CENTRALIZERS SATISFYING POLYNOMIAL[†] IDENTITIES

BY

SUSAN MONTGOMERY

ABSTRACT

The following results are proved: If R is a simple ring with unit, and for some $a \in R$ with a^n in the center of R, any n, such that the centralizer of a in R satisfies a polynomial identity of degree m, then R satisfies the standard identity of degree nm. When R is not simple, R will satisfy a power of the same standard identity, provided that a and n are invertible in R. These theorems are then applied to show that if G is a finite solvable group of automorphisms of a ring R, and the fixed points of G in R satisfy a polynomial identity, then R satisfies a polynomial identity, provided R has characteristic 0 or characteristic p where $p \nmid |G|$.

Introduction

The main result of this paper is that if R is a simple ring with unit, with an element $a \in R$ such that a^n is in the center of R and such that the centralizer of a satisfies a polynomial identity of degree m, then R satisfies the standard identity of degree nm. If R is a division ring, such a result is already known. For, it follows from the Double Centralizer theorem [6, p.165] that if the centralizer of an algebraic element is finite-dimensional over its center, then R must be algebraic over its center.

In the course of proving the main theorem, it is shown that if R is any ring with a^n in the center and $C_R(a)$ satisfying a polynomial identity, then R satisfies a polynomial identity provided a and n are invertible in R.

These theorems are analogous to a recent result of I. N. Herstein and L. Neumann. They have shown that if R has no nilpotent ideals, and R has an

[†] This research was supported in part by NSF Grant No. GP 29119X.

Received November 20, 1973

element a such that a^n is in the center of R and $C_R(a)$ is simple Artinian, then R itself must be simple Artinian [4].

As an application of the results on centralizers, we answer in the affirmative a special case of a question raised by J. E. Bjork: "If the fixed point set of a finite group G of automorphisms of R satisfies a polynomial identity, must R also satisfy a polynomial identity?" We show that this is indeed true when G is solvable and the order of G is relatively prime to the characteristic of R.

G. M. Bergman and I. M. Isaacs have given an example to show that Bjork's question is false in the case when R has characteristic $p \neq 0$ and G has no normal p-complement [3, p.83].

1. Centralizer of elements

In what follows, R will always be a ring. If $a \in R$, then $C_R(a) = \{x \in R \mid xa = ax\}$ will denote the *centralizer* of a in R. If n is any positive integer, R_n will denote the ring of all $n \times n$ matrices over R. When R has a center, it will be denoted by $Z(R)$, or simply by Z if no ambiguity can occur.

Since R will not necessarily be an algebra, to simplify the situation we will assume that all polynomial identities have integer coefficients. That is, a *polynomial identity* (PI) will be a non-zero element $p(x_1, \cdots x_m) \in \mathbb{Z}[x_1, \cdots, x_m]$, the polynomial ring over the integers $\mathbb{Z}$ in non-commuting indeterminates $\{x_i\}$, such that some monomial in $p(x)$ of maximal degree has coefficient $+1$. Thus R satisfies a PI if $p(r_1, \cdots, r_m) = 0$ for all choices of $r_1, \cdots, r_m \in R$. The *standard identity* of degree m will be denoted by $S_m[x]$; that is,

$$S_m[x] = S_m[x_1, \cdots, x_m] = \sum_{\sigma \in S_m} (-1)^{\operatorname{sgn} \sigma} x_{\sigma(1)} \cdots x_{\sigma(m)}.$$

The first lemma is a consequence of a very old theorem in linear algebra: the description of the centralizer of a matrix due to Frobenius. A clear, explicit computation of the matrices centralizing a given matrix appears in [10, pp. 102–104], and the lemma could be proved using this. Instead, however, we use the theory of modules over a principal ideal domain.

LEMMA 1. *Let F be a field and let $A \in F_n$. If $\delta_1 \mid \delta_2 \mid \cdots \mid \delta_t$ are the invariant factors of A, then $C_{F_n}(A)$ satisfies $S_{2t}[x]$ and no identity of lower degree.*

PROOF. The proof follows easily from [5, Th. 18, p. 109]; we give the details for completeness.

Let V be a vector space of dimension n over F, and make V into a module over the polynomial ring $F[\lambda]$ in the usual way via $p(\lambda)\cdot v = p(A)v$, for all $v \in V$ and $p(\lambda) \in F[\lambda]$. Since V is a finitely-generated module over the principal ideal domain $F[\lambda]$, $V = \{f_1\} \oplus \cdots \oplus \{f_t\}$, where the $\{f_i\}$ are cyclic submodules and δ_i generate the order ideal of f_i in $F[\lambda]$.

Now any element in $C_{F_n}(A)$, acting on V, is an $F[\lambda]$-module endomorphism of V. But any module endomorphism is determined by its action on the $\{f_i\}$, and thus an element in $C_{F_n}(A)$ determines a matrix in $F[\lambda]_t$. It follows that $C_{F_n}(A) \cong \mathcal{M}/\mathcal{N}$, where $\mathcal{M}$ is a subring of $F[\lambda]_t$. By a theorem of Amitsur and Levitzki [4, p. 228], $F[\lambda]_t$ (and so $C_{F_n}(A)$) satisfies the standard identity of degree $2t$.

To see that $C_{F_n}(A)$ cannot satisfy an identity of lower degree, one must examine more carefully the matrices in $\mathcal{M}$. If $\beta = (\beta_{ij}) \in \mathcal{M}$, where $\beta_{ij} \in F[\lambda]$, then β_{ij} is arbitrary if $i \geqq j$ (see [3], p. 110). Also, for $i \geqq j$, $\beta_{ij} \equiv \beta'_{ij} \bmod \mathcal{N}$ if $\beta_{ij} \equiv \beta'_{ij} \bmod \delta_j$. Thus, since each δ_j has degree at least one, distinct β_{ij}s of degree 0 will determine distinct cosets of $\mathcal{N}$ in $\mathcal{M}$.

The result of this is that $\mathcal{M}$ contains matrix units e_{ij} for $i \geqq j$ which determine distinct cosets of $\mathcal{N}$, and thus $\mathcal{M}/\mathcal{N}$ contains elements $\bar{e}_{ij}$, $i \geqq j$, which multiply like matrix units. But now, exactly as in [6, proof of Prop. 1, p. 226], $\mathcal{M}/\mathcal{N}$ can satisfy no PI of degree $< 2t$.

LEMMA 2. *Let R be a central simple algebra, with center Z, with $[R:Z] = r^2$. Assume that for some $a \in R$, a is algebraic of degree n over Z and that $C_R(a)$ satisfies a* PI *of degree m. Then $r \leqq nm/2$, and R satisfies the standard identity of degree nm.*

PROOF. Since $C_R(a)$ satisfies a PI of degree m, it satisfies a multilinear identity of degree $\leqq m$ [6, p. 225]. Thus we may assume that the identity satisfied by $C_R(a)$ is multilinear.

Now let F be the algebraic closure of Z. Since F is a splitting field for R, $R \otimes_Z F \approx F_r$, the $r \times r$ matrices over F. Identifying a with its image $a \otimes 1$ in $R \otimes F$, we have $C_{F_r}(a) \approx C_{R\otimes F}(a \otimes 1) = C_R(a) \otimes_Z F$. By [6, p. 225], $C_{F_r}(a)$ satisfies the same multilinear identity as $C_R(a)$. We can therefore assume that $R \approx F_r$.

Let $m(x)$ be the minimum polynomial for a. Since F is algebraically closed, we may write

$$m(x) = (x - \lambda_1)^{l_1}(x - \lambda_2)^{l_2} \cdots (x - \lambda_q)^{l_q},$$

where $\lambda_1, \cdots, \lambda_q$ are the distinct roots of $m(x)$ and $l_1 + l_2 + \cdots + l_q = n$.

Consider the Jordan form for a, and let k_i be the number of blocks appearing for λ_i, $i = 1, \cdots q$. Let $k = \max_i\{k_i\}$. Then k is precisely the number of invariant factors of a, and so by Lemma 1, the minimal identity satisfied by $C_R(a)$ has degree $2k$. Thus $2k \leqq m$.

Let $\chi_a(x)$ be the characteristic polynomial of a. Now for any i, the largest block appearing for λ_i in the Jordan form is an $l_i \times l_i$ matrix. Thus the multiplicity of λ_i in $\chi_a(x)$ is at most $k_i l_i$. Since r is the degree of $\chi_a(x)$, $r \leqq \Sigma_i k_i l_i \leqq k \ \Sigma_i l_i = kn \leqq mn/2$.

Now by the result of Amitsur and Levitzki mentioned before, R satisfies the standard identity of degree $2r$; since $2r \leqq nm$, R certainly also satisfies $S_{mn}[x]$.

Before proceeding, we recall that a left vector space V and a right vector space W over a division ring D are said to be *dual* if there exists a non-degenerate bilinear form $(\, , \,) : V \times W \to D$.

Using non-degeneracy, it is easy to show the following.

SUBLEMMA. *Let V and W be dual spaces with respect to $(\, , \,)$, and let V_0 be a k-dimensional subspace of V. Then there exists a k-dimensional subspace W_0 of W and dual bases $\{v_1, \cdots, v_k\}$ of V_0, $\{w_1, \cdots, w_k\}$ of W_0 such that*

(1) $(v_i, w_j) = \delta_{ij}$,

(2) $V = V_0 \oplus W_0^{\perp}$ and $W = W_0 \oplus V_0^{\perp}$, where $V_0^{\perp} = \{w \in W \mid (V_0, w) = 0\}$, the orthogonal complement of V_0 in W, and $W_0^{\perp}$ is the orthogonal complement of W_0 in V.

LEMMA 3. *Let R be a primitive ring with a minimal right ideal $V = eR$ such that the commuting ring $C \cong eRe$ of R on V is an algebraically closed field. Assume also that for some $a \in R$, acting as a linear transformation on V, a is algebraic over C of degree n and separable. If $C_R(a)$ satisfies a* PI *of degree m, then R satisfies $S_{nm}[x]$. In particular R is simple and finite-dimensional over its center.*

PROOF. By a theorem of Jacobson [6, p. 75], V and $W = Re$ are dual spaces, and R contains all finite-rank transformations on V which have adjoints re the form $(\, , \,)$.

We may denote by a_R the linear transformation induced on V by a, since the elements of R act by right multiplication. Since a_R is separable, we may write its minimum polynomial as $m(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$, where the $\alpha_i \in C$ are distinct. Thus we may decompose V as $V = V_1 \oplus \cdots \oplus V_n$, where V_i is the root space for α_i. Similarly a_L is a linear transformation on W, and so $W = W_1 \oplus \cdots \oplus W_n$. Using the non-degeneracy of the form and the fact that every element in the V_i and W_i is an eigenvector, one can check that

$$V_1^{\perp} = \sum_{i \neq 1} \oplus W_i \quad \text{and} \quad W_1^{\perp} = \sum_{i \neq 1} \oplus V_i.$$

If follows that $V = V_1 \oplus W_1^{\perp}$ and that $W = W_1 \oplus V_1^{\perp}$. Also, V_1 and W_1 are dual spaces since the form (,) restricted to $V_1 \times W_1$ is non-degenerate.

We will show that V is finite-dimensional. Assume not. Then some V_i is infinite-dimensional, so we may assume that V_1 is infinite-dimensional. Now the sublemma applies to V_1 and W_1 since V_1 and W_1 are dual spaces.

Let k be any positive integer and let V_0 be a k-dimensional subspace of V_1. Then we can find a dual space $W_0 \subseteq W_1$, with dual bases $\{v_i\}$ and $\{w_i\}$ by the sublemma. Also, $V_1 = V_0 \oplus W_0^{\perp}$ and $W_1 = W_0 \oplus W_0^{\perp}$.

Let (α_{ij}) be any $k \times k$ matrix in C_k. We define a linear transformation $T: V \to V$ by:

$$\begin{cases} v_i T = \sum_{j=1}^{k} \alpha_{ij} v_j, & i = 1, \cdots, k \\ v T = 0 \text{ for } v \in W_0^{\perp} \oplus V_2 \oplus \cdots \oplus V_n. \end{cases}$$

Clearly, T has finite rank. Also, T has an adjoint T^*: $W \to W$; namely, T^* is given by:

$$\begin{cases} T^* w_l = \sum_{m=1}^{k} w_m \alpha_{ml}, & l = 1, \cdots, k \\ T^* w = 0 \text{ for } w \in V_0^{\perp} \oplus W_2 \oplus \cdots \oplus W_n. \end{cases}$$

By Jacobson's theorem, $T \in R$.

Let R_1 be the set of all such Ts in R defined from matrices in C_k. Then $R_1 \cong C_k$. We claim that $R_1 \subseteq C_R(a)$. This is not difficult to check, using the definition of T and the fact that all of the spaces $V_0, W_0^{\perp}, V_2, \cdots, V_k$ are a-invariant.

But $C_R(a)$ satisfies a PI of degree m, and thus R_1 satisfies a PI of degree m. This can only happen if $k \leq m/2$, since the degree of the minimal identity satisfied by by C_k is $2k$ [6, p. 226]. This says that k is bounded, a contradiction. Thus V was finite-dimensional to start with. This implies that R is a simple ring, finite-dimensional over its center. By Lemma 2, R will satisfy the s tandard identity of degree mn.

We next consider the case of a prime ring. By a construction of Martindale, any prime ring R can be imbedded in a ring B with center C, a field, in such a way that RC is again a prime ring. C is called the *extended centroid* of R. If also R satisfies a generalized polynomial identity, then RC is a primitive ring with minimal one-sided ideals [7, Th. 3]. Thus if we can show that R satisfies a GPI under our hypotheses, we would be able to apply Lemma 3.

We need one more fact about extended centroids. If R and C are as above, let F be any field containing C. Then $RC \otimes_C F$ is again a prime ring whose extended centroid is just F. This follows from [8, Th. 2.2].

Recall that R satisfies a *generalized polynomial identity* (GPI) if there is a non-zero element $p(x_1, \cdots, x_m)$ in the free product $R *_C \langle X \rangle$, where X is a set of non-commuting indeterminates, such that $p(r_1, \cdots, r_m) = 0$ for all choices of $r_1, \cdots, r_m \in R$.

LEMMA 4. *Let R be a prime ring with center Z (possibly $Z = 0$) and assume that for some $a \in R$, we have $a^n \in Z$ and $C_R(a)$ satisfies a* PI. *Then R satisfies a* GPI *if any of the following conditions hold:*

(1) $a^n = 0$,

(2) *the characteristic of R is* 0 *or the characteristic of R is $p \neq 0$ and $p \nmid n$,*

(3) *the characteristic of R is $p \neq 0$, $n = p^t$, and Z is an algebraically closed field.*

PROOF. By linearizing if necessary, we may assume that the PI is multilinear and homogeneous. Thus we may write it as

$$g(x) = g(x_1, \cdots, x_m) = x_1 x_2 \cdots x_m + \sum_{\substack{\sigma \in S_m \\ \sigma \neq 1}} \alpha_\sigma x_{\sigma(1)} \cdots x_{\sigma(m)}, \text{ where } \alpha_\sigma \in \mathbb{Z}.$$

We also define, for any $r \in R$, the function

$$f_a(r) = ra^{n-1} + ara^{n-2} + \cdots + a^{n-1}r.$$

Note that $f_a(r) \in C_R(a)$, for any $r \in R$. If we let $y_1, \cdots, y_m$ be a new set of indeterminates, define $h(y) \in R * \langle Y \rangle$ by $h(y) = h(y_1, \cdots, y_m) = g(f_a(y_1), f_a(y_2), \cdots, f_a(y_m))$. R certainly satisfies $h(r_1, \cdots, r_m) = 0$, all $r_i \in R$; we will show that $h(y)$ is a non-trivial GPI in the three cases above.

Case 1. $a^n = 0$.

We may assume that $a^{n-1} \neq 0$, and thus $m(x) = x^n$ is the minimum polynomial for a. Now $f_a(r) \not\equiv 0$, for if $ra^{n-1} + \cdots + a^{n-1}r = 0$ for all $r \in R$, multiply on the left by a^{n-1}. Then $a^{n-1}Ra^{n-1} = 0$. Since R is prime, $a^{n-1} = 0$, a contradiction.

If we write $x_i = f_a(y_i)$, it will be enough to show that $x_1x_2 \cdots x_m \neq 0$ in $R*\langle Y\rangle$ in order to show $h(y) \neq 0$, since in each of the terms $x_{\sigma(1)} \cdots x_{\sigma(m)}$, $\sigma \neq 1$, the variables y_i occur in a different order. First consider $x_1x_2 = y_1a^{n-1}x_2 + ay_1a^{n-1}x_2 + \cdots + a^{n-1}y_1x_2$. Since $1, a, \cdots, a^{n-1}$ are linearly independent over C, $x_1x_2 \neq 0$ if $y_1a^{n-1}x_2 \neq 0$. But $y_1a^{n-1}x_2 = y_1a^{n-1}(y_2a^{n-1} + ay_2a^{n-2} + \cdots + a^{n-1}y_2) = y_1a^{n-1}y_2a^{n-1}$ since $a^n = 0$.

Similarly, $x_1x_2x_3$ will contain the term $y_1a^{n-1}y_2a^{n-1}y_3a^{n-1}$ and no other term will have an a^{n-1} after each y_i. Continuing in this way,

$$x_1x_2 \cdots x_m = y_1a^{n-1}y_2a^{n-1} \cdots y_ma^{n-1} + az, \text{ some } z.$$

Thus $x_1 \cdots x_m \neq 0$ in $R * \langle y\rangle$.

Case 2. As in Case 1, it will suffice to show that $x_1 \cdots x_m \neq 0$. Now $f_a(a) = na^n \neq 0$, since a is not nilpotent and R has characteristic 0 or $p \nmid n$. In fact, we have $[f_a(a)]^m = n^m a^{nm} \neq 0$. But this is simply the specialization of $x_1 \cdots x_m = f_a(y_1) \cdots f_a(y_m)$ in R when $y_1 = y_2 = \cdots = y_m = a$. Thus $x_1 \cdots x_m \neq 0$ in $R^* \langle y\rangle$.

Case 3. This case actually follows from Case 1. For, say $a^n = \alpha \in Z$. Since Z is algebraically closed, there exists $\beta \in Z$ such that $\alpha = \beta^n = \beta^{p^t}$. But then $(a - \beta)^{p^t} = a^{p^t} - \beta^{p^t} = a^n - \alpha = 0$; that is, $a - \beta$ is nilpotent. Since $C_R(a - \beta) = C_R(a)$, the result now follows from Case 1.

Before proving the first theorem, we need one more lemma. It is precisely [4, Lem. 3]. We state it here for convenience.

LEMMA 5. *Let R be a ring with $a^n \in Z$, some $a \in R$. Assume that a and n are invertible in R. Then if $\bar{R}$ is any homomorphic image of R, $C_{\bar{R}}(\bar{a}) = \overline{C_R(a)}$. That is, the centralizer of a is preserved in $\bar{R}$.*

THEOREM 1. *Let R be a semi-prime ring with a^n in the center of R, and such that a and n are invertible in R. Then if $C_R(a)$ is* PI *of degree m, R satisfies $S_{nm}[x]$, the standard identity of degree nm.*

PROOF. We first consider the case when R is prime. Let C be the extended centroid and RC the central closure of R.

We claim that $C_{RC}(a) = C_R(a) \cdot C$. For, define $\phi : RC \to RC$ by $\phi(x) = axa^{-1}$. Now $\phi^n = 1$, so for any $r \in R$, $r + \phi(r) + \phi^2(r) + \cdots + \phi^{n-1}(r) \in C_R(a)$. Choose $t \in C_{RC}(a)$, and write $t = \sum_{j=1}^{k} r_jc_j$. Since $\phi(t) = t$,

$$nt = \sum_{i=0}^{n-1} \phi^i(t) = \sum_{j=1}^{k} \left(\sum_{i=0}^{n-1} \phi^i(r_j)\right) c_j \in C_R(a) \cdot C.$$

Since n is invertible in R, $t \in C_R(a) \cdot C$. Thus $C_{RC}(a) = C_R(a) \cdot C$. Since we may assume that the PI satisfied by $C_R(a)$ is multilinear, $C_{RC}(a)$ satisfies the same identity as $C_R(a)$ (to see this, use the same proof as [6, Th. 1, p. 225]).

Let F be the algebraic closure of C, and consider $R' = RC \otimes_C F$. By the remark preceding Lemma 4, R' is a prime ring, with extended centroid F, and $R'F = R'$. Now $C_{R'}(a \otimes 1) = C_{RC}(a) \otimes F$, and so $C_{R'}(a \otimes 1)$ satisfies a PI of degree m. But $(a \otimes 1)^n = a^n \otimes 1$, and n is invertible in R'; thus by Lemma 4, part (2), R' satisfies a non-trivial GPI.

By Martindale's theorem, R' is primitive with a minimal right (left) ideal and the commuting ring is isomorphic to the extended centroid F, an algebraically closed field. Since $Z \subseteq C \subseteq F$, $a \otimes 1$ is separable over F (since $(a \otimes 1)^n \in F$ and n is invertible). By Lemma 3, R' is central simple and satisfies $S_{nm}[x]$. It follows that R also satisfies $S_{nm}[x]$.

We now let R be semi-prime. Let P be any prime ideal of R and let $\bar{R} = R/P$. $\bar{a}^{-n}$ is in the center of $\bar{R}$, $\bar{a}$ and $\bar{n}$ are invertible in $\bar{R}$, and by Lemma 5, $C_{\bar{R}}(\bar{a})$ satisfies a PI of degree m. Thus by the first part of the proof, $\bar{R}$ satisfies $S_{nm}[x]$. Since R is a subdirect product of its prime images, R must also satisfy $S_{nm}[x]$.

THEOREM 2. *Let R be any ring such that for some $a \in R$, $a^n \in Z$ with a and n invertible in R. Then if $C_R(a)$ is* PI *of degree m, R satisfies $(S_{nm}[x])^l$, for some positive integer l.*

PROOF. Let N be the lower nil radical of R. Then R/N is semi-prime, and inherits the hypotheses on a using Lemma 5. Thus by Theorem 1, R/N satisfies $S_{nm}[x]$. This means that for any choice of $x_1, \cdots, x_{nm} \in R$, $S_{nm}[x_1, \cdots, x_{nm}] \in N$. For convenience, let $d = nm$.

We complete the proof by following an argument of Amitsur [2, Th. 6]. Let $\bar{R}$ be the complete direct product of copies of R indexed by the d-tuples of elements of R. That is, $\bar{R} = \Pi_{\alpha \in I} R_\alpha$, where $R_\alpha = R$ and $I = \{(r_1, \cdots, r_d) \mid r_i \in R\}$. Choose $f_1, \cdots, f_d \in \bar{R}$ such that $f_i(\alpha) = r_i$, and let $f_a \in \bar{R}$ be given by $f_a(\alpha) = a$, for all α. Then f_a^n is in the center of $\bar{R}$, and $C_{\bar{R}}(f_a) = \Pi_{\alpha \in I} C_R(a)_\alpha$. Then $C_{\bar{R}}(f_a)$ satisfies the same PI as $C_R(a)$, so we may apply the above remark to f_a. Thus $S_d[f_1, \cdots, f_d] \in N(\bar{R})$. the lower nil radical of $\bar{R}$, and so for some positive integer l, $S_d[f_1, \cdots, f_d]^l = 0$. This implies that $(S_d[x])^l$ is an identity on R.

THEOREM 3. *Let R be a simple ring with unit such that for some element $a \in R$, $a^n \in Z$ and $C_R(a)$ is* PI *of degree m. Then R satisfies $S_{nm}[x]$, the standard identity of degree nm.*

PROOF. Since R is simple, the extended centroid C of R is just equal to Z, the center of R [8, p. 504]. But R is an algebra over its center, and thus $RC = R$. This means that if R satisfies a GPI, then R itself has a minimal one-sided ideal such that the commuting ring D is finite-dimensional over its center C (using Martindale's theorem [7]). Since R has a unit element, R would then be simple Artinian, and in fact central simple since $[D:C] < \infty$. Our theorem would then follow from Lemma 2. It will therefore suffice to show that R satisfies a GPI.

By Lemma 4, this will happen if a is nilpotent or if R has characteristic 0. We may therefore assume that the characteristic of R is $p \neq 0$ and that a is invertible. If $p \nmid n$, we would again be done, by Lemma 4. So, assume that $n = p^l m$, where $l > 0$ and $p \nmid m$. Let $b = a^m$ and let $R_1 = C_R(b)$. Then $a \in C_R(a) \subseteq R_1$ and $a^m = b$ is in the center of R_1. Also, a is invertible in R_1 since $Z \subseteq C_R(b)$. Finally, $C_{R_1}(a) = C_R(a)$, and so $C_{R_1}(a)$ satisfies a PI. We can now apply Theorem 2 to the ring R_1 to see that R_1 is PI. But now $b^{p^l} \in Z$ and $C_R(b)$ is PI. We may therefore assume that $n = p^l$.

Let F be the algebraic closure of Z, and let $R' = R \otimes_Z F$. Then R' is a simple ring with center F, and $(a \otimes 1)^{p^l} = a^{p^l} \otimes 1 \in Z \otimes F \approx F$. Also, $C_{R'}(a \otimes 1) = C_R(a) \otimes F$, and so $C_{R'}(a \otimes 1)$ satisfies a PI of degree m (we are assuming the PI to be multilinear). That is, we may assume that the center of R is an algebraically closed field. We are now done, for part (3) of Lemma 4 implies that R satisfies a non-trivial GPI.

A number of related questions remain open. For example, can the assumption of a unit element in Theorem 3 be dropped ? Also, could one assume only that a is algebraic over the center instead of a^n in the center?

II. Fixed-point sets of automorphisms

In this section, R will always denote an algebra over a field k. Let G be a group of automorphisms and anti-automorphisms of R as a k-algebra. Then $R^G = \{x \in R \mid x^\sigma = x, \text{ for all } \sigma \in G\}$ will denote the set of fixed points of G.

Note that if N is a normal subgroup of G, and $H = G/N$, then H is a group of automorphisms and anti-automorphisms of R^N and $R^G = (R^N)^H$. Thus when G is a finite solvable group, it will suffice to prove our results when G is cyclic. But when G is cyclic, say $G = \langle\sigma\rangle$, and σ happens to be an inner automorphism of R, say $\sigma(x) = a^{-1}x\,a$, all $x \in R$, for some $a \in R$, then $R^G = C_R(a)$. Thus the general method of proof here will be to reduce to the situation where σ is inner, so that the results of Section I may be applied.

We first prove a lemma which is an extension of both [9, Th. 2] and [4, Lem. 4].

LEMMA 6. *Let R be a semi-prime k-algebra, and σ an automorphism of R of period n. Assume either that k has characteristic 0 or that k has characteristic $p \neq 0$ and $p \nmid n$. Then $R^{\langle\sigma\rangle}$ is semi-prime.*

PROOF. We claim that without loss of generality, we may assume that k contains a primitive nth root of 1.

For, if not, let K be any finite normal extension of k, and consider $R_K = R \otimes_k K$. If $\alpha \in \mathscr{G}(K/k)$, the Galois group of K over k, α may be extended to R_K via $(r \otimes k)^\alpha = r \otimes k^\alpha$. It is not difficult to show that if I is any ideal of R_K invariant under every $\alpha \in \mathscr{G}$, then $I = J \otimes K$, where J is an ideal of R. It follows that R_K is semi-prime, for if not let N be a non-zero nilpotent ideal of R_K. Then $M = \sum_{\alpha \in \mathscr{G}} N^\alpha$ is a nilpotent ideal of R_K, invariant under $\mathscr{G}$, and so $M = L \otimes K$ by the above. But then L is a nilpotent ideal of R, a contradiction. Thus R_K is semi-prime.

Now σ can be extended to R_K via $(r \otimes k)^\sigma = r^\sigma \otimes k$, and $R_K^{\langle\sigma\rangle} = R^{\langle\sigma\rangle} \otimes_k K$. Thus if N were a nilpotent ideal of $R^{\langle\sigma\rangle}$, $N \otimes K$ would be a nilpotent ideal of $R_K^{\langle\sigma\rangle}$. Thus to prove the lemma, it will suffice to prove it for R_K, where K is any finite normal extension of k. Since k has characteristic 0 or p and $p \nmid n$, $k(\omega)$ is contained in a finite normal extension of k, where ω is a primitive nth root of 1. Thus we may assume $\omega \in k$.

Now the characteristic roots of σ are the n distinct nth roots of unity $1, \omega, \cdots, \omega^{n-1}$. Thus we may write

$$R = R_0 \oplus R_1 \oplus \cdots \oplus R_{n-1}$$

where $R_i = \{x \in R \mid x^\sigma = \omega^i x\}$, the root spaces for σ. Clearly $R_i R_j \subseteq R_{i+j}$, and $R_0 = R^{\langle\sigma\rangle}$.

Let U be an ideal of $R^{\langle\sigma\rangle}$ such that $U^2 = 0$. We claim that $(UR)^{n+1} = 0$ (and thus $U = 0$ by the semi-primeness of R). To show this, it will suffice to show that $UR_{i_1}UR_{i_2}U \cdots UR_{i_{n+1}} = 0$ for all choices of $i_1, \cdots, i_{n+1} \in \{0, 1, \cdots, n-1\}$. Now if $i_j = 0$ for any $j < n+1$, then $UR_{i_j}U \subseteq UR_0U \subseteq U^2 = 0$, and we are done. We may therefore assume that $i_1, i_2, \cdots, i_n \in \{1, 2, \cdots, n-1\}$. Consider the set

$A = \{i_1, i_1 + i_2, \cdots, i_1 + i_2 + \cdots + i_n\}$. Since A has n elements, either $i_1 + \cdots + i_l \equiv 0 \bmod n$ for some l, or for some $k < l$, $i_1 + \cdots + i_k \equiv i_1 + \cdots + i_l \bmod n$. But then $i_{k+1} + \cdots + i_l \equiv 0 \bmod n$; in either case, $i_j + \cdots + i_l \equiv 0 \bmod n$ for some $j < l$. Thus $R_{i_j} U R_{i_{j+1}} U \cdots U R_{i_l} \subseteq R_0$. Since $UR_0U \subseteq U^2 = 0$, $UR_{i_1}U \cdots UR_{i_{n+1}} = 0$ and we are done.

Note that the lemma is false when $p \mid n$. For, say that there exists $a \in R$, $a \notin k$, with $a^p = 1$. Then a determines an automorphism $\sigma : R \to R$ given by $\sigma(x) = a^{-1}xa$, $\sigma^p = 1$ and $R^{\langle\sigma\rangle} = C_R(a) = C_R(a - \omega)$, since we may assume that k contains a primitive nth root of 1, ω. But $(a - \omega)^p = a^p - \omega^p = 0$, and so $C_R(a - \omega)$ has a nilpotent ideal.

LEMMA 7. *Let R be any k-algebra satisfying $(S_{2m})^k$, and let R' be the algebra obtained from R by adjoining a unit element. Then R' also satisfies $(S_{2m})^k$.*

PROOF. We can describe R' as follows: R' is the set of all (r, k), where $r \in R$ and $k \in k$, with component-wise addition, and multiplication given by $(r_1, k_1) \cdot (r_2, k_2) = (r_1 r_2 + k_1 r_2 + k_2 r_1, k_1 k_2)$. Thus for purposes of computation, we may think of (r, k) as $r + k$.

$$\text{Let } p(x_1, \cdots, x_{2m}) = S_{2m}(x) = \sum_{\sigma \in \Sigma_{2m}} (-1)^{\operatorname{sgn}\sigma} x_{\sigma(1)} \cdots x_{\sigma(2m)}.$$

Choose $r_1 + k_1,\ r_2 + k_2, \cdots, r_{2m} + k_{2m} \in R'$. Then $p(r_1 + k_1, \cdots, r_{2m} + k_{2m}) = p(r_1, r_2 + k_2, \cdots, r_{2m} + k_{2m}) + p(k_1, r_2 + k_2, \cdots, r_{2m} + k_{2m})$. Since $p(x)$ has even degree and k_1 is in the center of R', $p(k_1, r_2 + k_2, \cdots, r_{2m} + k_{2m}) = 0$. Continuing in this way for each variable, we see that $p(r_1 + k_1, \cdots, r_{2m} + k_{2m}) = p(r_1, \cdots, r_{2m})$.

Before proceeding, we need the following fact, proved by Amitsur [1, p. 33]: Any k-algebra satisfying a PI satisfies some power of $S_{2m}(x)$, for some m. It is also true that if a semi-prime algebra satisfies a PI of degree n, then it satisfies some $S_{2m}(x)$, where $2m \leqq n$.

THEOREM 4. *Let R be a k-algebra and G a finite solvable group of k-automorphisms of R. Assume that either k has characteristic 0 or k has characteristic $p \neq 0$ and $p \nmid |G|$. Then if R^G satisfies a polynomial identity, so does R. In addition, if R is semi-prime and R^G satisfies a polynomial identity of degree m, then R satisfies the standard identity of degree $m|G|$.*

PROOF. As was observed at the beginning of this section, it will suffice to show the theorem when G is cyclic. Also, we may assume that R has a unit element. For, if R' is as described in Lemma 7, σ may be extended to R' by defining $(r,k)^\sigma = (r^\sigma, k)$. Then $(R')^{\langle\sigma\rangle} = (R^{\langle\sigma\rangle})'$, and so, since by Amitsur's theorem we may assume that $R^{\langle\sigma\rangle}$ satisfies $(S_{2m}(x))^k$, it follows from Lemma 7 that $(R')^{\langle\sigma\rangle}$ satisfies $(S_{2m}(x))^k$ also. Thus we may assume $1 \in R$.

Consider the ring of twisted Laurent polynomials $A = R[[x]]$. That is, $A = \{ \sum_{i=k}^{l} r_i x^i \mid r_i \in R,\ k < l \text{ integers}\}$. Define multiplication on A by $xr = r^\sigma x$, for $r \in R$. Then $C_A(x) = R^{\langle\sigma\rangle}[[x]]$. Thus if we assume that the PI satisfied by $R^{\langle\sigma\rangle}$ is multilinear, $C_A(x)$ will satisfy the same PI. Since $\sigma^n = 1$, x^n is in the center of A, and x is invertible in A. Thus by Theorem 2, A satisfies a PI, and so certainly R does also.

When R is semi-prime, so is $R^{\langle\sigma\rangle}$, by Lemma 6. Thus $R^{\langle\sigma\rangle}$ satisfies $S_{2l}(x)$, where $2l \leqq m$. When a unit element is adjoined to R, R' is also semi-prime and $(R')^{\langle\sigma\rangle}$ satisfies $S_{2l}(x)$, by Lemma 7. In addition A is semi-prime; this follows from the semi-primeness of R. As above, $C_A(x) = R^{\langle\sigma\rangle}[[x]]$. Thus by Theorem 3, A satisfies the standard identity of degree mn, where $n = |\langle\sigma\rangle|$.

We now consider the situation when G may contain anti-automorphisms. In this case, let H be the subgroup of G consisting of the automorphisms. Then $|G:H| = 2$. The following lemma is due to Sundstrom [9].

LEMMA 8. *R^H is a ring with involution * defined by $x^* = x^\sigma$ for any $\sigma \in G$, $\sigma \notin H$. R^G is the set of symmetric elements of R^H.*

Now, by using a result of Amitsur on rings with involution [2, Th. 6], we can prove our final result.

COROLLARY. *Let R be a k-algebra and G a finite solvable group of k-automorphisms and anti-automorphisms of R. Let H be the subgroup consisting of the automorphisms in G. Assume that either k has characteristic 0 or k has characteristic $p \neq 0$ and $p \nmid |H|$. Then if R^G satisfies a PI, so does R. In addition, if R is semi-prime, and R^G satisfies a PI of degree m, then R satisfies the standard identity of degree $m|G|$.*

PROOF. Amitsur's theorem states that if the symmetric elements in a ring with involution satisfy a PI, then the ring satisfies a PI. Thus, if R^G satisfies a PI, so does R^H, and we are done by applying Theorem 4 to R^H.

If R is semi-prime, then so is R^H by Lemma 6. For a semi-prime ring, Amitsur proved that if the symmetric elements satisfied an identity of degree m, then the ring satisfied $S_{2m}(x)$. Thus R^H satisfies $S_{2m}(x)$. But now by Theorem 4, R will satisfy the standard identity of degree $2m\,|H|$. Since $2\,|H| = |G|$, we are done.

If G is not solvable, Bjork's question remains open.

Acknowledgement

The author would like to thank the Hebrew University and the Weizmann Institute of Science for their hospitality while part of this work was being done.

References

1. S. A. Amitsur, *The identities of* PI-*rings*, Proc. Amer. Math. Soc. **4** (1953), 27–34.
2. S. A. Amitsur, *Rings with involution*, Israel J. Math. **6** (1968), 99–106.
3. G. M. Bergman and I. M. Isaacs, *Rings with fixed-point free group actions*, Proc. London Math. Soc. **27** (1973), 69–87.
4. I. N. Herstein and L. Neumann, *Centralizers in rings*, Annali di Matematica, to appear.
5. N. Jacobson, *Lectures in Abstract Algebra, Vol. II*, Van Nostrand, New York, 1953.
6. N. Jacobson, *Structure of Rings*, Amer. Math. Soc. Colloquium Publ. **37** (1964).
7. W. S. Martindale III, *Prime rings satisfying a generalized polynomial identity*, J. Algebra **12** (1969), 576–584.
8. W. S. Martindale III, *Prime rings with involution and generalized polynomial identities*, J. Algebra **22** (1972),
9. T. A. Sundstrom, *Groups of automorphisms of simple rings*, J. Algebra, to appear.
10. J. H. M. Wedderburn, *Lectures on Matrices*, Amer. Math. Soc. Colloquium Publ. **17** (1934).

Department of Mathematics
University of Southern California
Los Angeles, California, 90007 U. S. A.