Available at
www.ElsevierMathematics.com
POWERED BY SCIENCE DIRECT
Discrete Mathematics 275 (2004) 355–362

DISCRETE MATHEMATICS
www.elsevier.com/locate/disc

Note

A note on finite semifields and certain p-groups of class 2

N.R. Rocco*,[1], J.S. Rocha[2]

Department of Mathematics, University of Brasília, 70.910-900 Brasília, DF, Brazil

Received 6 March 2002; received in revised form 8 April 2003; accepted 28 April 2003

Abstract

In this paper the authors discuss a relationship between finite semifields of characteristic p and certain finite p-groups of nilpotence class 2.

MSC: primary: 17A35; 12K10; 20B25; secondary: 51A35

Keywords: Finite semifields; Isotopy; Finite p-groups; Projective planes

1. Introduction

A finite *semifield* is a finite algebraic system S containing at least two elements 0 and 1; S is endowed with two binary operations, addition and multiplication, written in the usual notation, and satisfying the following axioms:

A1 $(S,+)$ is a group with identity 0.
A2 If a and b are elements of S and $ab=0$ then $a=0$ or $b=0$.
A3 If a,b and c are any elements of S then $a(b+c)=ab+ac$ and $(a+b)c=ac+bc$.
A4 The element 1 satisfies the relationship $a1=1a=a$, for all a in S.

In this note the term semifield will mean finite semifield. The above axioms imply that $(S,+)$ is an abelian group and that, for every non-zero a and every b in S, the equations $ax=b$ and $ya=b$ are uniquely solvable for x and y. The additive group

* Corresponding author.
E-mail address: norai@unb.br (N.R. Rocco).
[1] Partially supported by FAPDF/Brazil.
[2] The author acknowledges a master's scholarship from CAPES/Brazil.

0012-365X/$ - see front matter
doi:10.1016/j.disc.2003.04.002

$(S,+)$ is actually an elementary abelian p-group for some prime p. This prime p is called the characteristic of the semifield S. It results that S has a vector space structure over the prime field $F = GF(p)$ and, consequently, S has p^n elements, where n is the dimension of S over F (see [4] for details).

A semifield is much like a field, except that the underlying multiplicative structure is required to be merely a loop instead of a group. The term *semifield* seems to be coined by Knuth [4]. Every finite field is an associative semifield; the term *proper semifield* will mean a semifield in which the multiplication is not associative. In the literature, semifields are also called division rings and division algebras; in fact some authors do not require that a division ring has a unity element (see also [2,3]).

Following the terminology in [4], we use the term *pre-semifield* to designate a system S satisfying axioms **A1**, **A2** and **A3** but not necessarily axiom **A4** of a semifield, i.e., a pre-semifield need not have a multiplicative identity.

Besides their intrinsic algebraic interest, proper semifields are also useful in finite geometries since they coordenatize non-Desarguesian projective planes.

If π is a projective plane coordenatized by a semifield S of order p^n, then the translations and generalized shears of π constitute a p-subgroup $\mathscr{H}$, of order p^{3n}, of the collineation group of π. This subgroup $\mathscr{H}$ has nilpotence class 2 and contains subgroups A and B of orders p^n, with the property that no non-trivial elements $a \in A$ and $b \in B$ commute (the reader is referred to [4, Theorem 3.4.4] and for instance [3, Chapters 4–8] for further details). Thus, $\mathscr{H}$ is a particular solution of the following generalization of Problem 10.1 of the Kourovka notebook [5]:

($\mathscr{P}$) *Let p be a prime number. Describe all groups of order p^{3n} of nilpotence class 2 containing subgroups X and Y such that $|X| = |Y| = p^n$ and no non-trivial elements $x \in X$ and $y \in Y$ commute.*

One of our purpose in this note is to discuss the possible solutions to problem ($\mathscr{P}$). A main result may be stated as the

Theorem. *Let $(S,+,\cdot)$ be a pre-semifield and G the set of all triples (a,b,c) of elements of S with an operation $*$ defined by*

$$(a,b,c) * (d,e,f) := (a+d, b+e, c+f+b\cdot d). \tag{1}$$

Then $(G,*)$ is a group which is a solution to ($\mathscr{P}$). Conversely, if a group G is a solution to ($\mathscr{P}$) then there exists a pre-semifield S such that G can be described as above.

It is natural to ask what happens with pre-semifields $(S_1,+,\cdot)$ and $(S_2,+,\circ)$ corresponding to isomorphic groups G_1 and G_2, as in the Theorem above. To answer this question it is convenient to recall the concept of isotopy. Given pre-semifields $(S_1,+,\cdot)$ and $(S_2,+,\circ)$, an *isotopy* from S_2 to S_1 is any triple of non-singular linear maps (A,B,C) from S_2 to S_1 such that $(x\circ y)C = (xA)\cdot(yB)$, for all $x,y \in S_2$. In this case we say that S_1 and S_2 are isotopic.

A discussion concerning the above question is in the final part of this note, where we find a necessary and sufficient condition in order that an isomorphism between the considered groups produces an isotopy between the corresponding pre-semifields (Theorem 4). Then we prove the

Proposition A. *If S_1 and S_2 are isotopic pre-semifields corresponding to the groups G_1 and G_2 respectively, then G_1 and G_2 are isomorphic.*

The converse of Proposition A is not true in general. However we can assert, in particular, the

Proposition B. *Let G be a group corresponding to a proper semifield and let the group G_1 correspond to a field. Then G and G_1 cannot be isomorphic.*

This paper extends part of the master's dissertation [7], written under the supervision of the first author, which was mainly based on Knuth [4]. The authors are grateful to the referees for their helpful comments.

2. The main results

We use the following standard notation (see, for instance, [6]). For elements x, y, z in a group G, the conjugate of x by y is $x^y = y^{-1}xy$; the commutator of x and y is $[x, y] = x^{-1}x^y$. The following commutator identities may be useful:

$$[xy, z] = [x, z]^y[y, z], \quad [x, yz] = [x, z][x, y]^z. \tag{2}$$

If X and Y are two subsets of G, then the subgroup of G generated by the union $X \cup Y$ is denoted by $\langle X, Y\rangle$ and the commutator of X and Y is the subgroup $[X, Y]$ of G, generated by all commutators $[x, y]$ with $x \in X$ and $y \in Y$. In particular, the derived subgroup of G is $G' = [G, G]$. The normal closure of X in G is the subgroup $\langle X\rangle^G$, generated by all conjugates x^g with $x \in X$ and $g \in G$; the order of G is written $|G|$. We say that G has nilpotence class 2 (class 2 for short) if G is non-abelian and $[G', G] = \{1\}$, i.e., the derived subgroup G' is contained in the center $Z(G)$ of G. Consequently, in a group of class 2 the commutator identities (2) become bilinearity relations:

$$[xy, z] = [x, z][y, z] \quad \text{and} \quad [x, yz] = [x, y][x, z]. \tag{3}$$

It is worth mentioning that if an arbitrary group H is generated by two subgroups X and Y, then the commutator $[X, Y]$ is a normal subgroup of H.

On looking over those relations holding in the subgroup $\mathscr{H}$ generated by all translations and generalized shears of a projective plane coordenatized by a semifield (see [4, Section 3.4]) we observe that such subgroup provide us with a particular solution to $(\mathscr{P})$ (as stated in the Introduction). We rephrase this first part of our Theorem as

Theorem 1. *Let $(S, +, \cdot)$ be a pre-semifield and G the set of all triples (a, b, c), where $a, b, c \in S$, with operation $*$ given by (1). Then $(G, *)$ is a group solution to $(\mathscr{P})$.*

Proof. Clearly $(G,*)$ is a group; the element $(0,0,0)$ is the identity of G and, for any elements $a,b\in S\setminus\{0\}$, we have

$$[(a,0,0),(0,b,0)] = (0,0,-b\cdot a) \neq (0,0,0)$$

and

$$[(0,b,0),(a,0,0)] = (0,0,b\cdot a) \neq (0,0,0).$$

The center of G consists of all elements of the form $(0,0,c)$, with $c\in S$. This can be verified by the following equivalences:

$$(a,b,c)*(d,e,f) = (d,e,f)*(a,b,c), \quad \forall a,b,c\in S$$

$$\Leftrightarrow (a+d,b+e,c+f+b\cdot d) = (d+a,e+b,f+c+e\cdot a), \quad \forall a,b,c\in S$$

$$\Leftrightarrow b\cdot d = e\cdot a, \quad \forall a,b\in S$$

$$\Leftrightarrow d=0 \text{ and } e=0.$$

In addition, $(a,0,0)*(0,b,0)*(0,0,c) = (a,b,0)*(0,0,c) = (a,b,c)$. Thus, on setting $X := \{(a,0,0)\mid a\in S\}$ and $Y := \{(0,b,0)\mid b\in S\}$, we see that X and Y are subgroups of G such that $G=\langle X,Y\rangle$, $Z(G)=G'=[X,Y]$, and no non-trivial elements $x\in X$ and $y\in Y$ commute. □

As for the converse we state the

Theorem 2. *Let the group G be a solution to $(\mathscr{P})$. Then there exists a pre-semifield S such that G can be written as the set of all triples (a,b,c), with a, b and c in S, and the group operation is realized as the operation $*$ given by (1).*

Proof. We refer to the statement of $(\mathscr{P})$ as in the Introduction, and let H denote the subgroup of G generated by X and Y, which satisfy the following non-commutativity relation:

$$\forall x\in X\setminus\{1\}, \quad \forall y\in Y\setminus\{1\}, \quad [x,y]\neq 1. \tag{4}$$

By the normality of $[X,Y]$ in H we have $\langle X\rangle^H = X\cdot[X,Y]$ and $\langle Y\rangle^H = Y\cdot[X,Y]$. Consequently,

$$H = XY[X,Y] = Y\langle X\rangle^H. \tag{5}$$

It follows straightforward from (4) that

$$X\cap Y=\{1\} \tag{6}$$

and, as $[G,G]\leqslant Z(G)$, we obtain $[G,G]\cap X=\{1\}=[G,G]\cap Y$. In particular,

$$[X,Y]\cap X=\{1\}=[X,Y]\cap Y \tag{7}$$

and $[X,X]=[X,X]\cap X=\{1\}=[Y,Y]\cap Y=[Y,Y]$. Therefore, X and Y are abelian groups. We claim that

$$Y\cap\langle X\rangle^H=\{1\}=X\cap\langle Y\rangle^H. \tag{8}$$

Indeed, if $y \in Y \cap \langle X\rangle^H (= Y \cap X[X,Y])$ then $y = x[x_1, y_1]\cdots[x_k, y_k]$ for some $k \in \mathbb{N}$, $x_1,\ldots,x_k \in X$ and $y_1,\ldots,y_k \in Y$, where by (6) and (7) $x \neq 1$ and $\prod_{i=1}^{k} [x_i, y_i] \neq 1$. Hence, by using (2) and (3),

$$\begin{aligned} 1 = [y,y] &= [x[x_1,y_1]\cdots[x_k,y_k], y] \\ &= [x,y]^{[x_1,y_1]\cdots[x_k,y_k]}[[x_1,y_1]\cdots[x_k,y_k], y] \\ &= [x,y], \end{aligned}$$

which contradicts (4). This proves the first half of our claim (8). The other part follows by symmetry. Now let $x \neq 1$ be any fixed element of X and $\varphi : Y \to [x,Y]$, $y \mapsto [x,y]$. Then φ is injective. In effect, for $y_1, y_2 \in Y$, the equality $[x,y_1]=[x,y_2]$ is equivalent to $[x, y_1 y_2^{-1}]=1$, since G has class 2. Once again (4) says that $y_1 = y_2$. Thus $|[X,Y]| \geqslant p^n$ and, by (5)–(8), it follows that

$$p^{3n} \geqslant |H| = |X|\cdot|Y|\cdot|[X,Y]| \geqslant p^{3n}.$$

Therefore, $H=G$ and $|[X,Y]| = p^n$. Furthermore, the above analysis shows that $\langle Y\rangle^G = Y[X,Y]$ is a direct product of the subgroups Y and $[X,Y]$ and $G = X\cdot(Y[X,Y])$, a semidirect product of X and $\langle Y\rangle^G$. Hence, any element of G has a unique expression as a product xyz, where $x \in X$, $y \in Y$ and $z \in [X,Y]$, and the product of any two such elements is performed as

$$(xyz)(abc) = x(ya)bzc = x(ay[y,a])bzc = (xa)(yb)([y,a]zc). \tag{9}$$

In addition, we see that $Z(G) = [X,Y]$. In fact, suppose that for any $x \in X$, $y \in Y$ and $z \in [X,Y]$, we have $(xyz)(abc) = (abc)(xyz)$, for all $abc \in G$ with $a \in X$, $b \in Y$ and $c \in [X,Y]$. Then by (9) and (3), and the fact that $[X,Y] \subseteq G' \subseteq Z(G)$, we obtain $[x,a][y,a][x,b][y,b] = 1$, for all $a \in X$, $b \in Y$ or, since X and Y are abelian groups, $[y,a][x,b] = 1$, for all $a \in X$, $b \in Y$. Consequently, $a = 1$ and $b = 1$, by (4).

Now by Cauchy's theorem and relations (3) we have $[x^p, y] = ([x,y])^p = [x, y^p] = 1$, for all $x \in X$ and $y \in G$. This together with (4) says that X, Y and $Z(G) = [X,Y]$ have exponent p. Thus X, Y and $Z(G)$ are elementary abelian p-groups. As these three groups have the same order p^n, they are all isomorphic:

$$X \cong Y \cong Z(G) \cong \underbrace{\mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p}_{n \text{ factors}}.$$

Let S denote the additive group

$$\underbrace{\mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p}_{n \text{ factors}}.$$

Then there exist isomorphisms τ, σ and θ, such that

$$X = S^\tau, \quad Y = S^\sigma \quad \text{and} \quad Z(G) = S^\theta.$$

In addition, as $[Y,X] = Z(G)$, it follows that $[S^\sigma, S^\tau] = S^\theta$. Thus by using additive notation we see that $(a+b)^\tau = a^\tau b^\tau$, $(a+b)^\sigma = a^\sigma b^\sigma$ and $(a+b)^\theta = a^\theta b^\theta$, for all $a,b \in S$. Moreover, we can define a multiplication $\bigstar$ on S by the rule

$$(a \bigstar b)^\theta = [a^\sigma, b^\tau]. \tag{10}$$

The bilinearity of commutators provided by the nilpotence class 2 of G is now more evident in additive notation:

$$(a+c) \bigstar b = a \bigstar b + c \bigstar b \text{ and } b \bigstar (a+c) = b \bigstar a + b \bigstar c, \quad \forall a,b,c \in S,$$

and the non-commutativity condition (4) implies that $a \bigstar b = 0$ if and only if $a = 0$ or $b = 0$. Consequently, $(S, +, \bigstar)$ is a pre-semifield and on putting $x_i = a_i^\tau$, $y_i = b_i^\sigma$ and $z_i = c_i^\theta$, $i = 1, 2$, we obtain from (9)

$$\begin{aligned}(x_1y_1z_1)(x_2y_2z_2) &= (x_1x_2)(y_1y_2)([y_1, x_2]z_1z_2)\\ &= (a_1+a_2)^\tau(b_1+b_2)^\sigma(c_1+c_2+b_1 * a_2)^\theta.\end{aligned}$$

The uniqueness of expression of the elements of G and the fact that σ, τ and θ are isomorphisms say that the above is not but (1). This finishes the proof. □

The following result may be useful in order to restrict our attention to semifields only.

Lemma 3 (Knuth [4, Theorem 4.5.4]). *Let $(S, +, \circ)$ be a pre-semifield and let $u \in S \setminus \{0\}$. If we define a new multiplication $\cdot$ by the rule $(a \circ u) \cdot (u \circ b) = a \circ b$, then we obtain a semifield $(S, +, \cdot)$ isotopic to $(S, +, \circ)$ with unit $u \circ u$.*

Now, let G and G_1 be groups constructed from pre-semifields $(S, +, \cdot)$ and $(S_1, +, \circ)$ respectively, as in Theorem 1. We shall find a relationship between S and S_1 in the assumption that we are given an isomorphism $\psi : G \to G_1$.

To this end, let us fix the subgroups X and Y of G, as in the proof of Theorem 1. Thus we can write the possible images of ψ on the elements of X and Y in the following manner:

$$(a,0,0)^\psi = (a^{\sigma_1}, a^{\sigma_2}, a^{\sigma_3}) \quad \text{and} \quad (0,a,0)^\psi = (a^{\beta_1}, a^{\beta_2}, a^{\beta_3}), \tag{11}$$

where σ_1, σ_2, σ_3, β_1, β_2 and β_3 are maps from S into S_1 and a is an arbitrary element of S. Since the center of G is mapped onto the center of G_1 under the action of ψ, there exists a non-singular linear map $\phi : S \to S_1$ such that

$$(0,0,a)^\psi = (0,0,a^\phi), \tag{12}$$

for all $a \in S$. From this we obtain the image of any element of G as follows:

$$\begin{aligned}(a,b,c)^\psi &= [(a,0,0) * (0,b,0) * (0,0,c)]^\psi\\ &= (a^{\sigma_1}, a^{\sigma_2}, a^{\sigma_3}) * (b^{\beta_1}, b^{\beta_2}, b^{\beta_3}) * (0,0,c^\phi)\\ &= (a^{\sigma_1} + b^{\beta_1}, a^{\sigma_2} + b^{\beta_2}, a^{\sigma_3} + b^{\beta_3} + c^\phi + a^{\sigma_2} \circ b^{\beta_1}).\end{aligned} \tag{13}$$

By the homomorphic properties of ψ we obtain the following identities:

(i) $(a+b)^{\sigma_1} = a^{\sigma_1} + b^{\sigma_1}$,
(ii) $(a+b)^{\sigma_2} = a^{\sigma_2} + b^{\sigma_2}$,
(iii) $(a+b)^{\beta_1} = a^{\beta_1} + b^{\beta_1}$,

(iv) $(a+b)^{\beta_2} = a^{\beta_2} + b^{\beta_2}$,
(v) $a^{\sigma_2} \circ b^{\sigma_1} = b^{\sigma_2} \circ a^{\sigma_1}$,
(vi) $a^{\beta_2} \circ b^{\beta_1} = b^{\beta_2} \circ a^{\beta_1}$,
(vii) $(a+b)^{\sigma_3} = a^{\sigma_3} + b^{\sigma_3} + b^{\sigma_2} \circ a^{\sigma_1}$,
(viii) $(a+b)^{\beta_3} = a^{\beta_3} + b^{\beta_3} + b^{\beta_2} \circ a^{\beta_1}$,
(ix) $(b \cdot a)^{\phi} = b^{\beta_2} \circ a^{\sigma_1} - a^{\sigma_2} \circ b^{\beta_1}$.

The above identities give us a lot of information. The first four of them say that σ_1, σ_2, β_1 and β_2 are linear maps. In fact, $\sigma_1, \sigma_2, \beta_1, \beta_2$ are non-singular or the zero map. To see this we assume for instance that σ_1 vanishes for some $x \neq 0$ of S. By identity (v) we would have $b^{\sigma_2} \circ x^{\sigma_1} = x^{\sigma_2} \circ b^{\sigma_1} = 0$ for all $b \in S$, thus implying that $x^{\sigma_2} = 0$ or $b^{\sigma_1} = 0$ for all $b \in S$. However, since ψ is an isomorphism,

$$1 = (X \cap Z(G))^{\psi} = X^{\psi} \cap Z(G_1) \tag{14}$$

and hence we cannot have $x^{\sigma_2} = 0$. Therefore, in the present situation, σ_1 is the zero map and σ_2 is non-singular. The same is true for β_1 and β_2.

On the other hand, suppose there exist maps $\phi, \sigma_1, \sigma_2, \sigma_3, \beta_1, \beta_2, \beta_3$ from S to S_1 satisfying identities (i)–(ix), where ϕ is linear and non-singular and σ_1, σ_2, β_1 and β_2 are null or non-singular. If we define ψ by (13), then we see that ψ is a homomorphism from G to G_1. Moreover, ψ is injective. In effect, let

$$(a,b,c)^{\psi} = (a^{\sigma_1} + b^{\beta_1}, a^{\sigma_2} + b^{\beta_2}, a^{\sigma_3} + b^{\beta_3} + c^{\phi} + a^{\sigma_2} \circ b^{\beta_1}) = (0,0,0). \tag{15}$$

Then $a^{\sigma_1} = -b^{\beta_1}$ and $a^{\sigma_2} = -b^{\beta_2}$, which by substitution in (15) imply that $(0,0,b \cdot a)^{\psi} = (0,0,(b \cdot a)^{\phi}) = (0,0,0)$. Since by hypothesis ϕ is non-singular, we get $b \cdot a = 0$ and thus $a = 0$ or $b = 0$; consequently, $a = b = 0$ by (15), which in turn forces $c = 0$, too. Therefore, ψ is an isomorphism.

We resume the above discussion in the

Theorem 4. *A necessary and sufficient condition for the existence of an isomorphism ψ between the groups G and G_1 constructed from the pre-semifields S and S_1, respectively, is that there exist maps $\phi, \sigma_1, \sigma_2, \sigma_3, \beta_1, \beta_2, \beta_3$ from S to S_1 satisfying the identities* (i)–(ix), *where ϕ is linear and non-singular and $\sigma_1, \sigma_2, \beta_1$ and β_2 are null or non-singular, such that the image of any element of G by ψ is given by* (13).

Proof of Proposition A. Clearly, if two semifields $(S,+,\cdot)$ and $(S_1,+,\circ)$ are isotopic then the groups G and G_1 constructed from them are isomorphic, since we can choose maps $\phi, \sigma_1, \sigma_2, \sigma_3, \beta_1, \beta_2, \beta_3$ from S to S_1 in such a way that $(\beta_2, \sigma_1, \phi)$ is an isotopy from S to S_1 and σ_2, σ_3, β_1 and β_3 are all zero. □

Remark 5. By the above analysis we see that an isomorphism between the groups G and G_1 can be found even if the corresponding pre-semifields $(S,+,\cdot)$ and $(S_1,+,\circ)$ are *anti-isotopic*, i.e., if there exists a triple of non-singular linear maps (A,B,C) such that $(x \cdot y)C = (yA) \circ (xB)$. This observation shows that the converse of Proposition A is not true in general.

Before embarking in the proof of Proposition B we quote the following lemma which is a consequence of the well-known theorem of Albert [1], that two finite semifields coordenatize isomorphic planes if and only if they are isotopic (see also [3, Theorem 8.11]).

Lemma 6. *A proper semifield cannot be isotopic to a field.*

Proof of Proposition B. Let G be a group constructed from a proper semifield $(S,+,\circ)$ and let the group G_1 be constructed from a field $(S_1,+,\cdot)$. Suppose, on the contrary, that G and G_1 are isomorphic and consider the maps ϕ, σ_1, σ_2, σ_3, β_1, β_2 and β_3, as in Theorem 4. In particular, we have the following possibilities for identity (ix):

1. $(b\circ a)^{\phi}=b^{\beta_2}\cdot a^{\sigma_1}-a^{\sigma_2}\cdot b^{\beta_1}$,
2. $(b\circ a)^{\phi}=b^{\beta_2}\cdot a^{\sigma_1}$,
3. $(b\circ a)^{\phi}=-a^{\sigma_2}\cdot b^{\beta_1}=-b^{\beta_1}\cdot a^{\sigma_2}$.

By Lemma 6, cases (b) and (c) are not possible. So we need to consider case (a) only. By the properties of ϕ, σ_1, σ_2, β_1 and β_2, and using identities (v) and (vi), we deduce that there exist $k_1,k_2\in S_1\setminus\{0\}$, such that

$$\frac{a^{\sigma_2}}{a^{\sigma_1}}=\frac{b^{\sigma_2}}{b^{\sigma_1}}=k_1 \quad \text{e} \quad \frac{a^{\beta_2}}{a^{\beta_1}}=\frac{b^{\beta_2}}{b^{\beta_1}}=k_2, \quad \text{for all } a,b\in S\setminus\{0\}. \tag{16}$$

Hence,

$$\begin{aligned}(b\circ a)^{\phi}&=b^{\beta_2}\cdot a^{\sigma_1}-a^{\sigma_2}\cdot b^{\beta_1}\\&=(k_2\cdot b^{\beta_1})\cdot a^{\sigma_1}-(k_1\cdot a^{\sigma_1})\cdot b^{\beta_1}\\&=k_2\cdot(b^{\beta_1}\cdot a^{\sigma_1})-k_1\cdot(b^{\beta_1}\cdot a^{\sigma_1})\\&=[(k_2-k_1)\cdot b^{\beta_1}]\cdot a^{\sigma_1}.\end{aligned}$$

But this also contradicts Lemma 6, proving our result. □

References

[1] A.A. Albert, Finite division algebras and finite planes, Proceedings of the Symposium in Applied Mathematics, Vol. 10, American Mathematical Society, Providence, RI, 1960, pp. 53–70.
[2] M. Cordero, G.P. Wene, A survey of finite semifields, Discrete Math. 208/209 (1999) 125–137.
[3] D.R. Hughes, F.C. Piper, Projective Planes, Springer, New York, 1982.
[4] D.E. Knuth, Finite semifields and projective planes, J. Algebra 2 (1965) 182–217.
[5] V.D. Mazurov, E.I. Khukhro, Unsolved Problems in Group Theory—The Kourovka Notebook, Institute of Mathematics, SO RAN, Novosibirski, Russia, 1995.
[6] D.J.S. Robinson, A Course in the Theory of Groups, Springer, New York, 1982.
[7] J.S. Rocha, Hipercubos não-singulares e aplicações ao estudo de semicorpos finitos, Master's Dissertation, University of Brasília, Brasília-DF, Brazil, 2001 (in Portuguese).