky invariants $\lambda'_i = \dim_{R/\operatorname{Rad} R}(M[\theta] \cap \theta^{i-1}M)$.

The partitions λ and λ' are called the shape, resp. conjugate shape, of ${}_RM$. The integer $k = \lambda'_1 = \dim_{R/\operatorname{Rad} R} M[\theta]$ is called the rank of ${}_RM$ and the integer λ'_m is called the free rank of ${}_RM$.

Denote by $\boldsymbol{M}_{m,n}(R)$ the set of all m-by-n matrices over the chain ring R.

Theorem 3 ([3]). *Let $A \in \boldsymbol{M}_{m,n}(R)$ be a matrix over R. Then the left module ${}_RL \leq {}_RR^n$ generated by the rows of A and the right module $M_R \leq {}_RR^n$ generated by the columns of A have the same shape.*

It is known that an n-dimensional vector space over the finite field $\mathbb{F}_q$ has exactly

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q^n-1)(q^{n-1}-1)\dots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\dots(q-1)}$$

k-dimensional vector subspaces.

A similar counting formula holds true for modules over finite chain rings. Let ${}_RM$ be a module of shape λ and $U \leq {}_RM$ be a submodule of shape μ. The conjugate partitions λ', μ' are related by $\mu' \leq \lambda'$ which is equivalent to $\mu \leq \lambda$. The next theorem is our main counting tool. For the special case of $R = \mathbb{Z}_m$ it is known from [1]. For the case of general R we refer to [7].

Theorem 4. *Let ${}_RM$ be a module of shape λ. For every partition μ satisfying $\mu \leq \lambda$ the module ${}_RM$ has exactly*

$$\begin{bmatrix} \lambda \\ \mu \end{bmatrix}_q := \prod_{i=1}^{\infty} q^{\mu'_{i+1}(\lambda'_i - \mu'_i)} \cdot \begin{bmatrix} \lambda'_i - \mu'_{i+1} \\ \mu'_i - \mu'_{i+1} \end{bmatrix}_q \tag{3.1}$$

submodules of shape μ. In particular, the number of free rank s submodules of ${}_RM$ equals

$$q^{s(\lambda'_1 - s) + \dots + s(\lambda'_{m-1} - s)} \cdot \begin{bmatrix} \lambda'_m \\ s \end{bmatrix}_q.$$

Corollary 1. *Let $\boldsymbol{m} = (\underbrace{m, \dots, m}_{n})$ and let $\mu = (\mu_1, \dots, \mu_n)$, where $m \geq \mu_1 \geq \dots \geq \mu_n \geq 0$. Then*

$$\begin{bmatrix} \boldsymbol{m} \\ \mu \end{bmatrix}_q = \begin{bmatrix} \boldsymbol{m} \\ \overline{\mu} \end{bmatrix}_q,$$

where $\overline{\mu} = (m - \mu_n, \dots, m - \mu_1)$.

Remark 1. The formula in Corollary 1 can be viewed as analogue of the usual binomial identity $\binom{n}{k} = \binom{n}{n-k}$.

4. THE STANDARD FORM OF A MATRIX OVER A FINITE CHAIN RING

Let R be a finite chain ring of cardinality q^m and with residue field $R/\operatorname{Rad} R \cong \mathbb{F}_q$, $q = p^r$, where p is a prime. Given a finite set of generators of a submodule M of ${}_RR^n$, we consider the problem of finding a standard generating set for M, which can be easily operated on, i.e., from the standard form we expect to be able to find easily the dual module, the span of two modules, as well as their intersection.

We denote by $\boldsymbol{M}_{k,n}$ the set of all k-by-n matrices over R.

Definition 1. We say that the matrix $A = (a_{ij}) \in \boldsymbol{M}_{k,n}$ is in standard form if

(1) $a_{ij_i} = \theta^{m-t_i}$ for some $t_i \in \{0, \ldots, m\}$;

(2) $a_{is} = \theta^{m-t_i+1}\beta$, $\beta \in R$, for all $s < j_i$;

(3) $a_{is} = \theta^{m-t_i}\beta$, $\beta \in R$, for all $s > j_i$;

(4) $a_{sj_i} \prec a_{ij_i}$ for all $s \neq i$ (here $\prec$ is the lexicographic order defined in section);

(5) $i_1 < i_2 < i_3 < \cdots$.

The integer t_i is called the type of row i, $i = 1, \ldots, k$. Let $\boldsymbol{a} = (a_1, \ldots, a_n) \in {}_RR^n$. The smallest $i \in \{0, \ldots, m\}$ such that $\theta^i a = 0$ is called the type of $\boldsymbol{a}$. The leftmost component a_j with $a_j \in (\operatorname{Rad} R)^{m-i} \setminus (\operatorname{Rad} R)^{m-i+1}$ is called the leader of $\boldsymbol{a}$. For a matrix $A \in \boldsymbol{M}_{k,n}(R)$ in standard form we denote the set of coordinate positions of the row-leaders of A by $J(A) = \{j_1, j_2, \ldots, j_k\}$.

Lemma 2. *Let ${}_RM \leq {}_RR^n$ be a module and let A be a matrix in standard form whose rows generate ${}_RM$. For an arbitrary element $\boldsymbol{v} \in {}_RM$ denote by s the position of its leader. Then $s \in J(A)$.*

Proof. Denote the rows of A by $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k$. Let further $J(A) = \{j_1, \ldots, j_k\}$, and let the respective leaders be $\theta^{m-t_1}, \ldots, \theta^{m-t_k}$. Without loss of generality we can assume that $t_1 \geq t_2 \geq \cdots \geq t_k \geq 1$. Then all elements in column j_s, $s = 1, \ldots, k$, that are under the leader of row s, are zeros.

Set $\boldsymbol{v} = \lambda_1\boldsymbol{v}_1 + \ldots + \lambda_k\boldsymbol{v}_k$. Let the leader of $\boldsymbol{v}$ be in position l. We consider three cases.

(1) Let $l < j_1$. Assume that $s \in \{1, \ldots, k\}$ is such an index that the type of $\lambda_s\boldsymbol{v}_s$ is the largest among the types of the vectors $\lambda_i\boldsymbol{v}_i$. If $\lambda_s \in (\operatorname{Rad} R)^{\tau_s}$ then the type of $\boldsymbol{v}$ is at most $t_s - 1 - \tau_s$. On the other hand, the element in the j_s-th coordinate of $\boldsymbol{v}$ is λ_s+(terms which are a linear combination of $1, \theta, \ldots, \theta^{m-t_s-1}$). Therefore the type of $\boldsymbol{v}$ is at least $t_s - \tau_s$, a contradiction.

(2) Let $j_{i-1} < l < j_i$. Assume $\lambda_s \neq 0$ for some $s \leq i-1$ and $\lambda - s\boldsymbol{v}_s$ is the largest type of a vector from $\{\lambda_1\boldsymbol{v}_1, \ldots, \lambda_i\boldsymbol{v}_i\}$. If $\lambda_s \in (\operatorname{Rad} R)^{\tau_s}$, this largest type is at most $t_s - \tau_s$. On the other hand, $\boldsymbol{v}$ has in position j_s the element

$\lambda_s\theta^{m-t_s}$+(terms which are a linear combination of $1, \theta, \ldots, \theta^{m-t_s-1}$). The first term is from $R\theta^{m-t_s+\tau_s}$, but is to the left of the leader, a contradiction. We have proved so far that $\lambda_j = 0$ for all $j \leq i-1$. Now we can use the argument from (1) to complete this case.

(3) Now let $l > j_k$. Now we can use the argument from the first part of (2).

By (1–3) l should be a coordinate position which is from $J(A)$. □

Theorem 5. *For every module $M \leq {}_RR^n$ there exists a unique matrix B in standard form such that M is spanned by the rows of B.*

Proof. 1) *Existence.* We prove the existence by induction on $k = \operatorname{rk} M$. There is nothing to prove for $k = 1$. One has only to note that by a suitable multiplication one can make the leader have the form θ^{m-t} for some t.

Let $\boldsymbol{v}'_1 \in M$ be an element of the maximal possible type in M, $m - t_1$ say. Without loss of generality we may assume that the leader is in position j_1 and is the leftmost among all leaders of elements of M. By a suitable multiplication, we can make this leader equal to θ^{m-t_1}. Now ${}_RM = {}_R\boldsymbol{v}'_1 \oplus {}_RM'$, where ${}_RM'$ has rank $k-1$ and is the submodule of ${}_RM$ containing all vectors having 0 in position j_1. This follows by the fact that for every vector $\boldsymbol{v} \in {}_RM$ one can find a $\lambda \in R$ such that $\boldsymbol{v} - \lambda_1\boldsymbol{v}'_1$ has zero in position j_1.

By the induction hypothesis, there exists a matrix $\boldsymbol{B}$ in standard form whose rows generate ${}_RM'$. Denote these rows by $\boldsymbol{v}_2, \ldots, \boldsymbol{v}_k$. Set $J(B) = \{j_2, \ldots, j_k\}$. Further, let the j_s-th component of $\boldsymbol{v}'_1$ be $\alpha_s + \beta_s\theta^{m-t_s}$, $s = 2, \ldots, k$, where $\alpha_s = x_0 + x_1\theta + x_{m-t_s-1}$, $\beta_s = y_0 + \cdots + y_{t_s-1}$, $x_i, y_i \in \Gamma$.

The element $\boldsymbol{v}_1 = \boldsymbol{v}'_1 - \beta_2\boldsymbol{v}_2 - \cdots - \beta_k\boldsymbol{v}_k$ has the property that the element in position j_s is smaller (with respect to $\prec$) than θ^{m-t_s} for all $s = 2, \ldots, k$. It is also clear that the components of $\boldsymbol{v}_1$ to the left of the leader belong to $\operatorname{Rad} R^{m-t+1}$ (since the i-th, $i < j_1$, component in each one of $\boldsymbol{v}'_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k$ is in $\operatorname{Rad} R^{m-t+1}$). Hence the matrix A having as rows the vectors $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k$ is the desired matrix.

2) *Uniqueness.* Assume $A' = (\boldsymbol{v}'_1, \ldots, \boldsymbol{v}'_k)^T$ and $A'' = (\boldsymbol{v}''_1, \ldots, \boldsymbol{v}''_k)^T$ are two matrices in standard form whose rows generate the same module ${}_RM$. By Lemma 2 $J(A') = J(A'') = \{j_1, \ldots, j_k\}$. Let the leaders of $\boldsymbol{v}'_i$ (resp. $\boldsymbol{v}''_i$) be $\theta^{m-t'_i}$ (resp. $\theta^{m-t''_i}$). With no loss of generality $t'_1 \geq t'_2 \geq \cdots \geq t'_k$. In particular, this means that all elements in A' in the columns $j_1, j_2, \ldots, j_k$ below the leader of the corresponding row are zeros, i.e. we have.

$$
\begin{array}{lccccccccc}
\boldsymbol{v}'_1 = & (\ldots & \theta^{m-t'_1} & v'_{1,j_2} & \ldots & v'_{1,j_i} & \ldots & v'_{1j_k} & \ldots) \\
\boldsymbol{v}'_2 = & (\ldots & 0 & \theta^{m-t'_2} & \ldots & v'_{2,j_i} & \ldots & v'_{2j_k} & \ldots) \\
\vdots & & \vdots & \vdots & & \vdots & & \vdots & \\
\boldsymbol{v}'_i = & (\ldots & 0 & 0 & \ldots & \theta^{m-t'_i} & \ldots & v'_{ij_k} & \ldots) \\
\vdots & & \vdots & \vdots & & \vdots & & \vdots & \\
\boldsymbol{v}'_k = & (\ldots & 0 & 0 & \ldots & 0 & \ldots & \theta^{m-t'_k} & \ldots)
\end{array}
$$

Now we can express $\boldsymbol{v}_i''$ as $\boldsymbol{v}_1'' = \lambda_1\boldsymbol{v}_1' + \cdots + \lambda_k\boldsymbol{v}_k'$. Since the leader of $\boldsymbol{v}_i''$ is in position j_i, we get that

$$\theta^{m-t_i''} = \lambda_i\theta^{m-t_i'} + \sum_{s=1}^{i-1}\lambda_s v'_{sj_s}.$$

Let us note that $\lambda_s = 0$ for all $s < i$; otherwise the leader of $\boldsymbol{v}_i''$ is in a position with a smaller number than j_i. Thus the above equality simplifies to $\theta^{m-t_i''} = \lambda_i\theta^{m-t_i'}$, which implies that $m - t_i' \leq m - t_i''$, i.e., $t_i' \geq t_i''$ for all $i = 1, \ldots, k$. Since the sets $\{t_i'\}$ and $\{t_i''\}$ (taken in non-increasing order) give the shape of ${}_RM$ we have $t_i' = t_i''$ for all i.

Now we can conclude that $\boldsymbol{v}_k$ have zeros in positions $j_1, \ldots, j_{k-1}$ and $\theta^{m-t_k'} = \theta^{m-t_k''}$ in position j_k. Then $\boldsymbol{v}_k' - \boldsymbol{v}_k''$ has zeros in positions $j_1, \ldots, j_k$. Let $\boldsymbol{v}_k' - \boldsymbol{v}_k'' \neq 0$. Then its leader is in position different from $j_1, \ldots, j_k$, a contradiction to Lemma 2. Hence $\boldsymbol{v}_k' = \boldsymbol{v}_k''$ and the proof is completed by induction on the rank of ${}_RM$. □

Corollary 2. *Let A be a $(k \times n)$-matrix in standard form over the chain ring R. There exist permutation matrices T_1 of size $(k \times k)$ and T_2 of size $(n \times n)$ such that*

$$T_1AT_2 = \begin{pmatrix} I_{k_0} & A_{01} & A_{02} & \ldots & A_{0,m-1} & A_{0,m} \\ 0 & \theta I_{k_1} & \theta A_{12} & \ldots & \theta A_{1,m-1} & \theta A_{1,m} \\ 0 & 0 & \theta^2 I_{k_2} & \ldots & \theta^2 A_{2,m-1} & \theta^2 A_{2,m} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & \theta^{m-1} I_{k_{m-1}} & \theta^{m-1} A_{m-1,m} \end{pmatrix}, \tag{4.1}$$

where the entries in the matrices A_{ij} are from Γ.

5. THE ORTHOGONAL MODULE

Let R be a finite chain ring and consider a left module ${}_RM \leq {}_RR^n$. For two vectors $\boldsymbol{x} = (x_1, \ldots, x_n)$ and $\boldsymbol{y} = (y_1, \ldots, y_n)$ we define their inner product by

$$\boldsymbol{xy} = x_1y_1 + \cdots + x_ny_n.$$

The right orthogonal to ${}_RM$ is defined by

$$M_R^{\perp} = \{\boldsymbol{y} \in R^n \mid \boldsymbol{xy} = 0 \text{ for all } \boldsymbol{x} \in M\}.$$

Analogously, we define the left orthogonal to right module $M_R \leq R_R^n$. The following theorem summarizes some basic properties of orthogonal modules [4, 5].

Theorem 6. *Let R be a chain ring with $|R| = q^m$, $R/\operatorname{Rad} R \cong \mathbb{F}_q$, and let ${}_RM \leq {}_RR^N$ be a left submodule of shape $\lambda = (\lambda_1, \ldots, \lambda_n)$.*

(1) The right module $M_R^\perp$ has shape $\overline{\lambda} = (m - \lambda_n, \ldots, m - \lambda_1)$. In particular $|M||M^\perp| = |R^n|$.

(2) ${}^\perp(M^\perp) = M$.

(3) $M \to M^\perp$ defines an antiisomorphism between the lattices of left (resp. right) submodules of R^n and hence

$$(M_1 \cap M_2)^\perp = M_1^\perp + M_2^\perp, (M_1 + M_2)^\perp = M_1^\perp \cap M_2^\perp,$$

for $M_1, M_2 \leq R^n$.

Assume A is a matrix over the chain ring R in (upper) standard form. Let ${}_RM$ be the left module generated by the rows of A. We are going to describe a method of finding a matrix B in lower standard form, whose rows generate the right orthogonal module $M_R^\perp$.

Theorem 7. *Let ${}_RM$ be a submodule of ${}_RR^n$ generated by the rows of the matrix A of the form (4.1). Then $M_R^\perp$ is generated by the matrix*

$$B = \begin{pmatrix} B_{01}\theta^{m-1} & I_{k_1}\theta^{m-1} & 0 & 0 & \ldots & 0 \\ B_{02}\theta^{m-2} & B_{12}\theta^{m-2} & I_{k_2}\theta^{m-2} & 0 & \ldots & 0 \\ B_{03}\theta^{m-3} & B_{13}\theta^{m-3} & B_{23}\theta^{m-3} & I_{k_2}\theta^{m-3} & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ B_{0,m} & B_{1,m-1} & B_{2,m-1} & B_{3,m-1} & \ldots & I_{k_{m-1}} \end{pmatrix}, \tag{5.1}$$

where

$$B_{ij} = -\big(A_{ij} - \sum_{1<k<j+1} A_{ik}A_{k,j+1} + \sum_{i<k<l<j+1} A_{ik}A_{kl}A_{l,j+1} - \cdots + (-1)^{j-i+1}A_{i,i+1}A_{i+1,i+2}\ldots A_{j,j+1}\big)^T.$$

Proof. We have to show that the dot product of any row of A with any row of B is zero. □

Corollary 3. *Let $A \in \boldsymbol{M}_{k,n}$ be a matrix over a chain ring R whose rows generate the module ${}_RM$. Let $A' = T_1AT_2$, where T_1 and T_2 are permutation matrices of orders k and n, respectively, be of the form (4.1). The module $M_R^\perp$ is generated by the rows of*

$$B = T_1^T B' T_2^T,$$

where B' is the matrix given by (5.1).

6. GENERATION OF ALL SUBMODULES OF ${}_RM$ OF FIXED SHAPE

Let ${}_RM$ be a module of shape

$$\lambda = (\underbrace{m,\dots,m}_{k_0},\underbrace{m-1,\dots,m-1}_{k_1},\dots,\underbrace{1,\dots,1}_{k_{m-1}}) = m^{k_0}(m-1)^{k_1}\dots 1^{k_{m-1}}$$

and let ${}_RN$ be a submodule of M of shape $\mu \le \lambda$. Assume M is generated by the rows of a matrix A in standard form. With no loss of generality, A has the form (4.1). Let further N be generated by the rows of another matrix B that is also in standard form. Under the above assumptions B can be represented as

$$B = CA,$$

where C is a matrix in standard form with the following properties:

(1) if the leader in row i of B is in position j_i then the leader of row i in C is in position l_i with $l_i \ge j_i$;

(2) the components of C contained in the j-th column where

$$k_0 + k_1 + \dots + k_{s-1} + 1 \le j \le k_0 + k_1 + \dots + k_s, \;\; k_{-1} = 0,$$

are from $\Gamma + \theta\Gamma + \dots + \theta^{m-s-1}\Gamma$.

The proof of this observation is straightforward. It allows us to generate all submodules with a fixed shape of a module generated by the rows of some matrix A. We demonstrate this by the following example.

Example 1. Let $R = \mathbb{Z}_4$ and let A be the matrix

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}.$$

The module M generated by the rows (but also by the columns) of A is of shape $\lambda = (2,2,1,1)$. By Theorem 4 the number of all submodule $N \le M$ of shape $\mu = (2,1)$ is

$$\begin{bmatrix} \lambda \\ \mu \end{bmatrix}_{2^2} = 2^{1\cdot(4-2)} \begin{bmatrix} 4-1 \\ 2-1 \end{bmatrix}_2 2^{0(2-1)} \begin{bmatrix} 2-0 \\ 1-0 \end{bmatrix}_2 = 84.$$

We are going to construct the possible matrices C satisfying the conditions described above. Note that the last two columns can contain only entries from $\Gamma = \{0,1\}$.Thus we have the following possibilities for C:

$$\begin{pmatrix} 1 & \Gamma & \Gamma & \Gamma \\ 0 & 2 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 1 & \Gamma & \Gamma \end{pmatrix}, \quad \begin{pmatrix} 1 & R & 0 & \Gamma \\ 0 & \operatorname{Rad} R & 1 & \Gamma \end{pmatrix}$$

$$\begin{pmatrix} 1 & R & \Gamma & 0 \\ 0 & \operatorname{Rad} R & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} \operatorname{Rad} R & 1 & 0 & \Gamma \\ \operatorname{Rad} R & 0 & 1 & \Gamma \end{pmatrix}, \quad \begin{pmatrix} \operatorname{Rad} R & 1 & \Gamma & 0 \\ \operatorname{Rad} R & 0 & 0 & 1 \end{pmatrix}$$

Here $R = \{0, 1, 2, 3\}$, $\Gamma = \{0, 1\}$, and $\operatorname{Rad} R = \{0, 2\}$. Thus the number of matrices C of the first type is 8, of the second type – 4, of the third type – 32 etc, giving a total of

$$8 + 4 + 32 + 16 + 16 + 8 = 84,$$

as given by Theorem 4.

ACKNOWLEDGEMENTS. This research has been supported by the Science Research Fund of Sofia University under Contract No. 29/11.04.2016.

7. REFERENCES

[1] Birkhof, G.: Subgroups of abelian groups. *Proc. London Math. Society*, **38**, no. 2, 1934/35, 385–401.

[2] Clark, W. E., Drake, D. A.: Finite chain rings. *Abh. Math. Sem. der Univ. Hamburg*, **39**, 1974, 147–153.

[3] Honold, Th., Landjev, I.: Linearly representable codes over chain rings. *Abh. Math. Sem. der Univ. Hamburg*, **69**, 1999, 187–203.

[4] Honold, Th., Landjev, I.: Linear codes over finite chain rings. *Electron. J. Combinatorics*, **7**, 2000, #11.

[5] Honold, Th., Landjev, I.: Linear codes over finite chain rings and projective Hjelmslev geometries. In: *Codes over Rings* (P. Solé, ed.), World Scientific, 2009, pp. 60–123.

[6] van Lint, J. H., Wilson, R. M.: *A Course in Combinatorics*. Cambridge University Press, 1992.

[7] MacDonald, I. G.: *Symmetric Functions and Hall Polynomilas*. Oxford University Press, Second edition, 1995.

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

[9] Nechaev, A. A.: *Finite Principal Ideal Rings*, Russian Acad. Sciences, Sbornik Mathematics 2091973, 364–382.

Received on December 19, 2016

Nevyana Georgieva
Department of Informatics
New Bulgarian University
21 Montevideo str., 1618 Sofia
BULGARIA
E-mail: nevyanag@fmi.uni-sofia.bg

Ivan Landjev
Department of Informatics
New Bulgarian University
21 Montevideo str., 1618 Sofia
BULGARIA
E-mail: i.landjev@nbu.bg