Quasigroups and Related Systems **19** (2011), 109 – 122

Semifields in loop theory and in finite geometry

Gábor P. Nagy

Abstract. This paper is a relatively short survey the aim of which is to present the theory of semifields and the related areas of finite geometry to loop theorists.

1. Introduction

The theory of finite semifields is an area of mathematics where finite geometry, group theory, field theory and algebra come together. There are several good survey papers ([7], [13], [6]) and monographs ([11], [12]), old and new, with different foci. The present paper is yet another survey paper, with mostly loop theoretic emphasis. We tried to collect some recent results and explain the finite geometric background such that the presentation could be understood with a graduate level knowledge. We completely omitted proofs, which certainly does not make the reading of the paper easier. We suggest the reader to try to figure out as much as he or she can, whereby drawing pictures can be of great help.

2. Translations of affine planes

A *quasigroup* is a set Q endowed with a binary operation $x \cdot y$ such that two of the unknowns $x, y, z \in Q$ determines uniquely the third in the equation $x \cdot y = z$. *Loops* are quasigroups with a unit element. The multiplication tables of finite quasigroups are Latin squares. The multiplication tables of finite loops are normalized Latin squares, that is, in which the first row and column contain the symbols $\{1, \ldots, n\}$ in increasing order. The *left and right multiplication maps* of a loop $(Q, \cdot)$ are the bijections $L_a : x \mapsto a \cdot x$

2010 Mathematics Subject Classification: 20N05, 12K10

Keywords: Semifield, multiplicative loop, multiplication group, translation plane, semifield plane.

Supported by the TAMOP-4.2.1/B-09/1/KONV-2010-0005 project. The author is a Bolyai János Research Fellow.

and $R_a : x \mapsto x \cdot a$, respectively. These are precisely the permutations which are given by the rows and columns of the corresponding Latin square. The group generated by the left and right multiplication maps of a loop Q is the *multiplication group* $Mlt(Q)$.

Loops arise naturally in geometry when coordinatizing point-line incidence structures, e.g., affine planes, cf. [7]. An *affine plane* consists of a set $\mathcal{P}$ of points, a set $\mathcal{L}$ of lines and an incidence relation $I \subset \mathcal{P} \times \mathcal{L}$ such that the following axioms hold:

(A1) Two points are incident with a unique line.

(A2) Two lines are incident with at most one common point.

(A3) (*Parallel axiom*) For a given line ℓ and a point P there is a unique line m such that PIm and $\ell \parallel m$.

(A4) (*Richness axiom*) There are three points not incident with a common line.

Concepts as *parallelism, parallel class* or *collineation* can be defined in the same way as for Euclidean planes. The notion of a *translation* needs a bit more attention. We say that a collineation is a translation if every line is parallel to its image, and, the invariant lines form a parallel class. This parallel class is called the *direction* of the translation.

In order to get familiar with the topic of translations, we suggest the reader to work out the following project.

(1) Show that a translation is determined by the image of one point. Conclude that a nontrivial translation has no fixed point. Show that if the collineation α has no fixed point and each line ℓ is parallel to its image ℓ^α, then α is a translation.

(2) Show that the translations of a given plane form a group. Show that if the directions of the translations τ_1, τ_2 differ, then the direction of $\tau_1\tau_2$ differs from both.

In the sequel, let us denote by T the group of translations of a given affine plane.

(3) Assume that T contains two translations with different directions. Show that T is an abelian group in which all nonidentical elements have the same order. [Hint:Study the possible directions of $\tau_1^{-1}\tau_2^{-1}\tau_1\tau_2$ and τ_1^k, τ_2^k, $(\tau_1\tau_2)^k$.]

(4) Show that if the underlying plane is finite and T contains two translations with different directions, then T is an elementary abelian p-group.

We remark that the conditions in (4) are neccesary, that is, there are affine planes with translations in one direction only, whose group of translations is not abelian.

3. Translation planes and quasifiels

An affine plane with a transitive group of translations is called a *translation plane.* Translation planes can be coordinatized by a field-like structure called *quasifields.*
The set Q endowed with two binary operations $+$, $\cdot$ is called a *quasifield*, if

(Q1) $(Q, +)$ is an abelian group with neutral element $0 \in Q$,

(Q2) $(Q \setminus \{0\}, \cdot)$ is a quasigroup,

(Q3) the right distributive law $(x + y)z = xz + yz$ holds, and,

(Q4) for each $a, b, c \in Q$ with $a \neq b$, there is a unique $x \in Q$ satisfying $xa = xb + c$.

It is easy to see that $0 \cdot x = x \cdot 0 = 0$ for all $x \in Q$. The right distributive law implies that the right multiplication maps R_a are in $Aut(Q, +)$, and, the right multiplication group is a transitive group of automorphisms of $(Q, +)$. This is a very strong restriction if Q is finite. Then, Q is an elementary Abelian group of exponent p. The prime p is called the *characteristic* of Q and the order of Q is p^n. The right multiplication maps R_a are in $GL(n, p)$. Moreover, (Q2) and (Q3) imply that for all $a, b \in Q$, $a \neq b$, $\det(R_a - R_b) \neq 0$, which means that (Q4) is automatically fulfilled.

In a well known manner, a quasifield Q gives rise to a translation plane by setting $Q \times Q$ as the point set and defining the lines by the equations $X = c$ and $Y = Xm + b$. Indeed, the translations have the form $(x, y) \mapsto (x + u, y + v)$ with fixed $u, v \in Q$. Conversely, any translation plane can be coordinatized by a quasifield. Moreover, if two quasifields are isotopic then they coordinatize isomorphic translation planes. However, the converse is not true: It may well happen that two nonisotopic quasifields give rise to isomorphic translation planes.

The remark above implies that we can switch to isotopic copies of Q without loosing any geometric information. In particular, we can, and in the sequel we will, assume that $Q^* = Q \setminus \{0\}$ is a loop with unit element 1.

As we see, in loop theoretical terms, a finite quasifield Q is the same as a loop Q^* whose right multiplication maps are linear maps of a finite dimensional vector space V over a finite field F. Clearly, if F' is a subfield of F then V can be considered as an F'-space, as well. For us, the opposite question is important: What is the *largest* field F such that V is an F-linear space and the right multiplication maps are

a) F-linear,

b) F-semilinear maps?

Many constructions of quasifields are given in such a way that the right translation maps are semilinear over a given field. However, if we start from a general quasifield then it is easier to answer the linearity. Indeed, by the right distributive law, the *left nucleus*

$$N_\lambda(Q) = \{c \in Q \mid (cx)y = c(xy)\}$$

of Q is a subfield of Q and the right translation maps are $N_\lambda(Q)$-linear maps. In the geometric theory of quasifields, $N_\lambda(Q)$ is called the *kernel* of Q.

We close this section by making a closer look at the set $S_r = \{R_x \mid x \in Q\}$ of right multiplication maps of a quasifield Q. Assume that these maps are linear over the finite field $\mathbb{F}_q$ and Q is an $\mathbb{F}_q$-linear space of dimension d. By fixing a basis in Q, the maps R_x can be written as $d \times d$ matrices over F. In the theory of loops, it is usual to look at S_r as a set of permutations such that for $R_x, R_y \in S_r$ $(x \neq y)$, the permutation $R_x R_y^{-1}$ is fixed point free. For matrices, this means that for all $z \in Q$,

$$z \neq z R_x R_y^{-1} \Longleftrightarrow 0 \neq z(R_x - R_y) \Longleftrightarrow 0 \neq \det(R_x - R_y).$$

In other words, a finite quasifield of dimension d over the field $\mathbb{F}_q$ can be equivalently given by the set Σ of $d \times d$ matrices over $\mathbb{F}_q$, such that $|\Sigma| = q^d$ and for any $A, B \in \Sigma$, $A \neq B$, $\det(A - B) \neq 0$.

Let A be a $d \times d$ matrix, $W = \mathbb{F}_q^{2d}$ vector space and define the d-dimensional subspace $U_A = \{(x, xA) \mid x \in \mathbb{F}_q^d\}$ of W. Furthermore, define $U_\infty = \{(0, x) \mid x \in \mathbb{F}_q^d\}$. Put

$$\tilde{\Sigma} = \{U_A \mid A \in \Sigma\} \cup \{U_\infty\}$$

where Σ is the set of right multiplication maps of Q. Then,

a) for any $A, B \in \Sigma$, $A \neq B$, $U_A \cap U_B = U_A \cap U_\infty = \{(0,0)\}$, and,

b) for any nonzero element $(x, y) \in W$ there is a unique element of $\tilde{\Sigma}$ containing it.

These two properties say that $\tilde{\Sigma}$ form a partition of W into d-dimensional subspaces. Such partitions are called *spreads.*

Conversely, any spread $\tilde{\Sigma}$ of W defines a quasifield. In order to see this, choose two elements $U_0, U_1 \in \tilde{\Sigma}$. Since $W = U_0 \oplus U_1$, we can define the projection maps $\pi_0 : W \to U_0$ and $\pi_1 : W \to U_1$. By the definion of a spread, for any subspace $V \in \tilde{\Sigma}$, $V \cap \ker \pi_i = V \cap U_{1-i} = 0$, thus, the restrictions $\tilde{\pi}_i = \pi_i|_V$ are bijections $V \to U_i$. In this way, any $V \in \tilde{\Sigma}$ defines a linear isomorphism $\alpha_V : U_0 \to U_1$ as presented by the following diagrams:

$$\begin{tikzcd} & W \arrow[dl, "\pi_0"'] \arrow[dr, "\pi_1"] & \\ U_0 & & U_1 \end{tikzcd} \qquad \begin{tikzcd} & V \arrow[dl, "\tilde{\pi}_0"'] \arrow[dr, "\tilde{\pi}_1"] & \\ U_0 \arrow[rr, dashed, "\alpha_V"'] & & U_1 \end{tikzcd}$$

When fixing a basis in U_0 and U_1, the matrices corresponding to the linear maps α_V, $V \in \tilde{\Sigma} \setminus \{U_0\}$, form the set of right translation maps of a quasifield.

4. Semifields

From an algebraic point of view, quasifields satisfying both distributive laws are of great importance. We define a *pre-semifield* as a set S endowed with two binary opertations $(S, +, \cdot)$ such that

(S1) $(S, +, 0)$ is an Abelian group,

(S2) $(S \setminus \{0\}, \cdot)$ is a quasigroup, and,

(S3) the distributive laws $x(y+z) = xy + xz$, $(x+y)z = xz + yz$ hold for all $x, y, z \in S$.

If $(S^*, \cdot\,)$ is a loop then $(S, +, \cdot\,)$ is called a *semifield.* Semifields are sometimes also called *nonassociative division rings.* We mention here that in abstract ring theory, the notion semifield is used in a different sense, where the additive structure does not need to be a group.

The link between semifields and translation planes is as follows. Let Π be a translation plane coordinatized by the quasifield Q. Then, it is straightforward to check that Q is a (pre-)semifield if and only for all elements $a \in Q$, the maps $\beta_a : (x, y) \mapsto (x, y + xa)$ are collineations of Π. The set $\{\beta_a \mid a \in Q\}$ forms a group isomorphic to $(Q, +)$. This group acts regularly on the set of lines of equation $Y = Xm$, $m \in Q$. One can equivalently show that a spread $\tilde{\Sigma}$ of W corresponds to a semifield if and only if there is a linear group of W which fixes an element of $\tilde{\Sigma}$ and acts regularly on the rest. Such spreads are called *semifield spreads.*

Without going into the details, we mention that a translation plane is coordinatized by a (pre-)semifield if and only if its dual plane is a translation plane, too.

We now turn our attention to the algebraic properties of a finite semifield S. From this point of view, we have a finite field $\mathbb{F}_q$, an $\mathbb{F}_q$-vector space S of dimension d and two sets of $\mathbb{F}_q$-linear transformations

$$S_r = \{R_x \mid x \in S\}, \quad \text{and} \quad S_\ell = \{L_x \mid x \in S\},$$

namely, the sets of left and right multiplication maps on S.

As we have seen before, the first question is the appropriate choice of the field $\mathbb{F}_q$. That is, we look for the largest field F such that the left and right multiplication maps are at least semilinear over F. The good news is that for semifields, semilinearity implies linearity. This result of Grundhöfer [10] is a generalization of the Cartan-Brauer-Hua theorem which says that a proper normal subring of a skewfield is contained in the center.

Proposition 4.1. *Let S be a semifield such that S is an F-vector space of finite dimension d. Assume that the left and right multiplication maps are semilinear over F. Then, they are linear over F.* □

This proposition implies that the center $Z(S)$ is the largest field such that the left and right multiplication maps are (semi)linear. In the sequel, we will always consider S as a vector field over its center $\mathbb{F}_q = Z(S)$. The dimension of S over $\mathbb{F}_q$ will be denoted by d.

In the rest of this section, we present some constructions of finite semifields which will show some possibilities for d and q. We start with two easy remarks.

1) A semifield cannot have dimension two over its center, that is, $d \geqslant 3$.

2) A semifield of order 8 is a field.

Albert's generalized twisted fields [1]. This is one of the oldest and simplest construction for finite semifields. Let F be the finite field $\mathbb{F}_{q^d}$. Let $\theta : x \mapsto x^{q^t}$ and $\sigma : x \mapsto x^{q^s}$ be automorphisms of F and $c \in F$ such that $c = x^{q-1}$ has no solution in F. Define the binary operation

$$x \circ y = xy - cx^\theta y^\sigma.$$

Then, $(F, +, \circ)$ is a pre-semifield, whose isotopic semifield is called *Albert's twisted field* corresponding to the quadruple (q, s, t, c).

Theorem 4.2. ([1] Theorem 1) *Let $1 \neq s \neq t \neq 1$. Then the right nucleus of $T = T(q^d, s, t, c)$ is $\mathbb{F}_{q^s}$ and the left nucleus of T is $\mathbb{F}_{q^t}$. The middle nucleus consists of the elements $x \in \mathbb{F}_{q^n}$ with $x^{q^s} = x^{q^t}$.* □

The following result was conjectured by Kaplansky and proved by Menichetti.

Theorem 4.3. ([15]) *Any three-dimensional semifield over a finite field is associative or a twisted field.* □

Knuth's binary semifields. The following construction by Knuth [14] gives a commutative semifield. Let $T : \mathbb{F}_{2^{nm}} \to \mathbb{F}_{2^m}$ be a map which is linear over the subfield $\mathbb{F}_{2^m}$. Define the multiplication

$$x \circ y = xy + (T(a)b + aT(b))^2.$$

Then $(\mathbb{F}_{2^{nm}}, +, \circ)$ is a commutative pre-semifield and the isotope $(\mathbb{F}_{2^{nm}}, +, *)$ defined by

$$(1 \circ x) * (1 \circ x) = x \circ y$$

is a commutative semifield with multiplicative unit 1.

The Cohen-Ganley commutative semifields. Let q be an odd prime power. We say that the maps $f, g : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ form a *Cohen-Ganley pair* if

(CG1) they are $\mathbb{F}_q$-linear, and

(CG2) $g(t)^2 + 4tf(t)$ is a non-square for all $t \in \mathbb{F}_{q^n}$.

Put $S = \mathbb{F}_{q^n} \times \mathbb{F}_{q^n}$, and define the multiplication

$$(x_1, y_1) \cdot (x_2, y_2) = (x_1x_2 + g(y_1y_2), x_1y_2 + x_2y_1 + f(y_1y_2)). \qquad (1)$$

Then the following hold.

Theorem 4.4. ([5])

(1) *$(S, +, \cdot)$ is a commutative semifield which has dimension two over its middle nucleus if and only if f, g form a Cohen-Ganley pair.*

(2) *Conversely, any commutative semifield of dimension two over its middle nucleus can be given the form* (1)*.*

(3) *There is no proper commutative semifield of even order which is of dimension two over its middle nucleus.* □

There are not many examples for Cohen-Ganley pairs f, g. Let $m \in \mathbb{F}_{q^n}$ be a non-square.

(1) The example $f(t) = mt$, $g(t) = 0$ gives rise to a field.

(2) The example $f(t) = mt^{q^s}$, $g(t) = 0$ gives a semifield which was first discovered by Dickson [8].

(3) There is an infinite class of examples in characteristic three due to Cohen and Ganley [5].

(4) The last known construction is a sporadic example $f(t) = t^9$, $g(t) = t^{27}$ for $q^n = 3^5$ due to Bader, Lunardon and Pinneri [2].

Knuth's cubical arrays. Let $(S, +, \cdot)$ be a pre-semifield of dimension d over its center F. If $\{e_1, \dots, e_d\}$ is an F-basis in S, then via the formula

$$e_i \cdot e_j = \sum_k a_{ijk} e_k,$$

the multiplication in S determines the structure constants $a_{ijk} \in F$. The *cubical array* (a_{ijk}) was introduced and studied by Knuth [13]. Moreover, Knuth observed that if (a_{ijk}) determines a pre-semifield then so does each such array obtained by applying any permutation in S_3 to the subscripts of the array. Thus, each pre-semifield produces as many as six pre-semifields. The geometric and algebraic connection between these six pre-semifield is not completely understood yet.

5. On the multiplication group of finite semifields

In this section, we investigate the structure of the multiplication group of semifields. It will turn out that this question is strongly related to the study of finite loops whose multiplication group is a classical projective linear group.

The first result is an immediate consequence of the definitions and the generalized Cartan-Brauer-Hua theorem.

Proposition 5.1. *Let S^* be the multiplicative loop of a finite semifield S with $\mathbb{F}_q = Z(S)$. Then, the nucleus of S^* equals to the center of S^*. Moreover, $Z(S^*)$ is cyclic and $Mlt(S^*)$ is a transitive subgroup of $GL(d,q)$ where $d \geqslant 3$.* □

The finite transitive linear groups are known, their classification is a corollary of the Classification Theorem of finite simple groups. Using this classification, some constructions, and results of Vesanen on multiplication groups of finite loops, one has the following result.

Theorem 5.2. ([16] Propositions 2.2 and 2.3)

(1) *Let S be a finite semifield of dimension d over its center $\mathbb{F}_q$. Let G be the multiplication group of the multiplicative loop S^*. Then, $SL(d,q) \leqslant G \leqslant GL(d,q)$.*

(2) *Let $d \geqslant 3$ be an integer and q a prime power such that $q^d > 8$. Then, there is a semifield S such that the multiplication group G of S^* satisfies $SL(d,q) \leqslant G \leqslant GL(d,q)$.*

(3) *For any integer $d \geqslant 3$ and prime power $q^d > 8$, there is a loop Q such that $PSL(d,q) \leqslant Mlt(Q) \leqslant PGL(d,q)$.* □

The last statement of the theorem gives a general affirmative answer to Drápal's problem [4, Problem 398]. Furthermore, this results pose two more questions in a natural manner.

The first question asks about the converse of part (3): If Q is a finite loop such that $PSL(d,q) \leqslant Mlt(Q) \leqslant PGL(d,q)$, then $Q = S^*/Z(S^*)$ for some semifield S? The second question is about the case when the equality $PSL(n,q) = Mlt(Q)$ holds? The latter is related to the more general problem of classifying finite simple groups which occur as multiplication groups of loops.

The following lemma answers the first question in the affirmative and can be useful for answering the second question, as well. The proof of this lemma is basically contained in the proof of [18, Theorem S].

Lemma 5.3. ([16] Proposition 2.3) *Let Q be a finite loop such that $Mlt(Q) \leqslant PGL(d,q)$ with $d \geqslant 3$. Then there is a semifield S of dimension d over its center $\mathbb{F}_q$ such that $Q \cong S^*/Z(S^*)$.* □

Concerning classical linear groups as multiplication groups of loops, the following results by Vesanen and Drápal are important.

Theorem 5.4. ([18] Theorem S) *Let $G = PSp(n,q)$ be the symplectic group acting on the set Ω of the points of the corresponding projective space and let Q be a loop defined on Ω such that $Mlt(Q) \leqslant G$. Then, $n = 2$ and Q is an Abelian group.* □

Theorem 5.5. ([18] Theorem U) *Let G be one of the following groups:*

(1) *$PGU(n,q)$, where $n \geqslant 6$,*

(2) *$PO(n,q)$, where n is odd and $n \geqslant 7$, or*

(3) *$PO^{\varepsilon}(n,q)$, where n is even and $n \geqslant 7 - \varepsilon$*

acting on the set Ω of the isotropic points of the corresponding projective space. Then there exists no loop Q defined on Ω such that $Mlt(Q) \leqslant G$. □

Theorem 5.6. ([9]) *If Q is a loop of order at least 5, and $Mlt(Q) \leqslant P\Gamma L(2,q)$ then Q is an Abelian group.* □

6. Semifield flocks

In the last section we give a survey on the results by Ball, Blokhuis and Lavrauw [3] on semifield flocks. Let q be an odd prime power and denote by $PG(3,q^n)$ the projective space of dimension 3 over the field $\mathbb{F}_{q^n}$. The points of $PG(3,q^n)$ are homogenous quadruples $\langle x_0, x_1, x_2, x_3 \rangle$ and the subspaces (lines and planes) are given by homogenous linear equations.

Fix a plane Π and a point $V \notin \Pi$. Take a non-degenerate conic $\mathfrak{C}$ in Π and define the *cone $\mathcal{K}$ with base $\mathfrak{C}$* as the union of the lines connecting V and the points of $\mathcal{K}$. Simple counting shows that $|\mathfrak{C}| = q^n + 1$ and $|\mathcal{K}| = q^{2n} + q^n + 1$. Any plane not incident with V intersects the cone in a non-degenerate conic. A *flock $\mathcal{F}$ of $\mathcal{K}$* is a partition of $\mathcal{K} \setminus \{V\}$ into q^n

conics. If all the planes that contain a conic of the flock share a line then the flock is called *linear.*

Up to a change of the system of homogenous coordinates, we can assume that $V = \langle 0,0,0,1\rangle$, $\Pi : X_3 = 0$ and the conic $\mathfrak{C}$ is given by the equation $X_0X_1 = X_2^2$. The point $U = \langle 1,0,0,0\rangle$ is in $\mathfrak{C}$, hence, the line $\ell = UV \subset \mathcal{K}$. The points of $\ell \setminus \{V\}$ have the form $\langle 1,0,0,t\rangle$, where $t \in \mathbb{F}_{q^n}$, and any such point is contained in a unique plane of the flock $\mathcal{F}$. Let us denote by Π_t the plane containing $\langle 1,0,0,t\rangle$, the equation of Π_t is

$$\Pi_t : tX_0 - f(t)X_1 + g(t)X_2 + X_3 = 0,$$

where $g, f : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$. This flock is denoted by $\mathcal{F}(f,g)$. If the maps f, g preserve the addition, in other words they are linear over a subfield, then the flock is called a *semifield flock.*

Let $\mathcal{F} = \mathcal{F}(f,g)$ be a semifield flock of $\mathcal{K}$. A standard calculation shows that

$$\Pi_t \cap \mathcal{K} = \{\langle u^2, v^2, uv, -tu^2 + f(t)v^2 - g(t)uv\rangle \mid u, v \in \mathbb{F}_{q^n}\}.$$

Substituting this in the equation of Π_s, $s \neq t$, we obtain

$$\begin{aligned} 0 &= (s-t)u^2 - (f(s) - f(t))v^2 + (g(s) - g(t))uv \\ &= (s-t)u^2 - f(s-t)v^2 + g(s-t)uv. \end{aligned}$$

As the flock property is equivalent with $\Pi_t \cap \Pi_s \cap \mathcal{K} = \emptyset$, the quadratic equation $(s-t)u^2 - f(s-t)v^2 + g(s-t)uv = 0$ has no non-trivial solution in $\mathbb{F}_{q^n}$ for u, v, that is, the discriminant $g(s-t)^2 + 4f(s-t)$ is a non-square for all s, t. This proves the following proposition.

Proposition 6.1. *The following are essentially the same:*

(*a*) *Cohen-Ganley pairs.*

(*b*) *Commutative semifields of dimension two over their middle nucleus.*

(*c*) *Semifield flocks.* □

The semifield flock corresponding to the Cohen-Ganley pair $f(t) = mt^{q^s}$, $g(t) = 0$ is called the *Kantor-Knuth flock.*

Theorem 6.2. ([17]) *If the planes of the semifield flock all share a common point, then the flock is either linear (in which case they share a line) or a Kantor-Knuth semifield flock.* □

Let $f, g : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ be a Cohen-Ganley pair which is linear over $\mathbb{F}_q$ and consider the set

$$\mathcal{W} = \{A_t = \langle t, -f(t), g(t)\rangle \mid t \in \mathbb{F}_{q^n}\}$$

of points of the projective plane $PG(2, q^n)$.

A non-degenerate quadratic form is either always a square on the external points of the conic it defines (points incident with tangents to the conic) and a non-square on the internal points (points not incident with a tangent) or the other way around. The quadratic form $Q(X_0, X_1, X_2) = X_2^2 + 4X_0X_1$ is a square on all external points to the conic $\mathfrak{C}' : X_2^2 + 4X_0X_1$ since $\langle 0, 0, 1\rangle$ is incident with a tangent and $Q(0, 0, 1) = 1$. Therefore it is a non-square on the internal points which implies that all points of $\mathcal{W}$ are internal points of $\mathfrak{C}'$.

If $\mathcal{W}$ is contained in the line of equation $\alpha_0 X_0 + \alpha_1 X_1 + \alpha_2 X_2 = 0$ then all planes Π_t share the common point $\langle \alpha_0, \alpha_1, \alpha_2, 0\rangle$, and by Theorem 6.2, the semifield flock is either linear or of Kantor-Knuth type. Assume that this is not the case. Then, there are values $t_0, t_1, t_2 \in \mathbb{F}_{q^n}$ such that A_{t_0}, A_{t_1}, A_{t_2} are linearly independent over $\mathbb{F}_{q^n}$. By the $\mathbb{F}_q$-linearity of the Cohen-Ganley pair f, g, we have

$$\lambda_0 A_{t_0} + \lambda_1 A_{t_1} + \lambda_2 A_{t_2} = A_{\lambda_0 t_0 + \lambda_1 t_1 + \lambda_2 t_2} \in \mathcal{W}$$

for all $\lambda_0, \lambda_1, \lambda_2 \in \mathbb{F}_q$. In other words, $\mathcal{W}$ contains a subplane of degree q.

Now, this is a problem in finite geometry which is interesting in its own: For which parameters q and n are the subplanes of $PG(2, q^n)$ of order q, which consists of interal points of a fixed conic? The answer was given by Blokhuis, Lavrauw and Ball:

Theorem 6.3. ([3] Theorem 3.1) *If there is a subplane of order q contained in the internal points of a nondegenerate conic $\mathfrak{C}$ in $PG(2, q^n)$ then $q < 4n^2 - 8n + 2$.* □

This implies:

Corollary 6.4. ([3] Theorem 1.1) *Let S be a commutative semifield of rank $2n$ over $\mathbb{F}_q$, q odd, and of rank 2 over its middle nucleus $\mathbb{F}_{q^n}$. If $q \geqslant 4n^2 - 8n + 2$ then S is either a Dickson semifield or a field.* □

References

[1] **A.A. Albert**, *Generalized twisted fields*, Pacific J. Math. **11** (1961), 1 – 8.

[2] **L. Bader, G. Lunardon and I. Pinneri**, *A new semifield flock*, J. Combin. Theory Ser. A **86** (1999), 49 – 62.

[3] **A. Blokhuis, M. Lavrauw and S. Ball**, *On the classification of semifield flocks* Adv. in Math. **180** (2003), 104 – 111.

[4] **P.J. Cameron**, *Research problems from the* 18*th British Combinatorial Conference*, Discrete Math. **266** (2003), 441 – 451.

[5] **S.D. Cohen and M.J. Ganley**, *Commutative semifields, two-dimensional over their middle nuclei*, J. Algebra **75** (1982), 373 – 385.

[6] **M. Corderoand and G.P. Wene**, *A survey of finite semifields*, Discrete Math. **208/209** (1999), 125 – 137.

[7] **P. Dembowski**, *Finite geometries*, Springer-Verlag, Berlin, 1968.

[8] **L.E. Dickson**, *On commutative linear algebras in which division is always uniquely possible*, Trans. Amer. Math. Soc. **7** (1906), 514 – 522.

[9] **A. Drápal**, *Multiplication groups of loops and projective semilinear transformations in dimension two*, J. Algebra **251** (2002), 256 – 278.

[10] **T. Grundhöfer**, *Projektivitätengruppen von Translationsebenen*, Resultate der Math. **6** (1983).

[11] **N. Johnson, V. Jha and M. Biliotti**, *Handbook of finite translation planes*, Pure and Applied Math. (Boca Raton), **289**, Chapman & Hall/CRC, Boca Raton, FL, 2007.

[12] **N. Knarr**, *Translation planes. Foundations and construction principles*, Lecture Notes Math. **1611** Springer-Verlag, Berlin, 1995.

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

[14] **D.E. Knuth**, *A class of projective planes*, Trans. Amer. Math. Soc. **115** (1965), 541 – 549.

[15] **G. Menichetti**, *n-dimensional algebras over a field with a cyclic extension of degree n*, Geom. Dedicata **63** (1996), 69 – 94.

[16] **G.P. Nagy**, *On the multiplication groups of semifields*, European J. Combinatorics **31** (2010), 18 – 24.

[17] **J.A. Thas**, *Generalized quadrangles and flocks of cones*, European J. Combin. **8** (1987), 441 – 452.

[18] **A. Vesanen**, *Finite classical groups and multiplication groups of loops*, Math. Soc. Camb. Phil. Soc. **117** (1995), 425 – 429.

Received April 20, 2011

Bolyai Institute, University of Szeged, Aradi vértanúk tere 1, H-6720 Szeged, Hungary
E-mail: nagyg@math.u-szeged.hu