Can. J. Math. Vol. **48** (3), 1996 pp. 596–606

RINGS WITH FINITE MAXIMAL INVARIANT SUBRINGS

CHARLES LANSKI

ABSTRACT. We prove that if φ is an (anti-) automorphism of a ring R with finite orbits on R, or integral over the integers, and if R contains a finite maximal φ-invariant subring, then R must be finite. Special cases are when φ has finite order or is an involution. Two corollaries are that R must be finite when R contains only finitely many φ-invariant subrings or has both ascending and descending chain conditions on φ-invariant subrings. These generalize results in the literature for the special case when $\varphi = \mathrm{id}_R$.

This paper is motivated by an interesting result of T. J. Laffey [8], obtained also by A. A. Klein [7], which proves that a ring with a finite maximal subring must be finite. Special cases of this result had been proven for commutative rings [2; Theorem 8, p. 542] and for rings satisfying a polynomial identity [3]. Also, Laffey's result implies related ones on finite subrings appearing in the literature ([5] and [13]). Our purpose here is to extend [8] to rings with a fixed (anti-) automorphism. The main theorem of the paper is that if φ is an (anti-) automorphism of a ring R having finite orbits on R, and if R contains a finite maximal φ-invariant subring, then R must be finite. We do not use [8], so Laffey's result is a consequence of ours, as is the case when φ is an involution. Results for invariant subrings corresponding to those in [5] and [13] are also consequences of our main theorem, so these papers are special cases of our result as well.

Throughout the paper R will be an associative ring, $Z(R) = Z$ is the center of R, $\mathrm{Aut}(R)$ is the group of automorphisms of R, and $\mathrm{Aut}^*(R)$ is the set of anti-automorphisms of R. Recall that $\varphi \in \mathrm{Aut}^*(R)$ means that $\varphi \in \mathrm{Aut}\big((R,+)\big)$ and that $\varphi(xy) = \varphi(y)\varphi(x)$ for all $x, y \in R$. Observe that $G = \mathrm{Aut}(R) \cup \mathrm{Aut}^*(R)$ is a group under composition and fix $\varphi \in G$. For any nonempty subset $B \subseteq R$, let $\langle B \rangle$ be the subring generated by B, and call B *φ-invariant* if $\varphi(B) = B$. Finally, S will henceforth denote a *finite* and *maximal φ-invariant subring* of R.

Our general approach, like that in [8] is to study the structure of S and R. We aim for a situation where $S = F$ or $S = M_n(F)$ for F a finite field, and try to find an element $x \in R - S$ with $\varphi(x) = x$ and with $x \in C_R(S)$, the *centralizer* of S. Then, when $\varphi \in \mathrm{Aut}(R)$, $R = S[x]$ has no invariant subring properly containing S, and it follows that x must be algebraic over F, so $S[x] = R$ is finite. In order to solve the problem we need to assume that every orbit of φ on R is finite, and until near the end of the paper, we will usually assume the special case that φ has finite order. As expected, our proofs are more involved than would be the case when $\varphi = \mathrm{id}_R$, the identity map on R. One result which

Received by the editors October 20, 1994.
AMS subject classification: Primary: 16P10; secondary: 16W20, 16P70.

is easy when $\varphi = \mathrm{id}_R$ is that R must have nonzero proper (invariant) subrings unless $\mathrm{card}(R) = p$, a prime, and either $R = \mathbf{F}_p$ a field, or $R^2 = 0$. This is a basic but important observation which is needed in considering rings with a finite maximal subring. Our first step is to see that the corresponding statement that R must contain nontrivial invariant subrings or be finite, is true for (anti-) automorphisms of finite order, but this is not so obvious. Our first theorem does this for a generalization of the finite order case. We use an argument which has probably appeared in the literature, but we are unaware of a reference. The computation in the middle of our proof can be essentially eliminated when φ has finite order by applying a well known and seminal result of G. Bergman and M. Isaacs [4, Proposition 2.4, p. 76] on fixed points of finite group actions. We note that our first theorem, and some of our later results are complicated a bit by the possibility that $\varphi \in \mathrm{Aut}^*(R)$, since when $B \subseteq R$ is φ-invariant we cannot assume that BR is also, which would be true if $\varphi \in \mathrm{Aut}(R)$. Also, our proof does not extend to the general case when φ has infinite order. Finally, we let $\mathbf{J}$ denote the ring of integers and $\mathbf{Q}$ the rational numbers. If one considers $\varphi \in G$ to be in $\mathrm{Hom}_{\mathbf{J}}(R, R)$, then it makes sense to consider polynomials in φ with coefficients in $\mathbf{J}$.

THEOREM 1. *Let $\varphi \in G$ be integral over $\mathbf{J}$. If R has no nonzero proper φ-invariant subring, then R is finite.*

PROOF. For any prime p, both pR and $\{r \in R \mid pr = 0\}$ are φ-invariant subrings of R, so either $pR = 0$ for some prime, or $pR = R$ has no p-torsion for any prime. Consequently, R is an algebra over F, for $F = \mathbf{F}_p$ the field of p elements, or $F = \mathbf{Q}$. Consider $\varphi \in \mathrm{Hom}_F(R, R)$ and let $X^m + a_{m-1}X^{m-1} + \cdots + a_1X + a_0 \in F[X]$ be the minimal polynomial for φ over F, where $a_0 \neq 0$, and if $F = \mathbf{Q}$ then $a_i = b_i/a$ for $b_i, a \in \mathbf{J}$ and set $b_0 = b$. Note that φ^{-1} is a polynomial in φ of degree $m - 1$, and if $F = \mathbf{Q}$ then $\varphi^{-1} = -\big((a/b)\varphi^{m-1} + (b_{m-1}/b)\varphi^{m-2} + \cdots + (b_1/b)\,\mathrm{id}_R\big)$. Thus if $F = \mathbf{Q}$ and $A = \mathbf{J}[1/ab] = \mathbf{J}_{(ab)}$, the localization at the powers of ab, then for all $j \in \mathbf{J}$ we have $\varphi^j \in A\varphi^{m-1} + \cdots + A\varphi + A\,\mathrm{id}_R$. We claim that R is finite or is not nilpotent. If R is nilpotent then $R^2 \neq R$, and since R^2 is φ-invariant, we must have $R^2 = 0$. But now, for any nonzero $x \in R$, if $B = \mathbf{F}_p$ or $B = \mathbf{J}_{(ab)}$ as appropriate, then $\langle Bx, B\varphi(x), \ldots, B\varphi^{m-1}(x)\rangle$ is φ-invariant, which means that $(R, +) = Bx + B\varphi(x) + \cdots + B\varphi^{m-1}(x)$. Clearly, R is finite when $B = \mathbf{F}_p$. If $B = \mathbf{J}_{(ab)}$, then R is a finitely generated torsion free module over the PID $B \neq QF(B) = \mathbf{Q}$, so as is well known and easy to see, R cannot be a $\mathbf{Q}$ algebra. Therefore, if R is nilpotent it must be finite, so we may assume that R is not nilpotent.

Observe that $\eta = \varphi^2 \in \mathrm{Aut}(R)$ and is still algebraic over F. If $R^\eta = \{r \in R \mid \eta(r) = r\}$ then R^η is a φ-invariant subring of R, so either $R^\eta = 0$ or $R^\eta = R$. Assuming that $R^\eta = 0$ we will show that R is nilpotent, a contradiction. We start by showing that we may extend F to an algebraic closure, and to this end consider $R_K = R \otimes_F K$ for K an algebraic closure of F. We may assume that $\eta \in \mathrm{Aut}(R_K)$ via $\eta(r \otimes k) = \eta(r) \otimes k$, and of course, η is algebraic over K. Since R embeds in R_K by $r \longrightarrow r \otimes 1$, and R is not nilpotent, neither is R_K. Finally, if $y = \sum r_i \otimes k_i \in (R_K)^\eta$ with $\{k_i\}$ independent over F, then $\sum r_i \otimes k_i = \eta(y) = \sum \eta(r_i) \otimes k_i$, so each $r_i \in R^\eta = 0$ forcing $y = 0$ and $(R_K)^\eta = 0$.

Therefore, since it suffices to show that R_K is nilpotent, there is no loss of generality in replacing R with R_K, so in assuming that R is an algebra over the algebraically closed field K, and that η is a K-algebra automorphism.

Now that K is algebraically closed, the minimal polynomial for η splits over K and R is the direct sum of its eigenspaces $R(\lambda_i) = \{r \in R \mid (\eta - \lambda_i)^t r = 0 \text{ for some } t \geq 1\}$, where $\lambda_1, \ldots, \lambda_s$ are all the distinct eigenvalues of η. Note that all $\lambda_i \neq 0$ since η is invertible. Since η satisfies a polynomial of degree m, for each $1 \leq j \leq s$, $(\eta - \lambda_j)^m R(\lambda_j) = 0$. Using the identity $(\eta - \lambda_i\lambda_j)(xy) = \lambda_i x\big((\eta - \lambda_j)y\big) + \big((\eta - \lambda_i)x\big)\lambda_j y + \big((\eta - \lambda_i)x\big)\big((\eta - \lambda_j)y\big)$ and induction, it follows that $(\eta - \lambda_i\lambda_j)^{2m}\big(R(\lambda_i)R(\lambda_j)\big) = 0$, forcing $R(\lambda_i)R(\lambda_j) \subseteq R(\lambda_i\lambda_j)$. If R is not nilpotent $R^{s+1} \neq 0$, so for some choice of $\mu_j \in \{\lambda_1, \ldots, \lambda_s\}$, $R(\mu_1)\cdots R(\mu_{s+1}) \neq 0$. Now since $\{\lambda_i\}$ has s elements and $\mu_1\mu_2\cdots\mu_k \in \{\lambda_i\}$ for all $1 \leq k \leq s+1$, we must have $\mu_1\cdots\mu_k = \mu_1\cdots\mu_{k+r}$ for some $k \geq 1$ and $r \geq 1$. Consequently $\mu_{k+1}\cdots\mu_{k+r} = 1 \in \{\lambda_i\}$, contracting $R^\eta = 0$. This shows that $R^\eta = 0$ forces R to be nilpotent, and so we may now assume that $R^\eta = R$.

From $R^\eta = R$ it follows that $\varphi^2 = \mathrm{id}_R$. Should $\varphi = \mathrm{id}_R$, then R is finite or contains nonzero proper (invariant) subrings, as we mentioned earlier. Therefore, we may assume that $\varphi \neq \mathrm{id}_R$. For any $x \in R$, $\langle x + \varphi(x)\rangle$ is φ-invariant, so if some $x + \varphi(x) \neq 0$ then $R = \langle x + \varphi(x)\rangle$ contradicting $\varphi \neq \mathrm{id}_R$. We are left with the assumption that $x + \varphi(x) = 0$ for all $x \in R$, so $\varphi(x) = -x$ and it follows that $x\varphi(x) = -x^2 = \varphi\big(x\varphi(x)\big)$. Now if some $x^2 \neq 0$, then $\langle x\varphi(x)\rangle = R$, and again $\varphi \neq \mathrm{id}_R$ is contradicted. Thus $x^2 = 0$ for all $x \in R$, and since $\varphi(x) = -x$, $\langle x\rangle$ is φ-invariant so $R = \langle x\rangle$, resulting in $R^2 = 0$. This contradiction forces us to conclude that R is finite and the proof of the theorem is complete.

The special case when φ has finite order and R has no φ-invariant subring is now done by Theorem 1, and it would be interesting to know if this result holds for any $\varphi \in G$. Our next result puts together two useful observations. The first is a consequence of Theorem 1, and the second is essentially [3; Lemma 2ii, p. 352]. Note that the proof is the same for either $\varphi \in \mathrm{Aut}(R)$ or $\varphi \in \mathrm{Aut}^*(R)$. Recall that S denotes a finite maximal φ- invariant subring of R.

LEMMA 1. *Let $\varphi \in G$ be integral over* $\mathbf{J}$. *Either R is finite or S contains no nonzero ideal of R and* $\mathrm{card}(S)R = 0$.

PROOF. Assume that R is infinite and note that $S \neq 0$ by Theorem 1. Should $I \subseteq S$ be a nonzero ideal of R, then the sum T of all such ideals of R is a finite φ-invariant ideal of R contained in S. It is immediate that φ induces an (anti-) automorphism η of R/T, integral over $\mathbf{J}$, and that S/T is a finite, maximal η-invariant subring of R/T. If $S = T$ then R/T is finite by Theorem 1, and if $S \neq T$ then $\mathrm{card}(S/T) < \mathrm{card}(S)$, so R/T is finite by induction on $\mathrm{card}(S)$. Since T is finite, R must be also, and this contradiction shows that S cannot contain a nonzero ideal of R. For the second statement, observe that $\{r \in R \mid \mathrm{card}(S)r = 0\}$ is a φ-invariant ideal of R containing S. We have just seen that S is not an ideal of R, so the maximality of S forces $\mathrm{card}(S)R = 0$.

It is now easy to show that we may assume that R has no nilpotent ideals. The end of the argument uses a computation which will arise again later. Until Theorem 7, we will assume the special case when φ has finite order.

LEMMA 2. *If $\varphi \in G$ has finite order m, then R is finite or semi-prime.*

PROOF. If I is a nonzero nilpotent ideal of R, then $T = I + \varphi(I) + \cdots + \varphi^{m-1}(I)$ is a φ-invariant nilpotent ideal of R, and $T+S$ is a φ-invariant subring of R containing S. We may assume that $T \not\subseteq S$ by Lemma 1, so $R = T+S$. Since T is nilpotent, there is a maximal integer $k \geq 1$ with $T^k \not\subseteq S$. Of course $N = T^k$ is φ-invariant, so $R = N + S$ and $N^2 \subseteq S$ by the choice of k. Choose $x \in N - S$ and note that $R = \langle S, x, \varphi(x), \ldots, \varphi^{m-1}(x)\rangle$, since this φ-invariant subring properly contains S. Now for any $i, j \geq 0$, $\varphi^i(x)\varphi^j(x) \in S$ and $\varphi^i(x)S\varphi^j(x) \subseteq S$, so we may conclude that $R = S+\sum_i\big(\mathbf{J}\varphi^i(x)+S\varphi^i(x)+\varphi^i(x)S+S\varphi^i(x)S\big)$, where $\mathbf{J}$ is the ring of integers. By Lemma 1 R is a torsion ring, so $\mathbf{J}\varphi^i(x)$ is finite forcing R to be finite and proving the lemma.

The next step in the argument is to show that S is semi-simple. Let $J(S)$ be the Jacobson radical of S; $J(S)$ is the unique maximal nilpotent ideal of S since S is finite. Observe that $\varphi(S) = S$ means that the restriction of φ to S is an (anti-) automorphism of S. In the next theorem, the initial computation is based on [2; p. 542].

THEOREM 2. *If $\varphi \in G$ has finite order m, then R is finite or S is semi-simple.*

PROOF. Assume that $J = J(S) \neq 0$ and consider the φ-invariant subring $JRJ + S$. Note that this is a subring because J is an ideal of S, and is φ-invariant because J is the unique maximal nilpotent ideal of S. If $JRJ \not\subseteq S$, then the maximality of S shows that $R = JRJ + S$, and it follows that $R = J(JRJ + S)J + S = J^2RJ^2 + S$. Continuing with this substitution for R yields $R = J^kRJ^k + S$ for any $k \geq 1$, and so $R = S$ is finite since J is nilpotent. Therefore we may assume that $JRJ \subseteq S$. For any integer $k \geq 1$, $(J^3R)^k = J^2\big((JRJ)J\big)^{k-1}JR \subseteq J^{k+2}R$, using that $JRJ \subseteq S$ and J is an ideal of S. The nilpotence of J forces J^3R to be nilpotent, and since we may assume that R is semi-prime by Lemma 2, $J^3 = 0$ results. It follows that $J^2R + RJ^2 + S$ is a φ-invariant subring, again using $JRJ \subseteq S$, so either $J^2R + RJ^2 \subseteq S$ or $R = J^2R + RJ^2 + S$. In the latter case we have $R = J^2(J^2R + RJ^2 + S) + (J^2R + RJ^2 + S)J^2 + S \subseteq S$, because $J^2RJ^2 \subseteq S$, so R is finite. Thus, we may take $J^2R + RJ^2 \subseteq S$.

If $J^2 \neq 0$, pick $x \in J^2$, define $D_x(r) = xr - rx$, and use $J^2R + RJ^2 \subseteq S$ to see that $D_x: R \longrightarrow S$ and is an additive map with a finite image. Hence $\operatorname{Ker} D_x = C_R(x)$, the centralizer of x in R, has finite index in $(R, +)$. Set $K = \cap\{C_R(x) \mid x \in J^2\}$ and observe that K is a subring of R of finite index in $(R, +)$, so K is infinite if R is. Furthermore, it is clear that $K = C_R(J^2)$, so K is φ-invariant, since $\varphi([a, b]) = \varphi(ab - ba) = \pm[\varphi(a), \varphi(b)]$. Consequently, if R is infinite, $K \not\subseteq S$, and so, $R = \langle K, S\rangle$. Consider $r = k_1s_1 \cdots k_ns_n$ for $k_i \in K$ and $s_i \in S$, let $y \in J^2$, and note that $yr = yk_1s_1 \cdots k_ns_n = k_1(ys_1)k_2 \cdots k_ns_n = k_1k_2(ys_1s_2)k_3 \cdots s_n = k_1 \cdots k_n(ys_1s_2 \cdots s_n) = (ys_1 \cdots s_n)k_1 \cdots k_n$. It follows from similar computations with the other possible forms for $r \in R$ that $J^2R \subseteq J^2 + J^2K$, so $(J^2R)^t \subseteq J^{2t} + J^{2t}K$, and the nilpotence of J forces J^2R to be nilpotent. As above, by Lemma 2, we may assume that $J^2 = 0$.

The argument above, that $J^3 = 0$ implies $J^2R + RJ^2 \subseteq S$, now shows that $J^2 = 0$ leads to R finite or $JR + RJ \subseteq S$ by considering the φ-invariant subring $JR + RJ + S$. Using the argument of the last paragraph, with J replacing J^2 and now considering D_x and $C_R(x)$ for $x \in J$, shows that either R is finite or $J = 0$, completing the proof of the theorem.

In view of Theorem 2, if R is infinite we may assume that S is the direct sum of finite simple rings by Wedderburn's Theorems, with each simple component either a finite field F, or $M_n(F)$. We will show that S is in fact a simple ring, and to do so we need to consider idempotents $e^2 = e \in S$. Recall that for any $e^2 = e \in R$, one has the Pierce decomposition of $(R, +)$ into a direct sum of subgroups, $(R, +) = eRe \oplus eR(1-e) \oplus (1-e)Re \oplus (1-e)R(1-e)$, where $R(1-e) = \{r - re \mid r \in R\}$, $(1-e)R = \{r - er \mid r \in R\}$, and $(1-e)R(1-e) = \{r - er - re + ere \mid r \in R\}$. It is immediate that $Re(1-e)R = R(1-e)eR = 0$. Finally, for any $x \in R$ one has the corresponding representation $x = exe + ex(1-e) + (1-e)xe + (1-e)x(1-e)$.

THEOREM 3. *Let $\varphi \in G$ have finite order m. If $e^2 = e = \varphi(e) \in Z(S)$, then either $e \in Z(R)$ or R is finite.*

PROOF. Assume that R is infinite. Using $\varphi(e) = e \in Z(S)$, it is clear that $eR(1-e)Re + S$ is a φ-invariant subring of R, so the maximality of S shows that either $eR(1-e)Re \subseteq S$ or else $R = eR(1-e)Re + S$. If the second possibility holds, $R = eR(1-e)Re + eS + (1-e)S$, so $eR(1-e) = 0$ and $R = S$ is finite, a contradiction. Thus we may assume that $eR(1-e)Re \subseteq S$. Should both $eR(1-e), (1-e)Re \subseteq S$, then $R = eRe + eR(1-e) + (1-e)Re + (1-e)R(1-e) = eRe + (1-e)R(1-e) + S$, and it follows easily that $e \in Z(R)$. We may proceed with the assumption that $eR(1-e) \not\subseteq S$, the case that $(1-e)Re \not\subseteq S$ being similar.

Choose $x \in eR(1-e) - S$ and observe that $R = B = \langle S, x, \varphi(x), \ldots, \varphi^{m-1}(x)\rangle$ since B is a φ-invariant subring of R which properly contains S. We argue that R is finite much as we did in Lemma 2. If $x = er(1-e)$, then $\varphi(x) = e\varphi(r)(1-e)$ if $\varphi \in \mathrm{Aut}(R)$ and $\varphi(x) = (1-e)\varphi(r)e$ if $\varphi \in \mathrm{Aut}^*(R)$. In the first case, since $e \in Z(S)$, $\varphi^i(x)\varphi^j(x) = \varphi^i(x)S\varphi^j(x) = 0$, and in the second case $\varphi^{2i}(x) \in eR(1-e)$ and $\varphi^{2j+1}(x) \in (1-e)Re$. From $eR(1-e)Re \subseteq S$, it now follows that any product of three elements from $\{\varphi^i(x)\}$ and elements of S is equal to a product involving only one $\varphi^i(x)$ and S. For example, $\varphi^{2i+1}(x)s\varphi^{2j}(x)t\varphi^k(x) \in \varphi^{2i+1}(x)S$ since $\varphi^{2j}(x)t\varphi^k(x) = 0$ if k is even, and is in $eR(1-e)Re \subseteq S$ if k is odd. Consequently, for $\mathbf{J}$ the rings of integers, $R = S + \sum_{i,j=0}^{m-1}\big((S+\mathbf{J})\varphi^i(x)(S+\mathbf{J}) + (S+\mathbf{J})\varphi^i(x)(S+\mathbf{J})\varphi^j(x)(S+\mathbf{J})\big)$. But by Lemma 1 we may assume that every element of R is a torsion element, so R is finite. With this contradiction, the proof of the theorem is complete.

COROLLARY. *If $\varphi \in G$ has finite order, then either R is finite or $1_S \in S$ and $1_S = 1_R$.*

PROOF. By Theorem 2 we may assume that S is semi-simple, so S has an identity element 1_S. Certainly $1_S^2 = 1_S = \varphi(1_S)$, so $1_S \in Z(R)$ by Theorem 3, unless R is finite. Now 1_SR is an ideal of R, is φ-invariant, and $1_SR \supseteq 1_SS = S$. Using Lemma 1 we may assume that $1_SR \neq S$, so $1_SR = R = R1_S$. A straightforward computation shows that $1_S = 1_R$.

Our next theorem is a key result which restricts further the structure of S.

THEOREM 4. *If $\varphi \in G$ has finite order m, then either R is finite or S is a simple ring.*

PROOF. Assume that R is infinite, so S is semi-simple by Theorem 2, and $S = S_1 \oplus \cdots \oplus S_k$, the direct sum of its simple components, which are the minimal ideals in S. Clearly, $\varphi^i(S_1)$ is a minimal ideal of S, so $\varphi^i(S_1) = S_j$ for some j. It is straightforward and easy to show that $\{S_1, \varphi(S_1), \ldots, \varphi^{m-1}(S_1)\} = \{S_1, \varphi(S_1), \ldots, \varphi^{t-1}(S_1)\}$ has t distinct elements where $t \geq 1$ is minimal with $\varphi^t(S_1) = S_1$. By re-ordering $\{S_j\}$ we may assume that $S_i = \varphi^{i-1}(S_1)$ if $1 \leq i \leq t$. If $e_i = \varphi^{i-1}(e_1)$ for $1 \leq i \leq t$ is the identity element of S_i, then $e = e_1 + \cdots + e_t$ is the identity of $S_1 + \cdots + S_t = eS$, and $e^2 = e = \varphi(e) \in Z(S)$. By Theorem 3, $e \in Z(R)$, so eR and $(1-e)R$ are φ-invariant ideals and $R = eR + (1-e)R$ is their direct sum. Should $eR = eS \subseteq S$, then S contains a nonzero ideal of R in contradiction to Lemma 1, so $eS \neq eR$. Hence $R \neq eS + (1-e)R = B$, a φ-invariant subring of R with $B \supseteq eS + (1-e)S = S$. The maximality of S forces $(1-e)R \subseteq S$, so again S would contain an ideal of R unless $(1-e)R = 0$. Therefore we may conclude that $e = 1_R = 1_S$. Since any ideal of S is a direct sum of a subcollection of $\{S_i\}$ and $S_i = \varphi^{i-1}(S_1)$, S has no nonzero proper φ-invariant ideal.

We have $1_R = 1_S = e_1 + \cdots + e_t$ is a sum of orthogonal idempotents, so $S = \oplus e_i S \subseteq \oplus e_i R e_i$. Clearly, $\oplus e_i R e_i$ is a φ-invariant subring of R containing S, so either $\oplus e_i R e_i = R$ or $\oplus e_i R e_i = S$. In the latter case, because R is infinite and $R = \sum_{i,j} e_i R e_j$, some $e_i R e_j \neq 0$ with $i \neq j$. Choose $x \in e_i R e_j$, observe that $x \notin S$ and that $B = \langle S, x, \varphi(x), \cdots, \varphi^{m-1}(x)\rangle$ is a φ-invariant subring properly containing S, so $B = R$. Now $\varphi^u(x) S \varphi^v(x) = 0$ unless $\varphi^u(x) \in e_d R e_q$ and $\varphi^v(x) \in e_q R e_w$. Since $\{e_i\}$ has only t distinct subscripts, any word $y_1 s_1 \cdots y_{t-1} s_{t-1} y_t$ with $s_j \in S$ and $y_j \in \{x, \varphi(x), \cdots, \varphi^{m-1}(x)\}$ must be zero or have a subword $y_c s_c \cdots y_{c+r} \in e_u R e_u \subseteq S$. It follows that $R = B = S + \sum\{S y_1 S y_2 \cdots S y_i S \mid 1 \leq i \leq t-1 \text{ and all } y_j \in \{x, \varphi(x), \ldots, \varphi^{m-1}(x)\}\}$ is finite. Therefore, we must have $R = \oplus e_i R e_i$ and $e_i \in Z(R)$ follows easily, so $e_i R e_i = e_i R$.

Recall that t is minimal with $\varphi^t(e_1 R) = e_1 R$. By restriction, φ^t induces an (anti-) automorphism of finite order on $e_1 R$. If A_1 is a φ^t-invariant subring of $e_1 R$ containing $e_1 S = S_1$, then $A = \sum_{j=0}^{t-1} \varphi^j(A_1)$ is a φ-invariant subring of R containing S. Consequently, if A_1 contains S_1 properly, then $A = R$, so $A_1 = e_1 R$ and S_1 is a finite maximal φ^t-invariant subring of $e_1 R$. But when $t > 1$, card$(S_1) <$ card(S) and by induction on card(S), $e_1 R$ is finite forcing $R = \sum \varphi^i(e_1 R)$ to be finite. This proves that $t = 1$, so $S = S_1$ is a simple ring.

Our next goal is to show that $Z(S) = Z(R)$. We need two lemmas to do this, the first of which is one of the inclusions and the other gives additional structural information on R.

LEMMA 3. *If $\varphi \in G$ has finite order m, then either R is finite or $Z(R) \subseteq Z(S)$.*

PROOF. From Theorem 4 we may assume that $S = M_n(F)$ for F a finite field and $n \geq 1$. Suppose that there is $z \in Z(R) - Z(S)$, in which case $B = \langle S, z, \varphi(z), \ldots, \varphi^{m-1}(z)\rangle$ is a φ-invariant subring of R properly containing S. Since S is maximal and $z \in Z(R) =$

$\varphi\big(Z(R)\big)$ we may write $R = \langle S, z, \varphi(z), \ldots, \varphi^{m-1}(z)\rangle = S[z, \varphi(z), \ldots, \varphi^{m-1}(z)]$. Let $q(X) = \prod_{j=0}^{m-1}\big(X - \varphi^j(z)\big) \in Z(R)[X]$, and note that the coefficients of $q(X)$ are symmetric functions in $\{z, \varphi(z), \ldots, \varphi^{m-1}(z)\}$, so each is fixed by φ. If any of these coefficients, say y, is not in S, then $R = \langle S, y\rangle = S[y]$, by the maximality of S. Set $A = S[y^2]$, a φ-invariant subring of R containing S, so $A = S$ or $A = R$. Should $A = S$ then $y^2 \in S$, so $R = S[y] = S + Sy$ is finite. If $A = R$, then $y \in S[y^2]$, so $y = \sum s_i y^{2i}$ with $s_i \in S = M_n(F)$. Now $R = S[y] = M_n(F)[y] = M_n(F[y])$, so if $\{e_{ij}\}$ are the usual matrix units we may regard $y = \sum e_{ii}y$ as a diagonal matrix. Therefore, using the diagonal entries of the equation $y = \sum s_i y^{2i}$ shows that each $e_{ii}y$, so y, is algebraic over F. Hence $F[y]$ is finite and it follows that $R = M_n(F[y])$ is finite. Consequently, we may assume that all the coefficients of $q(X)$ are in S. But this implies that each $\varphi^i(z)$ is integral over S, so $R = S[z, \varphi(z), \ldots, \varphi^{m-1}(z)]$ is a finitely generated S module, so is finite, proving the lemma.

LEMMA 4. *Let $\varphi \in G$ have finite order m. Then R is finite or every proper ideal I of R satisfies $I \cap S = 0$ and either:*

i) R is a simple ring with 1;

ii) R is a sum of proper ideals; or

iii) R contains a proper φ-invariant ideal I, $R = I + S$, and I properly contains a prime ideal P of R.

PROOF. By Theorem 4 we may assume that S is a simple ring, by the Corollary to Theorem 3 that $1_S = 1_R = 1$, by Lemma 1 that S contains no ideal of R, and by Lemma 2 that R is semi-prime. If $I \neq 0$ is any ideal of R, then $I \cap S$ is an ideal of S so $I \cap S = 0$ or $S \subseteq I$. In the latter case $1 \in S \subseteq I$ so $I = R$, and indeed $I \cap S = 0$ for any proper ideal I of R. Assume next that R is not a simple ring and has no proper φ-invariant ideal. Then since $1 \in R$, there is a proper maximal ideal I of R and $I \not\supset \varphi(I)$. But now $R = I + \varphi(I)$, so R is a sum of these proper ideals.

Finally assume that R is not simple and is not the sum of proper ideals. If I is the sum of all the proper ideals of R, then I is a proper φ-invariant ideal of R and $R = I + S$ by the maximality of S. Since R is a semi-prime ring, the intersection of all its prime ideals is zero, so there is a prime ideal P of R with $I \not\subseteq P$. By definition of I, P is properly contained in I.

We come now to our next to last preliminary result which is essential in proving our main theorem.

THEOREM 5. *If $\varphi \in G$ has finite order m, then either R is finite or $Z(S) = Z(R)$.*

PROOF. We may assume that $S = M_n(F)$ for F a finite field of p^a elements and $n \geq 1$ by Theorem 4, that $1 = 1_R = 1_S$ by the Corollary of Theorem 3, and that $Z(R)$ is a subfield of $Z(S) = F$ by Lemma 3. Suppose that there is $z \in F - Z(R)$ and let $z^k = 1$ for k the order of $z \in F - (0)$, so of course $k \mid p^a - 1$. Consider the expression $g(X) = z^{k-1}X + z^{k-2}Xz + \cdots + Xz^{k-1} \in F *_{Z(R)} Z(R)[X]$, the free product over $Z(R)$. It is straightforward to verify that for any $r \in R$, $g(r)z = zg(r)$; that is, $g(R) \subseteq C(z)$, the centralizer of z in R. If some $y = g(r) \notin S$, then the maximality of S implies that $R = \langle S, y, \varphi(y), \ldots, \varphi^{m-1}(y)\rangle$. Since $F = Z(S)$ and $\varphi(S) = S$, it follows that φ restricts to an automorphism of the finite field F over its prime field, so by elementary Galois theory $\varphi(z) = z^v$ for $v = p^b$ with $b \geq 0$. Now the order of $z \in F - (0)$ is $k \mid p^a - 1$, so k is relatively prime to p and the cyclic subgroups (z), $\big(\varphi(z)\big), \ldots, \big(\varphi^{m-1}(z)\big)$ in $F - (0)$ are all equal. Consequently, $C(z) = C\big(\varphi(z)\big) = \cdots = C\big(\varphi^{m-1}(z)\big)$ and $\varphi^i(y) \in C\big(\varphi^i(z)\big) = C(z)$. Since $z \in Z(S)$, $S \subseteq C(z)$, so $R = \langle S, y, \varphi(y), \ldots, \varphi^{m-1}(y)\rangle \subseteq C(z)$, which forces the contradiction $z \in Z(R)$. Therefore, we may assume that $g(R) \subseteq S$.

If I is any proper ideal of R, then $g(I) \subseteq I \cap S = 0$ by Lemma 4. Since $g(X)\colon R \longrightarrow S$ is additive, $g(R) = 0$ if R is the sum of proper ideals. But $g(z) = k \neq 0$ since $p \not| \; k$, so by Lemma 4 again, either R is a simple ring or for some proper ideal I, $R = I + S$ and I properly contains a prime ideal P of R. In the latter case, note that $(F + P)/P \cong F$, and up to isomorphism $Z(R)$ is in $Z(R/P)$, so we may now consider $g(X) \in (R/P) *_{Z(R/P)} Z(R/P)[X]$. Certainly, $g(I/P) = 0$ in R/P, and since I/P is a nonzero ideal in the prime ring R/P we may conclude that $g(R/P) = 0$ [9; Lemma 1, p. 766]. Once again $g(z+P) \neq 0$ shows that this situation cannot occur, so we may assume that R is a simple ring with 1.

Recall that $Z(R) \subseteq Z(S) = F$ is a finite field and set $\dim_{Z(R)} S = q$. It is well known that S satisfies the standard polynomial identity $S_{q+1}[x_1, \ldots, x_{q+1}] = \sum(-1)^\sigma x_{\sigma(1)} \cdots x_{\sigma(q+1)}$ over all permutations σ of $\{1, 2, \ldots, q+1\}$ [6; Lemma 6.2.2, p. 154]. Setting $h(x_1, \ldots, x_{q+1}) = S_{q+1}[g(x_1), \ldots, g(x_{q+1})] \in R *_{Z(R)} Z(R)\{x_1, \ldots, x_{q+1}\}$, where $Z(R)\{x_1, \ldots, x_{q+1}\}$ is the free algebra over $Z(R)$, we have that $h(x_1, \ldots, x_{q+1})$ is a generalized polynomial identity for R. Should $h \equiv 0$, then the sum of all its monomials with the variables appearing in the same order must be zero as well. In particular, $g(x_1) \cdots g(x_{q+1}) \equiv 0$, using the substitution of all $x_i = z$ gives the contradiction $0 = g(z)^{q+1} = k^{q+1} \neq 0$ since $\operatorname{char}(R) \not| \; k$. Hence $h(x_1, \ldots, x_{q+1})$ is a nontrivial generalized polynomial identity for R. By Martindale's Theorem [11; Theorem 3, p. 579], since $1 \in R$ and R is simple, one must have $R = \operatorname{soc}(R) \cong M_t(D)$ for D a division ring finite dimensional over $Z(R)$. It follows that R is finite, proving that $Z(S) = Z(R)$, when R is infinite.

In the proof of our main theorem we will be able to assume that $S = M_n(F)$ and will want to choose an element which centralizes S and is fixed by φ. This is possible since φ has infinitely many fixed points, which we prove next. Note that φ having infinitely many fixed points does not by itself contradict S finite. After all, S finite does not preclude the existence of some infinite φ-invariant subring not containing S.

THEOREM 6. *Let A be a semi-prime ring, $pA = 0$ for p a prime, $\eta \in \operatorname{Aut}(A) \cup \operatorname{Aut}^*(A)$ of finite order, $A^\eta = \{x \in A \mid \eta(x) = x\}$, and $A^{-\eta} = \{X \in A \mid \eta(x) = -x\}$. If A is infinite, then either A^η or $A^{-\eta}$ is infinite.*

PROOF. Assume first that $\eta \in \operatorname{Aut}(A)$ and write the order of η as $o(\eta) = p^a t$ with $p \not| \; t$. If σ is the p^a-th power of η, then $o(\sigma) = t$ and $p \not| \; t$, so $A^\sigma = \{x \in A \mid \sigma(x) = x\}$ is a semi-prime ring [12; Corollary 1.5, p. 9] and is infinite when A is [10; Theorem 3, p. 364].

Now η induces an automorphism of A^σ, so to prove the theorem when $\eta \in \mathrm{Aut}(A)$, it is enough to assume that $o(\eta) = p^a > 1$. Consider A to be a vector space over the field F of p elements and $\eta \in \mathrm{Hom}_F(A, A)$. Note that $A^\eta = \mathrm{Ker}(\eta - \mathrm{id}_A)$, so it suffices to let $T = \eta - \mathrm{id}_A$ and to show that $\mathrm{Ker}\, T$ is infinite. Since $o(\eta) = p^a$ and $\mathrm{char}\, F = p$, the minimal polynomial of T is X^c. Using the cyclic decomposition, any finite dimensional T-invariant subspace V of A is the direct sum of a finite number of T-cyclic subspaces, say n, each of dimension at most c. Clearly, T acting on any T-invariant subspace has a nonzero kernel, so $\mathrm{card}\big(\mathrm{Ker}(T|_V)\big) \geq p^n$. It follows that if $\mathrm{card}(\mathrm{Ker}\, T) = q$ is finite, then any finite dimensional T-invariant subspace M of A satisfies $\dim M \leq qc$. But if V is any finite dimensional T-invariant subspace, say $V = \mathrm{Ker}\, T$, then T induces a nilpotent transformation Y on A / V, so has a nonzero kernel when A is infinite. If $x + V \in \mathrm{Ker}\, Y - (0)$, then $Fx + V$ is a T-invariant subspace properly containing V. Thus there exist T-invariant subspaces of arbitrarily large dimension when A is infinite, so $\mathrm{Ker}\, T$ must be infinite and A^η is infinite also.

When $\eta \in \mathrm{Aut}^*(A)$, then $\eta^2 \in \mathrm{Aut}(A)$, so by the case above its fixed point ring B is infinite when A is. Clearly B is η-invariant, $B^\eta = \{b \in B \mid \eta(b) = b\} \subseteq A^\eta$, and $B^{-\eta} \subseteq A^{-\eta}$, so it suffices to replace A with B and assume that $\eta^2 = \mathrm{id}_A$. Thus we may assume that η is an involution, but cannot assume now that A is semi-prime. If $p > 2$, then A is the direct sum of the characteristic subspaces A^η and $A^{-\eta}$, so one of these is infinite when A is infinite. Finally, if $p = 2$ then A infinite forces A^η to be infinite [10; Lemma 5, p. 371]. To see this suppose that A^η is finite and let $A = A^\eta \oplus M$ for M an infinite subspace of A. If Y is any basis of M and $y \in Y$, then $y + \eta(y) \in A^\eta$ so the finiteness of A^η shows that $y + \eta(y) = x + \eta(x)$ for $x, y \in Y$ and $x \neq y$. Hence $x + y = \eta(x + y) \in M \cap A^\eta = 0$ gives a contradiction. Therefore A^η must be infinite, proving the theorem.

THEOREM 7. *If $\varphi \in \mathrm{Aut}(R) \cup \mathrm{Aut}^*(R)$ has finite order, and if S is a finite maximal φ-invariant subring of R, then R is finite.*

PROOF. From Theorem 4 we may assume that S is a simple ring, and from Theorem 5 that $Z(R) = Z(S)$. First assume that $S = Z(S) = F$, a finite field, so applying Theorem 6 yields an element $x \in R - S$ so that $\varphi(x) = \pm x$, unless R is finite. Clearly, the maximality of $S = F$ shows that $R = \langle S, x\rangle = F[x]$. But $F[x^2]$ contains F and is φ-invariant, so $F[x^2] = F = S$ or $F[x^2] = R = F[x]$. Therefore, x is algebraic over F, so $R = F[x]$ is finite. Next assume that $S = M_n(F)$ with $n > 1$ and $F = Z(S) = Z(R)$. Using a theorem of Wedderburn [1; Theorem 17, p. 19] shows that $R = SA$, where $A = C_R(S)$, the centralizer of S in R. Briefly, if $\{e_{ij}\}$ are the usual matrix units in S, then for $r \in R$ set $r_{ij} = \sum_k e_{ki} r e_{jk}$, and note that all $r_{ij} \in A$ and $r = \sum e_{ij} r_{ij}$. Consequently, since we can take R to be semi-prime by Lemma 2, we may assume that A is also semi-prime because for any ideal B of A, SB is an ideal of R. Observe that $SB \neq 0$ if $B \neq 0$ since $1 \in S$ by the Corollary of Theorem 3. Finally, since S is φ-invariant and $A = C_R(S)$, A is also φ-invariant. Now unless R is finite, A is infinite and Theorem 6 shows that there is $x \in A - S$ with $\varphi(x) = \pm x$. As above $R = \langle S, x\rangle = S[x] = M_n(F)[x] = M_n(F[x])$, and $S[x^2] = M_n(F[x^2])$ is a φ-invariant subring of R containing S. Therefore, $x^2 \in S \cap F$, so

x is algebraic over F, or $M_n(F[x^2]) = R = M_n(F[x])$, and as in the proof of Lemma 3, x is algebraic over F. In either case $R = M_n(F[x])$ is finite.

We immediately extend Theorem 7 to $\varphi \in G$ which is *locally finite*, that is, for all $x \in R$, and some $i = i(x) \geq 1$, $\varphi^i(x) = x$, or which is integral over $\mathbf{J}$.

THEOREM 8. *Let $\varphi \in \mathrm{Aut}(R) \cup \mathrm{Aut}^*(R)$ and S a finite maximal φ-invariant subring of R. If either φ is locally finite or integral over $\mathbf{J}$, then R is finite.*

PROOF. Assume first that φ is locally finite and for $i \geq 1$ set $R(i) = \{x \in R \mid \varphi^i(x) = x\}$. Clearly, each $R(i)$ is a φ-invariant subring and $R = \cup R(i)$ by the local finiteness of φ. Also, $\langle R(i), R(j)\rangle \subseteq R(ij)$, so $S \subseteq R(n)$ for some n because S is finite. Thus $R = R(n)$ and φ has order at most n, or $S = R(n)$. But $S = R(n) \neq R$ implies that some $R(t) \not\subseteq R(n)$, so $R(tn)$ is a φ-invariant subring properly containing S. This forces $R = R(tn)$, and φ has order at most tn. Consequently, φ must have finite order, and now Theorem 7 shows that R is finite.

When φ is integral over $\mathbf{J}$, we may assume that $S \neq 0$ by Theorem 1, so $\mathrm{card}(S)R = 0$ by Lemma 1. Thus R is a torsion ring and so is the direct sum of its p-torsion components $R(p) = \{r \in R \mid p^k r = 0 \text{ for some } k \geq 1\}$, over those primes with $p \mid \mathrm{card}(S)$. Now each $R(p)$ is φ-invariant, and the restriction φ_p of φ to $R(p)$ is integral over $\mathbf{J}$. Clearly $R(p) \cap S$ is a finite φ_p-invariant subring of $R(p)$. If T is a proper φ_p-invariant subring of $R(p)$ properly containing $R(p) \cap S$, then $R \neq T + S$ and $T + S$ is a φ-invariant subring properly containing S, a contradiction. Hence $R(p) \cap S$ is a finite maximal φ_p-invariant subring of $R(p)$, so either $\mathrm{card}\big(R(p) \cap S\big) < \mathrm{card}(S)$ and $R(p)$ is finite by induction on $\mathrm{card}(S)$, or $S \subseteq R(p)$. Since this holds for each $R(p)$, we may assume that R is finite unless $R = R(p)$ is p-torsion. Let $W = \{r \in R \mid pr = 0\}$, note that W is a φ-invariant ideal of R, and that R is finite or $W \not\subseteq S$ by Lemma 1. Therefore, because $W + S$ is a φ-invariant subring, $R = W + S$ and so $pR = pS \subseteq S$, again contradicting Lemma 1 unless R is finite or $pR = 0$. But if $pR = 0$, then R is an algebra over $\mathbf{F} = \mathbf{F}_p$ the field of p elements. It follows that φ is algebraic over $\mathbf{F}$, forcing φ to have finite order. To see this let $m(X) = \prod q_i(X)^{a(i)}$ be the prime factorization of the minimal polynomial of φ over $\mathbf{F}$. If $\mathbf{F}_t$ is the splitting field of $\prod q_i(X)$ over $\mathbf{F}$, then $\mathbf{F}_t$ has $t = p^r$ elements, and each $y \in \mathbf{F}_t$ satisfies $X^t - X$. Since each $q_i(X)$ has a root in $\mathbf{F}_t$, it follows that $\prod q_i(X) \mid (X^{t-1} - 1)$. For $k = \max\{a(i)\}$ and $n = p^k$, clearly $m(X) \mid (X^{t-1} - 1)^n = X^{n(t-1)} - 1$, so φ has finite order dividing $n(t-1)$. Consequently, Theorem 7 may be applied to show that R is finite.

To conclude the paper we give two special cases of Theorem 8 and two other consequences which extend results of Gilmer [5] and of Szele [13].

COROLLARY 1 (LAFFEY [8]). *If R contains a finite maximal subring, then R is finite.*

COROLLARY 2. *If R is a ring with involution * and S is a finite maximal *-invariant subring, then R is finite.*

COROLLARY 3. *If $\varphi \in \mathrm{Aut}(R) \cup \mathrm{Aut}^*(R)$ is either locally finite or integral over* $\mathbf{J}$, *and if R has only finitely many φ-invariant subrings, then R is finite.*

PROOF. Let $R = R_0 \supseteq R_1 \supseteq \cdots \supseteq R_{n+1} = 0$ be a maximal chain of φ-invariant subrings, with all inclusions proper. For each $i \leq n$, if φ_i is the restriction of φ to R_i, then R_{i+1} is a maximal φ_i-invariant subring of R_i, and of course each φ_i is locally finite or integral over $\mathbf{J}$. Thus R_n is finite by Theorem 1, so R_{n-1} is finite by Theorem 8, and using induction together with Theorem 8 shows that R is finite.

COROLLARY 4. *If $\varphi \in \mathrm{Aut}(R) \cup \mathrm{Aut}^*(R)$ is either locally finite or integral over* $\mathbf{J}$, *and if R satisfies the ascending and descending chain conditions on φ-invariant subrings, then R is finite.*

PROOF. Using the ascending chain condition there is a proper maximal φ-invariant subring S. By Theorem 8, it suffices to show that S is finite. By Zorn's Lemma and the descending chain condition there is a finite maximal descending chain of φ-invariant subrings $S = S_0 \supseteq S_1 \supseteq \cdots \supseteq S_{n+1} = 0$, with all inclusions proper. The argument in Corollary 3 now shows that S must be finite.

We do not know if Theorem 8 holds without any additional condition on $\varphi \in \mathrm{Aut}(R) \cup \mathrm{Aut}^*(R)$. Indeed, as we mentioned earlier, it would be interesting to know even if Theorem 1 holds in this case. That is, when R is infinite, must there always be a nonzero proper φ-invariant subring for any given (anti-) automorphism φ?

ACKNOWLEDGEMENT. The author would like to thank the referee for finding a minor error at the end of the proof of Theorem 1, and for bringing reference [7] to his attention.

REFERENCES

1. A. A. Albert, *Structure of Algebras*, Amer. Math. Soc. Colloq. Publ. **24**(1961).
2. H. E. Bell and F. Guerriero, *Some conditions for finiteness and commutativity of rings*, Internat. J. Math. Math. Sci. **13**(1990), 535–544.
3. H. E. Bell and A. A. Klein, *On finiteness of rings with finite maximal subrings*, Internat. J. Math. Math. Sci. **16**(1993), 351–354.
4. G. M. Bergman and I. M. Isaacs, *Rings with fixed-point-free group actions*, Proc. London Math. Soc. (3) **27**(1973), 69–87.
5. R. Gilmer, *A note on rings with only finitely many subrings*, Scripta Math. **29**(1973), 37–38.
6. I. N. Herstein, *Noncommutative Rings*, Carus Math. Monographs **15**, Math. Assoc. of Amer. (1968).
7. A. A. Klein, *The finiteness of a ring with a finite maximal subring*, Comm. Algebra **21**(1993), 1389–1392.
8. T. J. Laffey, *A finiteness theorem for rings*, Proc. Roy. Irish Acad. **92A**(1992), 285–288.
9. C. Lanski, *Differential identities in prime rings with involution*, Trans. Amer. Math. Soc. **291**(1985), 765–787.
10. ———, *On the cardinality of rings with special subsets which are finite*, Houston J. Math. **19**(1993), 357–373.
11. W. S. Martindale, III, *Prime rings satisfying a generalized polynomial identity*, J. Algebra **12**(1969), 576–584.
12. S. Montgomery, *Fixed rings of finite automorphism groups of associative rings*, Lecture Notes in Math, Springer-Verlag, New York, **818**(1980).
13. T. Szele, *On a finiteness condition for modules*, Publ. Math. Debrecen **3**(1954), 253–256.

Department of Mathematics
University of Southern California
Los Angeles, CA 90089–1113
U.S.A.
e-mail: clanski@mtha.usc.edu