IDENTITIES IN RINGS WITH INVOLUTIONS

BY

S. A. AMITSUR

ABSTRACT

A ring R with an involution $a \to a^*$ which satisfies a polynomial identity $p[x_1,\ldots,x_d;\ x^*_1,\ldots,x^*_d] = 0$ satisfies– an identity which does not include the x^*. This generalizes the result of [1] where the symmetric elements of R were assumed to satisfy an identity.

1. **Introduction.** Let R be a ring with an involution $*$: $a \to a^*$. Let R be an Ω-algebra, (Ω will be assumed to be a commutative ring). In [1] we have shown that if the set of symmetric (or antisymmetric) elements of R satisfy a polynomial identity then the ring R itself satisfies a polynomial identity, and certain relations between the bounds of the identities have been obtained. In this paper we generalise this result in the following:

THEOREM 1. *If R satisfies a polynomial identity of the form $p[x_1,\cdots,x_r;\ x^*_1 \cdots x^*_r] = 0$ of degree d, then R satisfies an identity $S_{2d}[x]^m = 0$[1]. If R is semi-prime then $m = 1$.*

This extends the result of [1], since if the symmetric elements of R satisfy a polynomial identity $p[z_1,\cdots,z_d] = 0$, then R satisfies the identity $p[x_1 + x^*_1,\ x_2 + x^*_2,\cdots,x_d + x^*_d] = 0$ which is of the form given in our theorem.

The proofs of the basic lemmas are obtained by refining those of [1] and by simplification of the case of primitive rings. Proofs which are the same as in [1] will just be quoted.

The polynomials $p[x;x^*]$ which appear in Theorem 1 can be described as follows: Let $\{x_j, y_j\}$ be an infinite set of pairs of non-commutative indeterminates over Ω, and construct the polynomial ring $\Omega[\cdots,x_j,y_j,\cdots] = \Omega[x;y]$, with Ω in the center. There is a unique involution $*$: $\Omega[x;y] \to \Omega[x;y]$ generated by the maps $*$: $x_j \to y_j$ and $y_j \to x_j$ for every j, Now $p[x;x^*]$ is an element in

[1] $S_{2d}[x] = S_{2d}[x_1,\ldots,x_{2d}] = \Sigma \pm x_{i_1}\, x_{i_2} \ldots x_{i_{2d}}$ is the standard identity of degree $2d$.

Received January 24, 1969.

$\Omega[x;y] = \Omega[x;x^*]$; by the degree of $p[x;x^*]$ we mean its total degree as a polynomial in $\Omega[x;x^*]$.

To simplify statement of results and proof we shall assume henceforth that:

(a) $p[x;x^*]$ is a polynomial of degree d, and the coefficient of one of its monomials of degree d is $=1$;

(b) R will be assumed to satisfy the identity $p[x;x^*] = 0$; meaning that $p[a;a^*] = 0$ for every substitution $x_i = a_i$, $x^*_i = a^*_i$ of elements $a_i \in R$.

The linearization process of polynomial identities can be also applied in our case, and will yield:

LEMMA 2. *If R satisfies the identity $\bar{p}[x;x^*] = \alpha m(x;x^*) + \cdots$ of degree d where $\alpha \neq 0$ and $m(x;x^*)$ is a monomial of degree d, then R satisfies also an identity $p[x;x^*] = \alpha x_1 x_2 \cdots x_d + p_0[x_1,\cdots,x_d; x^*_1,\cdots,x^*_d]$ where the monomials of $p_0[x;x^*]$ with non-zero coefficients are of degree d and each contain either x_i or x^*_i (not both!) for every $i = 1,\cdots,d$.*

The proof is by linearization and induction on the maximum of "the degree of p in x_i plus the degree of p in x^*_i". If the degree of p in x_i + the degree of p in x^*_i is l, then the polynomial $p[\cdots,x_i+z,\cdots;\ \cdots,x^*+z^*,\cdots] - p[\cdots,x_i,\cdots;\cdots,x^*_i,\cdots] - p[\cdots,z,\cdots;\cdots,z^*\ \cdots]$ which is obtained by replacing x_i by $x_i + z$ and x^*_i by $x^*_i + z^*$ (z is an additional x) and substraction, will also hold in R and will contain a monomial $\alpha m'(x;x^*)$ of degree d. The degree of this new polynomial in x_i + degree in x^*_i will be lower – and induction can be applied. The case where these degrees for each i is one will give a monomial $\alpha y_1,\cdots,y_d = \alpha\bar{m}(x,x^*)$ where each y_i is an x_j or x^*_j, but only one of them will appear. Replacing the x^*_j by x_j (and x_j in the other monomials by x^*_j) and changing the indices will clearly yield our lemma.

Since we assumed in (a) that one α is $=1$, hence we may assume that $p[x;x^*]$ is the of form:

$$\text{(a}'\text{)}\qquad p[x_1,\cdots,x_d;x^*_1\ \cdots,x^*_d] = x_1x_2\cdots x_d + p_0[x_1\ \cdots,x_d;x^*_1,\cdots,x^*_d]$$

and p_0 is of the form stated in Lemma 2.

If we use the polynomial of (a′) then clearly we have:

LEMMA 3. *If R satisfies $p[x;x^*] = 0$, and K is a commutative Ω ring then $R \otimes_\Omega K = R_K$ also satisfies $p[x;x^*] = 0$, where the involution of R_K is given by $(r \otimes k)^* = r^* \otimes k$, and every homomorphic image $R\phi$ of R, for which* $(\ker\phi)^* \subseteq \operatorname{Ker}\phi$ *will also satisfy the same identity.*

The proof is evident since $p[x,x^*]$ can be assumed to be of degree 1 in each x_i and x^*_i with no two of them in the same monomial.

2. **Nil subsets of** R. We are now in position to refine the proofs of 1, and to show our first result:

LEMMA 4. *Let P be a two sided ideal, and U a subset of R such that $U = U^* = \{r^* \mid R \in U\}$ and $U^m \subseteq P$ then U^d generates a nilpotent ideal modulo P.*

The proof is parallel to [1, Lemma 1]:

For $k > d$, consider the sets $T_{2j-1} = U^{k-j}RU^{j-1}$ and $T_{2j} = U^{k-j}RU^j$ for $j = 1,2 \cdots,k$. Since $U^* = U$, it follows that $T^*_\lambda = T_{2k-\lambda}$, and so if $\lambda \leqq d$, $2k - \lambda > d$. Note also that if $t_i \in T_i$ for all i, then $t_it_j \in RU^kR$ if $i > j$. Hence if we choose $x_i = t_i$ $i = 1,2,\cdots,d$ then $x^*_i = t^*_i \in T_{2k-i}$ and $2k - i > d$. Hence for every monomial $y_{j_1} \cdots y_{j_d}$ where the y_j is one of the t_i or t^*_i and which is not $t_1t_2\cdots t_d$, we have $y_{j_1}y_{j_2}\cdots y_{j_d} \cdot U^hR \subseteq RU^kR$ $(2h = d$, or $2h - 1 = d)$ (compare with [1, p. 101]). So that $p[t;t^*]U^hR \equiv t_1 \cdots t_dU^hR \pmod{RU^kR}$ and the rest of the proof is that of [1 lemma 1].

Next theorem is the extension of [1, Theorem 2]. The proof is the same and will not be repeated.

THEOREM 5. *If R satisfies an identity of degree d, then the nil radical $U(R)$ is equal to the lower radical $L(R)$ and $L(R)^d \subseteq N_1(R)$, where $N_1(R)$ is the union of all nilpotent ideals of R, In particular, if R is semi-prime (i.e. $L(R) = 0$) then R has no nil ideals.*

3. **Primitive images of** R, We turn now to the primitive case. Let R be an arbitrary ring with an involution, P a primitive ideal in R such that R/P is an irreducible ring of endomorphisms of a vector space V_D, over a division ring D.

Instead of [1, Lemma 3], we have a different result, which will enable us to prove that primitive rings with identities always have a minimal left ideal:

LEMMA 6. *If R is as above, then one of the following hold:*

1. *R/P has a minimal left ideal.*

2. *There is a finite dimensional D-subspace $W \subseteq V$, such that $L = (0: W) = \{r \mid rW = 0\}$, satisfies $L^* \subseteq P$.*

3. *For every finite dimensional subspace $W \subseteq V$, and every $v \notin W$, there exists $x \in R$ such that $xW = x^*W = 0$ $x^*v = 0$ and $xv \notin W + vD$.*

Proof. If R has no minimal left ideal. i.e. (1) is not valid, and neither (2) holds, then let W be a f.d. subspace of V and let $v \notin W$. Consider the f.d.-space $\bar{W} = W + vD$. $(0:\bar{W})^* \notin P$ since (2) does not hold, hence there exists $a \in R$ such that $a\bar{W} = 0$ and $a^*V \neq 0$: namely, take $a \in (0:\bar{W})$ such that $a^* \notin P$. The space a^*V is not finite dimensional, since a primitive ring which has a linear transformation of finite range has a minimal left ideal ([2]) p. 75). Let $L \neq (0:W)$ then since $v \notin W$ it follows by the density theorem that $Lv = V$. Hence, $a^*Lv = a^*V$, which is of infinite dimension, must contain a vector $u \notin W + vD$ as the latter is of finite dimension. We conclude therefore that there exists $b \in L$ such that $a^*bv = u$. Finally set $x = a^*b$; then $u = xv \notin W + vD$; $xW = 0$ since $b \in (0:W)$; $x^* = b^*a$ so that $x^*\bar{W} = 0$ i.e. $x^*W = x^*v = 0$. q.e.d.

With the help of this lemma we prove the parallel of [1, lemma 4]. That is:

LEMMA 7. *If R is a ring with an involution which satisfies an identity then every primitive image of R has a minimal left ideal.*

Proof. We have to consider cases (2) and (3) of Lemma 6. In case (2), and if (1) does not hold then $(V:D) = \infty$, and let $v_0, v_1, \cdots, v_d$ be D-independent elements of V which $\notin W$. W is finite dimensional hence, it follows by the density theorem that there exists $t_i \in (0:W)$ such that $t_iv_j = 0$ for $i \neq j$ $t_iv_i = v_{i-1}$ for $i = 1,2,\cdots d$. Since $(0:W)^* \subseteq P$ it follows that $t^*_iV = 0$. Hence:

$$0 = p[t_1,\cdots,t_d;\, t^*_1,\cdots,t^*_d]v_d = t_1t_2\cdots t_dv_d = v_0 \neq 0$$

which is a contradiction. Thus, even in this case R/P has a minimal left ideal.

In case (3), and if (1) does not hold then: we obtain a contradiction as follows: Start with $v \neq 0$ and choose $t_d \in R$ by (3) so that $t_dv \notin vD$, $t^*_dv = 0$ (use $W = 0$). Next choose $t_{d-1} \in R$ by (3) so that $t^*_{d-1}v = t^*_{d-1}t_dv = 0$, $t_{d-1}v = 0$ and $t_{d-1}t_dv \notin vD + t_dvD$ by applying (3) to $W = vD$ and v replaced by t_dv. We can continue this way to get a sequence of elements $t_1, t_2, \cdots, t_d$ such that $t_j(t_it_{i+1}\cdots t_dv) = 0$ for $i < j+1$; $t^*_j(t_it_{i+1}\cdots t_dv) = 0$ for $i \leqq j+1$ and $t_jt_{j+1}\cdots t_dv \notin vD + t_dvD + t_{d-1}t_dvD + \cdots + t_{j+1}t_{j+2}\cdots t_dvD$.

Consider now the substitution $x_i = t_i$ then

$$0 = p[t_1,\cdots,t_d;\, t^*_1,\cdots,t^*_d]v = p_1[t_1,\cdots,t_{d-1};t^*_1,\cdots,t^*_{d-1}]t_dv$$

since each monomial which does not end with t_d will annihilate v as it ends with t_j $(j \neq d)$ or a t^*_k $(k \leqq d)$ and all these annihilate v. The monomials ending with t_d will not contain t^*_d (by the way $p[x;x^*]$ was chosen) so that $p_1[\,,\,]$ does

not contain neither t_d nor t^*_d. The same reasoning replacing v by t_dv, and continuing for $t_{d-1}t_dv$ $t_{d-2}t_{d-1}t_dv$ etc., will yield: $0 = p[t,t^*]v = t_1t_2\cdots t_dv \neq 0$
Again a contradiction, which implies that R/P has a minimal left ideal.

Finally we reprove the crucial part of [1, Theorem 5].

LEMMA 8. *If R is a primitive ring with an involution satisfying an identity $p[x;x^*] = 0$ of degree d then R is a complete ring of linear transformations of a vector space V_D of dimension $\leqq d$.*

Proof. We proceed as in [1, p. 104], and get the Hermitian for (v,v) form $V = Re$, where Re is a mininmal left ideal. If there exists $v\in V$ such that $(v,v)\neq 0$, we have $V = vD + v^\perp$ and $R_0 = \{r\in R \mid rf = 0,\ rv^\perp \subseteq v^\perp\}$ is also an irreducible ring of endomorphism of $v^\perp$, and the involution (*) induces an involution on R_0 (the proofs are given in [1] p. 104 lines 7–20). Now R_0 will satisfy an identity of degree $d-1$, since choose $t_d = ur^*v^*$, $v\in V$ and u arbitrary in $v^\perp$, $r\in R$ arbitrary, and all $t_i\in R_0$ for $i<d$. Then:

$$0 = p[t_1,\cdots,t_d;t^*_1,\cdots,t^*_d]v =$$
$$= p_0[t_1,\cdots,t_{d-1};t^*_1,\cdots,t^*_{d-1}]t_dv + p_1[t_1,\cdots,t_{d-1};\ t^*_1,\cdots,t^*_{d-1}]t^*_dv + p_2[\ ,\ ]v$$

the monomials of p_2 will end in t_i or t^*_i which belong to R_0 and so annihilate v. Next $t^*_dv = (urv^*)^*v = vru^*v = vr(u,v) = 0$ since $u\in v^\perp$. Thus we remain with $0 = p_0[t_1,\cdots,t_{d-1};\ t^*_1,\cdots t^*_{d-1}]t_dv = p_0(t,t^*](urv^*v) = p_0[t;t^*]u\cdot r(v,v)$.

Hence since $(v,v)\neq 0$ and this being true for every $r\in R$ and $u\in v^\perp$ yields that $p_0[x_1,\cdots,x_{d-1};x^*_1,\cdots y^*_{d-1}] = 0$ is an identity in R_0, as required.

If $(v,v) = 0$ for every $v\in R$ we proceed as in [1] p. 104 line -12 to -2 and we get $V_0 = v_1D + v_2D$, $V =, V_0 + V_0^\perp$, and $R_0 = \{r \mid rV_0 = 0 \text{ and } rV_0^{\perp'}\subseteq V_0^\perp\}$, where $(v_1v_2)\neq 0$. R_0 is an irreducible ring of endomorphisms of $V_0^\perp$, and one has to show that R_0 satisfies and identity of degree $\leqq d-2$:

For arbitrary $r_1,r_2\in R$, and $u\in V_0^\perp$ we choose $t_d = v_1r_1v_2{}^*$ and $t_{d-1} = ur_2v_2{}^*$; and $t_i\in R_0$, $i\leqq d-2$. Computing $0 = p[t_1,\cdots,t_d;t_2^*,\cdots,t_d^*]v_1$ we observe that each monomial which ends with t_i or t_i^*, $i\leqq d-2$ will annihilate v_1 since $t_i,t^*_i\in R_0$ rnd so $t_iv_1 = t_i^*v_1 = t^*_iv_1 = 0$, as well as $t_it_dv_1 = t_iv_1r_1v^*_2v_1 = 0$ and similarly $t^*_it_dv = 0$. Furthermore, $t^*_dv_1 = v_2r^*_1v^*_1v_1 = 0$ since $(v_1,v_1) = v^*_1v_1 = 0$, and $t^*_{d-1}v_1 = v_2r^*_2u^*v_1 = v_2r^*_2(u,v_1) = 0$ and the same reason yields also that $t^*_{d-1}t_d = v_2r^*_2u^*v_1r_1v^*_2 = 0$. Thus we are left in $0 = p[t,t^*]v_1$ only with monomials ending with $t_{d-1}t_dv_1$ and with $t_{d-1}v_1$. Monomials of the form $y_1\cdots y_{d-1}t_{d-1}v_1$ with the y_i are all different t_j or t^*_j must contain either t_d or t^*_d and will not contain t^*_{d-1}; now t_d or t^*_d can not be in the middle since $t_i t_d = t^*_i t_d = t_i t^*_d = t^*_i t^*_d = 0$ for $i \leqq d-2$ as seen before. But then since $t^*_i, t_i \in R_0$ for $i \leqq d - 2$ it follows that $y_1 = t^*_d$ or t_d and $y_2 \cdots y_{d-1} t_{d-1} v_1 = y_2 \cdots y_{d-1} u r_2 v^*_2 = u_0 r_2 v^*_2$ for some $u_0 \in V_0^{\perp}$ and hence $t^*_d u_0 = v_2 r^*_1 v^*_1 u_0 = v_2 r^*_1 (v_1, u_0) = 0$ since $(v_1, u_0) = 0$; similarly $t_d u_0 = 0$. Thus we have

$$
\begin{aligned}
0 &= p[t, t^*] v_1 \\
&= \bar{p}[t_1, \cdots, t_{d-2}; t^*_1, \cdots, t^*_{d-2}] t_{d-1} t_d v_1 \\
&= \bar{p}[t_1, \cdots, t_{d-2}; t^*_1, \cdots, t^*_{d-2}] u r_2 v^*_2 v_1 r_1 v^*_2 v_1 \\
&= \bar{p}[t; t^*] u r_2 (v_2 v_1) r_1 (v_2 v_1).
\end{aligned}
$$

Since $(v_2, v_1) \neq 0$ and this being true for all $v_1, r_2 \in R$ and $u \in V_0^{\perp}$ implies that $\bar{p}[t_1, \cdots, t_{d-2}; t^*_1, \cdots, t^*_{d-2}] = 0$ hold in R_0 as required.

These are the only changes needed to complete the proof of our lemma and the rest is as in [1] p. 105.

We can now complete the proof of a theorem which is parallel to [1] Theorem 5, following the arguments of [1] pp. 103–105. We do not repeat the proof, but only state the result;

THEOREM 9. *If R satisfies an identity $p[x; x^*] = 0$ of degree d, then $R/L(R)$ satisfies an ordinary identity (not involving x^*) of degree $\leqq 2d$, and $R/N_1(R)$ satisfies an ordinary identity of degree $\leqq 2d^2$.*

Finally, the proof of our main Theorem 1 is exactly the same as that of [1] Theorem 6.

REFERENCES

[1] S. A. Amitsur, *Rings with involutions*, Israel J. Math. **6** (1968), 99–106.
[2] N. Jacobson, *Structure of rings*, Colloquia 37 (1956).

HEBREW UNIVERSITY OF JERUSALEM