УДК 512.145

Some Results on Isomorphisms of Finite Semifield Planes

Olga V. Kravtsova[*]
Institute of Core Undergraduate Programmes,
Siberian Federal University,
Киренского, 26, Красноярск, 660074,
Russia

Sergei V. Panov[†]
Institute of Mathematics and Computer Science,
Siberian Federal University,
Svobodny, 79, Krasnoyarsk, 660041
Russia

Irina V. Shevelyova[‡]
Institute of Core Undergraduate Programmes,
Siberian Federal University,
Киренского, 26, Красноярск, 660074,
Russia

Received 01.10.2012, received in revised form 08.11.2012, accepted 06.12.2012

The authors extend an approach to construct and classify the semifield projective planes using the linear space and spread set. Follows results are given: an estimate of the order of autotopism group and a number of isomorphic semifield planes defined by fixed linear space.

Keywords: semifield plane, linear space, spread set, isomorphism, autotopism group.

Introduction

This paper suggests the method to investigate the properties of *semifield* projective planes. The coordinatizing set of such plane is a semifield, or division ring. The features of coordinatizing set allow to consider semifield plane as a subclass of translation planes, and so allow to use a vector space of even dimension and the certain family of linear transformations (regular set, spread set) to construct semifield planes [1, 2].

A number of papers ([3, 4] and others), devoted to construction and investigation of translation planes of rank 2, was published in 1985–1995 years. Translation plane of rank 2 can be determined by four-dimension vector space and 2×2-matrices over the finite field of order p^n. However the functions which define the spread set are the polinoms of p^{n-1}-th degree (in a common case) and therefore the construction of such a plane of great order is so complicated even for small rank. The method that is presented by this paper is based on a consideration of a spread set consists of great dimension matrices over the field of prime order. So it is possible to use only linear functions for spread set that is simplifies all reasonings.

The authors obtained an estimate of autotopism group order for the finite semifield plane (Theorem 1) and determined a number of isomorphic semifield planes of a fixed order and a fixed rank (Theorem 2). The results are illustrated by some examples of semifield planes of order 27.

[*] ol71@bk.ru
[†] pansevakrasn@mail.ru
[‡] shiv@krasmail.ru

1. On Estimate of Autotopism Group Order

We shall use the notations and definitions from a paper [5].

A projective plane π is a set of points and lines together with an 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 four points such that no three are incident with one line.

If one of lines of projective plane is incident with finite number of points, that all lines of this plane are incident with finite number of points, moreover, the numbers are equal. Let this number be $M+1$, so all points of this plane are incident with $M+1$ lines, and there are M^2+M+1 points and as much lines in this plane. Such projective plane is called *finite plane* and the number M is called the *order* of plane.

One can introduce coordinatization for all points and lines of any finite projective plane using the elements of certain *coordinatizing set*. The incidence relation properties allow to determine an addition and multiplication on a coordinatizing set. The algebraic properties of this set are closely connected with geometric properties of coresponding projective plane. So, in particular, the classic, or *desarguesian* projective plane is coordinatized by the field, and the translation plane — by quasifield.

Let π be a semifield plane of order p^n for prime p, N be the coordinatizing semifield. The *right nucleus, middle nucleus and left nucleus* of semifield N are the follows subsets respectively:

$$\begin{aligned} N_r &= \{x \in N | (ab)x = a(bx)\ \forall a, b \in N\}, \\ N_m &= \{x \in N | (ax)b = a(xb)\ \forall a, b \in N\}, \\ N_l &= \{x \in N | x(ab) = (xa)b\ \forall a, b \in N\}. \end{aligned}$$

These sets are subfields of N and it is well known that any semifield plane can be considered as a linear space over any nucleus of semifield [5]. As a rule it is most convenient to use the left nucleus N_l.

Let $|N_l| = p^k$, $n = dk$, then any affine point of a plane π corresponds to element of $2d$-dimensional linear space over the field $GF(p^k) = F$:

$$(x, y) = (x_1, x_2, \ldots, x_d, y_1, y_2, \ldots, y_d), \quad x_i, y_i \in F, \quad i = 1, 2, \ldots, d,$$

any affine line corresponds to coset of follows subgroups:

$$V_i = \{(x, x\theta_i) | x \in F^d\}, \quad i = 1, 2, \ldots, p^n, \quad V_0 \ = \{(0, y) | y \in F^d\}.$$

Here θ_i are $d \times d$-matrices with elements of F, that formes a *regular set* R of plane π (spread set). The set R contains zero and identity matrices and also it satisfies to follows condition: $\det(\theta_i - \theta_j) \neq 0$ for all $i \neq j$. In particular, all non-zero matrices of R are nondegenerated.

The full collineation group (automorphism group) Autπ of semifield plane has a follows structure: Aut$\pi = T \leftthreetimes G$, where $T = \{\tau_{a,b} | a, b \in F^d\}$ is translation group,

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

and G is *translation complement*, the stabilizer of the point $(0, 0)$. The automorphisms from G are determined by semi-linear transformations of linear space F^{2d}:

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

Here σ is an automorphism of a field F, A, B, C, D are $d \times d$-matrices over F. It may be stated that $C = 0$ for any semifield plane. The subgroup G_0 of group G, that formed by linear transformations, is called a *linear translation complement.*

The subgroup $\Lambda < G$, that formed by triangle-fixed collineations, is *autotopism group*. It may be shown that one can choose any triangle to construct the autotopism group, and as a rule the triangle $(0,0),(0),(\infty),[0,0],[0],[\infty]$ is used for this purpose. The subgroup $\Lambda_0 = \Lambda \cap G_0$ is a linear autotopism group. The matrices which corresponds to any autotopism are block-diagonal,

$$(x,y)^{\lambda} = (x^{\sigma}, y^{\sigma}) \begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix}, \quad \lambda \in \Lambda,$$
$$(x,y)^{\lambda_0} = (x,y) \begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix}, \quad \lambda \in \Lambda_0.$$

Linear autotopism group Λ_0 is isomorphic to subgroup of $GL_d(p^k) \times GL_d(p^k)$, and Λ is isomorphic to subgroup of $\mathrm{Aut}F \times GL_d(p^k) \times GL_d(p^k)$. We shall state the conditions for matrices A and D to determine $\lambda_0 = \begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix}$ as autotopism.

As any collineation, λ_0 keeps the incidence relation. So for any vector $x = (x_1, \dots, x_d) \in F^d$ and any matrix from spread set $\theta \in R$ the image of a point $(x, x\theta)$ is incident with the line throw $(0,0)$, and there are $y \in F^d$ and $\theta' \in R$, such that

$$(x, x\theta)^{\lambda_0} = (x, x\theta) \begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix} = (xA, x\theta D) = (y, y\theta').$$

Thus $y = xA$, $y\theta' = xA\theta' = x\theta D$ for all $x \in F^d$. It follows that the matrices A and D determine a linear autotopism of semifield plane with a spread set R if and only if $A^{-1}\theta D \in R$ for any matrix $\theta \in R$.

We shall describe the matrices that form a spread set of semifield plane. Because of condition $\det(\theta_i - \theta_j) \neq 0$ for $i \neq j$ there is one-to-one correspondence between the matrix from R and any its line, for example, the first:

$$\theta(t_1, t_2, \dots, t_d) = \begin{pmatrix} t_1 & t_2 & \dots & t_d \\ f_{21} & f_{22} & \dots & f_{2d} \\ \multicolumn{4}{c}{\dots\dots\dots\dots\dots\dots} \\ f_{d1} & f_{d2} & \dots & f_{dd} \end{pmatrix}.$$

Here f_{ij} are the functions of d variables $t_1, t_2, \dots, t_d \in F$. It is known that spread set of any semifield plane is closed under addition, so f_{ij} are the additive functions of d arguments:

$$f_{ij}(t_1, \dots, t_d) = a_{ij}^{10} t_1 + a_{ij}^{11} t_1^{p} + \dots + a_{ij}^{1,k-1} t_1^{p^{k-1}} + \dots +$$
$$+ a_{ij}^{d0} t_d + a_{ij}^{d1} t_d^{p} + \dots + a_{ij}^{d,k-1} t_d^{p^{k-1}} = \sum_{m=1}^{d} \sum_{s=0}^{k-1} a_{ij}^{ms} t_m^{p^s}.$$

In the simplest case the semifield is a 2-dimensional linear space over the left nucleus, $d = 2$, and the spread set consists of 2×2-matrices. And the check of condition $A^{-1}\theta D \in R$ for all $\theta \in R$ is so complicated even in this case. We shall suggest another approach: one can consider π as a linear space over prime order subfield of left nucleus, $P = GF(p)$. Then the dimension of space be $2n = 2dk$, but all functions determine the spread set be only linear:

$$f_{ij}(t_1, \dots, t_n) = a_{ij}^{1} t_1 + a_{ij}^{2} t_2 + \dots + a_{ij}^{n} t_n = \sum_{m=1}^{n} a_{ij}^{m} t_m.$$

So we can consider any matrix from the spread set as a sum $\theta(t_1, t_2, \dots, t_n) = t_1 U_1 + t_2 U_2 + \dots + t_n U_n$, where first line of any U_i consists of zeros and unique identity i-placed. It is obvious that $U_1 = E$ is identity matrix. Because of spread set is closed under addition R be a linear space of dimension n over the field $P = GF(p)$, and the matrices $U_1, U_2, \ldots, U_n$ form a basis of R. So if one search the matrices that determine the linear autotopism of a semifeild plane then it is sufficient to check an condition $A^{-1}\theta D \in R$ only for basic elements U_i. Moreover, $\sigma = 1$ and $\Lambda = \Lambda_0$.

Since $A^{-1}\theta D = \theta' \in R$, the autotopism $\lambda = \begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix}$ determines the transformation $\overline{\lambda} : \theta \to \theta' = A^{-1}\theta D$ of linear space R. Since $(\theta_1+\theta_2)^{\overline{\lambda}} = A^{-1}(\theta_1+\theta_2)D = A^{-1}\theta_1 D + A^{-1}\theta_2 D = \theta_1^{\overline{\lambda}} + \theta_2^{\overline{\lambda}}$, then $\overline{\lambda}$ is a linear transformation of a linear space R. It is follows that the set of all transformations $\overline{\lambda}$ formes a subgroup $\overline{\Lambda} < GL_n(p)$.

The correspondence $\xi : \lambda \to \overline{\lambda}$ is a homomorphism from Λ to $GL_n(p)$. Let's find the kernel of this homomorphism and estimate an order of group Λ, taking into account that $\Lambda/Ker\xi \simeq \overline{\Lambda}$.

Let $\overline{\lambda} = 1$, then $\theta^{\overline{\lambda}} = A^{-1}\theta D = \theta \quad \forall \theta \in R$. In particular, at $\theta = E$ we obtaine $A = D$ and so $\theta A = A\theta$. Thus,

$$\operatorname{Ker}\xi = \{A \in GL_n(p) | A\theta = \theta A \ \forall \theta \in R\} = R_l^* \simeq N_l^*,$$

it is a multiplicative subgroup of left nucleus of the plane π.

Generalizing, we shall state the follows result.

Теорема 1. *Let π be a semifield plane of order p^n, p – prime. Autotopism group Λ of the plane π has an order*

$$|\Lambda| = (p^s - 1) \cdot q,$$

where p^s is an order of left nucleus of plane π, q is a divider of number

$$|GL_n(p)| = (p^n - 1)(p^n - p) \ldots (p^n - p^{n-1}).$$

2. On a Number of Isomorphic Planes

We shall apply the same approach to determine a number of isomorphic semifield planes, defined by a fixed dimension linear space over fixed finite field. If the semifield planes π and π' with spread sets R and R' respectively over same linear space are isomorphic there is a semilinear transformation φ of linear space with the condition that any matrix $\theta \in R$ corresponds to matrix $\theta' \in R'$, such that for any vector x there exists the vector y that satisfies

$$(x, x\theta)^{\varphi} = (y, y\theta').$$

Consider a set of all affine points of a semifield plane as a linear space of maximal dimension over the minimal subfield $P = GF(p)$ of field F, we can state that φ is linear transformation. Let's define φ by means of a matrix:

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

where A, B, D are $n \times n$-matrices over P. The matrix φ contains a zero block because isomorphic images of points $(0, 0)$ and (∞) of the plane π are the corresponding points of π', so for any vector y there exists such a vector y' that

$$(0, y)^{\varphi} = (0, y').$$

Let $W = P^n$, and $V = W \times W$ be the set of all affine points. We shall find the image of any point:

$$(x, x\theta)^{\varphi} = (x, x\theta) \begin{pmatrix} A & B \\ 0 & D \end{pmatrix} = (xA, xB + x\theta D) = (y, y\theta'),$$

where $x, y \in W$, $\theta \in R$, $\theta' \in R'$. Since $y = x\theta$ then

$$\theta' = A^{-1}(B + \theta D) \in R' \tag{1}$$

for all matrices $\theta \in R$. In particular, $\theta = 0$ follows $A^{-1}B = \theta'_0 \in R'$, $B = A\theta'_0$. The condition (1) becomes to

$$\theta'_0 + A^{-1}\theta D \in R',$$

and because a spread set of semifiels plane is closed under addition that

$$A^{-1}\theta D \in R' \quad \forall \theta \in R. \tag{2}$$

Rewrite the matrix φ as a product

$$\varphi = \begin{pmatrix} A & A\theta'_0 \\ 0 & D \end{pmatrix} = \begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix} \begin{pmatrix} E & \theta'_0 \\ 0 & E \end{pmatrix} = \psi\sigma.$$

Here the matrix ψ satisfies to condition (2) and so it determines an isomorphism from π to π', and σ is an elation of plane π' with axis $[0]$ and center (∞). Sets of all such elations

$$\Sigma' = \left\{ \begin{pmatrix} E & \theta' \\ 0 & E \end{pmatrix} \middle| \, \theta' \in R' \right\},$$

$$\Sigma = \left\{ \begin{pmatrix} E & \theta \\ 0 & E \end{pmatrix} \middle| \, \theta \in R \right\}$$

of planes π' and π respectively are the elementary abelian groups of order p^n, and

$$G_0 = \Sigma \leftthreetimes \Lambda_0, \qquad G'_0 = \Sigma' \leftthreetimes \Lambda'_0$$

(for π and π'). So, if one accounts all possible isomorphisms of semifield planes, it is sufficient to consider only linear transformations, defined by matrices

$$\psi = \begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix},$$

where A, D satisfy to condition (2). Let $A^{-1}\theta_1 D = E \in R'$, then $A = \theta_1 D$,

$$\psi = \begin{pmatrix} \theta_1 D & 0 \\ 0 & D \end{pmatrix}.$$

Thus, if we enumerate all possible nondegenerated $n \times n$-matrices D over P and all non-zero matrices θ_1 of the spread set R of semifield plane π, then we shall obtain the sets of matrices as

$$R^{\overline{\psi}} = A^{-1}RD,$$

where $A = \theta_1 D$. Any choice of D and θ_1 arises the set $R^{\overline{\psi}}$ to be a spread set of some semifield plane, because it is closed under addition, consists of nondegenerated matrices (except zero) and contains zero and identity matrices. Thus we obtain all semifield planes over fixed linear space, that are isomorphic to given plane π itself inclusive, if ψ is a collineation. Determine the order of homomorphism $\psi \to \overline{\psi}$ and state the result.

Theorem 2. *Let π be a semifield plane of order p^n, p be prime, R be its spread set over n-dimensional linear space, Λ be an autotopism group of π, and*

$$\Psi = \left\{ \psi = \begin{pmatrix} \theta_1 D & 0 \\ 0 & D \end{pmatrix} \middle| \, \theta_1 \in R, \ D \in GL_n(p) \right\}.$$

Then the number of rank n semifield planes, that are isomorphic to π, equals to

$$\frac{|\Psi|}{|\Lambda|} = \frac{(p^n - 1)|GL_n(p)|}{|\Lambda|}.$$

3. Construction of the Examples

In [6] authors present the result of construction the semifield planes of order 27 using spread set of 3×3-matrices over $GF(3)$.

The spread set of any such plane consists of matrices

$$\theta(x,y,z) = \begin{pmatrix} x & y & z \\ f_{21} & f_{22} & f_{23} \\ f_{31} & f_{32} & f_{33} \end{pmatrix},$$

where x, y, z are any elements of the field $GF(3)$, f_{ij} are some fixed additive functions of arguments x, y, z. Because of prime field order these functions are all linear and so the matrices of spread set can be considered as

$$\theta(x,y,z) = x \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 01 \end{pmatrix} + y \begin{pmatrix} 0 & 1 & 0 \\ b_{21} & b_{22} & b_{23} \\ b_{31} & b_{32} & b_{33} \end{pmatrix} + z \begin{pmatrix} 0 & 0 & 1 \\ c_{21} & c_{22} & c_{23} \\ c_{31} & c_{32} & c_{33} \end{pmatrix} = xE + yB + zC.$$

Thus the spread set of semifield plane is

$$R = \{\theta(x,y,z) = xE + yB + zC | x, y, z \in GF(3)\},$$

where E is an identity matrix, B, C are such nondegenerated 3×3-matrices over $GF(3)$ that the matrix $\theta(x,y,z)$ is also nondegenerated fo any non-zero set $x, y, z \in GF(3)$. Any pair of matrices B, C that satisfy this condition determines the semifield plane of order 27 with the left nucleus contains $GF(3)$.

Computer calculations show that there exists 2016 such pairs of matrices and so there exists 2016 semifield planes of rank 3 over $GF(3)$.

In 144 cases the spread set R is closed under multiplication, that is

$$B^2 \in R, \quad C^2 \in R, \quad BC \in R, \quad CB \in R,$$

and $BC = CB$. The corresponding plane are coordinatized by field, it is desarguesian and such all planes are isomorphic to each other.

The rest of set are 1872 non-desarguesian semifield planes that also are isomorphic to each other: we can construct the linear transformations (see II), that satisfy to conditions

$$A^{-1}BD \in R', \qquad A^{-1}CD \in R',$$

where the matrices B, C define the spread set R, and R' is a spread set of isomorphic plane.

Thus there is exactly two semifield planes or order 27, one of them is desarguesian. The spread sets can be defined by matrices:

1) $B = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 2 \end{pmatrix}$, $C = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 2 \\ 2 & 1 & 0 \end{pmatrix}$ for non-desarguesian plane,

2) $B = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 2 \end{pmatrix}$, $C = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 2 \\ 2 & 1 & 1 \end{pmatrix}$ for desarguesian plane.

Further we constructed the autotopism group for both planes by search the matrices $\begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix}$ that satisfies to conditions

$$A^{-1}BD \in R, \qquad A^{-1}CD \in R.$$

The autotopism group for non-desarguesian plane is of order 156 and for desarguesian is of order 2028. According to results 1–2 we calculate $|\Psi|$:

$$|\Psi| = (3^3 - 1) \cdot |GL_3(3)| = 26^2 \cdot 24 \cdot 18 = 292032.$$

For non-desarguesian plane $\dfrac{292032}{156} = 1872$ and for desarguesian $\dfrac{292032}{2028} = 144$, that equals to number of isomorphic planes in each case.

The constructed examples coresponds to the proved results stating the relation between the number of isomorphic planes and the order of autotopism group. Thus, an approach using the linear functions over prime order field is necessary to be effective to construct and investigate the finite semifield planes.

The authors were supported by RFBR, grant no. 10-01-00509-a (first author), grant no. 12-01-00968 (second author), and Ministry of Education grant, theme 1.34.11.

References

[1] H. Luneburg, Translation planes, Springer-Verlag Berlin Heidelberg NewYork, 1980.

[2] N.D.Podufalov, On spread sets and collineations of projective planes, *Contem. Math.*, **131**(1992), no. 1, 697-705.

[3] M.Biliotti, V.Jha, N.L.Johnson, G.Menichetti, A structure theory for two-dimensional translation planes of order q^2 that admit collineation group of order q^2, *Geom. Dedicata*, **29**(1989), 7–43.

[4] H.Huang, N.L.Johnson, 8 semifield planes of order 8^2, *Discrete Math*, **80**(1990), no. 1, 69–79.

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

[6] O.V.Kravtsova, S.V.Panov, Semifield planes defined by linear functions, Algebra, logic and applications, Thesis of reports, Krasnoyarsk, 2010, 56–57 (in Russian).

Некоторые результаты об изоморфизмах конечных полуполевых плоскостей

Ольга В. Кравцова
Сергей В. Панов
Ирина В. Шевелева

Развивается подход к построению и классификации полуполевых проективных плоскостей с использованием линейного пространства и регулярного множества. Приведены оценки порядка группы автотопизмов полуполевой плоскости и количества изоморфных полуполевых плоскостей, заданных фиксированным линейным пространством.

Ключевые слова: полуполевая плоскость, линейное пространство, регулярное множество, изоморфизм, группа автотопизмов.