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 $m^{h}\equiv 1 \pmod n$, 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.