INVARIANT SUBMODULES OF SIMPLE RINGS

S. A. AMITSUR

1. In his paper [**4**], I. N. Herstein states as a conjecture the following generalization of the Brauer-Cartan-Hua theorem, "If a subring T of a simple ring A is carried into itself by every automorphism of A, then $T=A$ or T is contained in the center of A."

The results on the Lie-structure of simple rings have been applied in [**2**] to prove this conjecture for simple rings satisfying the descending chain condition (with one exception) (see also [**5**; **6**]). The same method is taken up in this note and we prove this result for a far wider class of simple rings: simple rings which contain at least one idempotent $\neq 1$. Actually, we extend a result of Hattori [**3**] and Theorem 2 of [**2**] to these rings, from which our result follows immediately.

We show also by an example that the conjecture of Herstein is not true in the general case.

2. Let A be a simple algebra over a field $F \neq \mathrm{GF}$ [**2**]. In order that the results obtained here will be valid also for simple rings which do not contain a unit, we extend the meaning of "inner automorphism" to include the quasi-inner automorphism which is defined as follows: let $x \in A$ and let x' be the quasi-inverse of x, that is: $x+x'+xx'=0$; then the mapping: $y \rightarrow y+xy+yx'+xyx'$ is an automorphism of A. Such an automorphism will also be called an inner automorphism. If A contains a unit, denoted by 1, then we have $1+x'=(1+x)^{-1}$ and $y+xy+yx'+xyx'=(1+x)y(1+x)^{-1}$. Thus, in this case, the preceding automorphism is inner in the usual sense.

A subspace M of A is said to be an *invariant subspace* of A if $\sigma(M) \subseteq M$ for every inner automorphism σ of A. We shall use the notation $[x, y]=xy-yx$, and if C and B are subsets of A then $[C, B]$ will denote the module generated by the set $\{[c, b] \mid c \in C, b \in B\}$ over F.

Let $e \neq 1$ be an idempotent of A, then we set $e'=1-e$. If A does not contain the unit 1, we shall still write $ae'=a-ae$ and $e'a=a-ea$ for every $a \in A$.

We shall begin with some lemmas.

LEMMA 1. *Let M be an invariant subspace of A and let $u^2=0$, $u \in A$, then $[M, u] \subseteq M$.*

Received by the editors November 30, 1955.

Indeed, the quasi-inverse of u is $-u$ since $u-u-u^2=0$; hence, $m+um-mu-umu\in M$ for every $m\in M$. Since M is a submodule of A, it follows that $um-mu-umu\in M$. Let $\lambda\in F\neq \mathrm{GF}[2]$ such that $\lambda\neq 0$, 1. Then, since $(\lambda u)^2=0$ it follows that $\lambda um-\lambda mu-\lambda^2 umu \in M$. Consequently, $\lambda^2(um-mu)-\lambda(um-mu)=(\lambda^2-\lambda)\ [u, m]\in M$. Now $\lambda^2-\lambda\neq 0$; hence $[u, m]\in M$.

LEMMA 2. *The elements* $\{x, [x, y]\}$, *where* x *and* y *range over the sets* eAe', $e'Ae$ *generate the module* $[A, A]$.

This lemma is essentially the difference between our proof and the proof of [**2**, Theorem 2].

Every element $a\in A$ can be written in the form $a=eae+eae'+e'ae+e'ae'$. Hence the module $[A, A]$ is generated by elements of the form $[eae, ebe]$, $[eae, ebe']$, $[eae, e'be]$ and similar elements where e and e' change places. Now $[eae, ebe']=eaebe'$; hence, since $AeA=A$ it follows that the set eAe' and similarly $e'Ae$ belongs to $[A, A]$. The elements $[eae', e'be]$ and the similar elements are of the form required in the lemma and we just saw the elements of the form $[eae, e'be]$ are in eAe' or $e'Ae$. It remains, therefore, to show that the elements $[eae, ebe]$ and $[e'ae', e'be']$ are linear combinations of elements $[x, y]$, where x and y are elements of eAe' and $e'Ae$. Indeed, since $Ae'A=A$, it follows that $eAe=eAe'Ae$. Hence, the elements of eAe are linear combinations of elements of the form $eqe'e'pe$. Thus, it suffices to consider only the elements $[eqe'pe, ebe]$. But:

$$[eqe'pe, ebe] = [eqe', e'pebe] - [ebeqe', e'pe] \in [eAe', e'Ae].$$

A similar proof holds for elements of the form $[e'ae', e'be']$.

LEMMA 3. *If* M *is an invariant subspace of* A *then* $[M, [A, A]]\subseteq M$.

Indeed, let x, y be two elements of the sets eAe' and $e'Ae$, then $x^2=y^2=0$. Hence, Lemma 1 shows that $[m, x]$ and $[m, y]$ belong to M for every $m\in M$. Furthermore, $[m, [x, y]]=[[m, x], y]+[x, [m, y]]$. Hence, since $[m, x]$, $[m, y]\in M$, it follows that $[[m, x], y]$, $[[m, y], x]\in M$ and consequently, $[m, [x, y]]\in M$. This in view of Lemma 2 yields that $[M, [A, A]]\subseteq M$.

We apply now Theorem 10a of [**1**], which states: if A is a simple ring which is not a 4-dimensional algebra over a field of characteristic two and T is a submodule of A satisfying $[T, [A, A]]\subseteq T$, then either $T\supseteq [A, A]$ or T is contained in the center of A. We apply this theorem to the module M, and obtain the following extension of [**2**, Theorem 2]:

THEOREM 1. *If* A *is a simple algebra over a field* $F\neq GF[2]$, *contain-*

ing an idempotent $\neq 1$ *and* A *is not a* 4*-dimensional algebra over a field of characteristic two, then the invariant subspaces of* A *either contain* $[A, A]$ *or they are contained in the center of* A.

Similar to the proof of [2, Theorem 3] one obtains:

THEOREM 2. *If* A *satisfies the condition of Theorem* 1 *then the only invariant subalgebras of* A *are* 0, F *and* A.

The following simple proof of this theorem is due to the referee: If S is an invariant subalgebra of A then it follows by the previous theorem that either S is contained in the center of A, or $S\supset[A, A]$. In the first case $S=0$ or $S=F$ and in the latter we show that $S=A$. Indeed, by Lemma 2 it follows that since $S\supset[A, A]$, S contains eAe' and $e'Ae$, hence their products $eAe'Ae=eAe$ and $e'AeAe'=e'Ae'$, so that $S=A$.

3. We conclude this note with an example which disproves the conjecture of Herstein [4]:

Let F be a commutative field of characteristic zero which possesses a nontrivial derivation: $g\rightarrow g'$, e.g. $F=Q(x)$ be the field of all rational functions in a commutative indeterminate x over the rational field Q with the ordinary derivation d/dx. Consider the ring $A=F[t]$ of all differential polynomials in t defined by the relation $gt=tg+g'$. This ring is well known to be a simple ring (e.g. [1]). Since the degree of the product of two polynomials of $F[t]$ is the sum of their degrees, one readily verifies that the set of all invertible elements of $F[t]$ is the field F. Hence F is a subring of $F[t]$ which remains invariant under all automorphisms of $F[t]$. But clearly, $F\not\supset[F[t], F[t]]$ since the latter contains nonconstant polynomials, and F does not belong to the center of $F[t]$ since the derivation of F is nontrivial. This disproves the preceding conjecture.

BIBLIOGRAPHY

1. S. A. Amitsur, *Derivations in simple rings*, Proc. London Math. Soc. (To appear).

2. W. E. Baxter, *Lie simplicity of a special class of associative rings*, Proc. Amer. Math. Soc. vol. 7 (1956) pp. 855–863.

3. A. Hattori, *On invariant subrings* Jap. J. Math. vol. 21 (1951) pp. 121–129.

4. I. N. Herstein, *On the Lie ring of a simple associative ring*, Duke Math. J. vol. 22 (1955) pp. 471–476.

5. L. K. Hua, *A note on the total matrix ring over a non-commutative field*, Annales de la Société Polonaise de Mathématique vol. 25 (1952) pp. 188–198.

6. F. Kasch, *Invariante Untermoduln des Endomorphismenrings eine Vektoraums*, Archiv der Mathematik vol. 4 (1953) pp. 182–190.

HEBREW UNIVERSITY, JERUSALEM, ISRAEL