ISSN 1995-0802, Lobachevskii Journal of Mathematics, 2017, Vol. 38, No. 4, pp. 688–698. © Pleiades Publishing, Ltd., 2017.

Problems on Structure of Finite Quasifields and Projective Translation Planes

V. M. Levchuk* **and O. V. Kravtsova****

(Submitted by M. M. Arslanov)

Siberian Federal University, Svobodnyi pr. 79, Krasnoyarsk, 660041 Russia

Received June 26, 2016

Abstract—It is well-known that the constructions and classification of non-Desarguesian projective planes are closely connected with ones for quasifields. We consider the problems on structure of finite quasifields and semifields: automorphisms and autotopisms, maximal subfields and their orders, the spectrum of orders of non-zero elements and hypotheses about generated subsets of the multiplicative loop.

DOI: 10.1134/S1995080217040138

Keywords and phrases: *Quasifield, semifield, translation plane, semifield plane, spread set.*

1. INTRODUCTION

The failure from properties of commutativity and associativity of fields leads to concept of *semifield* (or *quasitelo*, by Kurosh [1, II.6.1]). It is a (simple) ring, where non-zero elements form a multiplicative loop, i.e., a group without property of associativity. The weakening also of two-sided distributivity to one-sided one gives a general concept of *quasifield*.

The investigations of quasifields had been more century ago when Veblen, Maclagan-Wedderburn [2] and Dickson [3] used quasifields in the constructions of projective translation planes. Also, this plane is Desarguesian iff its coordinatizating quasifield is a field.

The investigations of problems of construction and classification of projective planes and quasifields from 1960s (Kleinfeld [4], Knuth [5, 6], etc) usually use computer calculations. The development to 2007 is reflected by Johnson, Jha, Biliotti [7] in Handbook (861 pages). Note that the structure of even known *proper* (or not being a field) finite semifields is poorly studied.

We discuss certain problems on structure of finite quasifields and semifields in next section. Closely related constructions of projective translation planes and their coordinatizing quasifields are considered in section § 4. Further we consider some results.

2. SOME REMARKS AND QUESTIONS

Recall that the groupoid L with binary operation $\cdot$ is called *a quasigroup*, if for all $a, b \in L$ any equation $ax = b$ or $xa = b$ is uniquely solvable in L. A quasigroup is *a loop*, if it has an identity e (zero 0 in the additive terminology). Thus, the group is an associative loop.

Definition 1. *The finite set Q with binary operations of addition $+$ and multiplication $\cdot$ is called a* **right quasifield**, *if*

1) $(Q, +)$ *is an abelian group,*

2) $Q^* := (Q \setminus \{0\}, \cdot)$ *is a loop,*

3) $x0 = 0 \ (x \in Q)$,

*E-mail: vlevchuk@sfu-kras.ru

**E-mail: ol71@bk.ru

4) *it is satisfied the right distributivity* $(y+z)x = yx + zx\,(x, y, z \in S)$.

Evidently the right distributivity and 1) give the condition $0x = 0$.

Analogously finite *left quasifield* is defined with replacement of right distributivity onto left distributivity. Further we say "quasifield" instead of "right quasifield".

Remark 1. By Hughes, Piper [15], a system $(Q, +, \cdot)$ with arbitrary Q and conditions 1)–4) is said to be *a weak quasifield* and, also, *a quasifield*, if it is uniquely solvable in Q any equation $ax = bx + c$ $(a, b, c \in Q,\ a \neq b)$. According to [15, 7.3], any finite weak quasifield is a quasifield.

We now show that a characteristic of any quasifield is always determined, similarly to fields, and if the characteristic is positive, then the statement about minimal subfield is also satisfied.

Clearly that any quasifield Q gives a two-sided $\mathbb{Z}$-module, if for any integer coefficient $k \geq 0$ we set $0x := 0 = x0$ and also

$$kx := \underbrace{x + x + \ldots + x}_{k \text{ times}} = xk, \quad (-k)x := -(kx) = x(-k) \quad (x \in Q).$$

Proposition 1. *Let Q be a right quasifield with the identity e. Then:*

i) $\pi :\ k \to ke \ \ (k \in \mathbb{Z})$ *is a homomorphism of the integer ring* $\mathbb{Z}$ *into* Q *and* Q *is a left* $\pi(\mathbb{Z})$-*module;*

ii) $\pi(\mathbb{Z}) \simeq \mathbb{Z}$ for $p = 0$, *where* $p = char\ Q := char\ \pi(\mathbb{Z})$;

iii) *if* $p > 0$, *then* $\pi(\mathbb{Z}) \simeq \mathbb{Z}_p$ *and* $\pi(\mathbb{Z})$ *is unique minimal subfield of* Q.

Proof. Evidently, π preserves addition $+$ in Q. The associativity of addition and right distributivity in Q also give

$$ke \cdot me = k(e \cdot (me)) = k(me) = (km)e \quad (k, m \in \mathbb{Z}).$$

Thus, π is a homomorphism of ring $\mathbb{Z}$ into Q. Since any quasifield has no zero-divisors we obtain that $\pi(\mathbb{Z})$ is a domain.

Taking into account the equalities $me \cdot x = m(ex) = mx$ we have

$$(ke) \cdot (me \cdot x) = k(e \cdot (me \cdot x)) = (km)x = (ke \cdot me) \cdot x,$$
$$me \cdot (x + y) = m(x + y) = mx + my = (me \cdot x) + (me \cdot y).$$

It follows that Q is a left $\pi(\mathbb{Z})$-module. Clearly, if π is an isomorphism, then $\pi(\mathbb{Z}) \simeq \mathbb{Z}$. Let $Ker(\pi) \neq 0$. Then $\pi(\mathbb{Z})$ is a finite domain and therefore $\pi(\mathbb{Z}) \simeq \mathbb{Z}_p$ for $p := char\ \pi(\mathbb{Z}) > 0$. □

Since any semifield are a right and left quasifield, we obtain

Corollary 1. *The center of any semifield contains* $\pi(\mathbb{Z})$.

It seems that this statement is not true, for instance, for near-fields, see § 8. The order of any finite projective translation plane coincides with the order of its coordinatizing quasifield (§ 4). It follows directly

Corollary 2. *The order of any finite quasifield and hence the order of any finite projective translation plane equals to a prime number degree.*

It is well-known that all quasifield of even orders 2, 4 and 8 are the fields. The proper quasifield of order p^2 for prime $p > 2$ is constructed by Dickson (1906, [3]). According to Knuth [5], it is true

Theorem 1. *The proper semifield of order* p^n *for a prime* p *exists if and only if* $n \geq 3$ *and* $p^n \geq 16$.

Let L be a multiplicative loop. A product of m its multipliers is said to be *m-th degree of fixed element* v, if every multiplier coincides with v. The smallest integer $m \geq 1$ such that there exists 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 *a spectrum of loop L*.

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

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

we define right order $|v|_r$ and left order $|v|_l$ of v and, also, *right and left spectra* of L, respectively.

The following problems for finite proper quasifields were presented in 2013 by first author at research seminar of chair of algebra of Moscow State University and in [11, 14].

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

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

Hypotheses: *the loop of any finite semifield is one-generated.*

(C) *What loop spectra S^* of finite semifields and quasifields are possible?*

(D) *Find the automorphism group AutS.*

Note that hypotheses **(B)** is more weak than well-known **Wene's hypotheses (1991):** *any finite semifield is right-primitive.*

A semifield S and multiplicative loop S^* are called *right-primitive*, if all elements of loop S^* are the right-ordered degrees of fixed element (in other words, there exists an element $v \in S^*$ such that $|v|_r = |S^*|$).

Wene's hypotheses was refuted by Rúa [9] in 2004.

Clearly that complete classification of quasifields or semifields means classification up to isomorphisms. On the other hand, classification of their up to isotopisms (see § 4) is important for classification of projective translation planes. It is shown by the following theorem of Albert [18].

Theorem 2. *Projective semifield planes are isomorphic if and only if their coordinatizing semifields are isotopic.*

3. SEMIFIELDS OF ORDER 16

The proper finite semifields are completely classified only for smallest possible orders. In this section we consider the problems **(A)–(D)** for semifields of smallest even order 16.

According to Kleinfeld, the number of proper semifields of order 16, up to isomorphisms, equals to 23. These semifields form two isotopic classes of 18 (V_i, $1 \le i \le 18$) and 5 (T_{24}, T_{25}, T_{35}, T_{45} and T_{50}) pairwise non-isomorphic semifields with the nuclei of order 2 and 4 respectively.

Up to isomorphisms and anti-isomorphisms, we restrict the list to 16 semifields. For any ring (or quasifield) $R = (R, +, \cdot)$ 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.

Theorem 3. *Any proper semifield of order* 16 *up to isomorphisms is either one of* 7 *semifields* V_1, V_3, V_4, V_8, V_{11}, V_{15}, T_{25} *or one of opposite semifields to them* V_6, V_7, V_5, V_9, V_{14}, V_6, T_{50}, *respectively, or one of* 9 *semifields* $V_2, V_{10}, V_{12}, V_{13}, V_{17}, V_{18}, T_{21}, T_{35}, T_{45}$.

Kleinfeld characterizes the Caley table of loop W^* for any semifield $W = V_i$ or T_j by special generating sequence and forms the table as a latin square. The multiplication laws for all 16 semifields are obtained in [14, Table 3]. All above questions for semifields of order 16 are completely solved by Kravtsova, Levchuk and Shtukkert ([12–14]).

Let $\mathcal{M}$ be a set of all subfields of order 4 for given semifield. Then the following Table 1 resumes results.

The Kleinfeld method is not suitable for semifields of order more than 16. The general method to construct quasifields and translation planes will be presented in the following section.

4. PROJECTIVE TRANSLATION PLANES AND ITS COORDINATIZING QUASIFIELDS

The constructions of quasifields and projective translation planes are closely related. According to [10, 15], the *projective plane* is a set of points and lines with an incidence relation between them such that:

—any two distinct points are incident with a unique line,

—any two distinct lines are incident with a unique point,

—there exist four points such that no three are incident with one line.

For every projective plane π a *dual plane* π^d is determined. By definition, its points are lines of π and its lines are points of π and, also, the point and the line are incident in π^d if and only if they are incident in π.

The number n is called an *order of finite plane*, if some (equivalently, every) its line is incident to $n + 1$ points. Such plane consists of $n^2 + n + 1$ points and so many lines (see [10, Theorem 20.1.1]).

Table 1. The structure of non-isomorphic semifields of order 16

Semifield W	$\|\mathcal{M}\|$	Spectrum	Right spectrum	Left spectrum	$\|AutW\|$
$V_1 \simeq V_6^{op}$	0	$\{1,4,5\}$	$\{1,5,6,15\}$	$\{1,6,15\}$	1
V_2	1	$\{1,3,4,5,6\}$	$\{1,3,6,15\}$	$\{1,3,6,15\}$	2
$V_3 \simeq V_7^{op}$	0	$\{1,4,5,6\}$	$\{1,5,6,15\}$	$\{1,5,6,15\}$	1
$V_4 \simeq V_5^{op}$	1	$\{1,3,4,5,6\}$	$\{1,3,6,15\}$	$\{1,3,5,6,15\}$	1
$V_8 \simeq V_9^{op}$	2	$\{1,3,4,5,6\}$	$\{1,3,6,15\}$	$\{1,3,5,6,15\}$	2
V_{10}	1	$\{1,3,5,6\}$	$\{1,3,6,15\}$	$\{1,3,6,15\}$	3
$V_{11} \simeq V_{14}^{op}$	1	$\{1,3,4,5,6\}$	$\{1,3,5,6,15\}$	$\{1,3,6,15\}$	2
V_{12}	0	$\{1,4,5,6\}$	$\{1,5,6,15\}$	$\{1,5,6,15\}$	1
V_{13}	4	$\{1,3,5\}$	$\{1,3,15\}$	$\{1,3,15\}$	6
$V_{15} \simeq V_{16}^{op}$	2	$\{1,3,4,5\}$	$\{1,3,6,15\}$	$\{1,3,6,15\}$	2
V_{17}	1	$\{1,3,4,5,6\}$	$\{1,3,5,6,15\}$	$\{1,3,5,6,15\}$	1
V_{18}	2	$\{1,3,5,6\}$	$\{1,3,5,6,15\}$	$\{1,3,5,6,15\}$	2
T_{24}	2	$\{1,3,4,5,6\}$	$\{1,3,5,6,15\}$	$\{1,3,5,6,15\}$	2
$T_{25} \simeq T_{50}^{op}$	2	$\{1,3,4,5,6\}$	$\{1,3,5,6,15\}$	$\{1,3,6,15\}$	2
T_{35}	1	$\{1,3,4,5,6\}$	$\{1,3,6,15\}$	$\{1,3,6,15\}$	3
T_{45}	3	$\{1,3,5\}$	$\{1,3,5,15\}$	$\{1,3,5,15\}$	4

By Bruck—Ryser theorem, *there is no plane of order n, if n cannot be expressed as a sum of two integer squares and $n \equiv 1$ or $2 (mod\ 4)$.*

Bijective map of points and lines of projective plane π, respectively, to points and lines of projective plane π' is called an *isomorphism of planes* (for $\pi = \pi'$, also *automorphism or collineation*), if it preserves the incidence relation. Any collineation of projective plane π, that fixes the line $l \in \pi$ pointwise and the point $P \in \pi$ linewise, is (P,l)*-perspectivity*.

If there exists a line $l \in \pi$ such that for any point $P \in l$ the group of (P,l)-perspectivities acts transitively on points of affine plane $\pi \setminus l$, then π is called a *translation plane*. If dual plane π^d is translation plane too then π is a *semifield plane*.

Now we consider well-known coordinatization method of translation planes by quasifields using “spread set”. Recall that the *group partition* is a set of its subgroups (components of partition), which have trivial pairwise intersections and their set-theoretic union gives whole group.

Let G be abelian group with partition μ. For corresponding affine plane the points are the elements of G and the lines are cosets on subgroups of μ and, also, the incidence is set-theoretic. For construction of projective plane we should define *singular (or infinity) point and line*. We assume that the cosets on the same subgroup intersect in the same *singular point* of this plane; the set of all singular points gives a *singular line*.

A partition μ of additive group of $2n$-dimensional linear space V over the field F is called *spread* in V, if $V = M \oplus N$ for any distinct $M, N \in \mu$. Then all components are n-dimensional subspaces, according to [16]. We get a projective translation plane $\mu(V)$ as above. Inversely: any translation plane is isomorphic to suitable plane $\mu(V)$.

To construct a translation plane π of rank n over a field F we can use the n-dimensional linear space W over F (*coordinatizing set*), the outer direct sum of two copies of W,

$V = W \oplus W = \{(x,y) \mid x,y \in W\}$, and the spread μ with *axes* $V(0) := (W,0)$ and $V(\infty) := (0,W)$. Then the other components of μ are

$$V(\sigma) = \{(v, v^\sigma) \mid v \in W\}, \quad \sigma \in GL(W).$$

Let θ be an bijective map from linear space W to ring $M(n,F)$ of all $n\times n$-matrices over F. The image $R=\theta(W)$ is called a *spread set*, if:

1) identity and zero matrices E and O are in R,

2) $R\setminus\{O\}$ and the matrices $\theta(u)-\theta(v)$ are in $GL(n,F)$ for all $u,v\in W,\ u\neq v$.

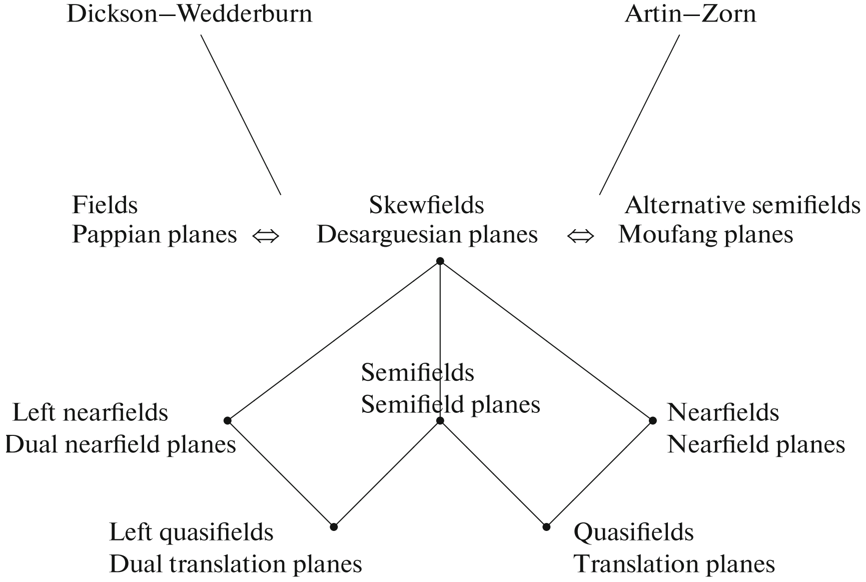
In this case we have a quasifield $(W,+,\circ)$ with multiplication law

$$x\circ y:=x\cdot\theta(y)\quad(x=(x_1,x_2,...,x_n),\ y\in W).$$

It is well known that projective translation plane is Desarguesian if and only if its coordinatizing set is a skewfield (a field in finite case). According to Theorem 6.1 [17], an affine plane is translation plane if and only if it is coordinatized by quasifield. In the case of semifield it is a semifield plane.

The connection between translation planes and coordinatizing quasifields is reflected by the following diagram of Lavrauw [27], see Table 2.

Table 2. Types of finite translation planes and their associated algebraic structures



Definition 2. *The triple of bijective maps* α,β,γ of groupoid $(S;\circ)$ *on* $(V;\cdot)$ *is called* **isotopism** *if* $\alpha(x\circ y)=\beta(x)\cdot\gamma(y)$ $(x,y\in S)$.

The isotopism of quasifields Q and W (**autotopism**, if $Q=W$) is a triple of isomorphisms α,β,γ of additive group $(Q,+)$ to $(W,+)$, if its restrictions to the loop Q^* is an isotopism to W^*.

Right, middle and left nuclei N_r, N_m and N_l of semifield S are the invariants of isotopism:

$$N_r(S)=\{k\in S\mid x\circ(y\circ k)=(x\circ y)\circ k\ \ (x,y\in S)\},$$
$$N_m(S)=\{k\in S\mid x\circ(k\circ y)=(x\circ k)\circ y\ \ (x,y\in S)\},$$
$$N_l(S)=\{k\in S\mid k\circ(x\circ y)=(k\circ x)\circ y\ \ (x,y\in S)\}.$$

Kernel in quasifield Q generalizes the left nucleus of semifield:

$$K=\{k\in Q\mid k\circ(x\circ y)=(k\circ x)\circ y,\ k\circ(x+y)=k\circ x+k\circ y\ \ (x,y\in Q)\}.$$

The kernel of quasifield is a skewfield, and the quasifield is a vector space over kernel. It is easy to show that any finite quasifield can be determined as a vector space over prime subfield.

Lemma 1. *Let* $\langle Q,+,\cdot\rangle$ *be a quasifield of order* p^n, W *be* n*-dimensional linear space over* $\mathbb{Z}_p$. *Then there exists such a spread set*

$$R=\{\theta(w)\mid w\in W\}\subset GL_n(p)\cup\{0\},$$

that $\langle Q,+,\cdot\rangle$ *is isomorphic to* $\langle W,+,*\rangle$, *where* $x*y=x\theta(y)$, $x,y\in W$.

5. WENE'S CONJECTURE

In 1991 Wene [8] wrote the hypotheses: *any finite semifield D is right or left primitive*, i.e. every element of the loop D^* is a the set of right- or left-ordered powers of an element in a semifield D. In 2004 Rúa [9] has indicated a counter-example to Wene's conjecture, using Knuth's semifield of order 32. This *Knuth–Rúa's semifield* is neither right nor left primitive. The second counter-example gives a *Hentzel–Rúa's semifield* of order 64 [29], which was constructed in 2007. We consider both counter-examples detail in §§ 6 and 7.

Now the primitivity investigations are completed for semifields of orders up to 125 (see [29] and refers ibid). There exist only two semifields of order ≤ 125 (as above), which are neither left nor right primitive.

Note that the counter-examples of odd order are not known still.

Further in this section we consider some general known results in investigations of primitivity. The following definition gives its weakening.

Definition 3. *Any finite semifield D, which is d-dimensional over its center $Z(D)$, is said to be left-ciclyc if for some element $a \in D$ the semifield D has $Z(D)$-base $\{e,\ a,\ a^{(2}, \ldots, a^{(d-1}\}$.*

Any left-primitive semifield is also left-ciclyc [29]. Nevertheless, even known non-primitive semifields are left-ciclyc. The investigations of primitivity are based on the properties of spread set. It is known that for any finite semifield D with $Z(D) \simeq GF(q)$ and spread set Σ the characteristic polynomial for any matrix from $\Sigma \setminus \{\lambda E \mid \lambda \in GF(q)\}$ has no linear factors. The following theorem gives the main tool, which was used in [29].

Theorem 4. *If D is a finite semifield of dimension d over its center $Z(D) = GF(q)$, then $w \in D$ is a left primitive element of D iff the characteristic polynomial of a linear map $L_w : D \to D$, given by $L_w(x) = wx$, is an irreducible primitive polynomial of degree d over $Z(D)$.*

Some conditions from [9] and [30] for primitivity of semifields gives

Theorem 5. *Let S be a semifield, which is n-dimensional over its center $GF(q)$. Then S is left and right primitive, if either $n = 3$* or n is prime and q is large enough.

Cordero and Jha ([28] and [31]) consider the problem of existence of non-primitive quasifields and geometric conditions for primitivity.

Lemma 2. *A non-primitive quasifield of square order q^2 exists iff $q > 4$.*

Lemma 3. *For all sufficiently large primes p, the semifields coordinatizing a semifield plane Π of order p^5 are all primitive (right and left) if Π does not contain any proper subplane Π_0 of order $> p$.*

6. SEMIFIELDS OF ORDER 32 AND KNUTH–RÚA'S COUNTER-EXAMPLE

The Knuth–Rúa semifield $\Re$ of order 32 with the identity $x^{(22} = x$ is commutative and presents the first counter-example to Wene's hypotheses of primitivity for finite semifields. We describe its automorphisms.

Theorem 6. *The automorphism group $Aut\Re$ of Knuth–Rúa semifield $\Re$ is a cyclic group of order 5 and the set $\Re \setminus \{0, e\}$ is an union of six disjoint orbits under $Aut\Re$.*

The problems **(A)–(C)** for semifield $\Re$ are solved in ([24, 14]).

Theorem 7. *The loop $\Re^*$ of Knuth–Rúa semifield $\Re$ of order 32 is generated by any non-identity element. Its spectrum is $\{1, 5, 6, 7, 8, 10\}$ and right and, also, left spectra are $\{1, 21\}$.*

Up to isomorphism, there are 2501 proper semifields of order 32; they form 6 isotopic classes corresponding to six pairwise nonisomorphic planes $\pi(i)$ $(0 \leq i \leq 5)$. The following Table 3 [9] reflects other information.

Let's consider as [24] the spread sets of non-isomorphic semifield planes from [20]. The correspondent coordinatizing semifields P_j $(1 \leq j \leq 5)$, up to isotopisms, exhauste all proper semifields of order 32. Their structure is determined by following theorems which are proved in [24].

Theorem 8. *For any semifields P_i, $1 \leq i \leq 4$, the subfield of order 2 is a maximal subfield. The loop P_i^* is generated by any non-identity element, and the spectrum of loop is $\{1, 4, 5, 6, 7, 8\}$* for $i = 3$, or $\{1, 5, 6, 7, 8, 9\}$ *for $i = 4$ or* $\{1, 4, 5, 6, 7\}$ *for $i = 1, 2$.*

Table 3. Isomorphic classes of semifields of order 32

Plane	$\pi(0)$	$\pi(1)$	$\pi(2)$	$\pi(3)$	$\pi(4)$	$\pi(5)$
Left and right primitive	1	961	961	180	186	186
Only left primitive	0	0	0	6	0	7
Only right primitive	0	0	0	6	7	0
Neither L. nor R. prim.	0	0	0	1	0	0

According to [9] there exists a semifield of order 32 with a subfield of order 4. By Theorem 7, the prime subfield of Knuth—Rúa semifield is unique its subfield. Evidently that order of any finite semifield equals to some powers of right and left nuclei orders. So the nuclei of semifield of order 32 are necessary prime subfield. Nevertheless such semifields can contain a subfield of order 4.

Theorem 9. *The semifield P_5 contains the subfield H of order* 4, *that is unique maximal subfield. Each element from $P_5 \setminus H$ is of order > 3 and generates the loop P_5^*, the spectrum of the loop is* $\{1, 3, 4, 5, 6, 7, 8\}$.

7. HENTZEL—RÚA SEMIFIELD OF ORDER 64

In 2007 Rúa and Hentzel has indicated [29] the second counter-example to Wene's conjecture. The Hentzel—Rúa semifield is the unique semifield of order 64 which is neither left nor right primitive. By [29], there exist also 35 semifields of order 64 that are not left-primitive but are right-primitive.

Now we consider a structure of Hentzel—Rúa semifield. Let $M(6,2)$ be the ring of all 6×6-matrices over $\mathbb{Z}_2$ and let W be a 6-dimensional linear space over $\mathbb{Z}_2$, $W = \{x = (x_1, \ldots, x_6) \mid x_i \in \mathbb{Z}_2,\ i = 1, \ldots, 6\}$. We define the map $\theta : W \to M(6,2)$ by the rule $\theta(x) = x_1A_1 + \cdots + x_6A_6, \quad x \in W$, where matrices $A_1, A_2, \ldots, A_6 \in GL_6(2)$ are determined in [29]. Then we obtain a bijection θ from W into $GL_6(2) \cup \{0\}$ and $R = \{\theta(x) \mid x \in W\}$ is a spread set. It seems we get a semifield $\langle W, +, * \rangle$ of order 64 (the Hentzel—Rúa semifield $\mathcal{H}\mathfrak{R}$), defining the multiplication $*$ on W by the rule

$$x * y = x \cdot \theta(y) = x \sum_{i=1}^{6} y_i A_i.$$

The vector $e = (1, 0, \ldots, 0)$ is an identity in this semifield.

We obtain the following description of its automorphisms and maximal subfields.

Theorem 10. *The automorphism group of Hentzel—Rúa semifield $\mathcal{H}\mathfrak{R}$ is isomorphic to the symmetric group S_3 and hence has exactly three involution automorphisms.*

Theorem 11. *The semifield $\mathcal{H}\mathfrak{R}$ contains exactly six maximal subfields:*

5 *subfields of order* 8, *three from them are stabilizators of different involution automorphisms;*

the unique subfield of order 4, *which is a stabilizator of automorphism of order* 3.

We introduce the following subsets for the description of spectra:

$$K(m,n,k) = \{x \in \mathcal{H}\mathfrak{R} \mid |x|_l = m,\ |x|_r = n,\ |x| = k\}, \quad m, n, k \in \mathbb{N}.$$

It was shown that $K(7,7,7) \cup \{0, e\}$ is an union of all subfields of order 8. Evidently, that $K(3,3,3) \cup \{0, e\}$ is a subfield of order 4. Moreover,

$$|K(6,6,6)| = 12, \quad |K(7,7,6)| = 6, \quad |K(12,12,7)| = 6, \quad |K(15,15,5)| = 6,$$

and also we have

$$\mathcal{H}\mathfrak{R}^* = K(1,1,1) \cup K(3,3,3) \cup K(7,7,7) \cup K(6,6,6) \cup K(7,7,6) \cup K(12,12,7) \cup K(15,15,5).$$

Using these equalities we show that the loop $\mathcal{H}\mathfrak{R}^*$ is one-generated.

Lemma 4. *For any $n \geq 10$ the loop $\mathcal{H}\mathfrak{R}^*$ is an union of all n-*th *degrees of any element* $x \in K(6,6,6) \cup K(7,7,6) \cup K(12,12,7) \cup K(15,15,5)$.

Exacting this statement, we find all spectra.

Theorem 12. *The spectrum of the loop $\mathcal{H}\mathfrak{R}^*$ is $\{1,3,5,6,7\}$. The left and right spectra coincide with $\{1,3,6,7,12,15\}$.*

Thus, the semifield $\mathcal{H}\mathfrak{R}$ has no elements with left or right order $63 = |\mathcal{H}\mathfrak{R}| - 1$, and hence it is not primitive.

8. SOME LEMMAS AND QUASIFIELDS WITH ASSOCIATIVE POWERS

It is easy to show that the orders of elements of any finite loop are also finite.

Lemma 5. *The order of finite loop is not less than order of any its element.*

Proof. The proof of order boundedness of any element v from finite loop $L = (L, \circ)$ uses right-ordered and left-ordered powers. It is clear that such the powers are no more than $|L|$ pairwise distinct elements.

Choose the sequence $e, v^{1)}, v^{2)}, \cdots, v^{m)}$, that contains two equal elements with minimal $m \geq 1$. Evidently that $v^{m)} = v^{j)}$ for some j, $0 \leq j < m$. If $j > 0$ that both elements $v^{m-1)}$ and $v^{j-1)}$ are the solutions of the equation $y \circ v = v^{j)}$ in a loop L and so are equal, that contradicts to choice of m. Hence, $j = 0$ and $v^{m)} = e$. From the proved we have

$$|v| \leq |v|_r \leq |L|, \quad |v| \leq |v|_l \leq |L|.$$

□

Lemma 6. *Let α be m-*th *power of an element v from commutative quasigroup. If α contains v^2 as a sub-product no more an once, then $\alpha = v^{(m}$.*

Proof. Let's suppose that $m \geq 3$ (the case $m \leq 2$ is trivial). By induction, the lemma is proved for k-th powers for any k. Using commutativity, we can suppose also that all multiplications of v^2 in α are only from the right. Then the minimal sub-product in α that contains v^2 and is not v^2 is of a form v^3; else v^2 is in α more than once. Analogously, the next minimal sub-product in α equals to v^4. So we get the equality $\alpha = v^{(m}$. □

Lemma 7. *Any power > 1 of an element v from commutative quasigroup is a product, with suitable positioning of brackets, of elements $v^{(m}$, $m \geq 2$, and, possible, of products at least two such factors to v.*

The quasifields with associative powers are the most studied. First of all it is alternative semifield. In a finite case it is a field, according Artin.

In 1952 Albert [34] proved the following theorem.

Theorem 13. *Any finite semifield with associative powers of characteristic $p \neq 2$, the center of which contains more than 5 elements, is a finite field.*

The associative quasifield is called *nearfield*. In 1936 Zassenhaus [41] described all finite nearfields. They are exhausted by Dickson nearfields and 7 exceptional Zassenhaus nearfields of order p^2 for prime $p = 5, 7, 11, 23, 29$ and 59 (see also Hall [10, Theorem 20.7.2]).

The known description of sub-nearfields for finite nearfield is considerably transferred from the description of subfields for finite field (see Dancs [35]). It is easy to prove

Lemma 8. *A nearfield Q is a finite field if its loop Q^* is one-generated.*

In connection with the statements of Proposition 1 (i) and Corollary 1 we note that the center even of finite nearfield is not necessary a field.

Remark 1. Let N be the exceptional Zassenhaus nearfield of order 25 [10, page 420]. Then the loop N^* is isomorphic to the group $SL(2,3)$ with the center of order 2. Therefore the center of nearfield N equals $\{0, e, -e\}$ and coincides no prime subfield of N.

The projective plane that is coordinatized by nearfield is called a nearfield plane. We now consider more wide class of translation planes which are coordinatized by Moufang quasifield, i.e., the quasifield with Moufang loop (cf. [10, Theorem 20.5.3]). The loop M is called *Moufang loop* if for all $x, y, z \in M$ the following holds:

$$(xy)(zx) = (x(yz))x, \quad ((xy)x)z = x(y(xz)), \quad x(y(zy)) = ((xy)z)y.$$

The Moufang loops of order less than 32 were described by Chein in 1974, [33]. Some group-theoretic theorems (Lagrange, Sylow and Hall theorems) are transferred to Moufang loops (Grishkov, Zavarnitsyn, 2005–2013, [36–38]; Gagola, 2010, [39]). See also Liebeck, 1987 [40]. It is possible to use these results for classification of certain Moufang quasifields.

9. QUASIFIELDS OF ORDERS 16, 32 AND 81

According to Dempwolff and Reifart (1983, [19]), the number of all non-desarguesian translation planes of order 16 equals to 7. Its spread sets allow to construct the representatives of quasifields isotopic classes.

For correspondent representatives Q_j, $1 \leq j \leq 5$, of isotopic classes without semifields the next theorem is proved [24].

Theorem 14. *Any quasifield Q_j, $j = 1, 2, 3$, is a set-theoretic union of 7 maximal subfields of order 4 and all its spectra coincide with $\{1, 3\}$.*

Theorem 15. *For the quasifield Q_4 the kernel is unique maximal subfield of order 4. The quasifield Q_5 contains 3 maximal subfields of order 4 and its kernel is of order 2. The loop Q_j^*, $j = 4, 5$, is generated by any element which is not from maximal subfields, and all its spectra are $\{1, 3, 5\}$.*

Knuth was constructed (see [6]) the projective planes $\pi(i)$ $(1 \leq i \leq 5)$ of order 32 and was proved that these planes exhauste, up to isomorphisms, all non-desarguesian semifield planes of order 32.

So the proper semifields of order 32 are determined, up to isotopisms, as corresponding coordinatizing sets P_j $(1 \leq j \leq 5)$ (the semifields of order 32 are classified also by Walker (1962, [23])). The structure of these semifields are determined by next two theorems [24].

Theorem 16. *The semifield P_5 contains the subfield H of order 4, that is a unique maximal subfield. Any element from $P_5 \setminus H$ generates the loop P_5^*, the element order is more than 3, the loop spectrum is $\{1, 3, 4, 5, 6, 7, 8\}$.*

Theorem 17. *Any semifield P_i, $1 \leq i \leq 4$, contains only minimal subfield. The loop P_i^* is generated by any non-identity element, the loop spectrum is $\{1, 4, 5, 6, 7, 8\}$ for $i = 3$, $\{1, 5, 6, 7, 8, 9\}$ for $i = 4$ and $\{1, 4, 5, 6, 7\}$ for $i = 1, 2$.*

The classification of translation planes of order 32 has been completed by Dempwolff and Rockenfeller in 2011 (see [20, 22]).

Up to isomorphisms, except 6 semifield planes (with Desarguesian plane) there exist exactly 3 translation non-semifield planes of order 32. Using their spread sets from [20], we can construct the coordinatizing quasifields Q_i, $i = 1, 2, 3$. Their structure is described in [14].

Theorem 18. *For quasifields Q_i $(i = 1, 2, 3)$ the prime subfield is maximal, the loop Q_i^* is right-primitive, its spectrum is $\{1, 4, 5, 6, 7\}$.*

Further we consider the semifields that coordinatize the semifield planes of order 81 admitting a Baer involution.

Definition 4. *The collineation of finite projective plane π is said to be Baer collineation if it fixes pointwise the subplane π_0 of order $|\pi_0| = \sqrt{|\pi|}$.*

Let π be a semifield plane of order 81 that admit a Baer involution. Then, using [32], we can consider coordinatizing semifield W as a 4-dimensional vector space over $\mathbb{Z}_3$ and spread set in $GL_4(3) \cup \{0\}$:

$$R = \left\{ \begin{pmatrix} m(U) & f(V) \\ V & U \end{pmatrix} \,\middle|\, U, V \in K \right\}.$$

Here K is the field of order 9 in $GL_2(3) \cup \{0\}$,

$$K = \left\{ U = u_1 \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} + u_2 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \,\middle|\, u_1, u_2 \in \mathbb{Z}_3 \right\},$$

m, f are injective maps from K to $GL_2(3) \cup \{0\}$, $m(E) = E$, $f(E) \neq E$.

Computer calculations lead to construction of 106 semifield planes of order 81 with Baer involution. Next considerations of isomorphisms give the result:

Theorem 19. *There exist exactly 8, up to isomorphisms, non-desarguesian semifield planes of order 81, which admit a Baer involution in translation complement.*

Table 4. The structure of non-isotopic semifields of order 81, that admit automorphism of order 2

Semifield W	$\lvert N_l \rvert$	Spectrum	Left spectrum
W_1	3	$\{1, 2, 4, 5, 6, 7, 8\}$	$\{1, 2, 4, 8, 16, 40, 80\}$
W_2	3	$\{1, 2, 4, 5, 6, 7, 8\}$	$\{1, 2, 4, 5, 8, 10, 16, 20, 40, 80\}$
W_3	3	$\{1, 2, 4, 6, 7, 8\}$	$\{1, 2, 4, 8, 16, 40, 80\}$
W_4	3	$\{1, 2, 4, 5, 6, 7, 8, 9, 10\}$	$\{1, 2, 4, 8, 16, 80\}$
W_5	9	$\{1, 2, 4, 5, 6, 7, 8\}$	$\{1, 2, 4, 8, 16, 40, 80\}$
W_6	9	$\{1, 2, 4, 6, 7, 8\}$	$\{1, 2, 4, 8, 16, 80\}$
W_7	9	$\{1, 2, 4, 6, 8, 9, 13\}$	$\{1, 2, 4, 8, 16, 40, 80\}$
W_8	9	$\{1, 2, 4, 6, 7, 8\}$	$\{1, 2, 4, 8, 16, 40, 80\}$

The structure of correspondent coordinatizing semifields W_i, $i = 1, \ldots, 8$, is determined. The results are summarized by Table 4.

Lemma 9. *Any semifield W_i admits an automorphism of order* 2 *and contains* 1 *or* 3 *maximal subfields of order* 9. *The loop W_i^* is left- and right-primitive, it contains a subloop of order* 16 *and* 1 *or* 3 *subgroup of order* 4.

Lemma 10. *The semifields W_3 and W_8 contains exactly three subfields of order* 9, *another semifields contain unique subfield of order* 9. *Tne order of automorphism group Aut W equals to* 8 *for W_8*, 2 *for W_1 and W_3 and* 4 *for other semifields.*

ACKNOWLEDGMENTS

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

REFERENCES

1. A. G. Kurosh, *Lectures on General Algebra* (Chelsea, New York, 1963).
2. O. Veblen and J. H. Maclagan-Wedderburn, “Non-Desarguesian and non-Pascalian geometries,” Trans. Am. Math. Soc. **8**, 379–388 (1907).
3. L. E. Dickson, “Linear algebras in which division is always uniquely possible,” Trans. Am. Math. Soc. **7**, 370–390 (1906).
4. E. Kleinfeld, “Techniques for enumerating Veblen–Wedderburn systems,” J. Assoc. Comput. Mach. **7**, 330–337 (1960).
5. D. E. Knuth, “Finite semifields and projective planes,” PhD Dissertation (California Inst. of Technology, Pasadena, 1963).
6. D. E. Knuth, “Finite semifields and projective planes,” J. Algebra **2**, 182–217 (1965).
7. N. L. Johnson, V. Jha, and M. Biliotti, *Handbook of Finite Translation Planes* (Chapman and Hall, Boca Raton, London, New York, 2007).
8. G. P. Wene, “On the multiplicative structure of finite division rings,” Aequationes Math. **41**, 791–803 (1991).
9. I. F. Rua, “Primitive and non-primitive finite Semifields,” Commun. Algebra **22**, 223–233 (2004).
10. M. Hall, *The Theory of Groups* (Chelsea, New York, 1976).
11. V. M. Levchuk, S. V. Panov, and P. K. Shtukkert, “The structure of finite quasifields and their projective translation planes,” in *Proceedings of the 12th International Conference on Algebra and Number Theory, Tula, Russia, 2014* (Tula, 2014), pp. 106–108.
12. O. V. Kravtsova and P. K. Kurshakova (Shtukkert), “On question of isomorphism of semifield planes,” Vestn. Krasnoyarsk Tekh. Univ. **42**, 13–19 (2006).
13. V. M. Levchuk and P. K. Shtukkert, “Problems on structure for quasifields of orders 16 and 32,” J. Sib. Fed. Univ., Ser. Math. Phys. **7**, 362–372 (2014).
14. V. M. Levchuk and P. K. Shtukkert, “The structure of quasifields of small even orders,” Proc. Steklov Inst. Math. Mech. **21**, 197–212 (2015).
15. D. R. Hughes and F. C. Piper, *Projective Planes* (Springer, New York, 1973).

16. J. Andre, "Über nicht-Desarguesche Ebenen mit transitiver Translationgruppe," Math. Z. **60**, 156–186 (1954).
17. M. Kallaher, *Affine Planes with Transitive Collineation Groups* (North-Holland, Amsterdam, 1982).
18. A. A. Albert, "Finite division algebras and finite planes," Proc. Symp. Appl. Math. **10**, 53–70 (1960).
19. U. Dempwolff and A. Reifart, "The classification of the translation planes of order 16, Part I," Geom. Dedic. **15**, 137–153 (1983).
20. U. Dempwolff, File of Translation Planes of Small Order. http://www.mathematik.uni-kl.de/∼dempw/dempw_Plane.html.
21. *The Kourovka Notebook, Unsolved Problems in Group Theory,* 15th ed. (Novosib. Inst. Mat. SO RAN, Novosibirsk, 1992) [in Russian].
22. R. Rockenfeller, "Translationsebenen der Ordnung 32," Diploma Thesis (FB Mathematik, Univ. of Kaiserslautern, 2011).
23. R. J. Walker, "Determination of division algebras with 32 Elements," in *Proceedings of the 15th Symposium on Applied Mathematics* (Am. Math. Soc., 1962), pp. 83–85.
24. P. K. Shtukkert, "Quasifields and translation planes of smallest even order," Byull. Irkutsk Univ. **7**, 144–159 (2014).
25. G. P. Nagy, "Linear groups as right multiplication groups of quasifields," arXiv: 1210.1652v1 [math.CO] (2012).
26. G. Menichetti, "On a Kaplansky conjecture concerning three-dimensional division algebras over a finite field," J. Algebra **47**, 400–410 (1977).
27. M. Lavrauw, "Finite semifields and nonsingular tensors," Designs, Codes Cryptogr. **68**, 205–227 (2013).
28. M. Cordero and V. Jha, "On the multiplicative structure of quasifields and semifields: cyclic and acyclic loops," Note Mat. **29**, 45–59 (2009).
29. I. R. Hentzel and I. F. Rua, "Primitivity of Finite Semifields with 64 and 81 elements," Int. J. Algebra Comput. **17**, 1411–1429 (2007).
30. R. Gow and J. Sheekey, "On primitive elements in finite semifields," Finite Fields Appl. **17**, 194–204 (2011).
31. M. Cordero and V. Jha, "Primitive semifields and fractional planes of order q^5," Rend. Mat., Ser. VII **30**, 1–21 (2010).
32. O. V. Kravtsova, "Semifield planes of odd order that admit the autotopism subgroup isomorphic to A_4," Russ. Math. (Izv. VUZ), No. 9, 10–25 (2016).
33. O. Chein, "Moufang loops of small order," Trans. Am. Math. Soc. **188** (2), 31–51 (1974).
34. A. A. Albert, "On nonassociative division algebras," Trans. Am. Math. Soc. **72**, 296–309 (1952).
35. S. Dancs, "The sub-near-field structure of finite near-fields," Bull. Austral. Math. Soc. **5**, 275–280 (1971).
36. A. N. Grishkov and A. V. Zavarnitsyn, "Lagrange's theorem for Moufang loops," Math. Proc. Phil. Soc. **139**, 41–57 (2005).
37. A. N. Grishkov and A. V. Zavarnitsyn, "Sylow's theorems for Moufang loops," J. Algebra **321**, 1813–1825 (2009).
38. A. N. Grishkov and A. V. Zavarnitsyn, "Abelian-by-cyclic Moufang loops," Comm. Algebra **41**, 2242–2253 (2013).
39. W. S. M. Gagola, "Hall's theorem for Moufang loops," J. Algebra **323**, 3252–3262 (2010).
40. M. Liebeck, "The classification of finite simple Moufang loops," Math. Proc. Phil. Soc. **102**, 33–47 (1987).
41. H. Zassenhaus, "Über endliche Fastkörper," Abh. Math. Sem. Hamburg **11**, 187–220 (1936).