## RENDICONTI

## del <br> SEminario Matematico della Università di Padova

## O. M. Di Vincenzo <br> A. Valenti <br> *-multilinear polynomials with invertible values

Rendiconti del Seminario Matematico della Università di Padova, tome 86 (1991), p. 47-55<br>[http://www.numdam.org/item?id=RSMUP_1991__86__47_0](http://www.numdam.org/item?id=RSMUP_1991__86__47_0)

© Rendiconti del Seminario Matematico della Università di Padova, 1991, tous droits réservés.

L'accès aux archives de la revue «Rendiconti del Seminario Matematico della Università di Padova » (http://rendiconti.math.unipd.it/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

## Numdam

# *-Multilinear Polynomials with Invertible Values. 

O. M. Di Vincenzo - A. Valenti ${ }^{*}$ )

Let $R$ be a ring with involution * and $S$ and $K$ the sets of symmetric and skew elements respectively. Several authors have related the algebraic structure of $S$ or $K$ to that of $R$. For instance, in [3, Theorem 2.18] the hypothesis that all non zero traces $x+x^{*}$ are invertible determines the structure of $R$. Similar results have been obtained for the skew case.

In this paper we will examine a more general situation. In fact we consider the case when all the non zero valuations of a *-multilinear polynomial $f$ are invertible in $R$.

More precisely, let $X=\left\{x_{1}, x_{1}^{*}, \ldots, x_{n}, x_{n}^{*}, \ldots\right\}$ be a countable set of unknows and $F\{X, *\}$ be the free associative algebra with involution * in the $x_{i}$ 's and $x_{i}^{* ' s . ~ T h e ~ e l e m e n t s ~ o f ~} F\{X, *\}$ are called *-polynomials. A *-polynomial $f\left(x_{1}, \ldots, x_{n}, x_{1}^{*}, \ldots, x_{n}^{*}\right) \in F\{X, *\}$ is multilinear if, for each $i=1, \ldots, n$, either $x_{i}$ or $x_{i}^{*}$, but non both, appears in each monomial of $f$.

We shall denote by $D$ a division ring, $Z(D)$ its center, $D_{m}$ the ring of $m \times m$ matrices over $D$ and $D_{m}^{\mathrm{op}}$ its opposite ring. Notice that $D_{m} \oplus D_{m}^{\mathrm{op}}$ has a natural exchange involution given by $(x, y)^{*}=(y, x)$.

We shall prove the following result.
ThEOREM. Let $F$ be a field of characteristic different from two such that $|F|>5$. Let $R$ be a semiprime $F$-algebra with involution * and let $f=f\left(x_{1}, \ldots, x_{n}, x_{1}^{*}, \ldots, x_{n}^{*}\right)$ be a*-multilinear polynomial such that for every $r_{1}, \ldots, r_{n}$ in $R$ either $f\left(r_{1}, \ldots, r_{n}, r_{1}^{*}, \ldots, r_{n}^{*}\right)=0$ or $f\left(r_{1}, \ldots, r_{n}, r_{1}^{*}, \ldots, r_{n}^{*}\right)$ is invertible in $R$.

If $f\left(x_{1}, \ldots, x_{n}, x_{1}^{*}, \ldots, x_{n}^{*}\right)$ is not $a^{*}$-polynomial identity for $R$ then there exists a division ring $D$ such that $R$ is either
(*) Indirizzo degli AA.: O. M. Di Vincenzo: Istituto di Matematica, Università della Basilicata, Via N. Sauro 85, 85100 Potenza; A. Valenti: Dipartimento di Matematica, Università di Palermo, Via Archirafi 34, 90123 Palermo.

1) $D_{m}$ where if $m \geqslant 2$ then $\operatorname{dim}_{Z(D)} D$ is finite and $f$ is $a^{*}$-central polynomial for $m \geqslant 3$; or
2) $D_{m} \oplus D_{m}^{\mathrm{op}}$ with exchange involution, where if $m \geqslant 2$ then $\operatorname{dim}_{Z(D)} D$ is finite and $f$ is a *-central polynomial.

The conclusion of the Theorem is not surprising, because one cannot to expect that $f$ is a *-central polynomial even if $m \leqslant 2$. Infact the polynomial $f=f\left(x, x^{*}\right)=x-x^{*}$ is not a *-central polynomial in the ring $R$ of $2 \times 2$ matrices over a field $F$ with transpose type involution but it still takes zero or invertible values. The same conclusion holds for $f$ and the ring $D \oplus D^{\mathrm{op}}$ with exchange involution.

We also remark that if $R$ is a ring and $f$ is a multilinear polynomial an analogous theorem was proved in [1].

Throughout this paper $F$ will be a field with more then five elements, char. $F \neq 2, R$ will be an associative $F$-algebra with 1 and $Z=Z(R)$ its center. Also, $f\left(x_{1}, \ldots, x_{n}, x_{1}^{*}, \ldots, x_{n}^{*}\right)$ will be a multilinear *-polynomial such that for every $r_{1}, \ldots, r_{n}$ in $R$ either $f\left(r_{1}, \ldots, r_{n}, r_{1}^{*}, \ldots, r_{n}^{*}\right)=0$ or $f\left(r_{1}, \ldots, r_{n}, r_{1}^{*}, \ldots, r_{n}^{*}\right)$ is invertible in $R$; moreover we will assume that $f$ is not a ${ }^{*}$-polynomial identity for $R$.

## We begin by looking the case when $R$ is a simple artinian ring.

In this case $R=D_{m}$ is the ring of $m \times m$ matrices over a division ring $D$ and two different types of involutions are defined in $R$ :

1) The transpose type involution: let -: $D \rightarrow D$ be an involution in $D$ and $X=\operatorname{diag}\left\{c_{1}, \ldots, c_{n}\right\} \in D_{m}$ such that $0 \neq c_{i}=\bar{c}_{i}$ for all $i$.

If $A=\left(a_{i j}\right) \in D_{m}$ then $*$ is given by

$$
A^{*}=\left(a_{i j}\right)^{*}=X\left(\bar{a}_{j i}\right) X^{-1}
$$

2) The symplettic type involution: in this case $D=F$ is a field, $m=2 k$ is even and ${ }^{*}$ is given by $\left(A_{i j}\right)^{*}=\left(A_{j i}^{*}\right)$, where the $A_{i j}$ 's are $2 \times 2$ matrices over $F$ with involution given by

$$
\left(\begin{array}{ll}
a & b \\
c & d
\end{array}\right) *=\left(\begin{array}{cc}
d & -b \\
-c & a
\end{array}\right)
$$

Given a sequence $\boldsymbol{u}=\left(A_{1}, \ldots, A_{n}\right)$ of matrices from $D_{m}$, the value of $\boldsymbol{u}$ is defined to be

$$
|\boldsymbol{u}|=A_{1} A_{2} \ldots A_{n}
$$

Now, let $\mathbb{Z}_{2}=\{1, *\}$ be the group with two elements, $S_{n}$ the symmetric group of $n$ symbols and $H_{n}=\mathbb{Z}_{2} \sim S_{n}$ the wreath product of $\mathbb{Z}_{2}$ and $S_{n}$.

Also, if $(g, \sigma)=\left(g_{1}, \ldots, g_{n} ; \sigma\right) \in H_{n}$, we write

$$
u^{(g, \sigma)}=\left(A_{\sigma(1)}^{g_{1}}, \ldots, A_{\sigma(n)}^{g_{n}} \text { where } A^{g_{2}}= \begin{cases}A & \text { if } g_{i}=1 \\ A^{*} & \text { if } g_{i}=*\end{cases}\right.
$$

Let $e_{i j}$ be the usual matrix units of $D_{m}(i, j=1, \ldots, m)$. We recall that a sequence $\boldsymbol{u}=\left(a_{1} e_{i_{1} j_{1}}, \ldots, a_{n} e_{i_{n} j_{n}}\right)$ where $a_{i} \in D$, is called simple. Moreover a simple sequence $\boldsymbol{u}$ is even if there exists $(1, \sigma) \in H_{n}$ such that $\left|\boldsymbol{u}^{(1, \sigma)}\right|=b e_{i i} \neq 0$, for some $b \in D ; \boldsymbol{u}$ is odd if $\left|\boldsymbol{u}^{(1, \sigma)}\right|=b e_{i j} \neq 0$ for some $(1, \sigma) \in H_{n}, b \in D$ and $i \neq j$ (see [5]).

For any simple sequence $\boldsymbol{u}=\left(a_{1} e_{i_{1} j_{1}}, \ldots, a_{n} e_{i_{n} j_{n}}\right)$ write $l(\boldsymbol{u}, t)$ (respectively $r(u, t)$ ) for the number of occurences of the number $t$ as a left (respectively right) index of one of the unit matrices occuring in $u$. It is proved in [5] that if $\boldsymbol{u}$ is a simple even sequence then $l(\boldsymbol{u}, t)=r(\boldsymbol{u}, t)$ for every $t$; and if $\boldsymbol{u}$ is an odd simple sequence then there exist two indices $i, j$ such that $l(\boldsymbol{u}, t)=r(\boldsymbol{u}, t)$ for every $t \neq i, j$ while $l(\boldsymbol{u}, i)=r(\boldsymbol{u}, i)+1$ and $l(\boldsymbol{u}, j)=r(\boldsymbol{u}, j)-1$.

Also, we remark that if $\boldsymbol{u}$ is a simple sequence of matrices from $D_{m}$ with $|\boldsymbol{u}| \neq 0$ then $|l(\boldsymbol{u}, t)-r(\boldsymbol{u}, t)| \leqslant 1$ for all $t=1, \ldots, m$; moreover $l(\boldsymbol{u}, t)-r(\boldsymbol{u}, t)=l\left(\boldsymbol{u}, t^{\prime}\right)-r\left(\boldsymbol{u}, t^{\prime}\right) \neq 0$ implies $t=t^{\prime}$ or $|\boldsymbol{u}|=0$.

Lemma 1. Let $\boldsymbol{u}$ be a simple sequence from $D_{m}$ and $(g, \sigma) \in H_{n}$. Then we have:

1) If $|\boldsymbol{u}|=a e_{i i} \neq 0$ then $\left|\boldsymbol{u}^{(g, \sigma)}\right|=b e_{j j}$ for some $b \in D, 1 \leqslant j \leqslant m$.
2) If $|\boldsymbol{u}|=a e_{i j} \neq 0$, with $i \neq j$, then, for some $b, c \in D$, either $\left|\boldsymbol{u}^{(g, \sigma)}\right|=b e_{i j}$ or $\left|\boldsymbol{u}^{(g, \sigma)}\right|=c e_{i j}^{*}$.

Proof. If * is of transpose type the conclusion of the Lemma follows by [2, Lemma 1].

Suppose now that * is of symplectic type. Recall that the involution * acts in the following way on the matrix units

$$
e_{i j}^{*}=\left\{\begin{aligned}
-e_{j+1 i-1} & \text { if } i \text { is even and } j \text { is odd } \\
-e_{j-1 i+1} & \text { if } i \text { is odd and } j \text { is even }, \\
e_{j+1 i+1} & \text { if } i \text { and } j \text { are odd } \\
e_{j-1 i-1} & \text { if } i \text { and } j \text { are even }
\end{aligned}\right.
$$

Hence, if we denote by

$$
t^{*}= \begin{cases}t+1 & \text { if } t \text { is odd } \\ t-1 & \text { if } t \text { is even }\end{cases}
$$

then for every simple sequence $\boldsymbol{u}$ and for each $(g, \sigma) \in H_{n}$ we have

$$
\left\{\begin{array}{l}
l\left(\boldsymbol{u}^{(g, \sigma)}, t\right)=l(\boldsymbol{u}, t)+d \Leftrightarrow r\left(\boldsymbol{u}^{(g, \sigma)}, t^{*}\right)=r\left(\boldsymbol{u}, t^{*}\right)-d \\
r\left(\boldsymbol{u}^{(g, \sigma)}, t\right)=r(\boldsymbol{u}, t)+f \Leftrightarrow l\left(\boldsymbol{u}^{(g, \sigma)}, t^{*}\right)=l\left(\boldsymbol{u}, t^{*}\right)-f
\end{array}\right.
$$

This says that

$$
l(\boldsymbol{v}, t)-l(\boldsymbol{u}, t)=r\left(\boldsymbol{u}, t^{*}\right)-r\left(\boldsymbol{v}, t^{*}\right)
$$

and

$$
r(\boldsymbol{v}, t)-r(\boldsymbol{u}, t)=l\left(\boldsymbol{u}, t^{*}\right)-l\left(\boldsymbol{v}, t^{*}\right)
$$

where $\boldsymbol{v}=\boldsymbol{u}^{(g, \sigma)}$ for some $(g, \sigma) \in H_{n}$.
Hence

$$
\begin{aligned}
{[l(\boldsymbol{v}, t)-r(\boldsymbol{v}, t)]+[r(\boldsymbol{u}, t)-l(\boldsymbol{u}, t)] } & = \\
& \left.=\left[r\left(\boldsymbol{u}, t^{*}\right)\right]-l\left(\boldsymbol{u}, t^{*}\right)\right]+\left[l\left(\boldsymbol{v}, t^{*}\right)-r\left(\boldsymbol{v}, t^{*}\right)\right]
\end{aligned}
$$

Now, let $|\boldsymbol{u}|=a e_{i i} \neq 0$, then as we said above $r(\boldsymbol{u}, t)-l(\boldsymbol{u}, t)=0$, for all $t=1, \ldots, m$, hence we can write $l(\boldsymbol{v}, t)-r(\boldsymbol{v}, t)=l\left(\boldsymbol{v}, t^{*}\right)-r\left(\boldsymbol{v}, t^{*}\right)$. Since $t \neq t^{*}$ it follows, by the above remarks, that either $|\boldsymbol{v}|=b e_{j j}$, for some $b \in D$, or $|\boldsymbol{v}|=0$.

Suppose now that $|\boldsymbol{u}|=a e_{i j} \neq 0$, and, first, assume that $i^{*} \neq j$ (hence $i \neq j^{*}$ too). In this case we have:

$$
l(\boldsymbol{v}, i)-r(\boldsymbol{v}, i)-1=l\left(\boldsymbol{v}, i^{*}\right)-r\left(\boldsymbol{v}, i^{*}\right)
$$

and

$$
l(\boldsymbol{v}, j)-r(\boldsymbol{v}, j)+1=l\left(\boldsymbol{v}, j^{*}\right)-r\left(\boldsymbol{v}, j^{*}\right) .
$$

Hence, in order to have $|\boldsymbol{v}| \neq 0$ it must happen one of the following case
a) $l(\boldsymbol{v}, i)-r(\boldsymbol{v}, i)=1$ and $l(\boldsymbol{v}, j)-r(\boldsymbol{v}, j)=-1$,
b) $l(\boldsymbol{v}, i)-r(\boldsymbol{v}, i)=0$ (that is $\left.l\left(\boldsymbol{v}, i^{*}\right)-r\left(\boldsymbol{v}, i^{*}\right)=-1\right)$ and $l(\boldsymbol{v}, j)-$ $-r(v, j)=0$ (that is $\left.l\left(v, j^{*}\right)-r\left(v, j^{*}\right)=1\right)$.

If $a$ ) holds then $|\boldsymbol{v}|=b e_{i j}$ for some $b \in D$; if $b$ ) holds it follows that $|\boldsymbol{v}|=c e_{j^{*} i^{*}}=c^{\prime} e_{i j}^{*}$ for some $c$ and $c^{\prime}$ in $D$.

Finally let $i^{*}=j$. In this case we have

$$
l(\boldsymbol{v}, i)-r(\boldsymbol{v}, i)-1=1+l(\boldsymbol{v}, j)-r(\boldsymbol{v}, j),
$$

therefore if $|\boldsymbol{v}| \neq 0$, by above remarks, we must have $l(\boldsymbol{v}, i)-r(\boldsymbol{v}, i)=1$ and $l(\boldsymbol{v}, j)-r(\boldsymbol{v}, j)=-1$; this implies $|\boldsymbol{v}|=b e_{i j}$.

We recall the following definition which is a slight generalization of that given above (see also [2]).

Definition. Let $\boldsymbol{u}$ be a simple sequence. Then $\boldsymbol{u}$ is called even if for some $(g, \sigma) \in H_{n}\left|\boldsymbol{u}^{(g, \sigma)}\right|=b e_{i i} \neq 0$, and it is odd if for some $(g, \sigma) \in H_{n}$ $\left|\boldsymbol{u}^{(g, \sigma)}\right|=b e_{i j} \neq 0$, where $i \neq j$.

Since $f\left(x_{1}, \ldots, x_{n}, x_{1}^{*}, \ldots, x_{n}^{*}\right)$ is a *-multilinear polynomial we may assume that $f$ is of the following form

$$
f\left(x_{1}, \ldots, x_{n}, x_{1}^{*}, \ldots, x_{n}^{*}\right)=\sum \alpha_{(g, \sigma} x_{g(1)}^{g_{l}} \ldots x_{g(n)}^{g_{n}}
$$

where

$$
(g, \sigma)=\left(g_{1}, \ldots, g_{n} ; \sigma\right) \in H_{n} \quad \text { and } \quad x^{g_{i}}=\left\{\begin{array}{lr}
x & \text { if } g_{i}=1 \\
x^{*} & \text { if } g_{i}=*
\end{array}\right.
$$

As a consequence of the previous result we have:
Lemma 2. Let $u \in D_{m}$ be a simple sequence. Then

1) If $\boldsymbol{u}$ is even, $f\left(\boldsymbol{u}, \boldsymbol{u}^{*}\right)=\sum_{1}^{m} \alpha_{i} e_{i i}$ with $\alpha_{i} \in D$.
2) If $\boldsymbol{u}$ is odd, for some $a, b \in D, f\left(\boldsymbol{u}, \boldsymbol{u}^{*}\right)=a e_{i j}+b e_{i j}^{*}$.

We are now ready to prove the main result for simple artinian ring.

Lemma 3. Let D be a division ring of characteristic different from two and with more then five elements. If $m \geqslant 3$, then $f$ is $a *$-central polynomial for $D_{m}$

Proof. Since all the nonzero valuations of $f$ are invertible in $R=$ $=D_{m}$, by Lemma 2, $f\left(\boldsymbol{u}, \boldsymbol{u}^{*}\right)=0$ for all odd simple sequences $\boldsymbol{u}$.

Therefore, by the previous Lemma, for all $A_{1}, \ldots, A_{n} \in D_{m}$ we have

$$
f\left(A_{1}, \ldots, A_{n}, A_{1}^{*}, \ldots, A_{n}^{*}\right)=\sum a_{i} f\left(\boldsymbol{u}_{i}, \boldsymbol{u}_{i}^{*}\right)
$$

where the $\boldsymbol{u}_{i}^{\prime}$ are even simple sequences. This says that $f$ takes diagonal values in $D_{m}$.

Let $W$ be the subalgebra of $D_{m}$ generated by all the elements of the form $f\left(r_{1}, \ldots, r_{n}, r_{1}^{*}, \ldots, r_{n}^{*}\right)$, for all $r_{1}, \ldots, r_{n} \in D_{m}$. We observe that $x W x^{*} \subseteq W$ for all $x$ unitary elements of $R$. Thus, if the involution * on $R$ is symplectic by [4, Theorem 5] we have either $W=0$ or $W \subseteq Z$, the center of $R$. The first case is impossible because $f$ is not a *-polynomial identity, so $W \subseteq Z$ and $f$ is a *-central polynomial. On the other hand, if * is an involution of transpose type, since $m \geqslant 3$ by [4, Theorem 17] $f$ is a *-central polynomial.

Lemma 4. Let $R=D_{2}$. Then $D$ is finite dimensional over its center and, if * is the symplectic involution, $f$ is a *-central polynomial.

Proof. If * is of transpose type for all $A \in D_{2}$ we have

$$
A^{*}=\left(\begin{array}{cc}
c_{1} & 0 \\
0 & c_{2}
\end{array}\right) \bar{A}^{t}\left(\begin{array}{cc}
c_{1} & 0 \\
0 & c_{2}
\end{array}\right)^{-1}
$$

where - is an involution in $D$ and the $c_{i}^{\prime}$ are non zero symmetric elements of $D$. Let ${ }^{(1)}: D \rightarrow D$ be the involution on $D$ defined by $x \rightarrow c_{1} \bar{x} c_{1}^{-1}$.

Then, for all $a_{1}, \ldots, a_{n} \in D$, we have

$$
f\left(a_{1} e_{11}, \ldots, a_{n} e_{11},\left(a_{1} e_{11}\right)^{*}, \ldots,\left(a_{n} e_{11}\right)^{*}\right)=f\left(a_{1}, \ldots, a_{n}, \bar{a}_{1}^{(1)}, \ldots, \bar{a}_{n}^{(1)}\right) e_{11} .
$$

Since this values is not invertible in $R$, then $f\left(a_{1}, \ldots, a_{n}, \bar{a}_{1}^{(1)}, \ldots, \bar{a}_{n}^{(1)}\right)$ is zero in $D$, so $D$ satisfies a *-polynomial identity and $D$ is finite dimensional over its center.

If * is the symplectic involution then $D=F$ is a field. Moreover, if $\boldsymbol{u}$ is an odd simple sequence, $f\left(\boldsymbol{u}, \boldsymbol{u}^{*}\right)=a e_{12}+b e_{21}^{*}=(a-b) e_{12}$ and this value is not invertible in $R$. It follows that $f\left(\boldsymbol{u}, \boldsymbol{u}^{*}\right)=0$ for all $\boldsymbol{u}$ odd simple sequences and so all the valuations of $f$ are diagonal elements.

As in Lemma 3, the subalgebra $W$ generated by $f\left(R, R^{*}\right)$ is invariant under conjugation by unitary elements of $R$. In particular, if we consider the unitary $u=\left(\begin{array}{ll}1 & 1 \\ 0 & 1\end{array}\right)$ then, for all $w=\left(\begin{array}{ll}a & 0 \\ 0 & b\end{array}\right) \in W$, we have $\left(\begin{array}{ll}1 & 1 \\ 0 & 1\end{array}\right)\left(\begin{array}{ll}a & 0 \\ 0 & b\end{array}\right)\left(\begin{array}{rr}1 & -1 \\ 0 & 1\end{array}\right)=\left(\begin{array}{cc}a & -a+b \\ 0 & b\end{array}\right) \in W$. This implies $a=b$ and so $f$ is a ${ }^{*}$-central polynomial.

## We will examine now the general case.

We shall use the notation $Z^{+}$for $Z \cap S$. We have the following:
Lemma 5. If $R$ is any ring then $Z^{+}$is a field. Moreover, if $R$ is prime then $Z$ is a field.

Proof. Let $z$ be an element of $Z^{+}$and $r_{1}, \ldots, r_{n} \in R$ such that $f\left(r_{1}, \ldots, r_{n}, r_{1}^{*}, \ldots, r_{n}^{*}\right)$ is invertible.

Then $f\left(z r_{1}, \ldots, r_{n}, z r_{1}^{*}, \ldots, r_{n}^{*}\right)=z f\left(r_{1}, \ldots, r_{n}, r_{1}^{*}, \ldots, r_{n}^{*}\right)$, hence, either $f\left(z r_{1}, \ldots, r_{n}, z r_{1}^{*}, \ldots, r_{n}^{*}\right)$ is invertible and this implies that $z$ is invertible or $f\left(z r_{1}, \ldots, r_{n}, z r_{1}^{*}, \ldots, r_{n}^{*}\right)=0$ and it follows that $z=0$.

Now, if $R$ is a prime ring, for all $z \in Z-\{0\}, 0 \neq z z^{*} \in Z^{+}$and by the above $z z^{*}$, and so $z$, is invertible.

We continue with the following:
Lemma 6. If $R$ is semiprime then $R$ is *-simple. Moreover, if $R$ is prime then $R$ is simple.

Proof. Let $0 \neq I=I^{*}$ be a proper ideal of $R$ invariant under the involution *. Since the values of $f\left(x_{1}, \ldots, x_{n}, x_{1}^{*}, \ldots, x_{n}^{*}\right)$ in $R$ are zero or invertible, we have $f\left(r_{1}, \ldots, r_{n}, r_{1}^{*}, \ldots, r_{n}^{*}\right)=0$ for all $r_{1}, \ldots, r_{n} \in I$.

Hence $f$ is a *-polynomial identity for $I$ and by [3, Theorem 1.4.2] $Z(I) \neq 0$. Also, by [3, Lemma 1.1.5], $Z(I) \subseteq Z(R)$. Now, if $Z(I) \cap S=0$ then, for all $z \in Z(I), z+z^{*}=z z^{*}=0$ and this implies $z^{2}=0$, a contradiction as $R$ is semiprime. Hence $0 \neq Z(I) \cap S \subseteq Z(R) \cap S=Z^{+}$. By Lemma $5, Z^{+}$is a field and so $I=R$, a contradiction again. Therefore $R$ is ${ }^{*}$-simple-.

Now, if $R$ is prime, let $I \neq(0)$ be an ideal of $R$; then $I I^{*}$ is a *-ideal. Since $R$ is ${ }^{*}$-simple then either $I I^{*}=(0)$ or $I I^{*}=R$ and this implies that $I=R$, that is $R$ is a simple ring.

In the following lemma we study the case when $R$ is a prime ring.

Lemma 7. If $R$ is a prime ring, char $\mathrm{R} \neq 2$, then

1) either $R$ is a division ring, or
2) $R \cong D_{m}$ is a finite dimensional central simple algebra and, if $m \geqslant 3, f\left(x_{1}, \ldots, x_{n}, x_{1}^{*}, \ldots, x_{n}^{*}\right)$ is a ${ }^{*}$-central polynomial.

Proof. By the previous Lemma, $R$ is a simple ring. If every symmetric element of $R$ is nilpotent or invertible, by [3, Theorem
2.3.3], then either $R$ is a division ring or the ring of $2 \times 2$ matrices over a field and we are done.

Therefore we may assume that there exists $s \in S$ such that $s$ is neither nilpotent or invertible. Let $R_{1}=s R s$; for all $r_{1}, \ldots r_{n} \in R$ we have $f\left(s r_{1} s, \ldots, s r_{n} s, s r_{1}^{*} s, \ldots, s r_{n}^{*} s\right)=s a s$, since $s$ is not invertible $s a s=0$ and so $f$ is a *-polynomial identity for $R_{1}$. By [3, Theorem 5.5.1] sRs satisfies an identity, hence $R$ satisfies a generalized polynomial identity.

Since $R$ is a simple ring with $1, R$ coincides with its central closure and so, by [3, Corollary 2 to the Theorem 1.2.2] either $R \cong D_{m}$ or, for all $m \geqslant 1, R$ contains a ${ }^{*}$-invariant subring $R^{(m)}$ such that $R^{(m)} \cong D_{m}$.

In the first case the conclusion follows by Lemma 3 and Lemma 4. In the second case, by Lemma 3 , for all $m \geqslant 3, f$ is a *-central polynomial for $D_{m}$. Then, by [3, Lemma 5.1.5] $D_{m}$ satisfies a polynomial identity of degree $2(\operatorname{deg} f+1)$ for all $m \geqslant 3$, a contradiction.

## We can now prove the main theorem of this note.

Proof of the Theorem. By Lemma $6, R$ is a $*$-simple ring thus either $R$ is simple or $R$ has a simple homomorphic image $R_{1}$ such that $R \cong R_{1} \oplus R_{1}^{\mathrm{op}}$ and ${ }^{*}$ is the exchange involution (see [6, Proposition 2.1.12]).

In the first case the result follows from Lemma 5. We may, therefore, assume that $R=R_{1} \oplus R_{1}^{\mathrm{op}}$ with involution ${ }^{*}$, where $R_{1}$ is a simple ring and ${ }^{*}$ the exchange involution.

By setting

$$
x_{i}=\frac{1}{2}\left[\left(x_{i}+x_{i}^{*}\right)+\left(x_{i}-x_{i}^{*}\right)\right] \quad \text { and } \quad x_{i}^{*}=\frac{1}{2}\left[\left(x_{i}+x_{i}^{*}\right)-\left(x_{i}-x_{i}^{*}\right)\right]
$$

we can write $f\left(x_{1}, \ldots, x_{n}, x_{1}^{*}, \ldots, x_{n}^{*}\right)$ as a polynomial in the symmetric variables $y_{i}=x_{i}+x_{i}^{*}$ and in the skew variables $z_{i}=x_{i}-x_{i}^{*}$.

Let $f=g\left(y_{1}, \ldots, y_{n}, z_{1}, \ldots, z_{n}\right)$, then $g\left(y_{1}, \ldots, y_{n}, z_{1}, \ldots, z_{n}\right)$, is a polynomial of degree $n$ in $2 n$ unknowns such that, for every monomial $M$ of $g$ we have

$$
\operatorname{deg}_{y_{\imath}} M+\operatorname{deg}_{z_{i}} M=1 \quad \text { and } \quad \operatorname{deg} M=n
$$

Moreover, for all substitutions

$$
\left\{\begin{array}{l}
y_{i} \rightarrow\left(a_{i}, a_{i}\right)=\bar{a}_{i}, \\
z_{i} \rightarrow\left(b_{i},-b_{i}\right)=\bar{b}_{i}
\end{array}\right.
$$

we have that $g\left(\bar{a}_{1}, \ldots, \bar{a}_{n}, \ldots, \bar{b}_{1}, \ldots, \bar{b}_{n}\right)$ is either zero or invertible in $R$.

Let $h$ be one of the blended components of $g$; that is $h$ is the sum of all the monomials of $g$ in which appear the variables $y_{i_{1}}, \ldots, y_{i_{i}}, z_{j_{1}}, \ldots, z_{j_{s}}$ for some partition of $\{1, \ldots, n\}$ in the disjoint subsets $\left\{i_{1}, \ldots, i_{t}\right\}$ and $\left\{j_{1}, \ldots, j_{s}\right\}$.

Then

$$
h\left(\bar{a}_{i_{1}}, \ldots, \bar{a}_{i_{i}}, \bar{b}_{j_{1}}, \ldots, \bar{b}_{j_{s}}\right)=g\left(0, \ldots, \bar{a}_{i_{1}}, \ldots, 0, \ldots, \bar{a}_{i_{t}}, \bar{b}_{j_{1}}, 0, \ldots, \bar{b}_{j_{s}}, 0, \ldots\right)
$$

is zero or invertible in $R$.
If $M$ is a monomial of $h$ we indicate with $M^{\mathrm{op}}$ the opposite monomial of $M$. Then

$$
\begin{aligned}
& M\left(\bar{a}_{i_{1}}, \ldots, \bar{a}_{i_{t}}, \bar{b}_{j_{1}}, \ldots, \bar{b}_{j_{s}}\right)= \\
& \quad=\left(M\left(a_{i_{1}}, \ldots, a_{i_{t}}, b_{j_{1}}, \ldots, b_{j_{s}}\right),(-1)^{s} M^{\mathrm{op}}\left(a_{i_{1}}, \ldots, a_{i_{t}}, b_{j_{1}}, \ldots, b_{j_{s}}\right)\right)
\end{aligned}
$$

and so

$$
\begin{aligned}
& h\left(\bar{a}_{i_{1}}, \ldots, \bar{a}_{i_{i}}, \bar{b}_{j_{1}}, \ldots, \bar{b}_{j_{s}}\right)= \\
& \quad=\left(h\left(a_{i_{1}}, \ldots, a_{i_{t}}, b_{j_{1}}, \ldots, b_{j_{s}}\right),(-1)^{s} h^{\mathrm{op}}\left(a_{i_{1}}, \ldots, a_{i_{t}}, b_{j_{1}}, \ldots, b_{j_{s}}\right) .\right)
\end{aligned}
$$

It follows that $h$ is a multilinear polynomial (without *) that assumes zero or invertible values in $R_{1}$

Since $R_{1}$ is a simple ring with 1 , by [1, Theorem] either $R_{1}$ is a division ring or $R_{1} \cong D_{m}$ where $m \geqslant 2, D$ is a finite dimensional central division ring and $h$ is a central polynomial in $D_{m}$.

This leads to desired conclusion.

## REFERENCES

[1] O. M. Di Vincenzo - R. Sagona, Multilinear polynomials with invertible values, Comm. Algebra, 19 (1991), pp. 539-550.
[2] A. Giambruno - A. Valenti, Nil *-polynomials in rings, Linear and Multilinear Algebra, 24 (1989), pp. 127-134.
[3] I. N. Herstein, Rings with involution, University of Chicago Press (1976).
[4] P. H. Lee, On unitary invariant subalgebras, Chinese J. Math. (17), 2 (1989), pp. 87-108.
[5] U. Leron, Nil and power central polynomials in rings, Trans. Amer. Math. Soc., 202 (1975), pp. 97-103.
[6] L. H. Rowen, Polynomials identity in ring theory, Academic Press, New York-London (1980).

Manoscritto pervenuto in redazione il 27 agosto 1990.

