УДК 512.554

Minimal Polynomials in Finite Semifields

Olga V. Kravtsova*
Institute of Mathematics and Computer Sciences
Siberian Federal University
Svobodny, 79, Krasnoyarsk, 660041
Russia

Received 13.2.2018, received in revised form 23.04.2018, accepted 20.06.2018

We consider the classical notion of a minimal polynomial and apply it to investigations in finite semifields. A proper finite semifield has non-associative multiplication, that leads to a number of anomalous properties of one-side-ordered minimal polynomials. The interrelation between the minimal polynomial of an element and the minimal polynomial of its matrix from the spread set is described and illustrated by some semifields of orders 16, 32 and 64.

Keywords: semifield, right-ordered degree, right-ordered minimal polynomial.
DOI: 10.17516/1997-1397-2018-11-5-588-596

Introduction

A finite semifield is an algebraic structure generalizing the notion of a finite field. Unlike any field, the multiplicative law in a proper semifield is non-associative. The absence of associativity even in a finite semifield leads to it having a number of specific properties, which are poorly studied.

The investigation of finite semifelds originated as a classical part of algebra in the works of Dickson [1] and Albert [2] at the start of the 20th century. The complete review is presented by Johnson at al. in Handbook [3]. At present the sphere of semifield studies is concerned with the calculation of element orders and automorphism groups [4]. The present paper is devoted to the application of classical algebraic concepts, such as minimal polynomials, in the specific area of finite semifields. We describe the interrelation between one-side-ordered minimal polynomials of the elements and minimal polynomials of its matrix from the spread sets of a semifield and the opposite semifield. This interrelation is illustrated by the examples of some semifields of orders 16, 32, 64. The research methods are closely related to linear spaces and spread sets, they combine both a theoretical and a computer approaches.

1. Definitions

According to [5], a *semifield* is a set W with two binary algebraic operations $+$ and $*$ such that:

1) $\langle W, + \rangle$ is an abelian group with neutral element 0;

2) $\langle W^*, * \rangle$ is a loop ($W^* = W \setminus \{0\}$);

*ol71@bk.ru

3) both distributivity laws hold, $a*(b+c)=a*b+a*c$, $(b+c)*a=b*a+c*a$ for all $a,b,c\in W$.

A semifield W contains subsets N_r, N_m, N_l which are called *right, middle* and *left nuclei* respectively:

$$N_r=\{n\in W\mid (a*b)*n=a*(b*n)\ \forall a,b\in W\},$$
$$N_m=\{n\in W\mid (a*n)*b=a*(n*b)\ \forall a,b\in W\},$$
$$N_l=\{n\in W\mid n*(a*b)=n*(a*b)\ \forall a,b\in W\}.$$

The intersection $N=N_l\cap N_m\cap N_r$ is called the *nucleus* of semifield W and its subset

$$Z=\{z\in N\mid z*a=a*z\ \forall a\in W\}$$

is the *center* of W. The center and all nuclei of a finite semifield are its subfields and the semifield is a linear space over any of them. Therefore, the order of finite semifield is the prime number degree p^n.

Any finite semifield may be constructed on the basis of a linear space over an appropriate finite field. Let W be a n-dimensional linear space over the field $\mathbb{F}_p$, θ is a bijective mapping from W to $GL_n(p)\cup\{0\}$ such that:

1) $\theta(u+v)=\theta(u)+\theta(v)\ \forall u,v\in W$,

2) $\theta(0,0,\dots,0)=0$ is zero matrix, $\theta(1,0,\dots,0)=E$ is identity matrix.

Define the multiplication law on W by the rule

$$u*v=u\theta(v),\qquad u,v\in W,$$

then $\langle W,+,*\rangle$ is a semifield of order p^n. Denote it $W=W(n,p,\theta)$. The multiplicative neutral element $\theta^{-1}(E)$ is denoted as e. The image $R=\{\theta(u)\mid u\in W\}$ is called a *spread set* (see [5]).

Note that the center Z of a semifield is usually used as a basic field $\mathbb{F}_{p^k}$ to construct a semifield. Nevertheless, it is more convenient to consider a linear space W and a spread set R over the prime subfield $\mathbb{F}_p$.

The product of m multipliers is said to be *m-th degree* of a fixed element $v\in W^*$, if every multiplier coincides with v. The smallest integer $m\geqslant 1$ such that there exists the m-th degree of v, which is equal to the identity, is called *the order of v* and denoted by $|v|$. The set of orders of all elements is called the *spectrum of multiplicative loop W^**.

Similarly, using the right-ordered and the left-ordered m-th degrees

$$v^{m)}=v^{m-1)}*v,\quad v^{(m}=v*v^{(m-1},\quad v^{1)}=v=v^{(1},$$

we define the right order $|v|_r$ and the left order $|v|_l$ of v and *the right and the left spectra* of W^* respectively.

Remind now the classical definition of a minimal polynomial for an element in a finite field and the main properties of minimal polynomials, according to [6].

Let $\mathbb{F}_{q^n}$ be a field of order q^n and $a\in\mathbb{F}_{q^n}$. The monic polynomial $M(x)\in\mathbb{F}_q[x]$ of a minimal degree such that $M(a)=0$ is called the *minimal polynomial* of an element a over $\mathbb{F}_q$.

Theorem 1.1. *Let $a\in\mathbb{F}_{q^n}$, a is of d-th degree over $\mathbb{F}_q$ and $M(x)$ is a minimal polynomial of the element a over $\mathbb{F}_q$.*

(i) $M(x)$ is irreducible over $\mathbb{F}_q$ and $\deg M=d$ *is a factor of n.*

(ii) For any polynomial $f\in\mathbb{F}_q[x]$ the equality $f(a)=0$ holds iff $M|f$.

(iii) If a is primitive element, then $\deg M=n$.

(iv) The roots of $M(x)$ are exactly a, $a^q, \ldots, a^{q^{d-1}}$, and $M(x)$ is a minimal polynomial for these elements.

(v) If $f(x)$ is monic irreducible polynomial from $\mathbb{F}_q[x]$ and $f(a) = 0$, then $f = M$.

(vi) $M(x)$ is a factor of $x^{q^d} - x$ and of $x^{q^n} - x$.

We attempt to apply classical notion of a minimal polynomial to study finite semifields. Consider the polynomial $f(x) \in \mathbb{F}_p[x]$,

$$f(x) = c_m x^m + c_{m-1}x^{m-1} + \cdots + c_2 x^2 + c_1 x + c_0, \quad c_i \in \mathbb{F}_p,\ i = 0, 1, \ldots, m.$$

For any element $a \in W$, define the *right-* and the *left-ordered value* of a polynomial $f(x)$:

$$f(a)) = c_m a^{m)} + c_{m-1}a^{m-1)} + \cdots + c_2 a^2 + c_1 a + c_0 e,$$
$$f((a) = c_m a^{(m} + c_{m-1}a^{(m-1} + \cdots + c_2 a^2 + c_1 a + c_0 e.$$

Here $a^{s)}$ and $a^{(s}$ are the right- and the left-ordered degrees of an element a. The product of the coefficient $c \in \mathbb{F}_p$ to element $a \in W$ equals to the sum of c items coinciding with a, for $c \neq 0$, and equals zero for $c = 0$.

Example. Let $f(x) = x^3 + x^2 + x + 1 \in \mathbb{F}_2[x]$, $a \in W(n, 2, \theta)$, then

$$f(a)) = a^{3)} + a^2 + a + e = a^2 * a + a^2 + a + e = a\theta(a)\theta(a) + a\theta(a) + a + e,$$
$$f((a) = a^{(3} + a^2 + a + e = a * a^2 + a^2 + a + e = a\theta(a\theta(a)) + a\theta(a) + a + e.$$

Evidently, in the case of degree $\leqslant 2$ the right- and the left-ordered values $f(a))$ and $f((a)$ are equal. Note that $(fg)(a))$ is not equal to $f(a)) * g(a))$ in general. If $f(a)) = 0$ then for any polynomial $g(x)$ holds $(fg)(a)) = 0$, but inverse is not true: an equality $(fg)(a)) = 0$ does not imply $f(a)) = 0$ or $g(a)) = 0$ (similarly for left-ordered values).

The *right-ordered minimal polynomial* of an element $a \in W(n, p, \theta)$ is said to be a monic polynomial $\mu_a^r(x) \in \mathbb{F}_p[x]$ of minimal degree such that $\mu_a^r(a)) = 0$. The *left-ordered minimal polynomial* $\mu_a^l(x)$ is defined likewise. Here we consider polynomials only over the prime subfield $\mathbb{F}_p$, but it is possible to apply the results to the case of the center Z of a semifield as a basic field.

2. Properties

Some properties of one-side-ordered minimal polynomials in a finite semifield correspond to similar results in finite fields.

Lemma 1. *If $a \neq 0$ then $m_a^r(0)) \neq 0$, $m_a^l((0) \neq 0$, i.e. x is not a factor of $m_a^r(x)$ and $m_a^l(x)$.*

Proof. If $m_a^r(x) = c_0 x^m + \cdots + c_{m-1}x = (c_0 x^{m-1} + \cdots + c_{m-1}) \cdot x$, then

$$m_a^r(a)) = (c_0 a^{m-1)} + \cdots + c_{m-1}) * a = 0, \qquad c_0 a^{m-1)} + \cdots + c_{m-1} = 0,$$

that contradicts the definition of a right-ordered minimal polynomial. For the left-ordered minimal polynomial the result can be obtained similarly. □

Theorem 2.2. *For any polynomial $f(x) \in \mathbb{F}_p[x]$ holds:*

(i) $f(a)) = 0$ iff $m_a^r(x) | f(x)$;

(ii) $f((a) = 0$ iff $m_a^l(x) | f(x)$.

Proof for the right-ordered polynomial. If $g(x) = m_a^r(x) \cdot x$ then $g(a)) = m_a^r(a)) * a = 0 * a = 0$, so for

$$f(x) = m_a^r(x) \cdot (d_0 x^k + \cdots + d_k) \in \mathbb{F}_p[x]$$

holds $f(a)) = 0$. And inverse, let $f(a)) = 0$, make division with residual:

$$f(x) = m_a^r(x) q(x) + r(x),$$

where $r(x)$ is zero polynomial or $\deg r < \deg m_a^r$. Then

$$f(a)) = (m_a^r \cdot q)(a)) + r(a)) = 0 + r(a)) = 0,$$

and minimality of $m_a^r(x)$ implies $r(x) = 0$. □

Evidently, this result leads the next theorem.

Theorem 2.3. *The right-(left-)ordered minimal polynomial of an element a is a factor of the polynomial $x^k - 1$, where k is right (left) order of a, $k = |a|_r$ ($k = |a|_l$).*

The right- or the left-ordered polynomial of an element $a \in W$ is not necessarily irreducible. Next lemma is a corollary from Theorem 2.1.

Lemma 2. *If $K \simeq \mathbb{F}_{p^m}$ is a subfield of a semifield W then for $a \in K$ right-ordered polynomial of a equals to the left one, $m_a^r(x) = m_a^l(x)$, it is an irreducible polynomial of order $s|m$.*

The inverse result is not true: if a one-side-ordered polynomial is irreducible, then the element does not necessarily lie in a subfield (see Section 4).

Lemma 3. *If φ is an automorphism of a semifield W then a and a^φ have the same right- and left-ordered minimal polynomials,*

$$m_{a^\varphi}^r(x) = m_a^r(x), \qquad m_{a^\varphi}^l(x) = m_a^l(x).$$

This result seems evident but note that the automorphism group of a finite field $\mathbb{F}_{p^n}$ is a cyclic group generated by the automorphism $x \to x^p$. In the case of a semifield of order p^n this mapping is not an automorphism in general and $m_{a^p}^r(x)$ may differ from $m_a^r(x)$.

Compare one-side-ordered polynomials of an element $a \in W = W(n, p, \theta)$ to minimal polynomial (in a classical sense) of a matrix from the spread set, $A = \theta(a)$.

Lemma 4. *For any polynomial $f(x) \in \mathbb{F}_p[x]$, $f(0) \neq 0$, any element $a \in W(n, p, \theta)$ and correspondent matrix $A = \theta(a)$ the equality $f(A) = 0$ implies $f(a)) = 0$.*

Proof. Let $f(A) = 0$. $f(0) \neq 0$, so we can assume $c_0 = -1$ without loss of generality and

$$c_m A^m + c_{m-1} A^{m-1} + \cdots + c_2 A^2 + c_1 A = E,$$

$$A(c_m A^{m-1} + c_{m-1} A^{m-2} + \cdots + c_2 A + c_1 E) = E.$$

Multiply the left and the right parts of equality by the identity of a semifield W:

$$eA(c_m A^{m-1} + c_{m-1} A^{m-2} + \cdots + c_2 A + c_1 E) = eE,$$

$$a(c_m A^{m-1} + c_{m-1} A^{m-2} + \cdots + c_2 A + c_1 E) = eE,$$

$$c_m a^{m)} + c_{m-1} a^{m-1)} + \cdots + c_2 a^2 + c_1 a = e$$

and $f(a)) = 0$. □

Note that inverse is not true in general, i. e. equality $f(a)) = 0$ does not imply $f(A) = 0$. Indeed, rewrite the equality

$$a(c_m A^{m-1} + c_{m-1}A^{m-2} + \cdots + c_2 A + c_1 E) = eE$$

in the form $aB = e$, then $a = eB^{-1}$. As $a = eA = e\,\theta(a)$ then $e(B^{-1} - A) = 0$ and it implies only that the first row of A equals to the first row of B^{-1}, but not the equality of matrices $A = B^{-1}$.

The similar result for the left-ordered polynomial is not true in general (a counter-example can be seen in Section 4).

The condition $f(0) \neq 0$ in the text of the lemma is not essential because the absence of zero divisors in a semifield.

Therefore we have the correspondence between minimal polynomials.

Theorem 2.4. *If $a \in W(n, p, \theta)$ and $A = \theta(a)$, then the right-ordered minimal polynomial of an element a is factor of the minimal polynomial of the matrix A.*

The bijective mapping φ from the semifield $\langle W, * \rangle$ to the semifield $\langle V, \circ \rangle$ is an *anti-isomorphism* if

$$(x * y)^\varphi = y^\varphi \circ x^\varphi \quad \forall x, y \in W.$$

Lemma 5. *If φ is an anti-isomorphism from W to V, then for any element $a \in W^*$ the right-ordered minimal polynomial $m_a^r(x)$ equals to the left-ordered minimal polynomial of the element $a^\varphi \in V$.*

Corollary 1. *If the semifield W is anti-isomorphic to itself then for any element $a \in W^*$ the right-ordered-minimal polynomial coincides with the left-ordered one.*

Lemma 6. *If φ is an anti-isomorphism from $W = W(n, p, \theta)$ to $V = V(n, p, \tau)$ then for any $a \in W^*$ the left-ordered minimal polynomial $m_a^l(x)$ is a factor of the minimal polynomial of the matrix $\tau(a^\varphi)$.*

3. Example

Illustrate previous results by the example of a semifield of order 16. It is known that there exist 23 pairwise non-isomorphic semifields of order 16 [4]. Let us consider one of them that is represented by a 4-dimensional linear space.

Let W be a 4-dimensional linear space over $\mathbb{F}_2$,

$$W = \{x = (x_1, x_2, x_3, x_4) \mid x_i \in \mathbb{F}_2,\ i = 1, \ldots, 4\}.$$

We define the map $\theta : W \to GL_4(2) \cup \{0\}$ by the rule

$$\theta(x_1, x_2, x_3, x_4) = x_1 E + x_2 \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix} + x_3 \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} + x_4 \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}.$$

Then, $R = \{\theta(x) \mid x \in W\}$ is a spread set and $\langle W, +, * \rangle$ is a semifield of order 16 where $x * y = x \cdot \theta(y)$. The vector $e = (1, 0, 0, 0)$ is an identity in this semifield.

Except for direct search of variants, we can use the following method to construct a one-side-ordered minimal polynomial of elements. Let e_1, $e_2, \ldots,$ e_n be the base of a linear space $W = W(n, p, \theta)$ over $\mathbb{F}_p$. Write down the right-ordered degrees e, a, a^2, $a^{3)}, \ldots,$ $a^{n)}$ as linear combinations of basic vectors:

$$a^{i)} = \sum_{j=1}^{n} \alpha_{ij} e_j,$$

here $\alpha_{ij} \in \mathbb{F}_p$, $i = 0, 1, \ldots, n$, $j = 1, \ldots, n$. Then make a matrix (α_{ij}) and lead it to a trapezoid form. The zero row corresponds to a linear combination of right-ordered degrees of a which equals to zero, i. e. to the right-ordered minimal polynomial of a.

For example, let's consider $e = (1, 0, 0, 0)$, $b = (0, 0, 1, 1)$, $b^2 = (1, 1, 0, 1)$, $b^{3)} = (0, 0, 1, 0)$, $b^{4)} = (0, 1, 0, 1)$ in the semifield $W = W(4, 2, \theta)$, then

$$\begin{pmatrix} 1 & 0 & 0 & 0 & e \\ 0 & 0 & 1 & 1 & b \\ 1 & 1 & 0 & 1 & b^2 \\ 0 & 0 & 1 & 0 & b^{3)} \\ 0 & 1 & 0 & 1 & b^{4)} \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & 0 & e \\ 0 & 1 & 0 & 1 & b^2 + e \\ 0 & 0 & 1 & 1 & b \\ 0 & 0 & 0 & 1 & b^{3)} + b \\ 0 & 0 & 0 & 0 & b^{4)} + b^2 + e \end{pmatrix}.$$

So, the right-ordered minimal polynomial of the element b is $m_b^r(x) = x^4 + x^2 + 1 = (x^2 + x + 1)^2$. Note that it is not irreducible. All one-side-ordered polynomials and all one-sided orders for $a \in W \setminus \{0, e\}$ are presented in Tab. 1. The last column shows the minimal polynomial of the matrix $A = \theta(a)$.

Table 1. Information on $W(4, 2, \theta)$

a	$\lvert a\rvert_l$	$\lvert a\rvert_r$	$\lvert a\rvert$	$m_a^l(x)$	$m_a^r(x)$	$m_A(x)$
$(0,0,1,0)$	3	3	3	x^2+x+1	x^2+x+1	$(x^2+x+1)^2$
$(1,0,1,0)$	3	3	3	x^2+x+1	x^2+x+1	$(x^2+x+1)^2$
$(0,1,0,1)$	3	3	3	x^2+x+1	x^2+x+1	x^2+x+1
$(1,1,0,1)$	3	3	3	x^2+x+1	x^2+x+1	x^2+x+1
$(0,0,0,1)$	5	6	4	$x^4+x^3+x^2+x+1$	$(x^2+x+1)^2$	$(x^2+x+1)^2$
$(1,0,1,1)$	5	6	4	$x^4+x^3+x^2+x+1$	$(x^2+x+1)^2$	$(x^2+x+1)^2$
$(0,1,0,0)$	5	15	5	$x^4+x^3+x^2+x+1$	x^4+x+1	x^4+x+1
$(0,1,1,0)$	5	15	5	$x^4+x^3+x^2+x+1$	x^4+x+1	x^4+x+1
$(0,1,1,1)$	6	15	6	$(x^2+x+1)^2$	x^4+x+1	x^4+x+1
$(1,1,1,1)$	6	15	6	$(x^2+x+1)^2$	x^4+x+1	x^4+x+1
$(0,0,1,1)$	15	6	5	x^4+x^3+1	$(x^2+x+1)^2$	$(x^2+x+1)^2$
$(1,0,0,1)$	15	6	5	x^4+x^3+1	$(x^2+x+1)^2$	$(x^2+x+1)^2$
$(1,1,0,0)$	15	15	5	x^4+x^3+1	x^4+x+1	x^4+x+1
$(1,1,1,0)$	15	15	5	x^4+x^3+1	x^4+x+1	x^4+x+1

The elements of order 3, together with 0 and e, form two subfields of order 4. The right- and the left-ordered minimal polynomials of these elements are equal to the irreducible polynomial $x^2 + x + 1$. Note that we have the polynomial of degree 2 that has four distinct roots. Similarly, the polynomial $x^4 + x + 1$ has 6 roots in W. In all cases, the right-ordered minimal polynomial of an element is a factor of the matrix minimal polynomial. Nevertheless, the left-ordered minimal polynomial is a factor of the matrix polynomial only for elements from the subfields.

The semifield $W(4,2,\theta)$ admits unique nontrivial automorphism φ of order 2,

$$\varphi : (x_1,x_2,x_3,x_4) \to (x_1,x_2,x_3,x_4) \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix}.$$

One can prove that for any element $a \in W$ the right- and left-ordered minimal polynomials of its image a^φ coincide with $m_a^r(x)$ and $m_a^l(x)$ respectively. For example, $(0,0,0,1)^\varphi = (1,0,1,1)$ (see Tab. 1).

The mapping $x \to x^2$ is not injective on W (compare with field $\mathbb{F}_{16}$). Indeed, $(0,0,0,1)^2 = = (0,1,0,1)^2 = (1,1,0,1)$ and one-sided minimal polynomials of $(0,0,0,1)$, $(0,1,0,1)$ and $(1,1,0,1)$ are not the same.

For any ring (or semifield) $R = (R,+,\cdot)$ the *opposite* ring $R^{op} = (R,+,\circ)$ is determined by $a \circ b = b \cdot a$ $(a,b \in R)$. It is clear that the rings R^{op} and R are anti-isomorphic. Now let $V = V(4,2,\tau) = W^{op}$, then we obtain the matrices $\tau(e_i)$ from the equality $e_i\theta(e_j) = e_j\tau(e_i)$, $i,j = 1,\dots,4$. So

$$\tau(x_1,x_2,x_3,x_4) = x_1E + x_2 \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix} + x_3 \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix} + x_4 \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}.$$

Direct calculations of minimal polynomials for all elements $a \in V = W^{op}$ serve the illustrations for Lemmas 5, 6: the left-ordered minimal polynomial of $a \in W^{op}$ coincides with the right-ordered minimal polynomial of $a \in W$ and inverse. Further, if $A = \theta(a)$ and $A^{op} = \tau(a)$, then the left-ordered minimal polynomial of $a \in W$ is a factor of $m_{A^{op}}(x)$. For example, the minimal polynomial of $\tau(1,1,1,0)$ is $x^4 + x^3 + 1$ (see Tab. 1 and compare to the last row).

4. Primitivity

In 1991 Wene [7] wrote the hypothesis: *any finite semifield W is right or left primitive*, i. e. the loop W^* is a set of right- or left-ordered degrees of some element in a semifield W. In 2004 Rúa [8] gave a counter-example to Wene's conjecture, using a Knuth semifield of order 32. This commutative *Knuth-Rúa semifield* is neither right nor left primitive. The second counter-example is *Hentzel-Rúa semifield* of order 64, which was constructed in 2007 [9]. Now the primitivity investigations are completed for all semifields of orders up to 125. There exist only two semifields of order $\leqslant 125$ (as can be seen above), which are neither left nor right primitive. Note that the counter-examples of odd order are still unknown.

The investigations of primitivity are based on the properties of a spread set. It is known that for any finite semifield W with the center $Z(W) \simeq \mathbb{F}_q$ and the spread set Σ the characteristic polynomial for any matrix from $\Sigma \setminus \{\lambda E \mid \lambda \in \mathbb{F}_q\}$ has no linear factors. The following theorem serves as the main tool, which was used in [9].

Theorem 4.5. *If W is a finite semifield of dimension n over its center $Z(W) = \mathbb{F}_q$, then $w \in W$ is a left primitive element of W iff the characteristic polynomial of a linear map $L_w : W \to W$, given by $L_w(x) = w * x$, is an irreducible primitive polynomial of degree n over $Z(W)$.*

Note that this result is formulated for a vector-column. In the case of a vector-row we must change the mapping L_w to $R_w : x \to x * w$. For the semifield $W(4, 2, \theta)$ above we have 6 right primitive elements (that is of right order 15) and 4 left primitive elements. Their matrix minimal polynomial is an irreducible polynomial of degree 4.

As it is stated in [4], Knuth-Rúa semifield of order 32 and Hentzel-Rúa semifield of order 64 have no elements of one-sided order 31 and 63 respectively. The following definition gives a weakening for the Wene's hypothesis.

Any finite semifield W, which is n-dimensional over its center $Z(W)$, is said to be *right-cyclic* if for some element $a \in W$ the semifield W has $Z(W)$-base

$$\{e,\ a,\ a^{2)}, \ldots, a^{n-1)}\}.$$

The next result seems evident, but we prove it for completeness.

Theorem 4.6. *Any right-primitive semifield is also right-cyclic.*

Proof. Let W be n-dimensional over its center and W have a right primitive element a, then the minimal polynomial of the matrix $\theta(a)$ is an irreducible polynomial of degree n. As the right-ordered minimal polynomial of an element a is a factor of matrix one then $m_a^r(x)$ is also of degree n. Thus, the elements e, a, $a^2, a^{3)}, \ldots, a^{n-1)}$ are linear independent and as such form the base of the n-dimensional linear space. □

Both non-primitive semifields of order 32 and 64 are left-cyclic and right-cyclic. These semifields contain the elements with one-side-ordered polynomials of degree 5 and 6 respectively (see Tab. 2 and Tab. 3).

Table 2. Information on Knuth-Rúa semifield of order 32

$\|a\|_l = \|a\|_r = \|a\|$	$m_a^l(x) = m_a^r(x) = m_A(x)$
5, 8	$x^5 + x^4 + 1 = (x^2 + x + 1)(x^3 + x + 1)$
6, 10	$x^5 + x + 1 = (x^2 + x + 1)(x^3 + x^2 + 1)$
7	$x^5 + x^4 + 1$ or $x^5 + x + 1$

Table 3. Information on Hentzel-Rúa semifield of order 64

$\|a\|_l = \|a\|_r$	$\|a\|$	$m_a^l(x) = m_a^r(x)$	$m_A(x)$
7	6	$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 =$ $= (x^3 + x + 1)(x^3 + x^2 + 1)$	$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 =$ $= (x^3 + x + 1)(x^3 + x^2 + 1)$
12	7	$x^6 + x^5 + x^3 + x + 1 =$ $= (x^2 + x + 1)^3$	$x^6 + x^5 + x^3 + x + 1 =$ $= (x^2 + x + 1)^3$
15	5	$x^4 + x + 1$	$x^6 + x^5 + x^4 + x^3 + 1 =$ $= (x^4 + x + 1)(x^2 + x + 1)$
6	6	$x^4 + x^2 + 1 =$ $= (x^2 + x + 1)^2$	$x^6 + x^5 + x^3 + x + 1 =$ $= (x^2 + x + 1)^3$
7	7	$x^3 + x + 1$ or $x^3 + x^2 + 1$	$x^6 + x^2 + 1 = (x^3 + x + 1)^2$ or $x^6 + x^4 + 1 = (x^3 + x^2 + 1)^2$
3	3	$x^2 + x + 1$	$x^2 + x + 1$

Further information on the structure of exceptional semifields can be found in [4].

This work was funded by Russian Foundation for Basic Research, project 16-01-00707.

References

[1] L.E.Dickson, Linear algebras in which division is always uniquely possible, *Trans. Amer. Math. Soc.*, **7**(1906), 370–390.

[2] A.A.Albert, Finite division algebras and finite planes, *Proc. Sympos. Appl. Math., AMS, Provid. R.I*, **10**(1960), 53–70.

[3] N.L.Johnson, V. Jha, M. Biliotti, Handbook of finite translation planes, Pure and applied mathematics. Chapman&Hall/CPC, 2007.

[4] V.M.Levchuk, O.V.Kravtsova, Problems on structure of finite quasifields and projective translation planes, *Lobachevskii Journal of Mathematics*, **38**(2017), no. 4, 688-–698.

[5] D.R.Hughes, F.C.Piper, Projective planes, Springer–Verlag New–York Inc., 1973.

[6] R.Lidl, G.Pilz, Applied Abstract Algebra, Springer–Verlag New York, 1984.

[7] G.P.Wene, On the multiplicative structure of finite division rings, *Aequationes Math.*, **41**(1991), 791–803.

[8] I.F.Rúa, Primitive and Non-Primitive Finite Semifields, *Commun. Algebra,* **22**(2004), 223–233.

[9] I.R.Hentzel, I.F.Rúa, Primitivity of Finite Semifields with 64 and 81 elements , *International Journal of Algebra and Computation*, **17**(2007), no. 7, 1411–1429.

Минимальные многочлены в конечных полуполях

Ольга В. Кравцова
Институт математики и фундаментальной информатики
Сибирский федеральный университет
Свободный, 79, Красноярск, 660041
Россия

Используется классическая техника минимальных многочленов для исследования конечных полуполей. Отсутствие ассоциативности умножения приводит к аномальным свойствам односторонне-упорядоченных минимальных многочленов. Описана связь минимального многочлена элемента полуполя и его матрицы из регулярного множества. Результаты иллюстрированы примерами некоторых полуполей порядков 16, 32 и 64.

Ключевые слова: полуполе, правоупорядоченная степень, правоупорядоченный минимальный многочлен.