Math-Net.Ru

Общероссийский математический портал

М. А. Goltvanitsa, Некоммутативная теорема Гамильтона–Кэли и корни характеристических многочленов скрученных линейных рекуррент над кольцами Га-
луа, *Матем. вопр. криптогр.*, 2017, том 8, выпуск 2, 65–76

DOI: <https://doi.org/10.4213/mvk224>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и
согласны с пользовательским соглашением

<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 35.173.219.12

26 апреля 2023 г., 14:15:02

**Non-commutative Hamilton – Cayley theorem and roots
of characteristic polynomials of skew maximal period
linear recurrences over Galois rings**

M. A. Goltvanitsa

Certification Research Center, LLC, Moscow

Получено 17.III.2016

Abstract. Let p be a prime number, $R = \text{GR}(q^d, p^d)$, where $q = p^r$, be a Galois ring, $S = \text{GR}(q^{nd}, p^d)$ be its extension. We prove a non-commutative generalization of the well-known Hamilton–Cayley theorem. Using this result we prove the existence of roots in some extension $\mathcal{K}$ of $\tilde{S}$ for characteristic polynomials of skew maximal period linear recurrent sequences over S . Also for these polynomials we investigate the structure of the set of their roots.

Keywords: non-commutative Hamilton–Cayley theorem, skew LRS, maximal period, Galois ring

**Некоммутативная теорема Гамильтона – Кэли и корни
характеристических многочленов скрученных линейных
рекуррент над кольцами Галуа**

М. А. Гольтованица

ООО «Центр сертификационных исследований», Москва

Аннотация. Пусть p – простое число, $q = p^r$, $R = \text{GR}(q^d, p^d)$ – кольцо Галуа, $S = \text{GR}(q^{nd}, p^d)$ – его расширение. Рассматриваются скрученные линейные рекуррентные последовательности максимального периода (ЛРП МП) над S . В работе доказано некоммутативное обобщение хорошо известной теоремы Гамильтона – Кэли. С использованием этого результата устанавливается существование корней характеристических многочленов скрученных ЛРП МП в некотором расширении $\mathcal{K}$ кольца $\tilde{S}$. Изучается структура множества корней этих многочленов.

Ключевые слова: некоммутативная теорема Гамильтона – Кэли, скрученные ЛРП, максимальный период, кольцо Галуа

Citation: *Mathematical Aspects of Cryptography*, 2017, v. 8, № 2, pp. 65–76 (Russian)

© Академия криптографии Российской Федерации, 2017 г.

1. Introduction. Main results

In what follows $R = \text{GR}(q^d, p^d)$, where $q = p^r$, is a Galois ring with identity e , $S = \text{GR}(q^{nd}, p^d)$ is a Galois extension of R [1]. It is known that the group $\text{Aut}(S/R)$ of automorphisms of S over R is a cyclic group of order n [2]. Let σ be a generator of this group and $\check{S} = S^\sigma \langle \sigma \rangle$ be a skew group ring of the group $\langle \sigma \rangle$ over the ring S , i. e. the set of formal sums $\psi = \sum_{i=0}^{n-1} s_i \sigma^i$, $s_0, \dots, s_{n-1} \in S$, with natural addition and multiplication, which is defined using distributive property by the identity $\sigma s = \sigma(s)\sigma$ for all $s \in S$.

Each element $\psi \in \check{S}$ defines an endomorphism of the module ${}_R S$ such that $\psi(s) = \sum_{i=0}^{n-1} s_i \sigma^i(s)$ for every $s \in S$. So we have the isomorphisms $\check{S} \cong \text{End}({}_R S) \cong R_{n,n}$, where $R_{n,n}$ is a ring of $n \times n$ matrices over R . The equality $\psi \cdot s = \psi(s)$ defines a structure of left $\check{S}$ -module on S .

The set $S^{(1)}$ of all sequences over S is a left module over the ring of polynomials $\check{S}[x]$, where a product of the sequence $v \in S^{(1)}$ and the polynomial $A(x) = \sum_{j \geq 0} a_j x^j \in \check{S}[x]$ is defined by the equality

$$A(x)v = w \in S^{(1)} : w(i) = \sum_{j \geq 0} a_j (v(i+j)), i \geq 0. \quad (1.1)$$

Following [3] we say that a sequence $v \in S^{(1)}$ is a *skew linear recurring sequence (LRS)* of order $m > 0$ over the ring S if it is an LRS of order m over the module ${}_S S$ [1, 4], i. e. $\Psi(x)v = 0$ for some monic polynomial

$$\Psi(x) = x^m - \psi_{m-1}x^{m-1} - \dots - \psi_0 \in \check{S}[x] \quad (1.2)$$

of degree m , called the *characteristic polynomial of LRS* v . In other words, the sequence v satisfies the law of recursion

$$\forall i \in \mathbb{N}_0 : v(i+m) = \psi_{m-1}v(i+m-1) + \dots + \psi_0 v(i).$$

Let $L_S(\Psi)$ be the set of all LRS v over S with characteristic polynomial Ψ . If $\Psi(x) \in S[x]$, then we say that the sequences from $L_S(\Psi)$ are *classical LRS*. Denote by $T(G)$ the period of the polynomial $G(x) \in S[x]$ and by $T(v)$ the period of the sequence $v \in S^{(1)}$ [2]. We say that a polynomial $A(x) \in \check{S}[x]$ *divides* $B(x) \in \check{S}[x]$ *on the right (respectively, on the left)* (in the ring $\check{S}[x]$), if there exists $C(x) \in \check{S}[x]$ such that $B(x) = C(x)A(x)$ (respectively, $B(x) = A(x)C(x)$).

Proposition 1. *For every polynomial $\Psi(x) \in \check{S}[x]$ of degree m there exists a polynomial $F(x) \in R[x]$ of degree nm such that $L_S(\Psi) \subset L_S(F)$ and for every LRS $v \in L_S(\Psi)$*

$$T(v) \leq T(F) \leq \tau = (q^{nm} - 1)p^{d-1}. \quad (1.3)$$

Moreover, $\Psi(x)$ divides $F(x)$ on the right.

If $T(v) = \tau$, then we say that v is a skew LRS of *maximal period* (MP LRS). A monic polynomial $\Psi(x) \in \check{S}[x]$ of degree m is called a *polynomial of maximal period* (MP-polynomial) if there exists an MP LRS v of order m in the set $L_S(\Psi)$. Systematic research of skew MP LRS over Galois rings had begun in [3, 5, 6], where, in particular, the results allowing to construct large classes of such sequences without brute force method were obtained. Digit sequences of skew MP LRS were investigated in [7, 8]. The results obtained indicate the high linear complexity of such sequences. In [9] a class of skew MP LRS permitting fast implementation was described. So, skew MP LRS and their complications are a promising source of pseudo-random sequences.

The fundamental results on the representation of the classical LRS by means of the trace-function obtained in [1, 2] are based on the following simple but crucial observation: every unitary polynomial $G(x) \in S[x]$ has a root in the extension $S[x] / S[x]G(x)$ of S . However, this observation is not true in the non-commutative case for polynomials $\Psi(x) \in \check{S}[x]$. This is due to the fact that the set $\check{S}[x] / \check{S}[x]\Psi(x)$ is not a ring in general, since the ideal $\check{S}[x]\Psi(x)$ is only one-sided, not two-sided. In this paper for an arbitrary unitary polynomial $\Psi(x) \in \check{S}[x]$ we prove the existence of an extension $\mathcal{K}$ of $\check{S}$ containing a root of $\Psi(x)$. Also we investigate the structure of the set of roots in $\mathcal{K}$ of MP-polynomials over $\check{S}$.

We go on to the main results. In what follows $\mathcal{K} = \check{S}_{m,m}$. For any element $\psi \in \check{S}$ let

$$D(\psi) = \text{diag}(\psi, \dots, \psi) \in \mathcal{K}.$$

To simplify the notation we will assume that $\check{S} \subset \mathcal{K}$, identifying the elements $\psi \in \check{S}$ and $D(\psi) \in \mathcal{K}$. For any polynomial $H(x) = \sum_{j \geq 0} h_j x^j$ over $\check{S}$ and element $\beta \in \mathcal{K}$ we put

$$H(\beta) = \sum_{j \geq 0} D(h_j) \beta^j \in \mathcal{K}. \quad (1.4)$$

If $H(\beta) = 0$, then we say that β is a *root* of $H(x)$. By the Bézout theorem the condition $H(\beta) = 0$ is fulfilled iff $x - \beta$ divides $H(x)$ on the right in the ring $\mathcal{K}[x]$ [10]. An element $\beta \in \mathcal{K}$ is said to be a *root of multiplicity* $k \in \mathbb{N}$ of the polynomial $H(x)$, if $(x - \beta)^k$ divides $H(x)$ on the right and $(x - \beta)^{k+1}$ does not divide $H(x)$ on the right. A root of multiplicity greater than 1 is called a *multiple root*. Denote by $RT_{\mathcal{K}}(H)$ the set of roots in $\mathcal{K}$ of the polynomial $H(x) \in \check{S}[x]$. Further, $\mathcal{K}^*$ denotes the multiplicative group of $\mathcal{K}$. For an element $\gamma \in \mathcal{K}^*$ the order of γ is denoted by $\text{ord } \gamma$ [10]. Our main result is the following theorem.

Theorem 2. Let $\Psi(x) = x^m - \sum_{j=0}^{m-1} \psi_j x^j$ be a polynomial over $\check{S}$. Then $RT_{\mathcal{K}}(\Psi) \neq \emptyset$. Furthermore, if $\Psi(x)$ is an MP-polynomial, then the following statements are true.

1. The cardinality $|RT_{\mathcal{K}}(\Psi)|$ of the set $RT_{\mathcal{K}}(\Psi)$ is divisible by m .
2. If $\gamma \in RT_{\mathcal{K}}(\Psi)$, then $\gamma \in \mathcal{K}^*$ and $\text{ord } \gamma = \tau$.
3. If $\gamma \in RT_{\mathcal{K}}(\Psi)$, then for every nonzero polynomial $H(x)$ over $\check{S}$ of degree less than m the condition $H(\gamma) \neq 0$ is fulfilled.
4. All roots of $\Psi(x)$ in $\mathcal{K}$ are conjugated modulo p , that is

$$\forall \beta, \gamma \in RT_{\mathcal{K}}(\Psi) \exists \mu \in \mathcal{K}^* : \gamma - \mu^{-1} \beta \mu \in p\mathcal{K}.$$

5. $\Psi(x)$ has no multiple roots in $\mathcal{K}$.

Let us note that in the proof of Theorem 2 we obtain the non-commutative generalization of the well-known Hamilton–Cayley theorem (see, for example, [11]), which is interesting by itself. So we give the formulation of this result here.

Let Q be a ring with identity (not necessary commutative). We say that a matrix $A = ||a_{i,j}|| \in Q_{m,m}$ has property $(*)$ if

$$\forall i_1, i_2, j_1, j_2 \in \overline{1, m}, j_1 \neq j_2 : a_{i_1 j_1} a_{i_2 j_2} = a_{i_2 j_2} a_{i_1 j_1}, \quad (*)$$

and has property $(**)$ if

$$\forall i_1, i_2, j_1, j_2 \in \overline{1, m}, i_1 \neq i_2 : a_{i_1 j_1} a_{i_2 j_2} = a_{i_2 j_2} a_{i_1 j_1}. \quad (**)$$

In what follows $\mathcal{P}(\overline{1, m})$ is the set of all permutations of the set $\overline{1, m} = \{1, 2, \dots, m\}$. For any permutation $(i_1 \dots, i_m) \in \mathcal{P}(\overline{1, m})$ we put $\delta(i_1 \dots, i_m)$ to be a *parity function* [10] taking values ± 1 . If $A \in Q_{m,m}$, then by $\text{Det}(A)$ we denote an element of Q which is called the *determinant* of A and may be calculated according to the formula

$$\text{Det}(A) = \sum_{(i_1, \dots, i_m) \in \mathcal{P}(\overline{1, m})} \delta(i_1, \dots, i_m) a_{1i_1} a_{2i_2} \dots a_{mi_m}. \quad (1.5)$$

We say that the determinant of $A \in Q_{m,m}$ is *determined correctly* if A has property $(*)$ or $(**)$. The set of matrices from $Q_{m,m}$ for which the determinant is correctly determined is denoted by $WD_m(Q)$. For matrix $A \in Q_{m,m}$ we define the transposed matrix A^T as usual. In what follows E_k is an identity $k \times k$ matrix of the corresponding matrix ring and $E = E_m$.

Theorem 3. *Let $A \in WD_m(Q)$. Then $Ex - A \in WD_m(Q[x])$ and if $H(x) = \text{Det}(Ex - A)$, then*

1. $H(A^T) = 0$, if A has property $(*)$,
2. $H(A) = 0$, if A has property $(**)$.

2. Proofs

2.1. Proof of Proposition 1

In [3] the existence of a polynomial $F(x) \in R[x]$ of degree mn such that $L_S(\Psi) \subset L_S(F)$ and inequalities (1.3) were proved. The last statement of the Proposition 1 follows from Lemma 4.

Lemma 4. *Let $\Psi(x), \Phi(x) \in \check{S}[x]$ be monic polynomials. Then condition $L_S(\Phi) \subseteq L_S(\Psi)$ is fulfilled iff $\Phi(x)$ divides $\Psi(x)$ on the right.*

Proof. The sufficiency is obvious since $L_S(\Phi)$ is a left $\check{S}[x]$ -module. Let us prove the necessity. Dividing $\Psi(x)$ by $\Phi(x)$ on the right with the remainder in $\check{S}[x]$ we obtain

$$\Psi(x) = H(x)\Phi(x) + G(x), \quad \deg G(x) < \deg \Phi(x) \quad (2.1)$$

for some polynomial $G(x) = \sum_{j \geq 0} G_j x^j \in \check{S}[x]$. Let us show that $G(x) = 0$. For an arbitrary sequence $u \in L_S(\Phi)$ formula (2.1) leads to $G(x)u = 0$. For every LRS $u \in L_S(\Phi)$ with the initial vector of the form $(a, 0, \dots, 0, 0)$, where $a \in S$, using (1.1), we get $G_0(a) = 0$. That is, for every $a \in S$ the endomorphism $G_0 \in \check{S}$ vanishes in a , so $G_0 = 0$. Considering the sequences $u \in L_S(\Phi)$ with initial vectors of the form $(0, a, \dots, 0, 0, 0)$, we get $G_1(a) = 0$ for every $a \in S$. Hence, $G_1 = 0$. Analogously, we can show that every coefficient of $G(x)$ is equal to zero. Lemma 4 is proved. $\square$

2.2. Proof of Theorem 3

Let $Z(Q) = \{s \in Q : rs = sr \ \forall r \in Q\}$ be the center of Q . By $\vec{A}_i, A_j^\downarrow$ we denote the i -th row and the j -th column of $A \in Q_{m,m}$ correspondingly.

Lemma 5. *Let $A \in Q_{m,m}$ has property $(**)$.*

1. *If there are two equal columns in A , then $\text{Det}(A) = 0$.*
2. *If we add to some column of A another column multiplied by an element $r \in Z(Q)$, then the obtained matrix B satisfies the condition $\text{Det}(B) = \text{Det}(A)$.*
3. *If $(i_1, \dots, i_m) \in \mathcal{P}(\overline{1, m})$ and matrix $B \in Q_{m,m}$ satisfies the condition $B_j^\downarrow = A_{i_j}^\downarrow$ for all $j \in \overline{1, m}$, then B has property $(**)$ and $\text{Det}(B) = \delta(i_1, \dots, i_m) \text{Det}(A)$.*
4. *The matrix A^T has property $(*)$ and $\text{Det}(A^T) = \text{Det}(A)$.*

Analogous results may be proved for the rows of matrix A having property $(*)$. The proof of Lemma 5 repeats word for word the proof of the corresponding proposition set out in [10, p. 110] for the case when Q is a commutative ring.

A *submatrix* of matrix A is the matrix obtained from A by deletion of some rows and columns. For $1 \leq i_1 < \dots < i_k \leq m$, $1 \leq j_1 < \dots < j_l \leq m$, where $k, l \in \overline{1, m-1}$, we denote by $A \left(\begin{smallmatrix} i_1 \dots i_k \\ j_1 \dots j_l \end{smallmatrix} \right)$ the matrix obtained from A by deletion of all rows except rows with numbers $i_1, \dots, i_k$ and all columns except columns with numbers $j_1, \dots, j_l$.

We note that if the determinant of matrix A is correctly determined, then all minors of A and their algebraic complements are correctly determined. Let $M_A \left(\begin{smallmatrix} i_1 \dots i_k \\ j_1 \dots j_k \end{smallmatrix} \right)$ denote the determinant of a submatrix $A \left(\begin{smallmatrix} i_1 \dots i_k \\ j_1 \dots j_k \end{smallmatrix} \right)$ and $\overline{CM}_A \left(\begin{smallmatrix} i_1 \dots i_k \\ j_1 \dots j_k \end{smallmatrix} \right)$ denote the algebraic complement of the minor $M_A \left(\begin{smallmatrix} i_1 \dots i_k \\ j_1 \dots j_k \end{smallmatrix} \right)$ [10].

Theorem 6. *If $k \in \overline{1, m-1}$, $1 \leq i_1 < \dots < i_k \leq m$ and $A \in WD_m(Q)$, then*

$$\text{Det}(A) = \sum_{1 \leq j_1 < \dots < j_k \leq m} M_A \left(\begin{smallmatrix} i_1 \dots i_k \\ j_1 \dots j_k \end{smallmatrix} \right) \overline{CM}_A \left(\begin{smallmatrix} i_1 \dots i_k \\ j_1 \dots j_k \end{smallmatrix} \right), \quad (2.2)$$

$$\text{Det}(A) = \sum_{1 \leq j_1 < \dots < j_k \leq m} \overline{CM}_A \left(\begin{smallmatrix} i_1 \dots i_k \\ j_1 \dots j_k \end{smallmatrix} \right) M_A \left(\begin{smallmatrix} i_1 \dots i_k \\ j_1 \dots j_k \end{smallmatrix} \right). \quad (2.3)$$

Corollary 7. *If $k \in \overline{1, m-1}$, $1 \leq j_1 < \dots < j_k \leq m$ and $A \in WD_m(Q)$, then*

$$\text{Det}(A) = \sum_{1 \leq i_1 < \dots < i_k \leq m} M_A \left(\begin{smallmatrix} i_1 \dots i_k \\ j_1 \dots j_k \end{smallmatrix} \right) \overline{CM}_A \left(\begin{smallmatrix} i_1 \dots i_k \\ j_1 \dots j_k \end{smallmatrix} \right), \quad (2.4)$$

$$\text{Det}(A) = \sum_{1 \leq i_1 < \dots < i_k \leq m} \overline{CM}_A \left(\begin{smallmatrix} i_1 \dots i_k \\ j_1 \dots j_k \end{smallmatrix} \right) M_A \left(\begin{smallmatrix} i_1 \dots i_k \\ j_1 \dots j_k \end{smallmatrix} \right). \quad (2.5)$$

The proof of Theorem 6 repeats word for word the proof of the Laplace Theorem set out in [10, p. 119]. Corollary 7 follows from Theorem 6 and the condition $\text{Det}(A) = \text{Det}(A^T)$.

For matrix $A \in Q_{m,m}$ we put $A_{ij} = \overline{CM}_A \left(\begin{smallmatrix} i \\ j \end{smallmatrix} \right)$.

Corollary 8. *Let $A = (a_{ij})_{i,j=1}^m \in WD_m(Q)$, $i, k \in \overline{1, m}$, $i \neq k$.*

1. *If A has property $(*)$, then*

$$\sum_{j=1}^m a_{kj} A_{ij} = \sum_{j=1}^m A_{ij} a_{kj} = 0. \quad (2.6)$$

2. *If A has property $(**)$, then*

$$\sum_{j=1}^m a_{jk} A_{ji} = \sum_{j=1}^m A_{ji} a_{jk} = 0. \quad (2.7)$$

We note that for matrix $A \in Q_{m,m}$ having property $(*)$ the condition (2.7) is not fulfilled in general. The proof of Corollary 8 repeats word for word the proof of the corresponding proposition in [10, p. 122].

Now we prove Theorem 3. Since $Ex \in Z(Q[x])$, it follows that $Ex - A \in WD(Q[x])$. Let $B = (Ex - A) = (b_{ij})_{i,j=1}^m$. We prove item 2 of Theorem 3. Let

$$C = (c_{ij})_{i,j=1}^m, \quad c_{ij} = B_{ji}, \quad D = C \cdot B = (d_{ij})_{i,j=1}^m.$$

Then $d_{ik} = \sum_{j=1}^m c_{ij} b_{jk} = \sum_{j=1}^m B_{ji} b_{jk}$. Making use of (2.5), (2.7), we obtain $d_{ik} = \text{Det}(Ex - A)$ if $i = k$, and $d_{ik} = 0$ if $i \neq k$. So, the equality $C(Ex - A) = E \cdot \text{Det}(Ex - A)$ is fulfilled. Now item 2 follows from the Bézout Theorem [10].

The matrix A^T has property $(**)$, therefore, by item 2 of Theorem 3 for polynomial $F(x) = \text{Det}(Ex - A^T)$ we have $F(A^T) = 0$. To complete the proof it remains to note that

$$F(x) = \text{Det}(Ex - A^T) = \text{Det}((Ex - A)^T) = \text{Det}(Ex - A) = H(x).$$

2.3. Proof of Theorem 2

Let us show that $RT_{\mathcal{K}}(\Psi) \neq \emptyset$. We put

$$\beta = \begin{pmatrix} 0 & e & 0 & \dots & 0 \\ 0 & 0 & e & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & e \\ \psi_0 & \psi_1 & \psi_2 & \dots & \psi_{m-1} \end{pmatrix}. \quad (2.8)$$

Evidently, $Ex - \beta$ has property $(**)$. By means of Lemma 5 we can show that $\text{Det}(Ex - \beta) = \Psi(x)$. Indeed, to compute $\text{Det}(Ex - \beta)$ we add to the j -th column of $Ex - \beta$ the $(j+1)$ -th column multiplied by $x \in Z(\check{S}[x])$, where $j = m-1, m-2, \dots, 1$, and use Theorem 6 for $k = 1$, $i_1 = m$. Using item 1 of Theorem 3 we obtain $\Psi(\beta) = 0$, that is $\beta \in RT_{\mathcal{K}}(\Psi)$.

Now we prove item 1. Let us fix some basis $\vec{\alpha} = (\alpha_0, \alpha_1, \dots, \alpha_{n-1})$ of the free module ${}_R S$ and denote by $a^\downarrow = (a_0, \dots, a_{n-1})^T \in R^{(n)}$ the column of coordinates of element $a \in S$ in the basis $\vec{\alpha}$. Then each linear transformation $\psi \in \check{S}$ of the module ${}_R S$ is defined by some matrix $A(\psi) \in R_{n,n}$ such that $\psi(a)^\downarrow = A(\psi)a^\downarrow$ for any $a \in S$. This matrix is called the *matrix of the linear transformation ψ in the basis $\vec{\alpha}$* . Evidently, the map $\Xi : \mathcal{K} \rightarrow R_{mn,mn}$, defined by the rule

$$\Xi((b_{ij})_{i,j=1}^m) = (A(b_{ij}))_{i,j=1}^m \quad (2.9)$$

is an isomorphism of rings $\mathcal{K}$ and $R_{mn,mn}$. For a matrix $\beta \in \mathcal{K}$ we denote by $\chi_\beta(x)$ the determinant $|E_{mn}x - \Xi(\beta)|$. Let us note that $\chi_\beta(x)$ is a unitary polynomial of degree mn over R which doesn't depend on the choice of basis $\vec{\alpha}$.

In what follows we denote by $\bar{a}$ the image of $a \in S$ under the canonical epimorphism $\rho : S \rightarrow S/pS$ [2]. Every linear transformation $\psi \in \check{S}$ of the module ${}_R S$ induces a linear transformation $\bar{\psi} \in \check{\bar{S}}$ of space $\bar{R}\bar{S}$ by the rule $\forall \alpha \in S : \bar{\psi}(\bar{\alpha}) = \overline{\psi(\alpha)}$. The correspondence $\psi \rightarrow \bar{\psi}$ gives an epimorphism of rings $\check{S} \rightarrow \check{\bar{S}}$ with kernel $p\check{S}$, and the canonical epimorphism $\check{\bar{S}} \cong \check{S}/p\check{S}$ allows to consider $\bar{\psi}$ as an element of the quotient ring $\check{S}/p\check{S}$, that is to say, allows to use the equality $\bar{\psi} = \psi + p\check{S}$. We extend $\rho : S \rightarrow S/pS$ to an epimorphism $\tilde{\rho} : \mathcal{K} \rightarrow \mathcal{K}/p\mathcal{K}$ by the rule $\tilde{\rho}((b_{ij})_{i,j=1}^m) = (\bar{b}_{ij})_{i,j=1}^m$, and the epimorphism $\tilde{\rho}$ to epimorphism $\hat{\rho} : \mathcal{K}[x] \rightarrow \mathcal{K}[x]/p\mathcal{K}[x]$ by the rule $\hat{\rho}(\sum_{j \geq 0} h_j x^j) = \sum_{j \geq 0} \bar{h}_j x^j$, and for all $s \in \mathcal{K}, H(x) \in \mathcal{K}[x]$ we put $\bar{s} = \tilde{\rho}(s)$, $\bar{H}(x) = \hat{\rho}(H(x))$.

By Proposition 1 there exists a polynomial $F(x) \in R[x]$ of degree mn such that $F(x) = \Delta(x)\Psi(x)$ for some $\Delta(x) \in \check{S}[x]$. Since $\Psi(x)$ is an MP-polynomial, it follows that there exists an MP LRS $v \in L_S(\Psi) \subset L_S(F)$ of period $T(v) = \tau$. So, from conditions $T(F) \leq \tau, T(F) \geq T(v)$ we obtain that $T(F) = \tau$, that is $F(x)$ is an MP-polynomial over R .

Lemma 9. *If $\gamma \in RT_{\mathcal{K}}(\Psi)$, then $\bar{\chi}_{\gamma}(x)$ is an irreducible polynomial over the field $\bar{R}$.*

Proof. Since $x - \gamma$ divides $\Psi(x)$ on the right, it follows that $x - \gamma$ divides $F(x)$ on the right. So, $F(\gamma) = 0$ and $\bar{F}(\bar{\gamma}) = \bar{0}$. From the other hand, $\bar{\chi}_{\gamma}(\bar{\gamma}) = \bar{0}$. Therefore, the polynomials $\bar{F}, \bar{\chi}_{\gamma} \in R[x]$ are not coprime. Since $\bar{F}(x)$ is an irreducible polynomial over $\bar{R}$ [2] and $\deg \bar{F} = \deg \bar{\chi}_{\gamma} = mn$, we have $\bar{F}(x) = \bar{\chi}_{\gamma}(x)$. Lemma 9 is proved. $\square$

Using (1.4) it is easy to see that if $\gamma \in RT_{\mathcal{K}}(\Psi)$, then for every $\varphi \in R_{m,m}^*$ we have $\varphi^{-1}\gamma\varphi \in RT_{\mathcal{K}}(\Psi)$. Now, the validity of item 1 follows from Lemma 10.

Lemma 10. *Let*

$$T = \begin{pmatrix} 0 & e & 0 & \dots & 0 \\ 0 & 0 & e & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & e \\ e & 0 & 0 & \dots & 0 \end{pmatrix} \in \mathcal{K}.$$

If $\gamma \in RT_{\mathcal{K}}(\Psi)$, then the elements $T^{-k}\gamma T^k$, $k \in \overline{0, m-1}$, are distinct.

Proof. Assume the contrary. Then $T^k\gamma = \gamma T^k$ for some $k \in \overline{1, m-1}$. Consider the case of coprime k, m . There exist numbers $u, v \in \mathbb{Z}$, $u > 0$ such that $uk + vm = 1$. Multiplying both sides of the equality $T^k\gamma = \gamma T^k$ by $T^{k(u-1)}$ on the left, after transformations we obtain $T^{1-vm}\gamma = \gamma T^{1-vm}$.

Using the equality $T^m = E$, we get $T\gamma = \gamma T$. Therefore, γ is a circulant matrix, that is,

$$\gamma = \begin{pmatrix} b_0 & b_1 & b_2 & \dots & b_{m-1} \\ b_{m-1} & b_0 & b_1 & \dots & b_{m-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ b_1 & b_2 & b_3 & \dots & b_0 \end{pmatrix} \quad \text{for some } b_0, \dots, b_{m-1} \in \check{S}.$$

We claim that $\overline{\chi_\gamma}(x)$ is reducible over $\overline{R}$. Let $B_j = A(b_j) \in R_{n,n}$ for every $j \in \overline{0, m-1}$. Then

$$\begin{aligned} \chi_\gamma(x) &= \begin{vmatrix} E_n x - B_0 & -B_1 & \dots & -B_{m-1} \\ -B_{m-1} & E_n x - B_0 & \dots & -B_{m-2} \\ \vdots & \vdots & \ddots & \vdots \\ -B_1 & -B_2 & \dots & E_n x - B_0 \end{vmatrix} = \begin{vmatrix} E_n x - \sum_{j=0}^{m-1} B_j & -B_1 & \dots & -B_{m-1} \\ E_n x - \sum_{j=0}^{m-1} B_j & E_n x - B_0 & \dots & -B_{m-2} \\ \vdots & \vdots & \ddots & \vdots \\ E_n x - \sum_{j=0}^{m-1} B_j & -B_2 & \dots & E_n x - B_0 \end{vmatrix} = \\ &= \begin{vmatrix} E_n x - \sum_{j=0}^{m-1} B_j & -B_1 & \dots & -B_{m-1} \\ 0 & E_n x - B_0 + B_1 & \dots & -B_{m-2} + B_{m-1} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & -B_2 + B_1 & \dots & E_n x - B_0 + B_{m-1} \end{vmatrix}. \end{aligned}$$

So, $\overline{\chi_\gamma}(x)$ is divisible by the monic polynomial $|\overline{E_n x - \sum_{j=0}^{m-1} B_j}|$ of degree n . This contradicts Lemma 9.

Now let the greatest common divisor (k, m) of k and m be equal to $s > 1$. As in the case $(k, m) = 1$ from the equality $T^k \gamma = \gamma T^k$ we obtain $T^s \gamma = \gamma T^s$. Applying the isomorphism Ξ to the both parts of the last equality, we get $\Xi(T^s) \Xi(\gamma) = \Xi(\gamma) \Xi(T^s)$. Let $t = ns$. Then for some matrices $C_0, C_1, \dots, C_{\frac{m}{s}-1} \in R_{ns, ns}$ we have

$$\Xi(T^s) = \begin{pmatrix} 0 & E_t & 0 & \dots & 0 \\ 0 & 0 & E_t & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & E_t \\ E_t & 0 & 0 & \dots & 0 \end{pmatrix}, \quad \Xi(\gamma) = \begin{pmatrix} C_0 & C_1 & C_2 & \dots & C_{\frac{m}{s}-1} \\ C_{\frac{m}{s}-1} & C_0 & C_1 & \dots & C_{\frac{m}{s}-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ C_1 & C_2 & C_3 & \dots & C_0 \end{pmatrix}.$$

As in the case $(k, m) = 1$ we prove that $|E_{mn} x - \Xi(\gamma)|$ is a polynomial reducible modulo p . This contradicts Lemma 9 and yields the proof of Lemma 10. $\square$

Now we prove item 2 of Theorem 2. Let $\gamma \in RT_{\mathcal{K}}(\Psi)$. Since $(x - \gamma)$ divides the reversible polynomial $F(x)$ on the right, we have $\gamma \in \mathcal{K}^*$ [10]. Let us prove that $\text{ord } \gamma = \tau$. Assume the contrary. Then there exists $0 < t < \tau$ such that $x - \gamma$ divides $x^t - e$ in the ring $\mathcal{K}[x]$. Dividing with the remainder $x^t - e$ by $F(x)$ in $R[x]$ we obtain

$$x^t - e = H(x) F(x) + \Lambda(x), \quad \deg \Lambda < mn. \quad (2.10)$$

We claim that $\Lambda(x) = 0$. Assume the contrary. Then we have $\Lambda(x) = p^k \Lambda_1(x)$, where $k \in \overline{0, d-1}$, $\Lambda_1(x) \in R[x]$ is a polynomial uniquely determined modulo p^{d-k} , $\overline{\Lambda_1}(x) \neq \overline{0}$. From condition (2.10) it follows that $\overline{\Lambda_1}(\overline{\gamma}) = \overline{0}$. Since $\overline{F}(x)$ is irreducible over $\overline{R}$, it follows that $\overline{F}(x)$ and $\overline{\Lambda_1}(x)$ are coprime. Now if we recall that $x - \overline{\gamma}$ divides polynomials $\overline{F}(x)$ and $\overline{\Lambda_1}(x)$ on the right, we get a contradiction. So, $\Lambda(x) = 0$.

Then from the equality (2.10) it follows that $F(x)$ is not an MP-polynomial. This is a contradiction. Item 2 of Theorem 2 is proved.

Lemma 11. *Let S be a field and $\Psi(x) = x^m - \sum_{j=0}^{m-1} \psi_j x^j \in \check{S}[x]$ be an MP-polynomial, then the ideal $J = \check{S}[x]\Psi(x)$ is a maximal left ideal of the ring $\check{S}[x]$.*

Proof. Let $\Phi(x) \in \check{S}[x]$ and $\Phi(x) \notin J$. We claim that if a left ideal includes J and $\Phi(x)$, then it is equal to $\check{S}[x]$. Dividing $\Phi(x)$ by $\Psi(x)$ on the right in the ring $\check{S}[x]$ we obtain

$$\Phi(x) = H(x)\Psi(x) + \Lambda(x), \deg \Lambda(x) < m, \Lambda(x) \neq 0, \quad (2.11)$$

where $\Lambda(x)$ has the form $\Lambda(x) = \sum_{j=0}^l \lambda_j x^j$, $\lambda_l \neq 0$.

Consider two cases. If $\lambda_l \in \check{S}^*$, then the unitary polynomial $\tilde{\Lambda}(x) = \lambda_l^{-1} \Lambda(x)$ of degree $l < m$ belongs to the ideal J . By Proposition 1 there exist polynomials $G_{\tilde{\Lambda}}(x), G_{\Psi}(x) \in R[x]$ of degrees ln and mn , correspondingly, which are divisible on the right by $\tilde{\Lambda}(x)$ and $\Psi(x)$, correspondingly. So, $G_{\tilde{\Lambda}}(x), G_{\Psi}(x) \in J$. Since $\Psi(x)$ is an MP-polynomial over $\check{S}$, it follows that $G_{\Psi}(x)$ is an MP-polynomial over R . Thus, we have that $G_{\tilde{\Lambda}}(x)$ and $G_{\Psi}(x)$ are coprime, since $\deg G_{\tilde{\Lambda}}(x) < \deg G_{\Psi}(x)$ and $G_{\Psi}(x)$ is irreducible over R . So, there exist polynomials $D_1(x), D_2(x) \in R[x]$ such that

$$D_1(x)G_{\Psi}(x) + D_2(x)G_{\tilde{\Lambda}}(x) = e \in J.$$

Therefore, $J = \check{S}[x]$.

Consider the case $\lambda_l \notin \check{S}^*$. We claim that there exists an element $\varphi \in \check{S}$ such that $e - \varphi \cdot \lambda_l \notin \check{S}^*$. Let $A = A(\lambda_l)$. It is sufficient to show that there exists a matrix $B \in R_{n,n}$ such that $E - BA \notin R_{n,n}^*$. There exists a matrix $C \in R_{n,n}^*$ such that $C \cdot A$ is a reduced row-echelon matrix form of A [10]. Evidently, $CA \neq 0$, since $A \neq 0$. If there exist a nonzero element on the main diagonal of CA , then we can put $B = C$. Suppose that all elements on the main diagonal of CA are zeros. Let D be a matrix obtained from CA by permutation of the last nonzero row so that there exists an identity e on the main diagonal of D . There exists a matrix $P \in R_{n,n}^*$ such that $D = PCA$. It is easily to see that $E - D \notin R_{n,n}^*$. So, we can put $B = PC$.

Since J is a left ideal of $\check{S}[x]$, we have $x^{m-l}\varphi\Lambda(x) \in J$ and

$$H(x) = (e - \varphi \cdot \lambda_l)\Psi(x) + x^{m-l}\varphi \cdot \Lambda(x) \in J. \quad (2.12)$$

Let us note that $H(x) \in \check{S}[x]$ is an unitary polynomial of degree $\deg H = m$, $H(0) = (e - \varphi \cdot \lambda_l)\psi_0 \notin \check{S}^*$. By Proposition 1 there exists an unitary polynomial $G_H(x) \in R[x]$ of degree mn such that $H(x)$ divides $G_H(x)$ on the right. So, $G_H(x)$ is not a reversible polynomial. Therefore $G_\Psi(x)$ and $G_H(x)$ are coprime, that is there exist polynomials $U(x), V(x) \in R[x]$ such that

$$U(x)G_\Psi(x) + V(x)G_H(x) = e \in J,$$

so $J = \check{S}[x]$. Lemma 11 is proved. $\square$

Now we prove item 3 of Theorem 2. Assume the contrary. Let $\Phi(\gamma) = 0$ for some nonzero polynomial $\Phi(x) \in \check{S}[x]$ such that $\deg \Phi(x) < m$. Then there exists a polynomial $\Phi_1(x) \in \check{S}[x]$ uniquely determined modulo p^{d-k} with the property $\Phi(x) = p^k \Phi_1(x)$ and $\deg \Phi_1(x) = \deg \Phi$, $\overline{\Phi_1(x)} \neq \overline{0}$, $\overline{\Phi_1(\gamma)} = \overline{0}$. Thus, polynomials $\overline{\Psi(x)}$, $\overline{\Phi_1(x)}$ are not coprime. Then by Lemma 11 the polynomial $\overline{\Psi(x)}$ divides $\overline{\Phi_1(x)}$ on the right. But $\overline{\Psi(x)}$ is an unitary polynomial of degree $m > \deg \overline{\Phi_1(x)}$. This is contradiction. Item 3 of Theorem 2 is proved.

Now we prove item 4. It is sufficient to show that the matrices $\overline{\Xi(\beta)}, \overline{\Xi(\gamma)} \in \overline{R}_{mn, mn}$ are similar. In the proof of Lemma 9 it was shown that if $\gamma \in RT_{\mathcal{K}}$, then $\overline{\chi_{\Xi(\gamma)}(x)} = \overline{F(x)}$. Since $\overline{F(x)}$ is an irreducible polynomial over $\overline{R}$ it follows that $\overline{\Xi(\beta)}, \overline{\Xi(\gamma)}$ are similar [11].

Now we prove item 5. Assume the contrary. Let $\gamma \in RT_{\mathcal{K}}(\Psi)$ be a root of $\Psi(x)$ of multiplicity $k \geq 2$. Then using equality $F(x) = \Delta(x)\Psi(x)$, we obtain $F(x) = H(x)(x - \gamma)(x - \gamma)$ for some polynomial $H(x) \in \mathcal{K}[x]$. For polynomial $A(x) = \sum_{j \geq 0} a_j x^j$ over $\mathcal{K}$ denote by $A'(x)$ its derivative, which is defined by the rule $A'(x) = \sum_{j \geq 1} j a_j x^{j-1}$.

Lemma 12. *For every $A(x), B(x) \in \mathcal{K}[x]$ the following equation is fulfilled $(A(x)B(x))' = A'(x)B(x) + A(x)B'(x)$*

Proof. The proof is straightforward. $\square$

By Lemma 12 we have

$$F'(x) = (H(x)(x - \gamma)(x - \gamma))' = (H(x)(x - \gamma))'(x - \gamma) + H(x)(x - \gamma).$$

So, $x - \gamma$ divides on the right $F(x)$ and $F'(x)$. Since $F(x)$ is an MP-polynomial, it follows that $F(x)$ and $F'(x)$ are coprime [2]. Therefore, there exist $U(x), V(x) \in R[x]$ such that $UF + VF' = e$. So, $x - \gamma$ divides on the right e . This is contradiction.

Theorem 2 is completely proved. $\square$

3. Acknowledgments

The author is grateful to professor A. A. Nechaev for helpful discussions and valuable remarks.

References

- [1] Kurakin V. L., Kuzmin A. S., Mikhalev A. V., Nechaev A. A., “Linear recurring sequences over rings and modules”, *J. Math. Sci.*, **76**:6 (1995), 2793–2915.
- [2] Nechaev A. A., “Kerdock code in a cyclic form”, *Discrete Math. Appl.*, **1**:4 (1991), 365–384.
- [3] Goltvanitsa M. A., Nechaev A. A., Zaitsev S. N., “Skew linear recurring sequences of maximal period over Galois rings”, *J. Math. Sci.*, **187**:2 (2012), 115–128.
- [4] Kurakin V. L., Mikhalev A. V., Nechaev A. A., Tsypyshev V. N., “Linear and polylinear recurring sequences over Abelian groups and modules”, *J. Math. Sci.*, **102**:6 (2000), 4598–4626.
- [5] Goltvanitsa M. A., Nechaev A. A., Zaitsev S. N., “Skew LRS of maximal period over Galois rings”, *Mathematical Aspects of Cryptography*, **4**:2 (2013), 59–72.
- [6] Goltvanitsa M. A., “A construction of skew LRS of maximal period over finite fields based on the defining tuples of factors”, *Mathematical Aspects of Cryptography*, **5**:2 (2014), 37–46.
- [7] Goltvanitsa M. A., “Digit sequences of skew linear recurrences of maximal period over Galois rings”, *Mathematical Aspects of Cryptography*, **6**:2 (2015), 189–197.
- [8] Goltvanitsa M. A., “The first digit sequence of skew linear recurrence of maximal period over Galois ring”, *Mathematical Aspects of Cryptography*, **7**:3 (2016), 5–18.
- [9] Goltvanitsa M. A., “About one class of skew linear recurrences of maximal period over Galois rings”, *Vysoko dostupnye systemy*, **11**:3 (2015), 28–48 (in Russian).
- [10] Glukhov M. M., Elizarov V. P., Nechaev A. A., *Algebra, I*, M.: Gelios ARV, 2003 (in Russian), 336 pp.
- [11] Glukhov M. M., Elizarov V. P., Nechaev A. A., *Algebra, II*, M.: Gelios ARV, 2003 (in Russian), 416 pp.