A COMPLETE DESCRIPTION OF SZEP'S (2,p)-SEMIFIELDS(*)

by Domenico LENZI(**)

SOMMARIO. - In questo lavoro noi dimostriamo che in una struttura $S(+,\cdot)$ introdotta di J. SZÉP, dove $S(\cdot)$ è un gruppo finito, $S(+)$ un semigruppo e sussistono certe proprietà distributive (vedi (1) e (2) con $p = 2$ oppure $q = 2$), il gruppo $S(\cdot)$ è necessariamente prodotto diretto di gruppi di ordine 3. Inoltre proviamo che $S(+)$ è anch'esso necessariamente un gruppo per il quale esiste $b \in S$ tale che per ogni $x,y \in S$ risulta $x+y = x\cdot b\cdot y$.

SUMMARY. - J. Szép in a work to be published introduced an algebra $S(+,\cdot)$ such that:

i) $S(\cdot)$ is a group;

ii) $S(+)$ is a semigroup;

iii) there exist $p,q \in N$ such that for all $x,y,z \in S$

(1) $x\cdot(y+z) = x^q\cdot y + x^q\cdot z$

(2) $(y+z)\cdot x = y\cdot x^p + z\cdot x^p$

hold.

We shall call such an algebra a "(q,p)-semifield" and we shall call "subsemifield" of $S(+,\cdot)$ every subset T of S closed (under $+$ and $\cdot$) such that $T(+,\cdot)$ is a(q,p)-semifield.

Szép proved, and this is easy to verify (for example by using sylow's first theorem,(1) and (2)) that if $|S| = n \in N$ then G.C.D.$(q,n) = 1$ and G.C.D.$(p,n) = 1$. In particular if $p = 2$ or $q = 2$ then $|S| = 2k+1$ (where $k \in N$). In such a case Szép proved in a very simple manner that $S(\cdot)$ is a solvable group; moreover A. Lenzi proved that $S(+)$ is abelian(see [1]).

Szép hoped that every finite group $S(\cdot)$ of odd order to become a (2,p)-semifield by defining in S a suitable operation in order to obtain a

---

(*) Lavoro eseguito nell'ambito del gruppo di ricerca G.N.S.A.G.A. del C.N.R.

(**) Adress of the author: Istituto Matematico dell'Università, 73100 LECCE (ITALY)

simpler proof of the theorem of Feit and Thompson on solvability of groups of odd order. But this is not possible. In fact in this paper before we prove that every finite (2,p)-semifield $S(+,\cdot)$ (with $|S|>1$) has a subsemifield $M(+,\cdot)$ such that $M(+)$ is a group and $M(\cdot)$ is a direct product of group of order 3. As a consequence of this fact we can prove that if $S(\cdot)$ is a finite group and it is a direct product of groups of order 3 then only by fixing $b\in S$ and putting $x+y = x\cdot b\cdot y$ does $S(\cdot)$ become a (2,p)-semifield. At last we prove that the subsemifield $M(+,\cdot)$ coincides with $S(+,\cdot)$;therefore $S(\cdot)$ id a direct product of groups of order 3.

Here we shall use the following result due to Szép: for every finite (2,p)-semifield $S(+,\cdot)$ a unique element $a\in S$ exists such that $a+a=a$ (cfr. [1]).

N.1. ON THE EXISTENCE OF A SUBSEMIFIELD $M(+,\cdot)$ SUCH THAT $M(+)$ IS A GROUP.

In the following we shall consider only finite (2,p)-semifields; then $|S| = 2k+1$; moreover we shall exclude the trivial case $n=1$.

Now we observe that $(k+1)\cdot 2 = 2k+2 \equiv 1 \pmod n$; moreover, since G.C.D.$(p,n) = 1$, there exists $p' \in N$ such that $p'\cdot p \equiv 1 \pmod n$. Then we can easily verify that $a^2 = a^p$(1). In fact $a^2 = a\cdot a = a\cdot(a+a)=a^3+a^3$, and $a\cdot a^{2p'}=(a+a)\cdot a^{2p'}= a\cdot a^{2p'p} + a\cdot a^{2p'p}=a\cdot a^2+a\cdot a^2=a^3+a^3$, then $a^2=a\cdot a^{2p'}$ and hence $a=a^{2p'}$. From this it follows immediately that $a^p=a^{2p'p}=a^2$.

Now we can prove the following

THEOREM 1. Let M be the set $\{b\in S : a\cdot b = a\cdot b\}$. Then M is a subsemifield of $S(+,\cdot)$.

PROOF. Clearly if $b,b_1\in M$ then $a\cdot(b\cdot b_1^{-1}) = (b\cdot b_1^{-1})\cdot a$, moreover $a\cdot(b+b_1) = a^2\cdot b + a^2\cdot b_1 = b\cdot a^2+ b_1\cdot a^2 = b\cdot a^p + b_1\cdot a^p = (b+b_1)\cdot a$. Then $M(+,\cdot)$ is a subsemifield of $S(+,\cdot)$.

Q.E.D.

THEOREM 2. Then semigroup $M(+)$ is a group.

PROOF. In fact if $b\in M$ then $2b=b+b=b^{2k+2}+b^{2k+2} = b^{k+1}(1+1)=b^{k+1}\cdot a^{k+1}$;

(1) Here and in the sequel a is the unique element of S such that a+a=a. It is easy to verify that $a=(1+1)^2$ (cfr. [1]).From this it follows that $1+1=a^{k+1}$; in fact $a^{k+1}(1+1) = a^{2k+2}+a^{2k+2}=a+a=a=(1+1)^2$.

then, since $a\cdot b=b\cdot a$, if $h\in N$ it follows that $2^h b=b^{[(k+1)^h]}\cdot a^\ell$, where $\ell\in N$ depends on h but does not depends on b.

Now we recall that the coset $k+1+(n)$ is invertible in $\frac{Z}{(n)}(\cdot)$, and hence $\bar{h}\in N$ exists such that $(k+1)^{\bar{h}} \equiv 1 \pmod{n}$. As a consequence $2^{\bar{h}} b = b\cdot a^{\bar{\ell}}$, therefore $(2^{\bar{h}})^n b = (\underbrace{2^{\bar{h}}\cdot\ldots\cdot 2^{\bar{h}}}_{n})b = b\cdot\underbrace{a^{\bar{\ell}}\cdot\ldots\cdot a^{\bar{\ell}}}_{n} = b$; then since a is the unique element in S such that $a+a = a$, in the semigroup $M(+)$ b generates a group whose zero-element is a. From this it follows that $M(+)$ is a group since b is an arbitrary element of M.

Q.E.D.

N.2. A CHARACTERIZATION OF $M(+,\cdot)$ AND $S(+,\cdot)$.

We shall now prove the following

THEOREM 3. For all $x,y\in M$ $x+y = x\cdot a^{-1}\cdot y$. Moreover $1+1=a^{-1}$ and $M(\cdot)$ is a direct product of groups of order 3.

PROOF. In fact $x = \bar{x}\cdot a$ and $y = \bar{x}\cdot\bar{y}$, where $\bar{x} = x\cdot a^{-1}\in M$ and $\bar{y}=\bar{x}^{-1}\cdot y = a\cdot x^{-1}\cdot y\in M$. Then $x+y = \bar{x}\cdot a + \bar{x}\cdot\bar{y} = \bar{x}^{k+1}(a+\bar{y}) = \bar{x}^{k+1}\cdot\bar{y} = x^k\cdot a^{-k}\cdot y$. Analogously $y+x = y^k\cdot a^{-k}\cdot x$ and hence, since $M(+)$ is commutative, $x^k\cdot a^{-k}\cdot y = y^k\cdot a^{-k}\cdot x$. Then, by putting $y = 1$, one has $x^k = x$; hence $x\cdot a^{-1}\cdot y = x+y = y+x = y\cdot a^{-1}\cdot x$. Therefore $M(\cdot)$ is a commutative group and $1+1=1\cdot a^{-1}\cdot 1 = a^{-1}$; moreover $k-1$ is a multiple of the period of x. As a consequence, since also $n=2k+1$ is a multiple of the period of x, $3=2k+1-2(k-1)$ is a multiple of the period of x too. Then we can conclude that $M(\cdot)$ is a direct product of groups of order 3.

Q.E.D.

Conversely it is easy to verify that if $S(\cdot)$ is a direct product of groups of order 3 then the following theorem holds

THEOREM 4. If we define an operation on S by putting $x+y=x\cdot b\cdot y$, where

b is a fixed element of S, then $S(+,\cdot)$ is a $(2,p)$-semifield and $b^{-1}+b^{-1}=b^{-1}$.

And now we want to prove that if $S(+,\cdot)$ is a $(2,p)$-semifield and $|S|>1$ then $S(\cdot)$ is a direct product of groups of order 3. This is an immediate consequence of the following two theorems

THEOREM 5. $S(+)$ is a group and a is its zero-element.

PROOF. In fact for all $b\in S$ one has $b+b=b^{k+1}\cdot(1+1)=b^{k+1}\cdot a^{-1}$; then, since $a^{-1}=a^2=a^p$, $4b=(b+b)+(b+b)=b^{k+1}\cdot a^p+b^{k+1}a^p=(b^{k+1}+b^{k+1})\cdot a=$ $=(b^{k+1})^{k+1}\cdot a^{-1}\cdot a=b^{[(k+1)^2]}$. Now then, since the coset $k+1+(n)$ is invertible in $\frac{Z}{(n)}(\cdot)$, the element $m=(k+1)^2$ is such that the coset $m+(n)$ is invertible too. As a consequence an element $h\in N$ exists such that $m^h\equiv 1$ (mod n), then $4^h b=b^{(m^h)}=b$. The conclusion now follows in the same way as in the proof of theorem 2.

Q.E.D.

THEOREM 6. The subset M coincides with S.

PROOF. In fact for all $x\in S$ one has:

$$1+x=a^2\cdot a+a^2\cdot a\cdot x=a(a+a\cdot x)=a\cdot a\cdot x=a^2\cdot x,$$

$$1+x=a\cdot a^2+x\cdot a\cdot a^2=a\cdot a^p+x\cdot a\cdot a^p=(a+x\cdot a)\cdot a=x\cdot a\cdot a=x\cdot a^2$$

Then a^2 is a central element in $S(\cdot)$ and hence $a=(a^2)^2$ is central too.

Q.E.D.

R E F E R E N C E

[1] A. LENZI *Su di una struttura introdotta da J. Szép* to be published.