Can. J. Math., Vol. XXVI, No. 5, 1974, pp. 1098–1108

HOMOMORPHISMS OF RINGS WITH INVOLUTION

CHARLES LANSKI

Introduction. The purpose of this paper is to examine the extent to which a homomorphism of a ring with involution is determined by its action on the symmetric elements of the ring. Assuming that the ring is "suitably free" of 2×2 matrix rings, we show that any homomorphism is uniquely determined if its image is semi-prime without nonzero central ideals. To obtain this result we first investigate automorphisms of quotients of rings with involution.

R will always denote a ring with involution, $*$; $S = \{r \in R | r^* = r\}$, the set of symmetric elements of R; and Z, the center of R. We write $\mathrm{Aut}(R/S)$ for the group of automorphisms of R which fix each element of S.

1. We begin by considering when $\mathrm{Aut}(R/S) = I_R$. Suppose $R^2 = 0$, R is 2-torsion-free, and $r^* = -r$ for all $r \in R$. Then any automorphism of R is in $\mathrm{Aut}(R/S)$. Hence to show $\mathrm{Aut}(R/S) = I_R$, R had better be semi-prime. Another problem which can arise is illustrated by taking $R = M_2(F)$, the 2×2 matrix ring over F, a field with $\mathrm{char} F \neq 2$. If

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^* = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix},$$

then $S = Z$ and again $\mathrm{Aut}(R/S)$ is the group of all automorphisms of R. So we need to eliminate the possibility that R has a direct summand which is a 2×2 matrix ring over a field. The following examples generalize the one above and show that the problem can persist even if R has no direct summands.

Example 1. Let $R = M_2(2J)$ where J is the ring of integers, and let $*$ be the symplectic involution as defined above for $M_2(F)$. Any inner automorphism of $M_2(J)$ restricts to an element of $\mathrm{Aut}(R/S)$. Thus $\mathrm{Aut}(R/S)$ can be large if R is only an order in $M_2(F)$.

Example 2. Let $A = F\{x, y, w, t\}$, the free algebra with identity in four indeterminates over the field F with char $F \neq 2$. Let I be the ideal of A generated by w^2, t^2, $wt + tw - 1$, pq, and qp, where p is either x or y and q is either w or t. Set $R = A/I$ with $*$ defined via: $x^* = x$, $y^* = y$, $w^* = -w$, and $t^* = -t$. Define $\varphi \in \mathrm{Aut}(R/S)$ by setting $(x)\varphi = x$, $(y)\varphi = y$, $(w)\varphi = w$, and $(t)\varphi = t - wt + tw - w$. If B is the ideal generated by x and y, and D the ideal generated by w and t, then $B \cong F\{x, y\}$, $D \cong M_2(F)$, and φ acts like the identity on B and like conjugation by $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ on D. Note that $R/B \cong D$.

Received March 8, 1973. This research was supported by NSF Grant GP-29119X.

The real problem Example 2 identifies is that a large piece of R, namely D in the example, has its symmetric elements in the center, allowing all "inner automorphisms" to be in $\mathrm{Aut}(R/S)$. It will be sufficient to make sure that R does not have many homomorphic images which are 2×2 matrix rings, as in the above examples. To this end we make the

Definition. R satisfies condition (C) *if R/P is commutative for any prime ideal P of R with $P^* = P$ and such that the images in R/P of the elements of S commute.*

The strength of condition (C) is that we may conclude that any element commuting with all symmetric elements lies in the center. A generalization of this fact is the content of our first theorem. Before stating this result, we need a well-known fact about $\bar{S}$, the subring generated by S.

Definition. T is the ideal of R generated by all $xy - yx$, for $x, y \in \bar{S}$.

Theorem. $T \subset \bar{S}$.

Proof. See [**2**, p. 4].

THEOREM 1. *Let R satisfy* (C), *let A be a semi-prime ideal of R and suppose that for some $x \in R$, $xt - tx \in A$ for all $t \in T$. Then $x + A \in Z(R/A)$.*

Proof. Let P be a prime ideal of R with $A \subset P$. If $T \not\subset P$, then $(T + P)/P$ is a nonzero ideal in R/P and commutes with $x + P$. Since R/P is a prime ring, $x + P \in Z(R/P)$, so $xr - rx \in P$ for all $r \in R$.

Next assume $T \subset P$ and $P^* = P$. Then the images of the elements of S commute, so R/P is commutative by (C). Hence $xr - rx \in P$ for $r \in R$. Lastly, if $P^* \neq P$ then $(P^* + P)/P$ is a nonzero ideal in R/P and for $w^* \in P^*$, $w^* + P = (w^* + w) + P$. Thus each element of $(P^* + P)/P$ is the image of an element of S. Since $T \subset P$, the ideal $(P^* + P)/P$ is commutative, forcing R/P to be commutative. Therefore, in all cases, $xr - rx \in P$. Since A is a semi-prime ideal, it is the intersection of all prime ideals which contain it. Consequently $xr - rx \in A$ for all $r \in R$, so $x + R \in Z(R/A)$, as claimed.

We can now use Theorem 1 to examine automorphisms of semi-prime images of R. Note that in the following results we are not assuming that the image under consideration has an involution.

THEOREM 2. *Let R satisfy* (C), *let A be a semi-prime ideal of R and suppose that φ is an automorphism of R/A such that $(s + A)\varphi = s + A$ for every $s \in S$. Then $(r + A)\varphi = (r + A) + (z + A)$ for $z + A \in Z(R/A)$.*

Proof. If $T \subset A$, then R/A is commutative by Theorem 1, so the theorem holds trivially. If $T \not\subset A$, let $t \in T$ and $x \in R$. Then $xt \in T$, so

$$(xt + A)\varphi = xt + A, \quad \text{since } T \subset \bar{S}.$$

https://doi.org/10.4153/CJM-1974-102-4 Published online by Cambridge University Press

Hence $(x + A)(t + A) = ((x + A)\varphi)(t + A)$ and so, for $(x + A)\varphi = y + A$,

$$(y - x + A)(t + A) \subset A$$

or $$(y - x)T \subset A.$$

Similarly $T(y - x) \subset A$, so by Theorem 1 $y - x \in Z(R/A)$. Equivalently we have

$$(x + A)\varphi = (x + A) + (z + A) \text{ for } z + A \in Z(R/A).$$

Our immediate goal is to show that $\mathrm{Aut}(R/S)$ is a group of exponent two. We can do this only under the assumption that $2R = 0$ or that R is 2-torsion-free. First we consider $2R = 0$.

THEOREM 3. *Suppose $2R = 0$, R satisfies* (C) *and A is a semi-prime ideal of R. If φ is an automorphism of R/A such that $(s + A)\varphi = s + A$ for all $s \in S$, then $(r + A)\varphi = (r + z) + A$ with $(z + A)\varphi = z + A$ and $z + A \in Z(R/A)$, consequently $\varphi^2 = I_{R/A}$.*

Proof. If $\varphi \neq I_{R/A}$, then for some $x \notin A$, $(x + A)\varphi = x + z + A$ for some $z + A \in Z(R/A)$ and $z \notin A$, using Theorem 2. Let $(x^* + A)\varphi = x^* + t + A$ for $t + A \in Z(R/A)$. Since $x + x^* \in S$, we have

$$\begin{aligned} x + x^* + A &= (x + x^* + A)\varphi = (x + A)\varphi + (x^* + A)\varphi \\ &= (x + x^* + A) + (z + t + A). \end{aligned}$$

Thus $z + t \in A$. Also, $xx^* \in S$, so

$$\begin{aligned} xx^* + A &= (xx^* + A)\varphi = (x + A)\varphi(x^* + A)\varphi \\ &= xx^* + z(x + x^*) + z^2 + A \end{aligned}$$

using $z + A = t + A$. Consequently,

$$(1) \qquad z^2 + A = z(x + x^*) + A.$$

If $(z + A)\varphi \neq z + A$, then using Theorem 2 again, we may conclude that $(z + A)\varphi = z + z_1 + A$ for $z_1 \notin A$ and $z_1 \in Z(R/A)$. As above, $(z^* + A)\varphi = (z^* + z_1) + A$. Now $xz + z^*x^* \in S$, so

$$\begin{aligned} (xz + z^*x^* + A) &= (xz + z^*x^* + A)\varphi \\ &= (x + z)(z + z_1) + (z^* + z_1)(x^* + z) + A. \end{aligned}$$

Equivalently,

$$(2) \qquad z^2 + z_1(x + x^*) + zz^* \in A.$$

Since $zz^* \in S$, $(zz^* + A)\varphi = zz^* + A$. If it were true that $(z_1 + A)\varphi = z_1 + A$, then using (2) we could conclude that

$$(z^2 + A) = (z^2 + A)\varphi = (z + z_1)^2 + A = z^2 + z_1^2 + A.$$

Thus $z_1^2 \in A$, and $z_1 + A$ is a nonzero nilpotent element in $Z(R/A)$, which is

https://doi.org/10.4153/CJM-1974-102-4 Published online by Cambridge University Press

impossible since R/A is semi-prime. Hence $(z_1 + A)\varphi \neq z_1 + A$, so by Theorem 2, $(z_1 + A)\varphi = z_1 + z_2 + A$ with $z_2 \notin A$ and $z_2 + A \in Z(R/A)$. Using (2) and the fact that $zz^* \in S$ gives

$$\begin{aligned} z^2 + z_1(x + x^*) + A &= (z^2 + z_1(x + x^*) + A)\varphi \\ &= (z + z_1)^2 + (z_1 + z_2)(x + x^*) + A. \end{aligned}$$

Canceling corresponding terms yields

(3) $\quad z_1^2 + A = z_2(x + x^*) + A.$

If $(z_2 + A)\varphi = z_2 + A$, then from (3) we could conclude that

$$(z_1^2 + A) = (z_1^2 + A)\varphi = z_1^2 + z_2^2 + A,$$

or $z_2^2 \in A$. This is impossible, as above, since R/A is semi-prime. Thus $(z_2 + A)\varphi = z_2 + z_3 + A$ with $z_3 \notin A$ and $z_3 + A \in Z(R/A)$. Applying φ to (3) yields

(4) $\quad (z_1 + z_2)^2 + A = (z_2 + z_3)(x + x^*) + A$, or $z_2^2 + A = z_3(x + x^*) + A$.

Now $(x + A)\varphi^2 = (x + z + A)\varphi = x + z_1 + A$. Hence

$$\begin{aligned} (x + A)\varphi^4 = (x + z_1 + A)\varphi^2 &= (x + z_1) + A + ((z_1 + z_2) + A)\varphi \\ &= x + z_1 + z_1 + z_3 + A = x + z_3 + A. \end{aligned}$$

Since $(s + A)\varphi^4 = s + A$ for all $s \in S$, φ^4 satisfies the hypothesis of the theorem, so we may use (1) to conclude

$$z_3^2 + A = z_3(x + x^*) + A.$$

This, together with (4) yields

$$z_2^2 + A = z_3^2 + A.$$

But now $(z_2 + z_3 + A)^2 = (z_2 + z_3)^2 + A = z_2^2 + z_3^2 + A = A$. Since R/A is semi-prime we must have $z_2 + A = z_3 + A$, and consequently,

$$(z_2 + A)\varphi = z_2 + z_3 + A = A.$$

As φ is an automorphism of R/A, this situation is impossible. Therefore, it must be that $(z + A)\varphi = z + A$, and so $\varphi^2 = I_{R/A}$, proving the theorem.

Under the hypothesis of Theorem 3 we know that the automorphisms of R/A which "fix S" form an abelian group of exponent 2. Clearly, any two automorphisms which agree on all $s + A$ for $s \in S$, differ by an element of this group. To show any automorphism of R/A is uniquely determined by its action on the image of S requires an additional assumption.

THEOREM 4. *Suppose* $2R = 0$, *R satisfies* (C), *A is a semi-prime ideal of R, and $Z(R/A)$ has no divisors of zero in R/A. If φ is an automorphism of R/A fixing the image of S, then $\varphi = I_{R/A}$ unless R/A is a commutative domain.*

Proof. If $\varphi \neq I_{R/A}$ and $(x + A)\varphi \neq x + A$, then from equation (1) in the proof of Theorem 3 we have $z(z + x + x^*) \in A$, where z is given as in Theorem 2. Since $z \notin A$ and $Z(R/A)$ has no divisors of zero in R/A, we must have $x^* + A = x + z + A = (x + A)\varphi$. On the other hand, if $(x + A)\varphi = x + A$ and $(y + A)\varphi \neq y + A$, then $(x + y + A)\varphi \neq x + y + A$, so we have $(x + y + A)\varphi = (x + y)^* + A = x^* + y^* + A$. Using that φ is a homomorphism gives $(x + y + A)\varphi = x + y^* + A$. Thus $x + A = x^* + A$. Consequently, for all $x \in R$ we may write $(x + A)\varphi = x^* + A$. It follows that $(x^*y^* + A)\varphi$ can be written as $yx + A$ and also as $xy + A$, and so, R/A is commutative. Under the hypothesis on $Z(R/A)$ it is a domain.

With regard to Theorem 4, we note that $Z(R/A)$ has no zero divisors in R/A if A is a prime ideal. Also the possibility that R is commutative and $\varphi = *$ always exists. We turn now to the situation when R/A is 2-torsion-free.

THEOREM 5. *Suppose R satisfies* (C) *and A is a semi-prime ideal of R with R/A 2-torsion-free. If φ is an automorphism of R/A with $(s + A)\varphi = s + A$ for all $s \in S$ then for any $r \in R$*

(i) $(r + A)\varphi = (r + z) + A$ *for* $z \notin A$, $z + A \in Z(R/A)$,

(ii) $(z + A)\varphi = -z + A$,

(iii) $\varphi^2 = I_{R/A}$,

(iv) $\{z + A | z \text{ is as in (i)}\}$ *generates an ideal which lies in* $Z(R/A)$.

Proof. (i) is just Theorem 2, and (iii) follows immediately from (i) and (ii). Thus it suffices to prove (ii) and (iv). Using Theorem 2, for any $r \in R$ we may write $(r + A)\varphi = r + z_1 + A$, $(z_1 + A)\varphi = z_1 + z_2 + A$, and generally $(z_i + A)\varphi = z_i + z_{i+1} + A$ where $z_i + A \in Z(R/A)$ and where we may assume $z_1 \notin A$ if $\varphi \neq I_{R/A}$.

As in Theorem 3, if $(r^* + A)\varphi = r^* + t + A$ for $t + A \in Z(R/A)$, then $r + r^* \in S$ implies that $z_1 + t \in A$. Using $rr^* \in S$ yields

$$\begin{aligned}(rr^* + A) &= (rr^* + A)\varphi = (r + z_1)(r^* - z_1) + A \\ &= rr^* - z_1^2 + z_1(r^* - r) + A\end{aligned}$$

and so

$$z_1^2 + A = z_1(r^* - r) + A. \tag{5}$$

Also, as in Theorem 3, since $z_1r + r^*z_1^* \in S$,

$$\begin{aligned}z_1r + r^*z_1^* + A &= (z_1r + r^*z_1^* + A)\varphi \\ &= (z_1 + z_2)(r + z_1) + (r^* - z_1)(z_1^* - z_2) + A\end{aligned}$$

or

$$z_2(r^* - r) + A = z_1^2 + 2z_1z_2 - z_1z^*_1 + A. \tag{6}$$

Applying φ to (5) gives

$$(z_1 + z_2)^2 + A = (z_1 + z_2)(r^* - r - 2z_1) + A.$$

https://doi.org/10.4153/CJM-1974-102-4 Published online by Cambridge University Press

Expanding these expressions and using (5) and (6) results in the relation

$$z_1^2 + 2z_1z_2 + z_2^2 + z_1z_1^* \in A,$$

or equivalently.

$$(7) \qquad -z_1z_1^* + A = (z_1 + z_2)^2 + A.$$

Thus $(z_1 + z_2)^2 + A$ is fixed by φ. If we begin with any z_i instead of r we would obtain that $(z_i + z_{i+1})^2 + A$ is fixed by φ. That is,

$$(8) \qquad ((z_i + z_{i+1})^2 + A)\varphi = (z_i + z_{i+1})^2 + A.$$

Using this expression and the definition of z_i we have

$$\begin{aligned}((z_i + A)\varphi)^2 &= ((z_i + A)\varphi)^2\varphi \\ &= ((z_i + A)\varphi^2)^2 \\ &= ((z_i + z_{i+1} + A)\varphi)^2 \\ &= ((z_i + A)\varphi + (z_{i+1} + A)\varphi)^2 \\ &= ((z_i + A)\varphi)^2 + (2z_iz_{i+1} + A)\varphi + ((z_{i+1} + A)\varphi)^2.\end{aligned}$$

Consequently,

$$((z_{i+1} + A)^2 + (2z_iz_{i+1} + A))\varphi \in A$$

and so, since φ is an automorphism of R/A,

$$(9) \qquad z_{i+1}^2 + 2z_iz_{i+1} \in A.$$

Since by (8), $(z_i^2 + A)\varphi = (z_i + z_{i+1})^2 + A$ is fixed by φ, we may conclude using (9) that $(2z_iz_{i+1} + A)\varphi$ is also fixed by φ. Thus

$$(2z_iz_{i+1} + A)\varphi^2 = (2z_iz_{i+1} + A)\varphi \text{ and so}$$
$$(z_iz_{i+1} + A)\varphi = z_iz_{i+1} + A$$

using the fact that φ is an automorphism and that R/A is 2-torsion free. In particular,

$$z_1z_2 + A = (z_1z_2 + A)\varphi = (z_1 + z_2)(z_2 + z_3) + A$$

or

$$(10) \qquad z_2^2 + z_3(z_1 + z_2) \in A.$$

From (10) we have that $xz_3 \in A$ implies $xz_2^2 \in A$. Since the annihilator of any power of a central element in a semi-prime ring is the annihilator of the element, $xz_2 \in A$. Applying this to (9) we have $(z_3 + 2z_2)z_3 \in A$, and so $(z_3 + 2z_2)z_2 \in A$. Together these yield $(z_3 + 2z_2)^2 \in A$. Semi-prime rings cannot have central nilpotent elements, so $z_3 + 2z_2 \in A$. Using the definition of z_i gives

$$(z_2 + A)\varphi = z_2 + z_3 + A = -z_2 + A.$$

https://doi.org/10.4153/CJM-1974-102-4 Published online by Cambridge University Press

It follows that

$$(r + A)\varphi^2 = r + 2z_1 + z_2 + A \text{ and } ((2z_1 + z_2) + A)\varphi = 2z_1 + z_2 + A.$$

Now φ^2 satisfies the same hypothesis as φ with respect to the image of S so using (5) with φ^2 replacing φ and $y = 2z_1 + z_2$ replacing z_1 gives

$$y^2 + A = y(r^* - r) + A.$$

Apply φ^2 to both sides remembering that $y + A$ is fixed and the result is

$$y^2 + A = y(r^* - r - 2y) + A, \quad \text{or } y^2 \in A.$$

Again, since R/A has no central nilpotent elements, $y = 2z_1 + z_2 \in A$. Thus $(z_1 + A)\varphi = -z_1 + A$ proving (ii).

To prove (iv), let r and $z = z_1$ be as above and for $x \in R$ let

$$(x + A)\varphi = (x + t) + A$$

for $t + A \in Z(R/A)$. Since $x + x^* \in S$,

$$(r(x + x^*) + A)\varphi = r(x + x^*) + z(x + x^*) + A$$

so $z(x + x^*) \in Z(R/A)$. Also

$$\begin{aligned}(z(x - x^*) + A)\varphi &= -z(x - x^* + 2t) + A \\ &= z(x - x^*) - 2z(x - x^*) - 2zt + A,\end{aligned}$$

and so, $2z(x - x^*) + 2zt + A \in Z(R/A)$. As $zt + A \in Z(R/A)$,

$$2z(x - x^*) \in Z(R/A).$$

Hence $4xz = 2z(x + x^*) + 2z(x - x^*) \in Z(R/A)$. Consequently $xz \in Z(R/A)$ since R/A is 2-torsion-free, establishing the theorem.

Note that if R/A is not commutative and has no ideals in its center then φ must be the identity. In particular, this holds if R/A is prime. Just as for the $2R = 0$ case, if $A = 0$ and R is commutative it is always possible that φ is *.

For the special case when $A = 0$, let us record some conditions which force $\mathrm{Aut}(R/S) = I_R$.

THEOREM 6. *Let R be a semi-prime, 2-torsion-free ring satisfying* (C). *Then unless R is commutative,* $\mathrm{Aut}(R/S) = I_R$, *and so automorphisms of R are uniquely determined by their effect on S, if any of the following hold:*

(1) *Z contains no divisors of zero (in R);*

(2) *$Z \subset S$;*

(3) *$\bar{S}$ is a non-commutative prime ring.*

Proof. If (1) holds, the result follows exactly as in Theorem 4. If (2) holds then by (ii) of Theorem 5, $\varphi = I_R$. Finally, if (3) holds and $(r)\varphi = r + z$, as in Theorem 5, then $z^* = -z$. We know $(z)\varphi = z - 2z$, so $z^*\varphi = z^* + 2z$, from the proof of Theorem 5. Hence $zz^* = (zz^*)\varphi = (-z)(z^* + 2z)$, and so $z(z + z^*) = 0$.

https://doi.org/10.4153/CJM-1974-102-4 Published online by Cambridge University Press

Applying * gives $z^*(z + z^*) = 0$, and combining yields $(z + z^*)^2 = 0$, so $z + z^* = 0$ since R is semi-prime. Consequently, $z^2 \in S$. If $z \neq 0$ then by (iv) of Theorem 5 the ideal generated by z^2 is in Z and intersects $\bar{S}$ nontrivially. But $\bar{S}$ prime would force $\bar{S}$ to be commutative contrary to assumption. Hence $z = 0$ and $\varphi = I_R$.

2. In this section we construct an example to show that the situation described in Theorem 5 can occur without $\varphi = I$. Let F be any field with char $F \neq 2$, $F[z]$ the polynomial ring over F in one indeterminate, and $F[z]\{x, y\}$ the free algebra with identity over $F[z]$ in indeterminates x and y. Consider the ideal of $F[z]\{x, y\}$ generated by $z(xy - yx)$ and $z(2x + z)$, and let B be the quotient. Define * on B by setting $z^* = -z$, $x^* = -x$, and $y^* = y$. Define φ via $(z)\varphi = -z$, $(x)\varphi = x + z$, and $(y)\varphi = y$. It is clear that φ is an automorphism of B of period 2. Note that $z(xy - yx) = 0$ implies that the ideal generated by z is in the center of B, so φ has the form indicated in Theorem 5. It remains to show that B is semi-prime, satisfies condition (C), and that $\varphi \in \mathrm{Aut}(R/S)$.

First, since x and y commute in the presence of z, any monomial in x and y with coefficient involving z^k has the form $z^k x^i y^j$. Since $2xz = -z^2$, $2^i z x^i = \pm z^{i+1}$. Consequently, if $r \in B$, for a suitable power of 2 we may write

$$2^m r = p_0(x, y) + \sum_{i=1}^{n} z^i p_i(y)$$

with p_j "polynomials" with coefficients in F. From this form for the elements of B, it follows that B is semi-prime.

To show that condition (C) is satisfied it will be helpful to denote $ab - ba$ by $[a, b]$.

THEOREM 7. *If P is a prime ideal of B such that the images of S commute in B/P, then B/P is commutative.*

Proof. Since $z[x, y] = 0$ in B and $z \in Z(B)$, either $z \in P$ or $[x, y] \in P$. If $[x, y] \in P$ then R/P is commutative. We may assume, then, that $z \in P$. We claim that $[y + P, [r + P, y + P]] = 0$ for all $r \in B$. If so, then by the sublemma in [**2**, p. 5], $y + P$ is in $Z(R/P)$, so R/P is commutative. It suffices to take r to be a monomial in x and y. The relation certainly holds for r of the form x^2 and xy^ix since these are in S, and for x since $[x, y] \in S$. If $r = ty$ then $[y, [ty, y]] = [y, [t, y]]y \in P$ by induction on the degree of r. Similarly, if $r = tx^i$ for $i \geqq 2$, since $[x^2, y] \in P$. Lastly take $r = txy^ix$. Again

$$[y, [txy^ix, y]] = [y, [t, y]]xy^ix \in P.$$

Thus $y + P \in Z(R/P)$ and R/P is commutative.

THEOREM 8. $\varphi \in \mathrm{Aut}(B/S)$.

Proof. For $r \in B$ write $2^m r = p_0(x,,y) + \sum_{i=1}^{n} z^i p_i(y)$. Clearly, $r \in S$ if and only if $2^m r \in S$. Also

$$\sum_{\text{even}} z^i p_i(y) \in S$$

and fixed by φ. If $r \in S$ then

$$\sum_{\text{odd}} z^i p_i(y) = 0,$$

so it is only necessary to consider $r = p_0(x, y)$.

Note $(x^2)\varphi = (x + z)^2 = x^2 + 2xz + z^2 = x^2$, and by induction $(x^{2n})\varphi = x^{2n}$.

For m a monomial in $p_0(x, y)$, write $m = m_0 x m_1 x \cdots x m_k$ where each m_i is a monomial in y and x^2. Since $p_0(x, y) \in S$, $m + m^*$ is a "part" of $p_0(x, y)$ where $m^* = (-1)^k m_k^* x \cdots x m_0^*$. (If $m = m^*$ use m in place of $m + m^*$.) Now

$$(m + m^*)\varphi = m_0(x + z) \cdots (x + z)m_k$$
$$+ (-1)^k m_k^*(x + z) \cdots (x + z)m_0^*.$$

Expanding gives

$$(m + m^*)\varphi =$$
$$m + m^* + \sum_{i=1}^{k} \binom{k}{i} z^i x^{k-i}(m_0 \ldots m_k + (-1)^k m_k^* \ldots m_0^*),$$

using the fact that x and y commute in the presence of z. Thus we may also write

$$z(m_0 \cdots m_k) = z(m_k^* \cdots m_0^*),$$

and so

$$(m + m^*)\varphi = m + m^* + 2 \sum_{i=1}^{k} \binom{k}{i} z^i x^{k-i} m_0 \ldots m_k$$

where we may assume that k is even. But

$$\sum_{i=1}^{k} \binom{k}{i} z^i x^{k-i} = (x^k)\varphi - x^k = 0$$

for k even. Thus φ fixes $p_0(x, y)$ so $\varphi \in \mathrm{Aut}(B/S)$ as claimed.

3. We intend next to investigate $\mathrm{Aut}(R/S)$ when R does not satisfy condition (C). As Example 1 and Example 2 illustrate, when (C) does not hold one might expect certain inner automorphism to arise. In a sense, all addition problems resulting from (C) not holding do come from inner automorphisms of certain quotients of R. To apply our previous results to quotients of R we must ensure that these quotients are either 2-torsion, or 2-torsion-free. If $2R = 0$, the same holds for all quotients of R. If R is 2-torsion-free we can consider $R_1 = R \otimes_J J_{(2)}$, for J the ring of integers and $J_{(2)}$ the localization at the powers of 2. The involution and automorphisms of R naturally go over to R_1, and since we will be considering embeddings of R, there is no loss of generality in assuming that R is an algebra over $J_{(2)}$.

THEOREM 9. *Let P be a prime ideal of R with $P^* = P$ and let $\varphi \in \mathrm{Aut}(R/S)$. Then $(P)\varphi = P$.*

Proof. For $x \in P$, both $x + x^* \in P$ and $x^*x \in P$. Since $x^2 = (x + x^*)x - x^*x$, $(x^2)\varphi = (x + x^*)(x\varphi) - x^*x \in P$. Hence $(x\varphi)^2 \in P$ and $(P)\varphi + P/P$ is a nil ideal of index 2 in R/P. By Levitzki's Theorem [**2**, Lemma 1.1] R/P has a nilpotent ideal, if this nil ideal is not zero. Since R/P is prime we must have $(P)\varphi \subset P$. The argument works for φ^{-1}, so $(P)\varphi = P$.

Let R be semi prime but not prime and let A be the intersection of all prime ideals $P \subset R$ with $P^* = P$, R/P not commutative, and $T \subset P$. Let B be the intersection of all the other prime ideals of R. If R is a prime ring and $T = 0$ take $A = 0$ and $B = R$. If R is prime and $T \neq 0$ take $B = 0$ and $A = R$. Since $A \cap B = 0$ in all cases, R is a subdirect sum of R/A and R/B, semi-prime rings. Furthermore, by Theorem 9, φ induces an automorphism on each of R/A and R/B. Now since condition (C) is equivalent to $P = P^*$ and $T \subset P$ implies that R/P is commutative, R/B vacuously satisfies (C). Note that if R is prime and $T \neq 0$ then any element commuting with T automatically lies in $Z(R)$, so the conclusion of Theorem 1, and so, Theorem 2 holds for elements of $\mathrm{Aut}(R/S)$. Thus in either case we may apply Theorem 3 or Theorem 5 to R/B (assuming either $2R = 0$ or R is a $J_{(2)}$ algebra) to conclude that automorphisms of R/B fixing the image of S have order 2.

Let $\{P_i\}$ be the primes whose intersection is A. Then R/A is a subdirect sum of $R_i = R/P_i$, and by Theorem 9, φ induces an automorphism φ_i on each of these rings. Also, since $P_i^* = P_i$, each R_i has an involution given by $(r + P_i)^* = r^* + P_i$. In each R_i the elements $(x + x^*) + P_i$ commute, since $T \subset P_i$, so by a Theorem of Amitsur [**1**], R_i satisfies a polynomial identity of degree 4. Thus the quotient ring of R_i, $Q(R_i)$, is a simple ring four dimensional over its center. Now φ_i naturally induces an automorphism of $Q(R_i)$ which must be inner by the Skolem-Noether Theorem. Consequently, the action of φ on R/A is the restriction to R/A of an inner automorphism of $Q(\bigoplus R_i)$, and we have proved the following theorem.

THEOREM 10. *Let R be semi-prime with either $2R = 0$ or R a $J_{(2)}$ algebra and let $\varphi \in \mathrm{Aut}(R/S)$. There exist rings* (with involution) *R_1 and R_2 such that*

(1) *R_1 is the direct product of 4-dimensional simple algebras;*

(2) *R_2 is a semi-prime homomorphic image of R;*

(3) *R is a subring of $R_1 \oplus R_2$;*

(4) *φ is the restriction of $\varphi_1 + \varphi_2$ where φ_1 is an inner automorphism on R_1 ana φ_2 is given as in Theorem 3 or Theorem 5.*

4. Finally, we consider homomorphisms of R where, again, we assume that R satisfies condition (C). Our first result will show that, once more, the center of the image plays a key role. Note that no assumption about an involution is placed on the image.

THEOREM 11. *Let R satisfy condition* (C) *and suppose that α and β are homomorphisms of R onto R' a semi-prime ring, such that $(s)\alpha = (s)\beta$ for all $s \in S$. Then for all $r \in R$, $(r)\alpha - (r)\beta \in Z(R')$, and* (Ker α)β *and* (Ker β)α *are central ideals in R'.*

Proof. The statements about the kernels of α and β follow trivially from $(r)\alpha - (r)\beta \in Z(R')$. To show this holds, consider $t \in T$ and $r \in R$. Then $tr \in T \subset \bar{S}$, so $(tr)\alpha = (tr)\beta$ and $(t)\alpha((r)\alpha - (r)\beta) = 0$. Since α is onto, there is $y \in R$ so that $(r)\alpha - (r)\beta = (y)\alpha$. Therefore we may write $(ty)\alpha = 0$. Similarly $(yt)\alpha = 0$, so $(ty - yt)\alpha = 0$. The kernel of α is a semi-prime ideal of R, so by Theorem 1, $y + \text{Ker } \alpha \in Z(R/\text{Ker } \alpha)$. But this yields

$$(y)\alpha = (r)\alpha - (r)\beta \in Z(R'),$$

which proves the theorem.

The following example shows how two homomorphisms can be quite different in the presence of central ideals.

Example 3. Let W be any semi prime ring with involution and V any commutative ring. Let $R = W \oplus V \oplus V$ with $(w, a, b)^* = (w^*, b, a)$. Assume that V_1 is a semi prime homomorphic image of V under the mapping φ. Let $R' = W \oplus V_1$ and define R onto R' by

$$(w, a, b)\alpha = (w, (a)\varphi) \qquad (w, a, b)\beta = (w, (b)\varphi).$$

By insisting that R' contain no central ideals, we can insure uniqueness.

THEOREM 12. *Let R satisfy* (C) *and suppose α and β are homomorphisms of R onto the semi-prime ring R, with α and β agreeing on S. If R' has no nonzero central ideals, and if R' is 2-torsion-free, then $\alpha = \beta$.*

Proof. By Theorem 11, Ker α = Ker $\beta = K$. Thus each of α and β induce a natural isomorphism from R/K to R'. Let φ be the automorphism of R/K obtained by taking one of these composed with the inverse of the other. Clearly $(s + K)\varphi = s + K$ for all $s \in S$, so by Theorem 5, $\varphi = I_{R/K}$ and $\alpha = \beta$.

REFERENCES

1. S. A. Amitsur, *Identities in Rings with involution*, Israel J. Math. *1* (1969), 63–68.
2. I. N. Herstein, *Topics in ring theory* (University of Chicago Press, Chicago, 1969).

University of Southern California,
Los Angeles, California