JOURNAL OF ALGEBRA 83, 26–32 (1983)

A Theorem on Invariant Subrings

I. N. HERSTEIN*

Department of Mathematics,
The University of Chicago,
Chicago, Illinois 60637

Communicated by the Editors

Received June 20, 1982

In [1] Amitsur proved, following an argument due to Baxter [2] involving the Lie structure of simple rings, that if R is a simple ring which is an algebra over a field $F \neq GF(2)$, and if R contains an idempotent $e^2 = e \neq 0, 1$, then, if $A \subset R$ is a subspace over F such that $(1+t)A(a+t)^{-1} \subset A$ for all $t \in R$ such that $t^2 = 0, A$ must be contained in Z, the center of R, or $A \supset [R, R]$, the additive subgroup of R generated by all $[x, y] = xy - yx$. This result generalizes an earlier result of Hattori [4], which had been proved for simple artinian rings. In particular, if A should also happen to be a subring of R then it follows that $A \subset Z$ or $A = R$.

We complete the story here, when A is a subring of R, when $F = GF(2)$. In carrying out our proof we do not divide the argument according as $F = GF(2)$ or $F \neq GF(2)$. Furthermore, instead of working in the context of a simple ring we work in that of a prime ring; we also do not require that A be a subalgebra over F. When $F \neq GF(2)$ these generalizations follow easily from the argument given by Amitsur. We shall make several applications of the result that we prove here in a joint paper with Bergen [3].

In what follows R will be a prime ring with center Z, and possessing a non-trivial idempotent e, where $e^2 = e \neq 0, 1$. Suppose that A is a subring of R such that $(1+t)A(1+t)^{-1} \subset A$ for all $t \in R$ such that $t^2 = 0$ (that is, even if R does not have 1, $(1+t)a(1-t) = a + ta - at - tat$ is in A for all $a \in A$).

We shall prove the

THEOREM. *Either $A \subset Z$ or A contains a non-zero ideal of R, except in the one case where R is the ring of all 2×2 matrices over $GF(2)$, the integers mod 2.*

* The research in this paper was supported by the *NSF* Grant, NSF-MCS810-2472 at the University of Chicago.

0021-8693/83 $3.00

If $t^2 = 0$ and $a \in A$ then $(1+t)a(1+t)^{-1} - a \in A$; hence

$$ta - at - tat \in A \text{ for all } a \in A, \text{ all } t \in R \text{ such that } t^2 = 0. \tag{1}$$

We begin with

LEMMA 1. (a) *Suppose that $u \in R$ commutes with all t such that $t^2 = 0$; then $u \in Z$.*

(b) *If $u \in R$ commutes with all idempotents in R then $u \in Z$.*

Proof. (a) If u commutes with all t such that $t^2 = 0$ then, for any $x \in R$, and $e \neq 0, 1$ an idempotent of R, since $ex(1-e)$, $(1-e)ye$ have square 0, u commutes with all these; hence u centralizes $eR(1-e)$ and $(1-e)Re$. Therefore u centralizes $eR(1-e)Re$. Let $W = R(1-e)R$; $W \neq 0$ is an ideal of R and, as we have seen, u centralizes eWe. Also, since $eW(1-e) \subset eR(1-e)$, u centralizes $eW(1-e)$. We thus get that u centralizes eW; similarly u centralizes We, and so u centralizes the non-zero ideal WeW of R. Since R is prime this forces u to be in Z.

(b) If u commutes with all idempotents in R, and if $e^2 = e \neq 0, 1$ then, for any $x \in R$, $f = e + xe - exe$ is an idempotent, so u commutes with $f - e = xe - exe = (1-e)xe$. Similarly u commutes with all $ey(1-e)$. The argument in the paragraph above then shows that $u \in Z$.

Recall that a ring is said to be *semi-prime* if it has no non-zero nilpotent ideals.

LEMMA 2. *A is semi-prime.*

Proof. Suppose that $a \in A$ is such that $aAa = 0$, $a^2 = 0$. If $t^2 = 0$, by (1) we have that $ta - at - tat \in A$; hence $a(ta - at - tat)a \in aAa = 0$, resulting in $atata = 0$. However, if $t^2 = 0$ then $(trt)^2 = 0$ for all $r \in R$; thus we have $atrtatrta = 0$, so every element in $Rtat$ is nilpotent of index of nilpotence at most 3; by a result of Levitzki (Lemma 1.1 [5]), since R is prime, we have that $tat = 0$.

If $e^2 = e \neq 0, 1$ then $t = ex(1-e)$ has square 0, therefore $ex(1-e)aex(1-e) = 0$, for all $x \in R$. This gives, as above, using the result of Levitzki, that $(1-e)ae = 0$, that is, $ae = eae$. Using the elements $t = (1-e)ye$ of square 0 leads us to $ea = eae$. Thus $ae = eae = ea$, and so a commutes with all idempotents; by Lemma 1, $a \in Z$. However, since $a^2 = 0$, and Z is an integral domain, we have that $a = 0$. Hence A is semi-prime.

We now come to the stickiest part of the proof.

LEMMA 3. *If A commutative and $A \not\subset Z$, then R is the ring of all 2×2 matrices over $GF(2)$.*

Proof. Since A is semi-prime by Lemma 2, and commutative, A has no nilpotent elements. We claim that if $a \neq 0 \in A$ then a is *not* a zero divisor in R. For, suppose that $ax = 0$ for some $x \in R$; thus $t = xra$ has square 0, so by (1), $(xra)\,a - a(xra) - (xra)\,a(xra) \in A$, that is, $xra^2 \in A$ for all $r \in R$. However, $(xra^2)^2 = 0$, so we have $xRa^2 = 0$. Since R is prime and $a^2 \neq 0$, we must have that $x = 0$.

If $t^2 = 0$ and $r, s \in R$ then $(t + trt)^2 = 0$ and $(trt + tst)^2 = 0$; using these values in (1) gives us

$$tatrt + trtat \in A, \tag{2}$$

$$trtatst + tstatrt \in A \tag{3}$$

for all $r, s \in R$.

Since the elements in (2) and (3) are nilpotent and in A, we must have

$$tatrt + trtat = 0 \qquad \text{and} \qquad trtatst + tstatrt = 0 \tag{4}$$

for all r, $s \in R$.

By a result of Martindale (see Lemma 1.3.2 in [6]) we get that $tat = \alpha t$, where $\alpha \in C$, the extended centroid of R. If $\alpha = 0$ for all t such that $t^2 = 0$, then (1) tells us that $ta - at \in A$; but $(ta - at)^2 = -ta^2t \in A$ and is nilpotent, hence $(ta - at)^2 = 0$, and so $ta - at = 0$. Thus, by Lemma 1, we would have that $a \in Z$.

So, since $A \not\subset Z$, if $a \in A$, $a \notin Z$ then $tat = \alpha t \neq 0$ for some t such that $t^2 = 0$. But then (4) tells us that $trtst + tstrt = 0$ for all r, $s \in R$. By a result of Martindale [6], $trt = \alpha(r)\,t$, where $\alpha(r) \in C$, for all $r \in R$. In addition, char $R = 2$ follows. Pick r such that $trt \neq 0$, that is, $\alpha(r) \neq 0$.

Now $\alpha(r)\,t \in R$ has square 0; hence

$$(1 + t)\,a = a_1(1 + t), \tag{5}$$
$$(1 + \alpha(r)\,t)\,a = a_2(1 + \alpha(r)\,t),$$

where $a_1, a_2 \in A$. Since $tat \neq 0$, we have $ta \neq at$; hence $a_1 \neq a$. From (5) we get

$$(\alpha(r) - 1)\,a = \alpha(r)\,a_1 - a_2 - \alpha(r)(a_1 - a_2)\,t.$$

Commuting this with a, since A is commutative, yields $\alpha(r)(a_1 - a_2)(at - ta) = 0$. But $at - ta \neq 0$, $\alpha(r) \neq 0$, so $a_1 - a_2 \in A$ is a zero divisor, therefore $a_1 - a_2 = 0$. So $(\alpha(r) - 1)\,a = \alpha(r)\,a_1 - a_2 = (\alpha(r) - 1)\,a_1$; since $a \neq a_1$ we must have $\alpha(r) = 1$. In particular, since $tat \neq 0$, we have $tat = t$.

If $\beta \neq 0, 1 \in C$ then, for some ideal W of R, $0 \neq W\beta \subset R$ [6], and since $tWt \neq 0$, $twt = t$ for some $w \in W$. Thus $t(\beta w)\,t = \beta twt = \beta t$, so $\alpha(\beta w) =$

$\beta \neq 0, 1$, a contradiction. In short, $C = GF(2)$, and $tRt = GF(2)\,t$. If $f = at$ then $f^2 = f$, $fRf = GF(2)f$. Hence R is a primitive ring with minimal right ideal fR, and $fRf \approx GF(2)$.

Since char $R = 2$, by (1), $ta + at + tat \in A$, that is, $ta + at + t \in A$; thus $(ta + at)^2 = (ta + at + t)^2 \in A$, giving us that $ta + at + ta^2t \in A$. Hence $t + ta^2t \in A$ and since $t + ta^2t$ is nilpotent, we have $ta^2t = t$. Thus $t(a^2 + a)\,t = 0$, which implies that $t(a^2 + a) = (a^2 + a)\,t$. Therefore $a^2 + a$ commutes with all t such that $t^2 = 0$, so, by Lemma 1, $a^2 + a \in Z$. But $a^2 \neq a$, otherwise $a = 1$ (since a is not a zero-divisor), so $a^2 + a \neq 0$ is in $Z \subset C = GF(2)$. So $a^2 + a = 1$. We see, in this way, that A is the field of four elements.

We claim that R is simple, for, if $W \neq 0$ is an ideal of R then $tWt \neq 0$; hence $twt = t$ for some $w \in W$. Thus $t \in W$. But then $b = ta + at + t \neq 0 \in A \cap W$; since b is invertible, being in A, we conclude that $W = R$. So R is simple, with 1, and minimal right ideal fR, where $fRf = GF(2)f$; this forces R to be artinian, and so by Wedderburn's theorem, $R \approx (GF(2))_k$, the $k \times k$ matrices over $GF(2)$. In this case it is easy to see that $k = 2$. For, if $k > 2$ and $t^2 = 0$, rank $t = 1$ then for $a \in A$, $b^2 = (ta + at)^2 \in A$ is of rank 2 at most, and is therefore not invertible; his gives $b^2 = 0$ and so $ta = at$. In particular a centralizes all e_{ij}, $i \neq j$; this forces $a \in Z$.

With this the lemma is proved.

We may thus assume henceforth that $R \neq (GF(2))_2$.

LEMMA 4. *If $B \neq 0$ is a subset of R such that $(1 + t)\,B(1 + t)^{-1} \subset B$ for all $t \in R$ such that $t^2 = 0$, then, if $xB = 0$, we must have $x = 0$.*

Proof. Let T be the subring generated by all t such that $t^2 = 0$. As we saw in the proof of Lemma 1, $T \supset WeW$, where $W = R(1 - e)\,R \neq 0$ is an ideal of R.

Now, if $xB = 0$ then $x(1 + t)\,B(1 + t)^{-1} \subset xB = 0$; hence $xtB = 0$. Continuing we get $xTB = 0$ and so $xWeWB = 0$. By the primeness of R we conclude that $x = 0$.

Recall that C is the extended centroid of R [6].

LEMMA 5. *If $A \not\subset Z$ and if $xAy = 0$ for some $x, y \in RC$, then $x = 0$ or $y = 0$.*

Proof. By the properties of RC [6] there is an ideal W of R such that $Wx \subset R$ and $yW \subset R$. If $x \neq 0, y \neq 0$ then $Wx \neq 0$ and $yW \neq 0$, and $(Wx)\,A(yW) = 0$. So, without loss of generality, we may assume that x and y are in R.

If $b \in A$, $r \in R$ then $(yrxb)^2 = 0$, so for $a \in A$, by (1), $yrxba - ayrxb - yrxbayrx \in A$. Because $xAy = 0$ this relation above reduces to $c = yrxba - ayrxb \in A$; since $xAy = 0$ we see that $cAc = 0$, so, by Lemma 2,

$c=0$. In other words, $yRxA \subset C_R(A) = \{u \in R \mid ua = au, \text{ all } a \in A\}$. Since $(xA)Ay = 0$, by the same argument as that just given shows that $yR(xA)A \subset C_R(A)$. Thus we get that $yRxA[A,A] = 0$; since $(1+t)A[A,A](1+t)^{-1} \subset A[A,A]$ for all t such that $t^2 = 0$, by Lemma 4 we get that $yRx = 0$ or $A[A,A] = 0$. If $A[A,A] = 0$ then, by Lemma 4 again, we end up with $[A,A] = 0$, that is, A is commutative. In this case we are done by Lemma 3. Therefore $yRx = 0$. Since R is prime we conclude that $x = 0$ or $y = 0$.

If $f^2 = f \neq 0, 1 \in RC$, there is an ideal $W \neq 0$ of R with $0 \neq Wf \subset R$ and $0 \neq fW \subset R$. Using this notation we have

LEMMA 6. *If $fW \cap A \neq 0$ and $Wf \cap A \neq 0$ then A contains a non-zero ideal of R.*

Proof. Let $fw \neq 0 \in A \cap fW$; if $V = W^2$ then, for $v \in V$, $fv(1-f) \in R$ has square 0, so by (1), for all $a \in A$, since $fwa \in A$,

$$(fwa)fv(1-f) - fv(1-f)(fwa) - fv(1-f)(fwa)fv(1-f) \in A,$$

which is to say, $fwafV(1-f) \subset A$. Therefore $AfwAfV(1-f) \subset A$.

If $0 \neq uf \in Wf \cap A$, as above we get that $(1-f)VfAuf \subset A$. By Lemma 5, $fAufAfwAf \neq 0$; hence $U = VfAufAfwAfV \neq 0$ is a non-zero ideal of R, $U \subset V \subset W$. However, by what we obtained above, $((1-f)vfAuf)(AfwAfV(1-f) \subset A$, that is, $(1-f)U(1-f) \subset A$.

Thus we have $0 \neq (1-f)W \cap A$ and $W(1-f) \cap A \neq 0$; the argument just given for f applied to $1-f$ gives us that $fU_0 f \subset A$ for some ideal $U_0 \neq 0$ of R, where $U_0 \subset W$. Thus $(1-f)U(1-f)AfU_0 f \subset A$, and since $(1-f)Af \neq 0$ by Lemma 5, we have $(1-f)U_1 f \subset A$ and $fU_1 f \subset fU_0 f \subset A$, where $U_1 = U(1-f)AfU_0$. Thus $U_1 f \subset A$. Similarly we get an ideal $U_2 \neq 0$ with $fU_2 \subset A$. We then have $0 \neq U_1 ffU_2 = U_1 fU_2 \subset A$, so A contains the non-zero ideal $U_1 fU_2$ of R. This proves the lemma.

We keep the notation of Lemma 6.

LEMMA 7. *If $fW \cap A = 0$ then fRC is a minimal right ideal of RC. Similarly, if $Wf \cap A = 0$ then fRC is a minimal right ideal of RC. Furthermore, char $R = 2$, and if $M = fRC$ then* $\mathrm{Hom}_{RC}(M,M) = C$.

Proof. By Lemma 5 there is an $a \in A$ such that $(1-f)af \neq 0$. If $x, v \in V = W^2$ using (4) in the proof of Lemma 3,

$$fv(1-f)afx(1-f) + fx(1-f)afv(1-f) \in A \cap fW = 0.$$

So

$$fv(1-f)afx(1-f) + fx(1-f)afv(1-f) = 0$$

for $x, v \in V$. By a result of Martindale [6], $fx(1-f)\,af=\alpha(x)f$, $\alpha(x)\in C$, for all $x \in V$, and, also, char $R=2$. Hence $fV(1-f)\,af \subset Cf$; now $fx(1-f)\,af=\alpha(x)f \neq 0$ for some $x \in V$ since R is prime. If $y \in V$ then

$$\alpha(yfx)f=f(yfx)(1-f)\,af=\alpha(x)fyf,$$

there $fyf=(\alpha(yfx)/\alpha(x))\,f$, whence $fRCf=Cf$. Thus fRC is a minimal right ideal of RC and if $M=fRC$ then $\mathrm{Hom}_{RC}(M,M)=C$.

Proof of the Theorem

If $e^2=e\neq 0, 1$ is in R and if e is *not* a minimal idempotent of RC then, by Lemma 7, $eR\cap A\neq 0$ and $Re\cap A\neq 0$ (since $W=R$ is an ideal of R such that $Re\subset R$, $eR\subset R$). Thus, by Lemma 6, A contains a non-zero ideal of R.

So, if $A\not\subset Z$ and A does not contain a non-zero ideal of R, we saw in the paragraph above that eRC is a minimal right ideal of RC; thus RC is a primitive ring with minimal right ideal, M, and $\mathrm{Hom}_{RC}(M,M)=C$. If $f\in RC, f^2=f\neq 0, 1$ is *not* a minimal idempotent then, by Lemmas 6 and 7, we are done. So every non-trivial idempotent in RC is minimal. This trivially forces RC to be the ring of all 2×2 matrices over C. So $RC=C_2$.

By Lemma 3 we may assume that A is not commutative, and by Lemma 5 we have that A is prime. Since $A\subset C_2$, A satisfies the polynomial identities of C_2, hence $Z(A)\neq 0$, where $Z(A)$ is the center of A. Since $(1+t)A(1+t)^{-1}\subset A$, and gives an automorphism of A for t such that $t^2=0$, we have that $(1+t)\,Z(A)(1+t)^{-1}\subset Z(A)$. So, if $R\neq (GF(2))_2$, by Lemma 3, $Z(A)\subset Z$ the center of R.

By Posner's theorem [5], A localized at $Z(A)$ is a 4-dimensional simple algebra over the field of quotients, K, of $Z(A)$, and since $Z(A)\subset Z$, lies in $RC=C_2$. Call this localization $Q(A)$; if $Q(A)$ is a 2×2 matrix algebra over K then there is an idempotent f, $f^2=f\neq 0, 1$ in $Q(A)$. But $f=a/\alpha$, where $a\in A$, $\alpha\in Z(A)$; hence $fW\cap A\neq 0$, where $0\neq W$ is an ideal of R such that $fW\subset R$, since $0\neq \alpha f\in fW\cap A$ and $\alpha f\in Wf\cap A$. By Lemma 6, A contains a non-zero ideal of R.

Suppose then that $Q(A)$ is a 4–dimensional division algebra over K. Therefore K is infinite and so $Z(A)$ is infinite. If $\gamma\neq 0, 1\in Z(A)$ and $t^2=0$, then $ta-at-tat\in A$ *and* $(\gamma t)\,a-a(\gamma t)-(\gamma t)\,a(\gamma t)\in A$, that is, $\gamma(ta-at)-\gamma^2 tat\in A$. However, $\gamma a\in A$, so $t(\gamma a)-(\gamma a)\,t-t(\gamma a)\,t\in A$, that is, $\gamma(ta-at)-\gamma tat\in A$. We therefore get that $(\gamma^2-\gamma)\,tat\in A$. But A is a domain, so $(\gamma^2-\gamma)\,tat=0$, and since $\gamma^2-\gamma\neq 0\in Z(A)$, we have $tat=0$ thus $ta-at\in A$; but $(ta-at)^2=-ta^2t\in A$ is nilpotent, so we get ta

$-at = 0$. Thus A centralizes all t such that $t^2 = 0$. By Lemma 1 we conclude that $A \subset Z$. This finishes the proof of the theorem.

A special case of this theorem is of interest, namely,

THEOREM 2. *If R is a simple ring having an idempotent e, $e^2 = e \neq 0, 1$, and if A is a subring of R such that $(1+t)A(1+t)^{-1} \subset A$ for all $t \in R$ such that $t^2 = 0$, then either $A \subset Z$ or $A = R$, except in the one case where R is the ring of all 2×2 matrices over the integers mod 2.*

It might be of some interest to find the analogous theorems if, instead of assuming that A is a subring of R, we merely suppose that A is an additive subgroup of R such that $(1+t)A(1+t)^{-1} \subset A$ for all t such that $t^2 = 0$; if R is prime with $e^2 = e \neq 0, 1$ in R it might be natural to conjecture that either $A \subset Z$ or A contains a non-central Lie ideal of R.

REFERENCES

1. S. A. AMITSUR, Invariant submodules of simple rings, *Proc. Amer. Math. Soc.* **7** (1958), 987–989.
2. W. E. BAXTER, "Lie simplicity of a special class of associative rings, *Proc. Amer. Math. Soc.* **7** (1958), 855–863.
3. JEFFREY BERGEN AND I. N. HERSTEIN, The algebraic hypercenter and some applications, to appear.
4. A. HATTORI, On invariant subrings, *Japan. J. Math.* **21** (1951), 121–129.
5. I. N. HERSTEIN, "Topics in Ring Theory," Chicago Lecture Notes in Mathematics, Univ. of Chicago Press, Chicago, 1969.
6. I. N. HERSTEIN, "Rings with Involution," Chicago Lecture Notes in Mathematics, Univ. of Chicago Press, Chicago, 1976.