EDN: GXJKAY
УДК 512.554

On Spectra and Minimal Polynomials in Finite Semifields

Olga V. Kravtsova[*]
Ilya K. Kuzmin[†]
Siberian Federal University
Krasnoyarsk, Russian Federation

Received 10.08.2024, received in revised form 26.09.2024, accepted 01.11.2024

Abstract. We apply the notion of a one-side-ordered minimal polynomial to investigations in finite semifields. A proper finite semifield has non-associative multiplication, that leads to the anomalous properties of its left and right spectra. We obtain the sufficient condition when the right (left) order of a semifield element is a divisor of the multiplicative loop order. The interrelation between the minimal polynomial of non-zero element and its right (left) order is described using the spread set. This relationship fully explains the most interesting and anomalous examples of small-order semifields.

Keywords: semifield, right order, right spectrum, right-ordered minimal polynomial, spread set.

Citation: O.V. Kravtsova, I.K. Kuzmin, On Spectra and Minimal Polynomials in Finite Semifields, J. Sib. Fed. Univ. Math. Phys., 2025, 18(1), 41–50. EDN: GXJKAY.

1. Introduction and preliminaries

The weakening of the field axioms leads to more general algebraic systems such as near-fields, semifields and quasifields. According to [1], a *semifield* is a set Q with two binary algebraic operations $+$ and $*$ such that:

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

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

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

The first examples of non-trivial semifields (not the fields) were constructed by L. E. Dickson in 1906, the multiplicative law in a proper semifield is non-associative. By replacing the two-sided distributivity with a one-sided one, we get the concept of a *quasifield* (left or right). A quasifield with associative multiplication is a *near-field*. Unlike the finite near-fields, which were completely classified by H. Zassenhaus in 1936, neither semifields nor even quasifields have received an exhaustive classification by now.

The absence of associativity even in a finite semifield and a finite quasifield leads to it having a number of specific properties, which are poorly studied. The identification of structural features and anomalous properties is an important step in solving the classification problem of finite quasifields. The most complete review is presented by N. L. Johnson at al. in Handbook [2].

The following problems for finite proper quasifields were presented in 2013 by V. M. Levchuk at research seminar of chair of algebra of Moscow State University, see also [3].

[*] ol71@bk.ru https://orcid.org/0000-0002-6005-2393
[†] ilyabarinovy@gmail.com

(A) *Enumerate maximal subfields and their possible orders.*
(B) *Find the finite quasifields Q with not-one-generated loop Q^*.*
(C) *What loop spectra Q^* of finite semifields and quasifields are possible?*
(D) *Find the automorphism group $Aut\,Q$.*

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

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

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

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

Even the weakened associativity of multiplication allows us to obtain important results about loops and, consequently, semifields and quasifields. Thus, Lagrange's theorem and some other classical group-theoretic theorems can be transferred to binary associative loops or *Moufang loops* (A. N. Grishkov, A. V. Zavarnitsin) [4]. In general, Lagrange's theorem is not valid for a multiplicative loop of a semifield or quasifield. In particular, even the semifields of the minimal order 16 contain the elements of the right and left order 6, which do not divide the order of the loop. In the exceptional non-primitive Knuth–Rúa semifield of order 32, all elements except 0 and 1 have the same right and left order 21.

To identify the patterns of the right and left spectra, we apply the classical concept of a minimal polynomial of a nonzero element to the study of finite semifields. Let Q be a semifield of order p^n, p be prime. The *right-ordered minimal polynomial* of an element $a \in Q$ is said to be a monic polynomial

$$\mu_a^r(x) = x^m + c_1 x^{m-1} + \dots + c_{m-1} x + c_m \in \mathbb{Z}_p[x] \tag{1}$$

of minimal degree such that

$$a^{m)} + c_1 a^{m-1)} + \dots + c_{m-1} a + c_m = 0.$$

The *left-ordered minimal polynomial* $\mu_a^l(x)$ is defined likewise. Some useful properties of one-sided-ordered minimal polynomials see in [5].

The main result of the paper is the following theorem, where «lcm» is a least common multiple of some numbers.

Theorem 1. *Let Q be a non-associative semifield of order p^n (p be prime), the right-ordered minimal polynomial of an element $a \in Q^*$ has the canonical decomposition into irreducible factors:*

$$\mu_a^r(x) = \varphi_1^{s_1}(x)\varphi_2^{s_2}(x)\dots\varphi_s^{s_d}(x) \in \mathbb{Z}_p[x].$$

Then the right order of an element a is a divisor of the number

$$\operatorname{lcm}(p^{m_1} - 1, p^{m_2} - 1, \dots, p^{m_d} - 1, k_1, k_2, \dots, k_d),$$

where m_i is the degree of irreducible polynomial $\varphi_i(x)$, the number k_i equals to 1 if $s_i = 1$, otherwise k_i is the minimal with conditions

$$C_{k_i}^1 \,\vdots\, p, \quad C_{k_i}^2 \,\vdots\, p, \ \dots, \ C_{k_i}^{s_i-1} \,\vdots\, p,$$

for all $i = 1, 2, \dots, d$.

As a corollary, we indicate the important special cases of small-rank semifields: for orders p^3, p^4, p^5. Moreover, we can say that our results are true for left orders and left-ordered minimal polynomials in finite semifields. Also, for right and left quasifield, respectively.

The research method is closely related to linear spaces and spread sets, is based on multiplication recording in a quasifield as a linear transformation in the associated linear space. The matrix operations allow us to effectively apply the method to prove the theoretical result and to illustrate it by the examples of some semifields of orders 2^4, 2^5, 2^6, 3^4, 5^4, 13^4.

2. Spread set and minimal polynomials

It is well-known, that the order of finite semifield or quasifield is the prime number degree p^n [1]. A finite quasifield may be constructed on the basis of a linear space over an appropriate finite field. Let Q be a n-dimensional linear space over the field $\mathbb{Z}_p$, θ is a bijective mapping from Q to $GL_n(p) \cup \{0\}$ such that:

1) $\det(\theta(u) - \theta(v)) \neq 0 \ \forall u, v \in Q$, $u \neq v$,

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

Define the multiplication law on Q by the rule

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

then $\langle Q, +, * \rangle$ is a right quasifield of order p^n. The multiplicative neutral element $\theta^{-1}(E)$ is denoted as e. The image

$$R = \{\theta(u) \mid u \in Q\} \subset GL_n(p) \cup \{0\} \tag{2}$$

is called a *spread set.* And inversely, the right multiplication $R_a : x \to x * a$ in a right quasifield Q is a linear transformation of the linear space Q over the prime subfield $\mathbb{Z}_p$. The set of R_a for all $a \in Q$ is the spread set of Q. For more information see [6], the well-known properties is presented by following preposition:

1) Q is a semifield iff its spread set R is closed under addition;

2) Q is a semifield iff R is closed under multiplication;

3) Q is a field iff R is a field.

Evidently, the matrix representation of the spread set depends on the base of Q as a vector space. Another base choice with the transition matrix T leads to the new spread set TRT^{-1}, so different spread sets can define the isomorphic quasifields. Next, we will choose the appropriate matrix representation of a spread set up to the matrices conjugation. As a rule, we will assume the first basic vector $e_1 = e$ and we will construct the base of Q such that the matrix $\theta(a)$ (for the chosen element a) be of more convenient form – Jordan normal form or close to it.

Some properties of one-side-ordered minimal polynomials in a finite semifield Q correspond to similar results in finite fields, see [5]. The right- or the left-ordered minimal polynomial of an element $a \in Q^*$ is not necessarily irreducible, but $\mu_a^r(0) \neq 0$, $\mu_a^l(0) \neq 0$. The right-(left-)ordered minimal polynomial is a factor of the polynomial $x^k - 1$, where $k = |a|_r$ ($k = |a|_l$). The minimal polynomial of a has the degree 1 or 2 iff a belongs to a subfield of order p^2 in Q, see [7].

Let $a \in Q^*$ and $A = \theta(a)$ is the corresponding matrix from the spread set $R \subset GL_n(p) \cup \{0\}$. Then the right-ordered minimal polynomial of an element a is factor of the minimal polynomial of the matrix A. Moreover, the right order of a is a factor of the order of the matrix A in the general linear group $GL_n(p)$ (proved in [8]).

For completeness, we will prove the following simple but useful result.

Lemma 1. *Let Q be a semifield of order p^n with the spread set R (2). If an elelment $a \in Q$ does not belong to the prime subfield $\mathbb{Z}_p$ then the characteristic polynomial of the matrix $A = \theta(a) \in R$ has no linear factors over $\mathbb{Z}_p$.*

Proof. Assume that the statement is false and the polynomial $\det(A - \lambda E)$ has the factor $\lambda - \alpha$, $\alpha \in \mathbb{Z}_p$. Then the linear transformation with the matrix A has an eigenvector $v \in Q^*$ with the eigenvalue α:

$$v\theta(a) = \alpha v \Rightarrow v * a = v * \alpha,$$

it contradicts the definition of a loop Q^*. □

Evidently that the statement is true for any (right) quasifield too, if $\mathbb{Z}_p \subset Z(Q)$.

Remind that for any square mathix A the characteristic matrix $A - \lambda E$ can be transform, by equivalent tranformations, to the normal diagonal form:

$$A - \lambda E \sim \begin{pmatrix} E_1(\lambda) & 0 & \dots & 0 \\ 0 & E_2(\lambda) & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & E_n(\lambda) \end{pmatrix},$$

where the non-zero invariant factors $E_i(\lambda) \in \mathbb{Z}_p[\lambda]$ are monic polynomials, and $E_i(\lambda)$ is a divisor of $E_{i+1}(\lambda)$, $1 \leqslant i < n$. Moreover, the characteristic polynomial of A is

$$\det(A - \lambda E) = (-1)^n E_1(\lambda) E_2(\lambda) \dots E_n(\lambda),$$

and the last invariant factor equals to the minimal polynomial of A: $E_n(\lambda) = \mu_A(\lambda)$.

3. Main results

We will prove the main Theorem 1 by the sequence of lemmas each of them can be considered as an independent result. These lemmas represent the necessary partial cases, and the theorem proof can be constructed by evident induction.

Consider the right-ordered minimal polynomial $\mu_a^r(x)$ for an element $a \in Q^*$, this polynomial is a divisor of $\mu_A(x)$ for $A = \theta(a)$. It is clear that the right order of a is uniquely defined by the polynomial $\mu_a^r(x)$; $|a|_r$ equals to the length of the neutral element orbit under the linear transformation $\psi = R_a : y \to y * a$. When the degree of the polynomial $\mu_a^r(x)$ is $m < n$, we can consider the map ψ, instead of n-dimensional linear space Q, in the m-dimensional linear sub-space $\mathcal{L}_a \subset Q$ with the base $e, a, a^2, a^{3)}, \dots, a^{m-1)}$.

Lemma 2. *If the right-ordered minimal polynomial $\mu_a^r(x) \in \mathbb{Z}_p[x]$ of an element $a \in Q^*$ is an irreducible polynomial of the degree m then the right order of a is a divisor of the number $p^m - 1$.*

Proof. Consider the right-ordered polynomial $\mu_a^r(x)$ (1) and construct the matrix A of the linear transformation $\psi : y \to y * a$ of the linear space $\mathcal{L}_a$ using the base above:

$$\begin{aligned}
&e^\psi = e * a = a = (0, 1, 0, 0, \dots, 0), \\
&a^\psi = a * a = a^2 = (0, 0, 1, 0, \dots, 0), \\
&(a^2)^\psi = a^2 * a = a^{3)} = (0, 0, 0, 1, \dots, 0), \\
&\dots, \\
&(a^{m-1)})^\psi = a^{m-1)} * a = a^{m)} = -c_m - c_{m-1}a - \dots - c_1 a^{m-1)} = (-c_m, -c_{m-1}, \dots, -c_1);
\end{aligned}$$

$$A = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ 0 & 0 & 0 & \dots & 1 \\ -c_m & -c_{m-1} & -c_{m-2} & \dots & -c_1 \end{pmatrix}.$$

It is the companion matrix of $\mu_a^r(x)$, and the set

$$F = \mathbb{Z}_p(A) = \{b_0 E + b_1 A + b_2 A^2 + \dots + b_{m-1}A^{m-1} \mid b_i \in \mathbb{Z}_p,\ i = 0, 1, \dots, m-1\}$$

is the field of order p^m, see [9]. So, the orbit length of the element $e \in \mathcal{L}_a$ under ψ equals to the order of the matrix A in the cyclic group F^*, $|a|_r$ is a divisor of $p^m - 1$. □

As can be seen, the lemma proven generalizes the corollary from Lagrange's theorem that the element order is a divisor of the finite group order. For any nonzero element a of an arbitrary finite semifield Q, the result is incorrect, see examples below. The result of the lemma is trivial when a belongs to the simple subfield $\mathbb{Z}_p$: the minimal polynomial is linear and the right (and left) order of the element divides $p-1$. It is clear that the result is also valid for an element from any subfield of a finite semifield Q.

Note that the transition from the semifield $Q = (Q, +, *)$ to the *opposite semifield* $Q^{op} = (Q, +, \circ)$ with the multiplication $x \circ y = y * x$ interchanges the right order and the left order of a, also the right-ordered minimal polynomial and the left-ordered minimal polynomial. Thus, all results proved for the right spectrum can be transferred to the left spectrum.

Lemma 3. *If the right-ordered minimal polynomial of an element $a \in Q^*$ is $\mu_a^r(x) = \varphi^2(x)$, where $\varphi(x)$ is irreducible polynomial of degree m, $n = 2m$, then the right order of a is a divisor of the number $p(p^m - 1)$.*

Proof. Clear that the normal diagonal form of the matrix $\theta(a) - \lambda E$ is $\mathrm{diag}(1, 1, \dots, 1, \varphi^2(\lambda))$. Choose the base of Q such that the matrix $\theta(a)$ be of the form

$$A = \begin{pmatrix} B & E \\ 0 & B \end{pmatrix},$$

where all the blocks are $(m \times m)$-dimensional, so the normal diagonal form of $B - \lambda E$ is $\mathrm{diag}(1, 1, \dots, 1, \varphi(\lambda))$. For instance, we can write the matrix B as the companion matrix of the polynomial $\varphi(x)$ by the manner above. Such the base choice is possible because the matrices A and $\theta(a)$ are conjugated, see the previous section.

Evidently, for any $k \in \mathbb{N}$ we have

$$A^k = \begin{pmatrix} B^k & kB^{k-1} \\ 0 & B^k \end{pmatrix}.$$

The image of the neutral element $e = (1, 0, 0, \dots, 0)$ under the linear transformation $\psi^k : y \to yA^k$ coincides to e iff $k \equiv 0 \pmod{p}$ and $B^k = E$. The second condition follows from the irreducibility of the polynomial $\varphi(x)$, because the set $\mathbb{Z}_p(B)$ of $(m \times m)$-matrices is the field of order p^m. So, the order of matrix A in the group $GL_n(p)$ is a divisor of $p(p^m - 1)$, the lemma is proved. □

Additionally, we note that this reasoning shows the need for the divisibility of $|a|_r$ by the number p. We will not focus on this condition because of the complexity in the general case.

Lemma 4. *If the right-ordered minimal polynomial of an element $a \in Q^*$ is the product of two different irreducible polynomials $\mu_a^r(x) = \varphi_1(x)\varphi_2(x)$ of orders m_1 and m_2, $n = m_1 + m_2$, then the right order of a is a divisor of the least common multiple of numbers $p^{m_1} - 1$ and $p^{m_2} - 1$.*

Proof. The normal diagonal form of the matrix $\theta(a) - \lambda E$ is $\mathrm{diag}(1, \ldots, 1, \varphi_1(\lambda)\varphi_2(\lambda))$, so, up to conjugation, the matrix $\theta(a)$ can be chosen as

$$A = \begin{pmatrix} B & 0 \\ 0 & C \end{pmatrix}.$$

Here the block B is $(m_1 \times m_1)$-matrix and $B - \lambda E \sim \mathrm{diag}(1, 1, \ldots, 1, \varphi_1(\lambda))$, the block C is $(m_2 \times m_2)$-matrix and $C - \lambda E \sim \mathrm{diag}(1, 1, \ldots, 1, \varphi_2(\lambda))$. The order of the matrix A evidently equals to the least common multiple of the orders of B and C in general linear groups $GL_{m_1}(p)$ and $GL_{m_2}(p)$, or, more precisely, in cyclic multiplicative groups of associated fields

$$F_1 = \{f(B) \mid f(x) \in \mathbb{Z}_p[x]\} \simeq GF(p^{m_1}) \quad \text{and} \quad F_2 = \{f(C) \mid f(x) \in \mathbb{Z}_p[x]\} \simeq GF(p^{m_2}).$$

The lemma is proved. □

Remark 1. *It is clear that the case of more than two irreducible factors in the polynomial $\mu_a^r(x)$ decomposition is considered by induction. Moreover, in the case when $m_1 + m_2 < n$, we must replace the linear space Q with its linear subspace $\mathcal{L}_a$.*

It remains to consider the case when the irreducible polynomial $\varphi(x)$ is s-times factor of $\mu_a^r(x)$, $s > 2$. It is easy to show, that in this case, the choice of the base allows us to write the corresponding $(ms \times ms)$-dimensional block in the form:

$$A = \begin{pmatrix} B & E & 0 & 0 & \ldots & 0 \\ 0 & B & E & 0 & \ldots & 0 \\ 0 & 0 & B & E & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & 0 & \ldots & E \\ 0 & 0 & 0 & 0 & \ldots & B \end{pmatrix}.$$

Now we can raise it to the k-th degree using Newton's binomial:

$$A^k = \begin{pmatrix} B^k & C_k^1 B^{k-1} & C_k^2 B^{k-2} & C_k^3 B^{k-3} & \ldots & 0 \\ 0 & B^k & C_k^1 B^{k-1} & C_k^2 B^{k-2} & \ldots & 0 \\ 0 & 0 & B^k & C_k^1 B^{k-1} & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & 0 & \ldots & C_k^1 B^{k-1} \\ 0 & 0 & 0 & 0 & \ldots & B^k \end{pmatrix}.$$

The image of the neutral element $e = (1, 0, \ldots, 0)$ equals to $eA^k = e$ when two condition hold:

1) the order of the matrix B in $GL_m(p)$ (or in multiplicative group of the associated field $GF(p^m)$) is a divisor of the number k and

2) the characteristic p is a divisor of the binomial coefficients C_k^1, $C_k^2, \ldots, C_k^{s-1}$.

These arguments, together with the lemmas and the remark, complete the proof of the Theorem 1.

Remark 2. *The result of the theorem remains valid for the right order and right-ordered minimal polynomial in a finite right quasifield, as well as for the left order and left-ordered minimal polynomial in a finite left quasifield (including a semifield).*

The following corollary represents some important cases of small-rank semifield.

Corollary 1. *Let Q be non-associative semifield of order p^n, $a \in Q^*$. The right order and the left order of an element a are divisors of:*
1) p^3-1, when $n=3$;
2) p^4-1 or $p(p^2-1)$, when $n=4$;
3) p^5-1 or $(p^2-1)(p^3-1)$, when $n=5$.

Thus, any three-dimensional finite semifield satisfies to the corollary of Lagrange's theorem. We can not guarantee it for arbitrary four- and five-dimensional semifield. In the case of $n=6$ the listing of all the variants is too complicated.

4. Examples

1. Illustrate the results by the example of a semifield of order 16. It is known that there exist 23 pairwise non-isomorphic semifields of order 16, see enumeration by E. Kleinfeld and results of P K. Shtukkert and V. M. Levchuk, see [3]. The detailed table in that review contains the information on spectra, subfields and automorphisms. All the semifields of order 16 are *right and left primitive*, that is the multiplicative loop Q^* is the set of left-ordered and right-ordered degrees of some element a. So, the right and left spectra contains the number 15, these spectra are the following (for different semifields): $\{1,3,15\}$, $\{1,3,6,15\}$, $\{1,3,5,6,15\}$, $\{1,5,6,15\}$. The number 6 in the spectra is not the divisor of $|Q^*|=15$, but from corollary we have $p(p^2-1)=2\cdot 3=6$, in this case we see the right- or left-ordered minimal polynomial $(x^2+x+1)^2$.

2. The results on 3-primitive semifield projective planes of order 81 are presented in [10]. There exist exactly 8 non-isomorphic semifield planes of order 81 that admit an involution automorphism which fixes pointwise a subplane of order 9. Corresponding 8 non-isotopic semifields of order 81 have the right and left spectra containing only divisors of $|Q^*|=80$: $\{1,2,4,8,16,40,80\}$ or $\{1,2,4,8,16,80\}$.

Another example of semifields of order 81 is the commutative Cohen–Ganley semifield [11]

$$Q=\{(x,y)\mid x,y\in F\simeq GF(9)\}$$

with the multiplication

$$(x,y)\circ(u,v)=(xv+yu+x^3u^3,\, yv+\eta xu+\eta^{-1}xu),\qquad x,y,u,v\in F,$$

η is non-square in F. The spread set of this semifield considered as 4-dimensional linear space over $\mathbb{Z}_3$ consists of matrices

$$\theta(x_1,x_2,x_3,x_4)=x_1E+x_2\begin{pmatrix}0&1&0&0\\0&0&1&0\\0&0&0&1\\2&0&1&0\end{pmatrix}+x_3\begin{pmatrix}0&0&1&0\\0&0&0&1\\2&0&2&2\\1&2&0&1\end{pmatrix}+x_4\begin{pmatrix}0&0&0&1\\2&0&1&0\\1&2&0&1\\0&1&0&0\end{pmatrix},$$

$x_1,x_2,x_3,x_4\in\mathbb{Z}_3$. The next two tables present the elements $a\in Q^*$, their minimal polynomials $\mu_a^r(x)=\mu_a^l(x)$ and their right (left) orders $|a|_r=|a|_l$ calculated by the second author.

Note that the elements with minimal polynomials of degree 1 and 2

$$\{(1,0,0,0),(2,0,0,0),(0,1,2,0),(0,2,1,0),(1,1,2,0),(1,2,1,0),(2,1,2,0),(2,2,1,0)\},$$

together with zero vector form the subfield of order 9. It is so-called *middle nucleus* of Q:

$$N_m=\{b\in Q\mid (a*b)*c=a*(b*c)\ \ \forall b,c\in Q\}.$$

Table 1. Right order is a divisor of $p^4 - 1 = 80$

Element $a \in Q^*$	$\mu_a^r(x)$	$\|a\|_r$
(1, 0, 0, 0)	$x - 1$	1
(2, 0, 0, 0)	$x - 2$	2
(0, 1, 2, 0), (0, 2, 1, 0)	$x^2 + 1$	4
(2, 0, 1, 0), (2, 1, 0, 2), (2, 1, 1, 0), (2, 1, 1, 1)	$x^4 + x^3 + x^2 + x + 1$	5
(1, 1, 2, 0), (1, 2, 1, 0)	$x^2 + x + 2$	8
(2, 1, 2, 0), (2, 2, 1, 0)	$x^2 + 2x + 2$	8
(1, 0, 2, 0), (1, 2, 0, 1), (1, 2, 2, 0), (1, 2, 2, 2)	$x^4 + 2x^3 + x^2 + 2x + 1$	10
(0, 0, 0, 1), (0, 0, 0, 2), (0, 1, 2, 2), (0, 2, 1, 1)	$x^4 + x^2 + 2$	16
(0, 0, 1, 0), (0, 1, 0, 2), (0, 1, 1, 0), (0, 1, 1, 1)	$x^4 + x^2 + x + 1$	40
(0, 0, 2, 0), (0, 2, 0, 1), (0, 2, 2, 0), (0, 2, 2, 2)	$x^4 + x^2 + 2x + 1$	40
(1, 0, 0, 1), (1, 0, 0, 2), (1, 1, 2, 2), (1, 2, 1, 1)	$x^4 + 2x^3 + x^2 + 1$	40
(2, 0, 0, 1), (2, 0, 0, 2), (2, 1, 2, 2), (2, 2, 1, 1)	$x^4 + x^3 + x^2 + 1$	40
(1, 0, 1, 0), (1, 1, 0, 2), (1, 1, 1, 0), (1, 1, 1, 1)	$x^4 + 2x^3 + x^2 + x + 2$	80
(2, 0, 2, 0), (2, 2, 0, 1), (2, 2, 2, 0), (2, 2, 2, 2)	$x^4 + x^3 + x^2 + 2x + 2$	80

Table 2. Right order is a divisor of $p(p^2 - 1) = 24$

Element $a \in Q^*$	$\mu_a^r(x)$	$\|a\|_r$
(0, 1, 1, 2), (0, 2, 2, 1)	$(x^2 + 2x + 2)(x^2 + x + 2)$	8
(1, 1, 1, 2), (1, 2, 2, 1)	$(x^2 + 1)(x^2 + 2x + 2)$	8
(2, 1, 1, 2), (2, 2, 2 ,1)	$(x^2 + 1)(x^2 + x + 2)$	8
(0, 0, 1, 1), (0, 0, 1, 2), (0, 0, 2, 1), (0, 0, 2, 2), (0, 1, 0, 0), (0, 1, 0, 1), (0, 1, 2, 1), (0, 2, 0, 0), (0, 2, 0, 2), (0, 2, 1, 2)	$(x^2 + 1)^2$	12
(1, 0, 1, 1), (1, 0, 1, 2), (1, 0, 2, 1), (1, 0, 2, 2), (1, 1, 0, 0), (1, 1, 0, 1), (1, 1, 2, 1), (1, 2, 0, 0), (1, 2, 0, 2), (1, 2, 1, 2)	$(x^2 + x + 2)^2$	24
(2, 0, 1, 1), (2, 0, 1, 2), (2, 0, 2, 1), (2, 0, 2, 2), (2, 1, 0, 0), (2, 1, 0, 1), (2, 1, 2, 1), (2, 2, 0, 0), (2, 2, 0, 2), (2, 2, 1, 2)	$(x^2 + 2x + 2)^2$	24

The feature of this example is the number of «right roots» of the polynomials. This number equals m for irreducible polynomials of degree m (see Tab. 1), and it does not equal m for reducible ones (see Tab. 2).

Question. *How many «right roots» and «left roots» does a polynomial $f(x) \in \mathbb{Z}_p[x]$ have in a semifield Q of order p^n, if deg$(f) = m$?*

3. The results of the first author on the semifield planes of order p^4 with the special automorphisms subgroup $H \simeq Q_8$ in [12] were illustrated by the examples of semifield planes and semifields of order 5^4 and 13^4. It was proved that all the coordinatizing semifields are both left and right primitive, non-commutative. Each of them have 1, 2 or $p + 2$ maximal subfields of order p^2, the automorphism group is $\mathbb{Z}_2$ or $\mathbb{Z}_{p+1}$.

Let M_n be the set of all divisors of integer n. According to the corollary, the right spectrum of semifields of order 625 above is contained in

$$M_{5^4-1} \cup \{15, 30, 40, 60, 120\} \subset M_{5^4-1} \cup M_{5\cdot(5^2-1)},$$

for the semifields of order 13^4 the right spectrum is the subset of

$$M_{13^4-1} \cup \{21, 91, 104, 182, 273, 312, 364, 546, 728, 1092, 2184\} \subset M_{13^4-1} \cup M_{13\cdot(13^2-1)}.$$

4. Consider two exceptional non-primitive semifields, for more information see [3]. In 1991 G.P. Wene wrote the hypothesis: *any finite semifield is right or left primitive*. In 2004 I.F. Rúa gave the counter-example to Wene's conjecture, using a Knuth semifield $\mathcal{R}$ of order 32. This commutative *Knuth-Rúa semifield* is neither right nor left primitive. The second counter-example is *Hentzel-Rúa semifield* $\mathcal{H}$ of order 64, which was constructed in 2007. These semifields have no elements of one-sided order 31 and 63 respectively. Another counter-examples are still unknown.

Note that even non-primitive Knuth–Rúa and Hentzel–Rúa semifields are *right-cyclic*, these semifields admit a $\mathbb{Z}_p$-base

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

for some element a.

It is known that any element $a \in \mathcal{R} \setminus \{0,1\}$ has the right (and left) order 21. The direct calculation presented in [5] shows that the right-ordered minimal polynomial $\mu_a^r(x)$ is

$$x^5 + x^4 + 1 = (x^2 + x + 1)(x^3 + x + 1) \text{ or } x^5 + x + 1 = (x^2 + x + 1)(x^3 + x^2 + 1).$$

So, by the corollary, we obtain $(p^2 - 1)(p^3 - 1) = 21$, which is consistent with earlier results [3].

Now consider the Hentzel–Rúa semifield $\mathcal{H}$ of order 64, using the information from [5]. Note that the right-ordered minimal polynomial of $a \in \mathcal{H}$ is not necessarily equal to the minimal polynomial of the associated matrix $A = \theta(a)$.

The most interesting situation we see when the right-ordered minimal polynomial of a is $(x^2 + x + 1)^3$. According the main theorem 1 for $m_1 = 2$ and $s_1 = 3$, the right order of a must be a divisor of the number $\mathrm{lcm}(2^2 - 1, k_1)$, where k_1 is the minimal with the conditions $C_{k_1}^1 \vdots\, 2$, $C_{k_1}^2 \vdots\, 2$. From Pascal's triangle

$$\begin{array}{c} 1 \\ 1\ 1 \\ 1\ 2\ 1 \\ 1\ 3\ 3\ 1 \\ 1\ \underline{4\ 6}\ 4\ 1 \end{array}$$

we see that $k_1 = 4$, $\mathrm{lcm}(2^2 - 1, 4) = 12 = |a|_r$. One can check the rest of the cases in the Tab. 3.

Table 3. Orders and minimal polynomials in $\mathcal{H}$

$\lvert a\rvert_l = \lvert a\rvert_r$	$m_a^l(x) = m_a^r(x)$	$m_A(x)$
7	$(x^3 + x + 1)(x^3 + x^2 + 1)$	$(x^3 + x + 1)(x^3 + x^2 + 1)$
12	$(x^2 + x + 1)^3$	$(x^2 + x + 1)^3$
15	$x^4 + x + 1$	$(x^4 + x + 1)(x^2 + x + 1)$
6	$(x^2 + x + 1)^2$	$(x^2 + x + 1)^3$
7	$x^3 + x + 1$ or $x^3 + x^2 + 1$	$(x^3 + x + 1)^2$ or $(x^3 + x^2 + 1)^2$
3	$x^2 + x + 1$	$x^2 + x + 1$

This work is supported by the Krasnoyarsk Mathematical Center and financed by the Ministry of Science and Higher Education of the Russian Federation (Agreement no. 075-02-2024-1429).

References

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

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

[3] 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.
DOI: 10.1134/S1995080217040138

[4] A.N.Grishkov, A.V.Zavarnitsyn, Lagrange's theorem for Moufang loops, *Math. Proc. Phil. Soc.*, **139**(2005), 41–57.

[5] O.V.Kravtsova, Minimal polynomials in finite semifields, *Journal of Siberian Federal University. Mathematics & Phisics*, **11**(2018), no. 5, 588–596.
DOI: 10.17516/1997-1397-2018-11-5-588-596

[6] O.V.Kravtsova, D.S.Skok, The spread set method for the construction of finite quasifields, *Trudy Inst. Mat. i Mekh. UrO RAN*, **28**(2022), no. 1, 164–181.
DOI: 10.21538/0134-4889-2022-28-1-164-181

[7] O.V.Kravtsova, Minimal proper quasifields with additional conditions, *Journal of Siberian Federal University. Mathematics & Physics*, **13**(2020), no. 1, 104–113.
DOI: 10.17516/1997-1397-2020-13-1-104-113

[8] O.V.Kravtsova, V.S.Loginova, Questions of the structure of finite Hall quasifields, *Trudy Inst. Mat. i Mekh. UrO RAN*, **30**(2024), no. 1, 128–141.
DOI: 10.21538/0134-4889-2024-30-1-128-141

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

[10] O.V.Kravtsova, I.V.Sheveleva, On some 3-primitive projective planes, *Chebyshevskii Sb.*, **20**(2019), no. 3, 316–332. DOI: 10.22405/2226-8383-2018-20-3-316-332

[11] S.D.Cohen, M.J.Ganley, Commutative semifields, two dimensional over their middle nuclei, *Journal of Algebra*, **75**(1982), Is. 2, 373–385.

[12] O.V.Kravtsova, Semifield planes admitting the quaternion group Q_8, *Algebra and Logic*, **59**(2020), no. 1, 71–81. DOI: 10.1007/s10469-020-09583-y

О спектрах и минимальных многочленах в конечных полуполях

Ольга В. Кравцова
Илья К. Кузьмин
Сибирский федеральный университет
Красноярск, Российская Федерация

Аннотация. Для исследования конечных полуполей применяется понятие односторонне-упорядоченного минимального многочлена. Отсутствие ассоциативности умножения в собственном полуполе приводит к аномальным свойствам его левого и правого спектра. Получено достаточное условие делимости порядка мультипликативной лупы на правый (левый) порядок элемента. С использованием регулярного множества полуполя описана связь минимального многочлена ненулевого элемента и его правого (левого) порядка. Эта взаимосвязь дает исчерпывающее объяснение наиболее интересным аномальным примерам полуполей малых порядков.

Ключевые слова: полуполе, правый порядок, правый спектр, правоупорядоченный минимальный многочлен, регулярное множество.