O.V. KRAVTSOVA

ON AUTOMORPHISMS OF SEMIFIELDS AND SEMIFIELD PLANES

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

E-mail address: ol71@bk.ru

Received 01.09.2016

Abstract. We consider relations between a semifield projective plane and its coordinatizing semifield using the linear space and a spread set. We state the geometrical sense of an involutory automorphism for a finite semifield and study some of its properties.

1. Introduction

The coordinatization of points and lines in a finite projective plane allows to study its geometrical properties through the investigation of algebraic properties of the coordinatizing set. So, a desarguesian (classic) finite projective plane is coordinatized by the field, and the weakening of axioms of commutativity and associativity leads to translation planes that are coordinatized by quasifields. If the dual to a translation plane is also translation, then such the plane is coordinatized by a semifield and is called a semifield plane. The most complete review on semifields, quasifields and correspondent projective planes is presented in [1].

The construction of a finite semifield plane (as a translation plane) usually uses a linear space over finite field and a certain set of linear maps, a so-called spread set. This method is considerably related with computer calculations, and so, it is necessary to represent the elements in a convenient form. This paper uses the matrix representation of a spread set over a field of prime order and it allows to simplify the considerations and calculations.

Key words and phrases. Semifield, semifield projective plane, autotopism, automorphism, Baer involution..

This work is supported by RFBR (projects 15-01-04897, 16-01-00707).

We state the results describing the relationship between autotopisms and automorphisms of finite semifield and collineations of the corresponding semifield plane. For instance, we determine the geometrical sense of an involution automorphism and its stabilizer. These results are illustrated by the examples of semifields of orders 64 and 81.

2. Semifield and spread set

A *semifield*, according to [2], is a set S with two binary algebraic operations $+$ and $*$ such that:

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

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

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

The weakening of two-sided distributivity to one-sided leads to the notion of *quasifield*, right or left. Further we shall say "quasifield" instead of "right quasifield" , i.e. a structure with the rule $a*(b+c) = a*b+a*c$.

The semifield S contains the subsets N_r, N_m, N_l which are called *right, middle* and *left nuclei* respectively:

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

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

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

is the *center* of semifield. The center and all nuclei of a finite semifield are subfields, and the semifield is a linear space over any of them. So, the order of finite semifield equals to p^n where p is a prime number.

Let W be a d-dimensional linear space over the field $GF(p^k)$, and let R be a set of linear maps, $R \subset GL_d(p^k) \cup \{0\}$, such that:

1) R has exactly p^{dk} square $(d \times d)$-matrices over $GF(p^k)$;

2) R contains the zero and the identity matrices (0 and E);

3) for any two different matrices $A, B \in R$, $A \neq B$ the difference $A - B$ is a non-singular matrix.

Such a set R is said to be a *spread set* (see [2]).

The enumerated conditions imply that a matrix of a given spread set is uniquely determined by the choice of any of its rows or columns. In particular, we can consider the elements of the matrix as the functions

of the first row, and so, we define the bijective map θ from W onto R such that

$$R = \{\theta(y) \mid y \in W\},$$

where y is the first row of $\theta(y)$. So, from the definition, we have

$$\theta(0, 0, \dots 0) = 0, \quad \theta(1, 0, \dots, 0) = E.$$

If we define the multiplication on W by the rule

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

then $\langle W, +, * \rangle$ is a (right) quasifield ([3], [4]). Moreover, if R is closed under addition then W is a semifield.

Note that the center Z of a semifield is usually used as a basic field $GF(p^k)$ to construct a semifield. Nevertheless, it is more convenient to consider a linear space W and the spread set R over the prime subfield $\mathbb{Z}_p$. Then the map θ can be written only by linear functions, which considerably simplifies the considerations and calculations. It is true, more general, also for a quasifield.

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

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

such that $\langle Q, +, \cdot \rangle$ is isomorphic to $\langle W, +, * \rangle$, where

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

Proof. The quasifield Q is an n-dimensional linear space over the field $\mathbb{Z}_p$; let $e_1, \dots, e_n$ be its base. Let's consider any base $\varepsilon_1, \dots, \varepsilon_n$ of the space W and state the correspondence

$$\varphi : e_i \to \varepsilon_i, \quad i = 1, 2, \dots, n,$$

which is continued to a isomorphism of linear spaces Q and W.

For any fixed element $q \in Q$, the right multiplication

$$\beta_q : x \to x \cdot q, \quad x \in Q,$$

is a linear map of the space Q over $\mathbb{Z}_p$, because of the right distributivity. Let

$$\overline{\beta_q} : \varphi(x) \to \varphi(\beta_q(x))$$

be the correspondent linear map of the space W and $\theta(\varphi(q))$ be its matrix in the base $\varepsilon_1, \dots, \varepsilon_n$. Evidently, $R = \{\theta(y) \mid y \in W\}$ is a subset in $GL_n(p) \cup \{0\}$, $\theta(0) = 0$ is the zero matrix, $\theta(\varphi(1)) = E$ is the identity

matrix (where 1 is the identity of the quasifield Q). If we define the multiplication $*$ on W by the rule

$$x * y = x\theta(y), \quad x, y \in W,$$

then $\langle Q, +, \cdot \rangle$ is isomorphic to $\langle W, +, * \rangle$. Further we prove the condition $\theta(x) - \theta(y) \in GL_n(p)$ for $x \neq y$. Indeed, if $\det(\theta(x) - \theta(y)) = 0$ then for some element $z \in W \setminus \{0\}$

$$z(\theta(x) - \theta(y)) = 0 \Rightarrow z\theta(x) = z\theta(y) \Rightarrow z * x = z * y$$

and for the pre-images $z_0, x_0, y_0 \in Q$ we have $z_0 \cdot x_0 = z_0 \cdot y_0$, which contradicts the definition of quasifield. □

In the case of a semifield it is sufficient to define the multiplication only for basic elements because of the two-sided distributivity. Let $e_1, \ldots, e_n$ be the base of a semifield W as of an n-dimensional linear space over $\mathbb{Z}_p$ and

$$e_i * e_j = a_{ij1}e_1 + a_{ij2}e_2 + \cdots + a_{ijn}e_n, \qquad i, j = 1, 2, \ldots, n.$$

All coefficients a_{ijk} $(i, j, k = 1, \ldots, n)$ form so-called *cubic array, or hypercube*, which is used for semifield classification (see also [5]).

Let's illustrate this method by construction of Dickson's commutative semifield of order 81 and the spread set in $GL_4(3) \cup \{0\}$.

Let $F = GF(p^2)$, let σ be an automorphism of the field F, and let a be a non-square element of F. Then the set $S = \{x + \lambda y \mid x, y \in F\}$ with the addition

$$(x + \lambda y) + (z + \lambda t) = (x + z) + \lambda(y + t)$$

and the multiplication

$$(x + \lambda y)(z + \lambda t) = (xz + ay^\sigma t^\sigma) + \lambda(yz + xt)$$

is a commutative semifield (Theorem 9.12, [2]).

If we assume $F \simeq \mathbb{Z}_3[x]/(x^2 - x - 1)$,

$$F = \{0, 1, -1, \alpha, \alpha + 1, \alpha - 1, -\alpha, -\alpha + 1, -\alpha - 1\}, \qquad \alpha^2 = \alpha + 1,$$

and choose $a = \alpha$, $x^\sigma = x^3$, then the multiplication law is defined as

$$(x + \lambda y)(z + \lambda t) = (xz + \alpha y^3 t^3) + \lambda(yz + xt).$$

Further, we choose the base $1, \alpha, \lambda, \lambda\alpha$ of S and calculate all products of the basic elements:

$$\begin{array}{cccc} 1\cdot 1=1 & 1\cdot\alpha=\alpha & 1\cdot\lambda=\lambda & 1\cdot\lambda\alpha=\lambda\alpha \\ \alpha\cdot 1=\alpha & \alpha\cdot\alpha=\alpha+1 & \alpha\cdot\lambda=\lambda\alpha & \alpha\cdot\lambda\alpha=\lambda\alpha+\lambda \\ \lambda\cdot 1=\lambda & \lambda\cdot\alpha=\lambda\alpha & \lambda\cdot\lambda=\alpha & \lambda\cdot\lambda\alpha=-1 \\ \lambda\alpha\cdot 1=\lambda\alpha & \lambda\alpha\cdot\alpha=\lambda\alpha+\lambda & \lambda\alpha\cdot\lambda=-1 & \lambda\alpha\cdot\lambda\alpha=\alpha-1 \end{array}$$

Let W be a 4-dimensional linear space over $\mathbb{Z}_3$, and let

$$f_1=(1,0,0,0),\ f_2=(0,1,0,0),\ f_3=(0,0,1,0),\ f_4=(0,0,0,1)$$

be the canonical base. Using the correspondence

$$1\to f_1,\ \alpha\to f_2,\ \lambda\to f_3,\ \lambda\alpha\to f_4,$$

we calculate the matrices $\theta(f_2)$, $\theta(f_3)$, $\theta(f_4)$ ($\theta(f_1)=E$):

$$\begin{array}{l} f_1\circ f_2=f_1\theta(f_2)=f_2, \\ f_2\circ f_2=f_2\theta(f_2)=f_2+f_1, \\ f_3\circ f_2=f_3\theta(f_2)=f_4, \\ f_4\circ f_2=f_4\theta(f_2)=f_3+f_4, \end{array} \qquad \theta(f_2)=\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix};$$

$$\begin{array}{l} f_1\circ f_3=f_1\theta(f_3)=f_3, \\ f_2\circ f_3=f_2\theta(f_3)=f_4, \\ f_3\circ f_3=f_3\theta(f_3)=f_2, \\ f_4\circ f_3=f_4\theta(f_3)=-f_1, \end{array} \qquad \theta(f_3)=\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix};$$

$$\begin{array}{l} f_1\circ f_4=f_1\theta(f_4)=f_4, \\ f_2\circ f_4=f_2\theta(f_4)=f_3+f_4, \\ f_3\circ f_4=f_3\theta(f_4)=-f_1, \\ f_4\circ f_4=f_4\theta(f_4)=-f_1+f_2, \end{array} \qquad \theta(f_4)=\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ -1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 \end{pmatrix}.$$

So, the spread set $R\subset GL_4(3)\cup\{0\}$ consists of all matrices

$$\theta(y_1,y_2,y_3,y_4)=y_1\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}+y_2\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}+$$

$$+y_3\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix}+y_4\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ -1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 \end{pmatrix}.$$

It can be immediately proved that for any non-zero vector $y = (y_1, y_2, y_3, y_4)$, $y_i \in \mathbb{Z}_3$, the matrix $\theta(y)$ is non-singular. Thus we constructed a representation of Dickson's commutative semifield of order 81 over $\mathbb{Z}_3$.

In previous reasoning we used the first row to determine the matrix from the spread set. Evidently, another row of column will imply to another multiplication law and another semifield which is not necessarily isomorphic to the first semifield.

For instance, let's consider the first of 12 spread sets from the paper [6]. U. Dempwolff enumerated the basic elements of a spread set R as of a 4-dimensional linear space over $\mathbb{Z}_3$:

$$E, \quad B = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 2 & 0 & 0 & 2 \\ 2 & 2 & 2 & 2 \end{pmatrix}, \quad C = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 2 & 2 \\ 1 & 1 & 2 & 2 \end{pmatrix}, \quad D = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 \\ 2 & 2 & 2 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix}.$$

We define the map θ by the rule

$$\theta(y_1, y_2, y_3, y_4) = y_1E + y_2B + y_3C + y_4D,$$

i.e., we determine the matrix through its first row. So, we obtain the semifield $\langle W, +, * \rangle$ which contains the subfield $\{(y_1, y_2, 0, 0) \mid y_1, y_2 \in \mathbb{Z}_3\}$ of order 9.

Further we consider another base of the same spread set R:

$$B' = \begin{pmatrix} 1 & 2 & 0 & 2 \\ 2 & 0 & 1 & 0 \\ 2 & 1 & 2 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad C' = \begin{pmatrix} 2 & 2 & 2 & 1 \\ 2 & 1 & 2 & 2 \\ 0 & 1 & 2 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \quad D' = \begin{pmatrix} 2 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 2 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad E;$$

here, evidently, $B' = 1 \cdot E + 2 \cdot B + 0 \cdot C + 2 \cdot D$ etc. Hence we corresponde a matrix from the spread set to its fourth row and obtain another map $\sigma : W \to R$,

$$\sigma(y_1, y_2, y_3, y_4) = y_1B' + y_2C' + y_3D' + y_4E,$$

and another operation:

$$x \circ y = x \cdot \sigma(y), \quad \forall x, y \in W.$$

Then the semifield $\langle W, +, \circ \rangle$ does not contain any proper subfield except the prime subfield $\mathbb{Z}_3$; it can be calculated directly.

The semifields determined by different bases of the same spread set R are isotopic, as was proved in [5]. Remind that two semifields $\langle S, +, * \rangle$

and $\langle W, +, \circ\rangle$ are called *isotopic* if there exists a triple (φ, ψ, ξ) of non-singular additive maps from S to W such that

$$\varphi(x) \circ \psi(y) = \xi(x * y) \qquad \forall x, y \in S.$$

This triple (φ, ψ, ξ) is called an *isotopism* from S to W. For completeness of a consideration, we will prove the result from [5] using our notation.

Lemma 2. *Let W be an n-dimensional linear space over $\mathbb{Z}_p$; let $R \subset GL_n(p) \cup \{0\}$ be the spread set closed under addition, let*

$$R = \{\theta(x) \mid x \in W\} = \{\sigma(x) \mid x \in W\},$$

where θ and σ are two additive bijections from W to R, and let

$$x * y = x\theta(y), \qquad x \circ y = x\sigma(y), \quad x, y \in W.$$

Then the semifield $\langle W, +, *\rangle$ is isotopic to the semifield $\langle W, +, \circ\rangle$.

Proof. For every $y \in W$, the matrix $\theta(y) \in R$ is equal to a certain matrix $\sigma(y')$, $y' \in W$, then

$$x * y = x\theta(y) = x\sigma(y') = x \circ y' = x \circ \sigma^{-1}(\theta(y)), \quad x, y \in W.$$

The bijective map $y \to \sigma^{-1}(\theta(y))$ is, evidently, additive and satisfies the definition. □

Paying attention to the example above, we will specify that an isotopism does not preserve, in general, the subfields orders. But the corresponding nuclei N_l, N_m, N_r of isotopic semifields are isomorphic.

3. Semifield and semifield plane

In this section, we consider the projective planes which are coordinatized by semifields (semifield planes) and specify the relationship between the plane automorphisms and semifield automorphisms and autotopisms. We use definitions and main results from [2, 5] (and change the notation, if it is necessary).

A *projective plane* π is the set of points and lines with the incidence relation between the points and lines such that:

1) any two distinct points are incident with a unique line;

2) any two distinct lines are incident with a unique point;

3) there exists a non-degenerated quadrangle, i.e. four points such that no three of them are incident with a common line.

The *order* of a projective plane is the number N such that at least one line (equivalently, any line) is incident to exactly $N + 1$ points. In this case the plane has exactly $N^2 + N + 1$ points and the same number of

lines. It is possible to coordinatize the points and the lines of a projective plane of order N using the set with N elements [2]. Then the algebraic properties of the coordinatizing set determine the geometric properties of the projective plane.

Recall that an *isomorphism* of a projective plane π onto a projective plane π' is a bijective map from the points of π to the points of π' and from the lines of π to the lines of π' which preserves the incidence relation. An isomorphism of a projective plane onto itself is called an *automorphism*, or a *collineation*. All collineation of a projective plane π form the *full collineation group* $Aut\,\pi$.

Let W be an n-dimensional linear space over $\mathbb{Z}_p$,let

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

be a spread set closed under addition, and let $\langle W, +, * \rangle$ be the semifield with multiplication $x * y = x\theta(y)$. Let's consider the outer direct sum $V = W \oplus W$ and define the projective plane π:

1) the elements (x, y), $x, y \in W$, from the space V are the affine points;

2) the cosets to subgroups

$$V(m) = \{(x, x\theta(m)) \mid x \in W\}, \quad m \in W,$$
$$V(\infty) = \{(0, y) \mid y \in W\}$$

are the affine lines;

3) the set of all cosets to the same subgroup $V(m)$ or $V(\infty)$ is the singular point (m) or (∞) respectively;

4) the set of all singular points is the singular line $[\infty]$;

5) the incidence is set-theoretical.

This projective plane is a semifield plane and its full collineation group is $Aut\,\pi = T\lambda G$, where $T = \{\tau_{a,b} \mid a, b \in W\}$ is the translation group,

$$\tau_{a,b} : (x, y) \to (x + a, y + b), \quad x, y \in W,$$

G is the translation complement, the stabilizer of the point $(0, 0)$. The automorphisms from G are determined by the linear maps of the space V:

$$\alpha : (x, y) \to (x, y) \begin{pmatrix} A & B \\ C & D \end{pmatrix}.$$

Here A, B, C, D are $(n \times n)$-matrices over $\mathbb{Z}_p$ (it is possible to prove that $C = 0$ for any semifield plane). Note that a representation of collineations from G only by linear maps is possible because we use a prime order field as the basic field. In the general case, these collineations are represented by semi-linear maps, which complicates the reasoning.

The subgroup $\Lambda < G$ of all collineations fixing the triangle with the vertices $(0,0),(0),(\infty)$ and the sides $[0,0],[0],[\infty]$ (see [2]), is called the *autotopism group*. The corresponding matrices are block-diagonal,

$$(x,y)^\lambda = (x,y)\begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix}, \tag{1}$$

$\lambda \in \Lambda$. Because λ is an automorphism, then the block-matrices A and D must satisfy the certain condition.

As any collineation, λ preserves the incidence relation. Hence, for any vector $x \in W$ and any matrix from spread set $\theta(y) \in R$ the image of a point $(x, x\theta(y))$ is incident to the line through $(0,0)$. So, there exists $z \in W$ and $\theta(t) \in R$ such that

$$(x,x\theta(y))^\lambda = (x,x\theta(y))\begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix} = (xA, x\theta(y)D) = (z, z\theta(t)).$$

Thus, $z = xA$, $z\theta(t) = xA\theta(t) = x\theta(y)D$ for any $x \in W$. And finally we obtain (see also [5]):

Lemma 3. *The map* (1) *defines an autotopism of a semifield plane π with the spread set R iff $A^{-1}\theta(y)D \in R$ for any matrix $\theta(y) \in R$.*

Further, we consider an autotopism of a semifield $\langle W, +, * \rangle$ (as an isotopism from W to W):

$$\varphi(x) * \psi(y) = \xi(x * y), \quad x, y \in W.$$

As the maps φ, ψ, ξ are additive then they are linear maps of the space W, so

$$\varphi(x) = xA, \quad \psi(x) = xB, \quad \xi(x) = xD, \quad x \in W, \tag{2}$$

$A, B, D \in GL_n(p)$.

Lemma 4. *If a triple of matrices (A,B,D) from $GL_n(p)$ defines an autotopism* (2) *of the semifield W, then the matrix*

$$\begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix} \tag{3}$$

defines an autotopism of the semifield plane π coordinatized by W. And inversely, if the matrix (3) *is an autotopism of the plane π, then there exists a matrix $B \in GL_n(p)$ such that (A,B,D) is an autotopism of the semifield W.*

Proof. According to the definition of autotopism,

$$xA * yB = (x * y)D, \quad xA\theta(yB) = x\theta(y)D \quad \forall x, y \in W.$$

Then, $\theta(yB) = A^{-1}\theta(y)D$ and the matrix (3) defines an autotopism of a plane. Inversely, the map

$$y \to A^{-1}\theta(y)D$$

from W to $GL_n(p)$ is linear; so, Lemma 3 implies the condition $A^{-1}\theta(y)D = \theta(yB)$ for certain matrix B. □

Let φ be an automorphism of a semifield W; then

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

Analogous reasoning with replacing $\varphi(x) = xA$ leads to the following result.

Lemma 5. *If the matrix $A \in GL_n(p)$ defines an automorphism of a semifield W, then the matrix*

$$\begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix} \tag{4}$$

defines an autotopism of the semifield plane π coordinatized by W (such an autotopism fixes the line $y = x$, not necessarily pointwise). Inversely, if the matrix (4) *defines an autotopism of the plane π and satisfies the condition*

$$A^{-1}\theta(y)A = \theta(yA) \qquad \forall y \in W, \tag{5}$$

then the matrix A defines an automorphism of the semifield W.

Note also the important result on semifields and semifield planes:

Theorem 1 ([2], Theorem 8.11)**.** *Two semifields coordinatize the isomorphic semifield planes iff they are isotopic.*

4. An involution automorphism of finite semifield

In this section, we consider the automorphism of order 2 of a finite semifield W and some special collineations of a semifield plane π, which is coordinatized by W.

A collineation of a projective plane π is called *central*, if it fixes some line l pointwise (the axis) and some point A linewise (the center). If the center is incident to the axis, then the collineation is said to be an *elation*, else a *homology*.

For any semifield plane all elations with the axis [0] and the center (∞) form an elementary abelian subgroup in the translation complement G:

$$\left\{ \begin{pmatrix} E & \theta(m) \\ 0 & E \end{pmatrix} \;\middle|\; m \in W \right\}.$$

All homologies in the autotopism group Λ form the cyclic subgroups

$$\left\{ \begin{pmatrix} E & 0 \\ 0 & \theta(m) \end{pmatrix} \;\middle|\; m \in N_r^* \right\}, \qquad \left\{ \begin{pmatrix} \theta(m) & 0 \\ 0 & E \end{pmatrix} \;\middle|\; m \in N_m^* \right\},$$

$$\left\{ \begin{pmatrix} M & 0 \\ 0 & M \end{pmatrix} \;\middle|\; M \in C_{GL_n(p)}(R) \right\}.$$

Here N_r and N_m are right and middle nuclei of the semifield W, the centralizer of a spread set R in $GL_n(p)$, together with 0, forms a subfield isomorphic to the left nucleus N_l of W [3].

A collineation of a projective plane π of order N is called a *Baer collineation*, if it fixes pointwise a subplane of maximal order $\sqrt{N}$ (Baer subplane). According to [2, Theorem 4.3], a collineation of order 2 is either central or a Baer collineation.

Let π be a semifield plane of square order p^{2n} that admits a Baer involution τ in the translation complement. The author in [7], [8] represents the coordinatizing semifield W as a $2n$-dimensional linear space over the field $\mathbb{Z}_p$ and constructs the unified form for the matrices of the spread set and for a Baer involution τ. We will denote for convenience $\overline{W}$ the n-dimensional space over $\mathbb{Z}_p$; then

$$W = \{(x_1, x_2) \mid x_1, x_2 \in \overline{W}\}.$$

The spread set $R \subset GL_{2n}(p) \cup \{0\}$ of a semifield plane π consists of matrices

(6)
$$\theta(x_1, x_2) = \begin{pmatrix} u(x_2) + v(x_1) + m(x_1) + w(x_1) & f(x_1) + m(x_2) \\ v(x_1) & u(x_2) + w(x_1) \end{pmatrix}, \quad p = 2,$$

(7)
$$\theta(x_1, x_2) = \begin{pmatrix} m(x_2) & f(x_1) \\ v(x_1) & u(x_2) \end{pmatrix}, \quad p > 2.$$

Here $x_1, x_2 \in \overline{W}$, u, v, w, m, f are linear maps from $\overline{W}$ to the ring of $(n \times n)$-matrices over $\mathbb{Z}_p$, such that (x_1, x_2) is a lower row of the matrix $\theta(x_1, x_2)$. We denote $e = (0, \ldots, 0, 1) \in \overline{W}$ and notice that the row-vector $(0, e)$ is a neutral element under multiplication in the semifield W. The

Baer involution τ is determined by the matrix

$$\tau = \begin{pmatrix} E & E & 0 & 0 \\ 0 & E & 0 & 0 \\ 0 & 0 & E & E \\ 0 & 0 & 0 & E \end{pmatrix} \text{ for } p = 2, \tag{8}$$

$$\tau = \begin{pmatrix} -E & 0 & 0 & 0 \\ 0 & E & 0 & 0 \\ 0 & 0 & -E & 0 \\ 0 & 0 & 0 & E \end{pmatrix} \text{ for } p > 2. \tag{9}$$

The set of all matrices $\{u(x_2) \mid x_2 \in \overline{W}\}$ is a spread set of a Baer subplane π_0, which is fixed by the involution τ.

Further, we prove some results on the involution automorphisms of a semifield W and the corresponding semifield plane π.

Lemma 6. *Let φ be an automorphism of order 2 of a semifield W,*

$$\varphi(x) = xA, \quad A \in GL_n(p).$$

Then $\overline{\varphi} = \begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix}$ is a Baer involution of a semifield plane π, which is coordinatized by W.

Proof. According to Lemma 5, $\overline{\varphi}$ is an autotopism of the plane π. As $|\varphi| = 2$, then $|\overline{\varphi}| = 2$ and $\overline{\varphi}$ is either central or a Baer involution.

If $p = 2$, then the central collineation of order 2 is necessarily the elation [2],

$$\begin{pmatrix} E & \theta(y) \\ 0 & E \end{pmatrix};$$

it is not an autotopism.

If $p > 2$ is an odd prime number, then the central collineation $\overline{\varphi}$ of order 2 is the homology with the axis $[\infty]$ and the center $(0, 0)$. All such the homologies form a cyclic group of even order $p^k - 1$, where p^k is the order of the left nucleus. The unique element of order 2 in this subgroup is determined by the matrix

$$\begin{pmatrix} -E & 0 \\ 0 & -E \end{pmatrix},$$

but the condition (5) does not hold:

$$(-E)^{-1}\theta(y)(-E) = \theta(y) \neq \theta(y(-E)).$$

Hence, we conclude that $\overline{\varphi}$ is a Baer involution of the plane π. $\square$

Inversely, let τ be a Baer involution (8) or (9) for $p = 2$ and $p > 2$, respectively. We consider the matrix

$$A = \begin{pmatrix} E & E \\ 0 & E \end{pmatrix}, \quad p = 2; \text{ or } A = \begin{pmatrix} -E & 0 \\ 0 & E \end{pmatrix}, \quad p > 2,$$

and prove the condition (5). Indeed, let

$$(v, u) = (v_1, \ldots, v_n, u_1, \ldots, u_n)$$

be a lower row of the matrix $\theta(v, u)$ (6), (7). We calculate now the product $A^{-1}\theta(v, u)A$ in a case of even or odd p.

If $p = 2$ then $(v, u)A = (v, v + u)$,

$$A^{-1}\theta(v, u)A = \begin{pmatrix} E & E \\ 0 & E \end{pmatrix} \theta(v, u) \begin{pmatrix} E & E \\ 0 & E \end{pmatrix} = \theta(v, v + u) = \theta((v, u)A),$$

the condition (5) holds.

If $p > 2$ then $(v, u)A = (-v, u)$,

$$A^{-1}\theta(v, u)A = \begin{pmatrix} -E & 0 \\ 0 & E \end{pmatrix} \theta(v, u) \begin{pmatrix} -E & 0 \\ 0 & E \end{pmatrix} = \theta(-v, u) = \theta((v, u)A),$$

the condition (5) holds too. These considerations lead to the following result.

Lemma 7. *Let π be a semifield plane of order p^{2n} that admits a Baer involution in the translation complement. Then at least one of its coordinatizing semifields admits an automorphism of order 2.*

This lemma states the existance of an involution automorphism only up to isotopism of semifields, because in general the Baer involution, possibly, does not fix the line $y = x$. The necessary base replacement in this case leads to another, isotopic semifield. Also we formulate an evident corollary.

Corollary 1. *If a finite semifield W admits an involution automorphism then the semifield order is a square, $|W| = p^{2n}$.*

Note also that an involution automorphism of a semifield is not necessarily unique. In Section 5, we will consider the semifield with three involution automorphisms.

Using the obtained relationship between an automorphism of semifield and a Baer involution of the semifield plane, we will prove the results on some subsets of a semifield.

Theorem 2. *If $\langle W, +, * \rangle$ is a semifield of order p^{2n} (p be prime) that admits an automorphism φ of order 2, then the stabilizer of φ*

$$U = \{x \in S \mid \varphi(x) = x\} \tag{10}$$

is a sub-semifield of order p^n.

Proof. Evidently, U contains both neutral elements of W and it is closed under addition and multiplication. Thus, U is a sub-semifield of W. To calculate its order we consider the set of points

$$\{(x, y) \mid x, y \in W\}$$

of a semifield plane π coordinatized by W. Then

$$\{(x, y) \mid x, y \in U\}$$

is a set of the Baer subplane π_0, which is fixed by the Baer involution

$$\overline{\varphi} : (x, y) \to (\varphi(x), \varphi(y)), \quad (x, y) \in W.$$

So $|\pi| = |W| = p^{2n}$, $|U| = |\pi_0| = \sqrt{|\pi|}$, $|U| = p^n$. □

Note that any semifield of order p^2 is a field (see [5]), which implies the following.

Lemma 8. *If $\langle W, +, * \rangle$ is a semifield of order p^4 that admits an automorphism φ of order 2, then the stabilizer U (10) is a subfield of order p^2. Any maximal subfield of W has the order p^2.*

Proof. According to the previous theorem, U is a sub-semifield of order p^2; so, it is a subfield. Let's assume that H is a subfield of order p^3 in W.

1. If $\varphi(H) = H$, then φ is an involution automorphism on H. It is impossible, $|Aut\ H| = 3$.

2. If $\varphi(H) \neq H$, then $\varphi(H)$ is another subfield of order p^3. We consider subfields H and $\varphi(H)$ as linear subspaces and use the Grassman's identity:

$$\dim H + \dim \varphi(H) = \dim(H \cap \varphi(H)) + \dim(H + \varphi(H)),$$

$3 + 3 = \dim(H \cap \varphi(H)) + 4$ and $\dim(H \cap \varphi(H)) = 2$, i.e. the intersection $H \cap \varphi(H)$ is a subfield of order p^2 in a field of order p^3, which is impossible. Thus, any maximal subfield in W is of order p^2. □

Lemma 9. *If a semifield of odd order p^{2n} ($p > 2$ is prime) admits an automorphism of order 2, then its multiplication loop contains a subloop of order $2(p^n - 1)$.*

Proof. Let $\langle W, +, * \rangle$ be a semifield of order p^{2n}, let φ be an involution automorphism, let U (10) be the stabilizer of φ (it is the sub-semifield of order p^n). We consider the subspace

$$U' = \{x \in S \mid \varphi(x) = -x\} \tag{11}$$

and the Jordan's normal form (9) of the matrix φ. Thus we conclude that $|U'| = p^n$. The union $U \cup U'$ is closed under the multiplication. Indeed, if $x, y \in U'$ then

$$\varphi(x * y) = \varphi(x) * \varphi(y) = (-x) * (-y) = x * y, \qquad x * y \in U;$$

if $x \in U$, $y \in U'$ (or inverse) then

$$\varphi(x * y) = \varphi(x) * \varphi(y) = x * (-y) = -(x * y), \qquad x * y \in U'.$$

Moreover, the sub-semifield U contains the identity e of the semifield W. So, the union $(U \setminus \{0\}) \cup (U' \setminus \{0\})$ is a subloop of W^* of order $2(p^n - 1)$. Note that this set is not closed under the addition. □

5. Involution automorphisms of some semifield of orders 81 and 64

Let W be the semifield of order 81, which is represented as a 4-dimensional linear space over $\mathbb{Z}_3$ with the spread set (7), where $x_1 = (t_1, t_2)$, $x_2 = (t_3, t_4)$, $t_i \in \mathbb{Z}_3$. We define the linear functions m, f, v, u as

$$\begin{aligned} m(t_3, t_4) &= t_3 M + t_4 E, & f(t_1, t_2) &= t_1 F_1 + t_2 F_2, \\ v(t_1, t_2) &= t_1 D + t_2 E, & u(t_3, t_4) &= t_3 D + t_4 E, \end{aligned}$$

for the appropriate matrices $M, F_1, F_2, D \in GL_2(3)$. Here we can suppose that $D = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ (see [8]). There exists eight pairwise non-isotopic semifields of order 81 with the spread set of this form. For instance, if we choose the matrices

$$M = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \quad F_1 = \begin{pmatrix} 0 & -1 \\ -1 & 1 \end{pmatrix}, \quad F_2 = \begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix}$$

then we obtain a semifield with the unique non-trivial automorphism

$$\tau = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

which is an involution. Its stabilizer is a subfield of order 9 $\{(0,0,t_3,t_4) \mid t_3,t_4 \in \mathbb{Z}_3\}$, which coincides with the middle nucleus N_m of W. The right and left nuclei are other subfields of order 9 and τ is an automorphism on each of this subfields,

$$N_r^* = \langle (1,0,0,0) \rangle, \qquad N_l^* = \langle (0,1,0,0) \rangle.$$

The set

$$\{(t_1,t_2,0,0) \mid t_1,t_2 \in \mathbb{Z}_3\} \cup \{(0,0,t_3,t_4) \mid t_3,t_4 \in \mathbb{Z}_3\} \setminus \{(0,0,0,0)\}$$

is a subloop of order 16 in W^*.

As another example, we consider the exceptional Hentzel–Rúa semifield of order 64, which was constructed in [9]. Its spread set consists of all linear combinations

$$\theta(x_1,\dots,x_6) = x_1A_1 + \cdots + x_6A_6, \qquad x_1,\dots,x_6 \in \mathbb{Z}_2$$

of matrices $A_1,\dots,A_6 \in GL_6(2)$:

$$A_1 = E, \quad A_2 = \begin{pmatrix} 0&1&0&0&0&0 \\ 0&0&1&0&0&0 \\ 1&1&0&0&0&0 \\ 0&0&0&0&1&0 \\ 0&0&0&0&0&1 \\ 1&0&0&1&1&0 \end{pmatrix}, \quad A_3 = \begin{pmatrix} 0&0&1&0&0&0 \\ 1&1&0&0&0&0 \\ 0&1&1&0&0&0 \\ 1&1&0&0&0&1 \\ 0&0&0&1&1&0 \\ 1&1&1&0&1&1 \end{pmatrix},$$

$$A_4 = \begin{pmatrix} 0&0&0&1&0&0 \\ 0&1&0&0&1&0 \\ 0&1&1&0&0&1 \\ 0&1&1&0&1&1 \\ 1&1&0&0&0&0 \\ 1&0&0&0&0&1 \end{pmatrix}, \quad A_5 = \begin{pmatrix} 0&0&0&0&1&0 \\ 1&0&0&0&0&1 \\ 1&0&0&1&1&0 \\ 1&1&0&0&1&0 \\ 0&0&1&1&0&1 \\ 1&1&0&1&1&0 \end{pmatrix},$$

$$A_6 = \begin{pmatrix} 0&0&0&0&0&1 \\ 0&1&0&1&1&0 \\ 0&1&0&0&1&1 \\ 1&0&0&1&0&0 \\ 0&1&0&1&0&0 \\ 0&0&1&0&0&1 \end{pmatrix}.$$

The automorphism group of Hentzel–Rúa semifield is isomorphic to the symmetric group S_3 and so contains three involutions:

$$T_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}, \quad T_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

$$T_3 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 \end{pmatrix}.$$

Next we consider the stabilizers of T_j:

$$H_j = \{x \in W \mid xT_j = x\}, \quad j = 1, 2, 3.$$

The set H_1 contains 8 elements; among them are $h_1 = (0, 0, 0, 1, 0, 1)$, $h_1^3 = e + h_1^2$, so $H_1 \simeq GF(8)$ (here $e = (1, 0, 0, 0, 0, 0)$ is the identity of semifield). Analogously,

$$|H_2| = 8, \quad h_2 = (0, 0, 1, 0, 0, 0) \in H_2, \quad h_2^3 = e + h_2;$$

$$|H_3| = 8, \quad h_3 = (0, 0, 0, 1, 1, 1) \in H_3, \quad h_3^3 = e + h_3.$$

So, H_1, H_2, H_3 are different subfields of order 8 of semifield W. Note that there exist also two subfields H_b, H_c, $|H_b| = |H_c| = 8$,

$$H_b^* = \langle b = (0, 0, 0, 0, 1, 0) \rangle, \quad b^3 = e + b;$$

$$H_c^* = \langle c = (0, 0, 1, 0, 1, 0) \rangle, \quad c^3 = e + c^2.$$

Each of the automorphisms T_j stabilizes the corresponding subfield H_j and interchanges the other two subfields. Moreover, each T_j interchanges H_b with H_c.

These results were announced at the International conferences G2A2 ("Groups and Graphs, Algorithms and Automata", Yekaterinburg, 2015) and G2S2 ("Graphs and Groups, Spectra and Symmetries", Novosibirsk, 2016).

References

[1] N.L. Johnson, V. Jha, M. Biliotti, *Handbook of Finite Translation Planes*, Pure and applied mathematics. Chapman&Hall/CRC, Boca Raton, FL, 2007. Zbl 1136.51001

[2] D.R. Hughes, F.C. Piper, *Projective Planes*, Springer-Verlag, New York–Heidelberg–Berlin, 1973. Zbl 0267.50018

[3] N.D. Podufalov, *On spread sets and collineations of projective planes*, Contemp. Math., **131**:1 (1992), 697–705. Zbl 0779.51001

[4] H. Lüneburg, *Translation Planes*, Springer-Verlag, Berlin–Heidelberg–New York, 1980. Zbl 0446.51003

[5] D.E. Knuth, *Finite semifields and projective planes*, J. Algebra, **2** (1965), 182–217. Zbl 0128.25604

[6] U. Dempwolff, *Semifield planes of order* 81, J. Geom., **89**:1–2 (2008), 1–16. Zbl 1175.12003

[7] O.V. Kravtsova, *Semifield planes of even order that admit the Baer involution*, Izv. Irkutsk. Gos. Univ., Ser. Mat., **6**:2 (2013), 26–37 (Russian; English summary). Zbl 1295.51006

[8] O.V. Kravtsova, *Semifield planes of odd order that admit a subgroup of autotopisms isomorphic to* A_4, Russ. Math., **60**:9 (2016), 7–22. Zbl 06641220

[9] I.R. Hentzel, I.F. Rua, *Primitivity of Finite Semifields with* 64 *and* 81 *elements*, Int. J. Algebra and Comput., **17**:7 (2007), 1411–1429. Zbl 1143.17009