DOI: 10.17516/1997-1397-2020-13-1-104-113
УДК 512.554

Minimal Proper Quasifields with Additional Conditions

Olga V. Kravtsova*
Siberian Federal University
Krasnoyarsk, Russian Federation

Received 10.10.2019, received in revised form 22.11.2019, accepted 26.12.2019

Abstract. We investigate the finite semifields which are distributive quasifields, and finite near-fields which are associative quasifields. A quasifield Q is said to be a minimal proper quasifield if any of its sub-quasifield $H \neq Q$ is a subfield. It turns out that there exists a minimal proper near-field such that its multiplicative group is a Miller–Moreno group. We obtain an algorithm for constructing a minimal proper near-field with the number of maximal subfields greater than fixed natural number. Thus, we find the answer to the question: Does there exist an integer N such that the number of maximal subfields in arbitrary finite near-field is less than N? We prove that any semifield of order p^4 (p be prime) is a minimal proper semifield.

Keywords: quasifield, semifield, near-field, subfield.

Citation: O.V.Kravtsova, Minimal polynomials in finite semifields, J. Sib. Fed. Univ. Math. Phys., 2020, 13(1), 104–113.
DOI: 10.17516/1997-1397-2020-13-1-104-113.

1. Introduction and preliminaries

Closely related problems of classification and construction of projective translation planes and their coordinatizing quasifields have been studied from the beginning of the 20th century (Dickson [1], Veblen and Maclagan-Wedderburn [2]; see also [3, 4]). Recall that a set L with a binary operation $\circ$ is called a *loop* if L contains a neutral element and equations $a \circ x = b$ and $x \circ a = b$ are uniquely solvable for any $a, b \in L$ [5, 6]. So, a group is an associative loop. A set Q with binary operations of addition $+$ and multiplication $\cdot$ is called a *right quasifield* [3] if the following conditions are satisfied

1) $(Q, +)$ is an abelian group with zero 0,

2) $Q^* = (Q \setminus \{0\}, \cdot)$ is a loop with an identity e,

3) $x0 = 0$ for any $x \in Q$,

4) Q satisfies the right distributivity $(x + y)z = xz + yz$ for any $x, y, z \in Q$,

5) if $a, b, c \in Q$ and $a \neq b$ then the equation $xa = xb + c$ has an unique solution in Q.

A left quasifield is defined in the same way by replacing the right distributivity with the left distributivity. Any associative right quasifield is called a right *near-field*. Any distributive quasifield is called a *semifield*.

As for finite quasifields the following problems are studied (see also [7]).

(A) *Enumerate maximal subfields and their possible orders.*

*ol71@bk.ru https://orcid.org/0000-0002-6005-2393

(B) *Find finite quasifields Q with not-one-generated loop Q^*.*

The **hypothesis** is as follows: *a loop Q^* of any finite semifield Q is generated by one element.*

(C) *Define a spectra of a loop Q^* if Q is a finite quasifield or a semifield.*

(D) *Find the automorphism group $Aut\, Q$.*

The problems were studied earlier for certain semifields and quasifields of small orders [7–9]. See also Theorem 3.4 in Section 3. In Section 2 of the paper the question **(A)** is studied on maximal subfields for the finite near-fields.

Clearly that a field is a trivial example of a quasifield. Any finite quasifield which is not a field is said to be a *proper* quasifield. A quasifield Q is called a *minimal proper quasifield* if any of its sub-quasifield $H \neq Q$ is a subfield. For instance, any of non-trivial quasifields of order p^2 (p is a prime number) is evidently a minimal proper quasifield. Therefore, by the well-known Zassenhaus theorem, studies of question **(A)** are reduced to Dickson near-fields.

According to Dancs [10, 11] and Felgner [12], the maximal subfield of Dickson near-field containing the center is unique. Certain near-fields have only two or three maximal subfields [13]. However, earlier V. M. Levchuk noted that the answer to the following question is unknown:

Does there exist an integer N such that the number of maximal subfields in arbitrary finite near-field is less than N?

The Dancs description of sub-near-fields in a Dickson near-field is used (see also [13]). Developing Dancs and Felgner approach, the method of construction of some minimal proper near-fields is proposed (Theorem 2.1). Main theorem 2.2 in Section 2 provides the negative answer to the question above even in the class of minimal proper near-fields.

In the case of a finite semifield (Section 3), it is proved that any semifield W of order p^4 is a minimal proper semifield, and any of its sub-semifields $H \neq W$ is a subfield of order p or p^2 (Theorem 3.3). A semifield of order $p^3 > 8$ is also a minimal proper semifield. According to Knuth's theorem [14], such semifield contains only the prime subfield.

2. Subfields in finite near-fields

First examples of finite near-fields were constructed by Dickson in 1906. All finite near-fields were described by Zassenhaus [15] in 1936. His construction of *Dickson near-field* is based on the special expansion of a Galois field $GF(q)$, $q = p^l$ for a prime p. The additive group of a Galois field $GF(q^n)$ is used and it is characterized by the *Dickson pair* (q, n), where

1) any prime divisor of n divides $q - 1$;

2) if $q \equiv 3 \pmod 4$ then $n \not\equiv 0 \pmod 4$.

By Zassenhaus theorem [15], *all finite near-fields are Dickson near-fields, except seven near-fields of order p^2 where $p = 5, 7, 11$ (two near-fields), 23, 29 and 59* (see also [6]).

Clearly that the prime subfield $P = \{ke \mid k \in \mathbb{Z}\}$ of any finite near-field Q is in the *kernel*

$$K(Q) = \{x \in Q \mid x(y+z) = xy + xz,\ (y+z)x = yx + zx\ \forall y, z \in Q\}.$$

However, the center $Z(Q)$ is not necessary a subfield. In fact, it was shown [13, Th. 1] that *for any finite near-field the center coincides with the kernel except Zassenhaus near-fields Q of orders 5^2, 7^2, 11^2 and 29^2 with $|Z(Q^*)| = 2$, 2, 2 and 14, respectively.*

According to [16], the prime subfield is a unique maximal subfield in a near-field of order p^r for any prime number r. So, in this case the near-field is a minimal proper near-field, and question **(A)** is reduced to the case of Dickson near-fields, where $r = ln$ is not prime number.

The class of all Dickson near-fields of order q^n with the center $GF(q)$, $q = p^l$ is denoted by $DF(q, n)$. The well-known correspondence between the subfields in a Galois field $GF(p^m)$ and the divisors of m may be generalized to Dickson near-fields and their sub-near-fields (see [10,11]). The following lemma describes this generalized correspondence.

Lemma 1. *For any sub-near-field H of a Dickson near-field $Q \in DF(p^l, n)$ there are $h \,|\, (ln)$ and $0 < j \leqslant n$ such that $|H| = p^h$, $H \in DF(p^z, h/z)$, $z = \mathrm{GCD}(jl, h)$ and*

$$j \equiv \frac{p^{ln} - 1}{p^h - 1} \,(\mathrm{mod}\ n). \tag{1}$$

Inversely, if $h \,|\, (ln)$ then Q contains the unique sub-near-field H of order p^h.

Felgner [12] proved that any Dickson near-field Q has the unique maximal subfield $M(Q)$ containing the center $Z(Q)$. By [13], if $|M(Q)| = q^\lambda$, then for the canonical decomposition of n and λ we have:

$$n = p_1^{n_1} p_2^{n_2} \dots p_r^{n_r}, \qquad \lambda = p_1^{[n_1/2]} p_2^{[n_2/2]} \dots p_r^{[n_r/2]}.$$

Example 1. Let Q be any near-field of order 2^{180} from the class $DF(2^4, 45)$. Lemma 1 is used to construct the lattice of sub-near-fields of Q (see Fig. 1). The commutative sub-near-fields, i.e. subfields, are shown in colour. The near-field Q contains three maximal subfileds, their orders are 2^{45}, 2^{30} and $2^{12} = |M(Q)|$. Maximal sub-near-fields of orders 2^{90}, 2^{36}, 2^{60} are not subfields.

Further, examples of minimal proper Dickson near-fields Q will be given. Next we consider the following Lemma.

Lemma 2. *Let H be a sub-near-field of order p^h in a Dickson near-field $Q \in DF(p^l, n)$ and $H \in DF(p^z, h/z)$. Then $(h/z)|n$.*

Proof. It is enough to consider the case where $k = (ln)/h$ is a prime number. Let k divides n. Then $n = kn'$, $h = ln'$,

$$z = \mathrm{GCD}\,(jl, h) = \mathrm{GCD}\,(jl, ln') = l \cdot \mathrm{GCD}\,(j, n') = ln'',$$

where n'' divides n. So, we have

$$\frac{h}{z} = \frac{ln'}{ln''} = \frac{n'}{n''} | n.$$

Let k divides l. Then $l = kl'$, $h = l'n$,

$$z = \mathrm{GCD}\,(jl, h) = \mathrm{GCD}\,(jkl', l'n) = l' \cdot \mathrm{GCD}\,(jk, n) = l'n',$$

where n' divides n. So,

$$\frac{h}{z} = \frac{l'n}{l'n'} = \frac{n}{n'}$$

divides n. □

Let us denote the set of all prime divisors of $m \in \mathbb{N}$ by $\pi(m)$. Firstly, we consider the case of the minimal expansion degree $n = 2$.

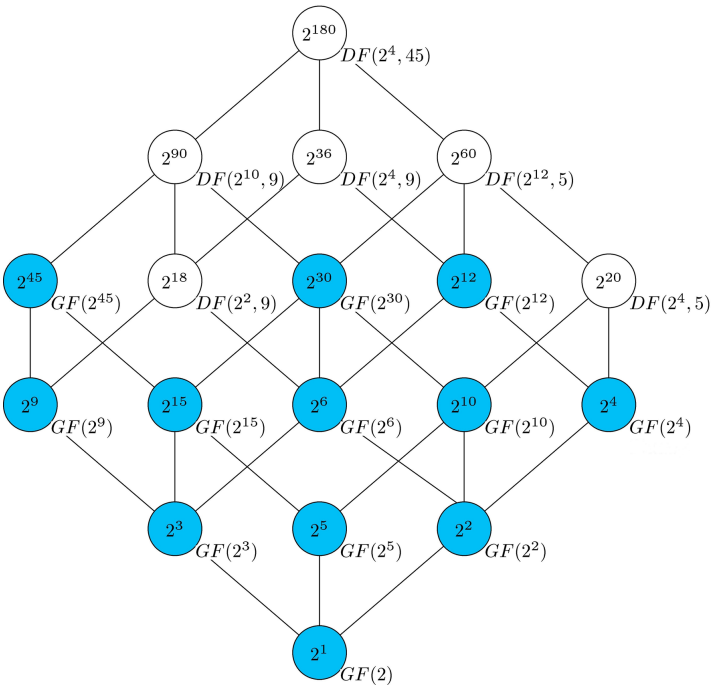

Fig. 1. Sub-near-fields lattice in the Dickson near-field of order 2^{180} with the center $GF(2^4)$

Lemma 3. *The center $Z(Q) \simeq GF(p^l)$ is the unique maximal subfield in any finite Dickson near-field $Q \in DF(p^l, 2)$.*

Proof. It is evident that $p > 2$ and $Z(Q)$ is a maximal subfield of Q. Let H be another maximal subfield of Q. Then $H \not\subset Z(Q)$ and $|H| = p^{2l'}$, where l' divides l. Let us consider the sub-near-fields sequence

$$Q = H_0 \supset H_1 \supset \cdots \supset H_{k-1} \supset H_k = H,$$

where $|H_i| = p^{h_i}$ and h_{i-1}/h_i are prime numbers. The maximality of subfield H leads to $H_k \in DF(p^{2l'}, 1)$ and $H_{k-1} \in DF(p^{l''}, 2)$, where $l'|l''$, $l''|l$ and $l''/l' = m$ is a prime number. Let us determine parameter j (1) for the sub-near-field H_k in H_{k-1} and obtain

$$j = \frac{p^{2l''} - 1}{p^{2l'} - 1} = \frac{p^{2ml'} - 1}{p^{2l'} - 1} = p^{2l'(m-1)} + p^{2l'(m-2)} + \cdots + p^{2l'} + 1 \equiv m (\bmod 2),$$

that is $j = 1$ if $m > 2$ and $j = 2$ if $m = 2$.

If $m > 2$ then $z = \mathrm{GCD}(jl'', h) = \mathrm{GCD}(l'm, 2l') = l'$ so $H_k \in DF(p^{l'}, 2)$ and H_k is not a subfield. This is contradictory to the supposition.

If $m = 2$ then $z = \mathrm{GCD}(jl'', h) = \mathrm{GCD}(2l'', 2l') = 2l'$. We have $H_k \in DF(p^{2l'}, 1)$ and $H_{k-1} \in DF(p^{2l'}, 2)$, where $2l'$ divides l, so H_k is in the center $Z(Q)$ and it is not a maximal subfield. This is contradictory to the supposition. □

If the expansion degree n is greater than two then one can choose the prime number p such that a Dickson near-field $Q \in DF(q, n)$ is a minimal proper near-field.

Theorem 2.1. *There exist infinitely many minimal proper near-fields $Q \in DF(q, n)$ for any fixed prime number $n > 2$.*

Proof. Let $n > 2$ be a prime number. Let us consider the field $GF(n)$ and choose its primitive element p_0, $p_0^{n-1} \equiv 1(\bmod n)$ and $p_0^m \not\equiv 1(\bmod n)$ for any $0 < m < n-1$. The arithmetical progression $\{p_0 + nt\}_{t=0}^{\infty}$ contains infinitely many prime numbers. Let $p = p_0 + nt$ be one of them. Then (p^{n-1}, n) is a Dickson pair. Indeed,

$$p^{n-1} = (p_0 + nt)^{n-1} \equiv p_0^{n-1} \equiv 1(\bmod n),$$

that is, n divides $q - 1 = p^{n-1} - 1$. Now let Q be any near-field from the class $DF(p^{n-1}, n)$. Let us consider all its maximal sub-near-fields. Number n is a prime number. It is clear that the center $Z(Q) \simeq GF(p^{n-1})$ is a maximal sub-near-field in Q. Suppose that $H \neq Z(Q)$ is another maximal sub-near-field of Q. Then $|H| = p^h$, where $h = nl'$ and $k = (n-1)/l'$ is a prime number. Let us determine parameters j and z (1) for H and obtain

$$j \equiv \frac{p^{(n-1)n} - 1}{p^{l'n} - 1}(\bmod n),$$

$$p^{(n-1)n} - 1 \equiv 0(\bmod n), \qquad p^n \equiv p(\bmod n),$$

$$p^{l'n} - 1 = (p^n)^{l'} - 1 \equiv p^{l'} - 1(\bmod n) \not\equiv 0(\bmod n),$$

so $j = n$. Further, $z = \mathrm{GCD}(jl, h) = \mathrm{GCD}(n(n-1), nl') = nl' = h$ and $H \in DF(p^h, 1)$, that is, H is a subfield of Q. So, all maximal sub-near-fields of Q are subfields, and their number is equal to $|\pi(n-1)| + 1$. □

The following theorem proposes a method to construct the minimal proper near-field where the number of maximal subfields is greater than any fixed integer.

Theorem 2.2. *For any $s \in \mathbb{N}$ there exists a minimal proper Dickson near-field that has more than s maximal subfields.*

Proof. Let s be any integer. Let us consider the product of s different prime numbers $N = r_1 \cdot r_2 \cdot \cdots \cdot r_s$. Then the arithmetical progression $\{1 + Nt\}_{t=1}^{\infty}$ contains infinitely many prime numbers. Let $n = 1 + Nt_0$ be one of them. According to Theorem 2.1, one can choose the prime number p such that the class $DF(p^{n-1}, n)$ contains a minimal proper near-field Q. The number of maximal subfields in Q is equal to $1 + |\pi(n-1)| \geqslant 1 + s$. □

Example 2. Using these results, one can give an example of a minimal proper near-field with five maximal subfields. Let $n = 2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211$. It is a prime number. The Galois field $GF(211)$ contains the primitive element 3: $3^{210} \equiv 1(\bmod 211)$ and $3^m \not\equiv 1(\bmod 211)$ for any $0 < m < 210$. Then the near-field $Q \in DF(3^{210}, 211)$ contains five subfields H_i of orders 3^{h_i}, $i = 1, \ldots, 5$, where

$$h_1 = \frac{210 \cdot 211}{2}, \quad h_2 = \frac{210 \cdot 211}{3}, \quad h_3 = \frac{210 \cdot 211}{5}, \quad h_4 = \frac{210 \cdot 211}{7}, \quad h_5 = \frac{210 \cdot 211}{211}.$$

Indeed, the calculation of j and z (1) shows that $j = n$ and $z = h_i$ so $h_i/z = 1$ and $H_i \simeq GF(3^{h_i})$. Numbers n/h_i are all prime numbers so these subfields are maximal sub-near-fields in Q.

A minimal proper near-field with exactly one maximal subfield is also determined.

Lemma 4. *A Dickson near-field Q is a minimal proper near-field that has unique maximal subfield iff Q is from one of classes $DF(p, r)$, $DF(p, r^2)$, $DF(p^r, r)$, where p and r are possible prime number.*

Proof. According to [16], in a near-field $Q \in DF(p,r)$ the center $\mathbb{Z}_p$ is a unique maximal subfield, and Q has no another sub-near-fields by Lemma 1. For a near-field $Q \in DF(p,r^2)$ or $Q \in DF(p^r,r)$ of order p^{r^2} the unique maximal sub-near-field is the subfield $M(Q)$ because $\lambda = r$. Inversely, let $Q \in DF(p^l,n)$ satisfies the condition. It is clear that ln is a degree of one prime number, $ln = r^t$. The maximal subfield $M(Q)$ which contains the center $GF(p^l)$ has the order p^λ, where $\lambda = r^{[t/2]}$. If $H \neq Q$ is a maximal sub-near-field in Q of order $p^{r^{t-1}}$ then $H = M(Q)$. So, $t = 1$ or $t = 2$. The case $DF(p^r,1)$ is evidently corresponds to the field $GF(p^r)$. □

Clearly, that the multiplicative group Q^* of the minimal proper near-field $Q \in DF(2^2,3)$ is a *Miller–Moreno group* [17]. On the other hand, the multiplicative group Q^* of the near-field Q from Example 2 is not a Miller–Moreno group.

3. Subfields in finite semifields

Let $\langle W,+,\circ\rangle$ be a semifield of order p^n (p is a prime number). The universal method to determine a finite semifield (see, for example, [3, 18]) is to introduce n-dimensional linear space over the field $\mathbb{Z}_p$ with a multiplication law

$$x \circ y = x \cdot \theta(y) \qquad (x,y \in W).$$

Here, θ is an injective linear mapping from W to $GL_n(p) \cup \{0\}$ with the property $\theta(e) = E$ (the identity matrix) for some vector $e \in W$ (neutral under the multiplication $\circ$). Then, the set $R = \{\theta(y) \mid y \in W\}$ is called a *spread set* of a semifield W. The notation $W = W(n,p,\theta)$ is used. Elements of the prime subfiled $P \simeq \mathbb{Z}_p$ correspond to the scalar matrices $kE = \theta(k \circ e) \in R$. Note that $k \circ a$ ($k \in \mathbb{N}$, $a \in W$) is the sum of k items equal to a. According to the definition of a semifield, the following result is evident (see also [19]).

Lemma 5. *Let W be a semifield of order p^n, and $R \subset GL_n(p) \cup \{0\}$ is its spread set. Then, for any non-scalar matrix $A \in R$ the characteristic polynomial $\chi_A(x) \in \mathbb{Z}_p[x]$ has no linear divisors $x - \lambda$.*

Proof. Indeed, let $A = \theta(a)$, $a \in W$, and $x - \lambda$ divides $\chi_A(x)$. If $b \in W$ is a correspondent eigenvector then

$$b\theta(a) = \lambda b, \quad b\theta(a - \lambda \circ e) = 0, \quad b \circ (a - \lambda \circ e) = 0, \quad b \neq 0.$$

So, we have $a = \lambda \circ e$ because a semifield has no zero divisors. □

In what follows the results on minimal polynomials in finite semifields which were proved in [20] are used. For any polynomial $f(x) \in \mathbb{Z}_p$,

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

and any element $a \in W$ the *right-* and *left-ordered value* of the polynomial are defined:

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

Here, $a^{s)}$ and $a^{(s}$ are the *right-* and *left-ordered degrees* of an element a, respectively. They are determined inductively by the rule

$$a^{s)} := a^{s-1)} \circ a, \quad a^{(s} := a \circ a^{(s-1}, \quad a^{1)} := a = a^{(1}.$$

Evidently, in the case of degree $\leqslant 2$, the right- and the left-ordered values $f(a))$ and $f((a)$ are equal.

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 the minimal degree such that $\mu_a^r(a)) = 0$. The *left-ordered minimal polynomial* $\mu_a^l(x)$ is defined in a similar way. According to [20], we have

Lemma 6. *If $a \in W(n,p,\theta)$ and $A = \theta(a)$ then the right-ordered minimal polynomial of an element a is a factor of the minimal polynomial of the matrix A.*

Now consider semifields of small orders p^3 and p^4 and their subfields. It is well-known [14] that a semifield of order p^2 or 8 is a field. So, it is clear that any semifield of order $p^3 > 8$ is a minimal proper semifield. Let us specify the possible orders of subfields in such a semifield.

Lemma 7. *Let W be a semifield of order p^n with the multiplicative identity e. If a non-zero element $a \in W$ has the right-ordered minimal polynomial $\mu_a^r(x) \in \mathbb{Z}_p[x]$ then $deg(\mu_a^r) = 1$ iff a belongs to the prime subfield P and $deg(\mu_a^r) = 2$ iff $K = \{\alpha_1 \circ e + \alpha_2 \circ a \mid \alpha_1, \alpha_2 \in \mathbb{Z}_p\}$ is a subfield in W of order p^2.*

Proof. The first proposition is evident. Let $deg(\mu_a^r) = 2$. Then the system of vectors e, a is linear independent over $\mathbb{Z}_p$, $a^2 \in K$, so $|K| = p^2$. Moreover, K is closed with respect to multiplication and multiplication in K is associative. Inversely, if K is a subfield of order p^2 then $a \notin P$ and $a^2 \in K$. □

Corollary 1. *Let W be a semifield of order p^n. The subset of elements with the minimal polynomial of degree 1 or 2 (together with 0) is the union of all subfields of order p^2 in W.*

Let us note that for a sub-semifield (or a subfield) U of order p^m in a semifield W of order p^n the condition $m|n$ need not be satisfied. This fact can be explained by the absence of multiplicative associativity: in general a semifield W is not a linear space over U. Moreover, a finite semifield may contain more than one sub-semifields (subfields) of the same order.

For example, there exists the semifield of order 32 containing the subfield of order 4, and also semifields of order 81 with three disjoint subfields of order 9 (see [7, 9, 21]).

The evident examples of subfields in the finite semifields are the *left, middle and right nuclei* [3]

$$N_l = \{x \in W \mid x \circ (y \circ z) = (x \circ y) \circ z \ \forall y, z \in W\},$$
$$N_m = \{x \in W \mid y \circ (x \circ z) = (y \circ x) \circ z \ \forall y, z \in W\},$$
$$N_r = \{x \in W \mid y \circ (z \circ x) = (y \circ z) \circ x \ \forall y, z \in W\},$$

the nucleus $N = N_l \cap N_m \cap N_r$ and the center $Z = \{z \in N \mid z \circ x = x \circ z \ \forall x \in W\}$. Let us consider now another example of a semifield of order p^4 with a subfield of order p^2 (see [18]).

Lemma 8. *Let W be a semifield of order p^4 and φ be an involutory automorphism of W. Then the stabilizer $U = \{x \in W \mid \varphi(x) = x\}$ is a subfield of order p^2.*

It is natural to assume that for a semifield of order p^n any sub-semifield is of order p^m, where $m \leqslant n/2$. Let us show that it is true, at least, for the semifields of order p^3 and p^4.

Theorem 3.3. *For a semifield W of order p^n, where $n = 3$ or $n = 4$, any proper sub-semifield is a subfield of order p^m, $m \leqslant n/2$.*

Proof. Let W be a semifield of order p^3, U be its subfield of order p^2, and the element $a \in U$ does not belong to the prime subfield P. Then, its minimal polynomial $\mu_a(x) \in \mathbb{Z}_p[x]$ is of degree

two and it divides the minimal polinomial $\mu_A(x)$ of the correspondent matrix $A = \theta(a) \in GL_3(p)$ from the spread set. Then, the characteristic polynomial $\chi_A(x)$ of matrix A has a linear factor that is impossible.

Let W be a semifield of order p^4, U be its sub-semifield of order p^3. It was proved above that it does not contain the subfields of order p^2. So, any of its elements $a \in U$, not from the prime subfield P, has the right-ordered minimal polynomial $\mu_a^r(x) \in \mathbb{Z}_p[x]$ of degree 3. Then, the characteristic polynomial $\chi_A(x)$ of the correspondent matrix $A = \theta(a) \in GL_4(p)$ from the spread set has a linear factor. □

One can generalize the obtained result using the notion of the *right-cyclic* semifield. An element a of a semifield W of order p^n is called *right-cyclic* over $\mathbb{Z}_p$, if elements

$$e, a, a^2, a^{3)}, \ldots, a^{n-1)}$$

form a base of W as a n-dimensional linear space over $\mathbb{Z}_p$. So, the semifield W is called *right-cyclic* over $\mathbb{Z}_p$. A left-cyclic element and a left-cyclic semifield are defined in a similar way. Let us note that all known up to now finite semifields are right- and left-cyclic even non-primitive semifields of order 32 and 64 (see, for example, [19, 22, 23] and [7].

Corollary 2. *A semifield W of order p^n contains no right-cyclic over $\mathbb{Z}_p$ sub-semifields of order p^{n-1}.*

Proof. It is enough to consider the right-ordered minimal polynomial of a right-cyclic element a of a sub-semifield of order p^{n-1}. The characteristic polynomial of correspondent matrix $A = \theta(a)$ from a spread set has a linear factor. □

Let us now illustrate these results by the examples of semifields of order 5^4 and 13^4 with additional condition to autotopisms. Remind that the triple of automorphisms $\langle \alpha, \beta, \gamma \rangle$ of the additive group $(W, +)$ is called an *autotopism* of a semifield W if for all $x, y \in W$ the equality $x^\alpha \circ y^\beta = (x \circ y)^\gamma$ is satisfied. It is simple to prove (see [18]) that fixed α and γ defines the automorphism β.

Let W be a semifield of order p^4 (p is a prime number, $p \equiv 1 (\mathrm{mod}\, 4)$) determined as a 4-dimensional linear space over $\mathbb{Z}_p$. Now consider its mappings

$$\begin{aligned} &\alpha_1 : (x_1, x_2, x_3, x_4) \to (-ix_1, -ix_2, ix_3, ix_4), \\ &\alpha_2 : (x_1, x_2, x_3, x_4) \to (-x_3, -x_4, x_1, x_2), \qquad x_j \in \mathbb{Z}_p,\ j = 1, 2, 3, 4, \end{aligned} \tag{2}$$

where $i \in \mathbb{Z}_p$, $i^2 = -1$. Let $\sigma_1 = \langle \alpha_1, \beta_1, \alpha_1 \rangle$, $\sigma_2 = \langle \alpha_2, \beta_2, \alpha_2 \rangle$ be the autotopism of W, where α_1 and α_2 are defined by (2), and $H = \langle \sigma_1, \sigma_2 \rangle$ be the autotopism subgroup. Then, H is isomorphic to the quaternion group Q_8. It can be verified by direct calculation. Let us denote the numbers of non-isomorphic and non-isotopic semifields of order p^4 admitting H by $n(p)$ and $n'(p)$, respectively. Questions **(A)**–**(D)** from the introduction can be solved with the use of computer constructions.

Theorem 3.4. *Let W be a semifield of order p^4, where $p = 5$ or $p = 13$, which admit an autotopism subgroup $H = \langle \sigma_1, \sigma_2 \rangle \simeq Q_8$. Then W is not commutative. It is left- and right-primitive, and it has the center of order p and the left nucleus N_l of order p^2, and*

$$n(5) = 9, \quad n'(5) = 3, \qquad n(13) = 99, \quad n'(13) = 33.$$

The number of maximal subfields of order p^2 in W equals 1, 2 or $p+2$. The automorphism group $Aut\, W$ is the cyclic group $\mathbb{Z}_2$ or $\mathbb{Z}_{p+1}$.

Note that any such semifield is a minimal proper semifield but it may contain more than one subfiled of order p^2. It is anomalous property in comparison with the properties of finite fields and finite near-fields. The theorem does not concern the question **(C)** on the spectra of elements of multiplicative loop because of its complicated statement. But it is another anomalous property of finite semifields that the spectra contain the integers which does not divide the order of W^*.

This work was funded by Russian Foundation for Basic Research (project no. 19-01-00566 A).

References

[1] L.E.Dickson, *Trans. Amer. Math. Soc.*, **7**(1906), no. 3, 370–390. DOI:10.2307/1986324

[2] O.Veblen, J.H.Maclagan–Wedderburn, *Trans. Amer. Math. Soc.*, **8**(1907), no. 3, 379–388.

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

[4] N.L.Johnson, V.Jha, M.Biliotti, Handbook of finite translation planes, London, New York, Chapman Hall/CRC, 2007.

[5] A.G.Kurosh, Lectures on general algebra, Elsevier Ltd., 1965.

[6] M.Hall, The theory of groups, Chelsea Pub. Co., 1976.

[7] V.M.Levchuk, O.V.Kravtsova, *Lobachevskii J. Math.*, **38**(2017), no. 4, 688–698. DOI:10.1134/S1995080217040138

[8] V.M.Levchuk, P.K.Shtukkert, *Trudy Inst. Mat. i Mekh. UrO RAN*, **21**(2015), no. 3, 197–212 (in Russian).

[9] O.V.Kravtsova, I.V.Sheveleva, *Chebyshevskii Sbornik*, **20**(2019), no. 3, 187.

[10] S.Dancs, The sub-near-field structure of finite near-fields, *Bull. Austral. Math. Soc.*, **5**(1971), 275–280.

[11] S.Dancs Groves, Locally finite near-fields, *Abh. Math. Sem. Univ. Hamburg.*, **48**(1979), 89–107. DOI:10.1017/S0004972700043914

[12] U.Felgner, Pseudo-finite near-fields, Near-rings and near-fields, Elsevier Science Publisher B. V., North-Holland, vol. 137, 1987, 15–29.

[13] O.V.Kravtsova, V.M.Levchuk, Questions of the structure of finite near-fields, *Trudy Inst. Mat. i Mekh. UrO RAN*, **25**(2019), no. 4, 107–117 (in Russian).

[14] D.E.Knuth, *J. Algebra*, **2**(1965), 182–217. DOI:10.1016/0021-8693(65)90018-9

[15] H.Zassenhaus, Uber endliche Fastkörper, *Abh. Math. Sem. Hamburg*, **11**(1936), 187–220. DOI: 10.1007/BF02940723

[16] T.N.Yakovleva, *The Bulletin of Irkutsk State University. Series Mathematics*, **29**(2019), 107–119 (in Russian). DOI:10.26516/1997-7670.2019.29.107

[17] G.A.Miller, H.C.Moreno, *Trans. Amer. Math. Soc*, **4**(1903), 398–404.

[18] O.V.Kravtsova, *Siberian Electronic Mathematical Reports*, **13**(2016), 1300–1313. DOI:10.17377/semi.2016.13.102

[19] I.F.Rua, *Commun. Algebra.*, **22**(2004), 223–233.

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

[21] P.K.Shtukkert, *The Bulletin of Irkutsk State University*, **7**(2014), 144–159 (in Russian).

[22] G.P.Wene, *Aequationes Math.*, **41**(1991), 222–233.

[23] I.R.Hentzel, I.F.Rua, *Int. J. Algebra and Comput.*, **17**(2007), no. 7, 1411–1429.

Минимальные собственные квазиполя с дополнительными условиями

Ольга В. Кравцова
Сибирский федеральный университет
Красноярск, Российская Федерация

Аннотация. Мы рассматривем конечные полуполя, то есть дистрибутивные квазиполя, и конечные почти-поля, то есть ассоциативные квазиполя. Квазиполе Q называем минимальным собственным квазиполем, если всякое его подквазиполе $H \neq Q$ является подполем. Оказывается, существует минимальное собственное почти-поле, мультипликативная группа которого есть группа Миллера–Морено. Найден алгоритм построения минимального собственного почти-поля, в котором количество максимальных подполей больше любого заданного числа. Таким образом, получен ответ на вопрос: существует ли такое натуральное число N, что количество максимальных подполей в произвольном почти-поле меньше N? Доказано, что всякое полуполе порядка p^4 (p – простое) есть минимальное собственное полуполе.

Ключевые слова: квазиполе, полуполе, почти-поле, подполе.