

CERTAIN SUBMODULES OF SIMPLE RINGS WITH INVOLUTION, II

I. N. HERSTEIN

Let R be a simple ring, of characteristic not 2, having an involution $*$. Let $S = \{x \in R | x^* = x\}$ and $K = \{x \in R | x^* = -x\}$ be the set of symmetric and skew elements, respectively, of R .

In [1] we discuss the structure of S as a Jordan ring and K as a Lie ring. In [2] we considered cross-over submodules, namely additive subgroups $U \subset K, V \subset S$ such that

$$U \circ S = \{ \sum (us + su) | u \in U, s \in S \} \subset U, \text{ and } [V, K] \\ = \{ \sum (vk - kv) | v \in V, k \in K \} \subset V,$$

and characterized these.

For the case of characteristic 3 we did leave open the question of additive subgroups $V \subset S$ such that $[V, K] \subset V$. We point out here that the 3×3 matrices over a field of characteristic 3 do give rise to examples which would not satisfy the dichotomy established in [2] if the characteristic is not 3.

Let F be a field of characteristic 3 and consider $R = F_3$, the 3×3 matrices over F relative to the involution given by transpose. Then, as is readily verified,

$$A = \left\{ \begin{pmatrix} \alpha & \beta & \gamma \\ \beta & \alpha + \beta - \gamma & -\beta - \gamma \\ \gamma & -\beta - \gamma & \alpha + \gamma - \beta \end{pmatrix} \mid \alpha, \beta, \gamma \in F \right\}$$

is a commutative subring consisting of symmetric elements, satisfies $[A, K] \subset A$, yet $A \not\subset F$ the center of R .

The first, and most difficult, theorem of the paper characterizes subrings A , in a simple ring with involution, such that $[A, K] \subset A$. We make use of this result in [3] to extend the Brauer-Cartan-Hua theorem to subdivision rings, in a division ring with involution, which are invariant with respect to conjugation by all the unitary elements.

LEMMA 1. *Let R be a simple ring with involution of the second kind. Suppose that A is a commutative set of elements of R such that $[A, K] \subset A$. Then $A \subset Z$.*

Proof. Since the subring generated by A satisfies the condition imposed on A in the theorem, we may assume, without loss of generality, that A is a subring of R , containing Z .

Received December 11, 1973. This research was supported by NSF Grant GP-2969 at the University of Chicago, and was carried out while the author was a guest at UCLA.

Because $*$ is of the second kind, there is an element $\lambda \in Z$ with $\lambda^* = -\lambda \neq 0$. Thus $S = \lambda K$. Consider $B = A + \lambda A$; it is a subring of R and is commutative. Moreover, $[B, K] \subset B$ since $[A, K] \subset A$. Also, since $[A, S] = [A, \lambda K] = \lambda[A, K] \subset \lambda A \subset B$, and $[\lambda A, S] = [A, \lambda S] = [A, K] \subset A \subset B$ we have that $[B, S] \subset B$. Therefore $[B, R] = [B, S + K] = [B, S] + [B, K] \subset B$, whence B is a Lie ideal of R . But B is also a commutative subring of R . Since $\text{char } R \neq 2$, by [1, Theorem 1.2] we have $B \subset Z$, hence $A \subset Z$.

LEMMA 2. *Let R be a simple ring with involution of the first kind. Suppose that A is a commutative set of symmetric elements such that $[A, K] \subset A$. Then:*

- (1) if $\text{char } R \neq 3$ and $\dim_Z R > 4$, $A \subset Z$;
- (2) if $\text{char } R = 3$ and $\dim_Z R > 9$, $A \subset Z$.

Proof. The subring generated by A satisfies the same condition as A does, hence, without loss of generality, we may assume that A is a subring of R . Furthermore, since the involution is of the first kind, we may assume that $A \supset Z$. Finally, we may assume that $Z = 0$ or that Z is algebraically closed; to see this, if $Z \neq 0$, merely pass to $R \otimes_Z F$ where F is the algebraic closure of Z . Since $\lambda^* = \lambda$ for all $\lambda \in Z$, we can extend $*$ to $R \otimes_Z F$ as $*$ $\otimes 1$.

If $a \in A$ define $d(x) = xa - ax$ for $x \in R$. Our hypothesis tells us that $d^2(k) = 0$ for $k \in K$. If $s \in S$, since $a \in S$ we have $d(s) \in K$, hence $d^3(s) = d^2(d(s)) = 0$. Because $R = S + K$, we get $d^3(x) = 0$ for all $x \in R$. Note that $d^2(x) \in A$ for all $x \in R$.

If $\text{char } R \neq 3$ expanding $d^3(xd(x)) = 0$ using Leibniz' rule yields $3(d^2(x))^2 = 0$, hence $(d^2(x))^2 = 0$. Thus $(d^2(k^2))^2 = 0$ for $k \in K$. But, since $d^2(k) = 0$, $d^2(k^2) = 2d(k)^2$, hence we get $d(k)^4 = 0$.

We claim that if $b \in A$ is nilpotent, then $b^2 = 0$. From the discussion above, $b^3x - 3b^2xb + 3bxb^2 - xb^3 = 0$ for all $x \in R$. If $b^n = 0$, $b^{n-1} \neq 0$, multiplying this above relation from the right by b^{n-1} yields $b^3xb^{n-1} = 0$. Since R is simple and $b^3Rb^{n-1} = 0$, $b^{n-1} \neq 0$, we have $b^3 = 0$. The relation above thus reduces to $3b^2xb = 3bxb^2$; multiplying from the right by b gives $3b^2xb^2 = 0$, and so $b^2xb^2 = 0$. Since $b^2Rb^2 = 0$ and R is simple, we have $b^2 = 0$.

Now, we have seen that $d(k)^4 = 0$ where $d(k) = ak - ka \in A$, for all $a \in A$, $k \in K$. Thus $(ak - ka)^2 = 0$ by the paragraph above. If $t \in K$, $b = ak - ka$ then $bt - tb \in A$ hence $b(bt - tb) = (bt - tb)b$; because $b^2 = 0$ we have $2btb = 0$ and so, $btb = 0$. That is, $bKb = 0$. Also, $(bt - tb)^2 = 0$. Expanding this, using $btb = 0 = b^2$, we get $b^2tb = 0$. Since $\dim_Z R > 4$, by a result of Baxter [1, Theorems 2, 3], the additive group generated by all t^2 , $t \in K$, is S . Hence $bSb = 0$. Since $R = S + K$, we get that $bRb = bSb + bKb = 0$. The simplicity of R forces $b = 0$.

Thus $b = ak - ka = 0$ for all $a \in A$, $k \in K$. This says that A centralizes K . However, since $\dim_Z R > 4$, K generates R [1, Theorem 2.2]. The upshot of this is that $A \subset Z$; this proves the lemma in case $\text{char } R \neq 3$.

Suppose that $\text{char } R = 3$. If $a \in A$ we have seen that $d^3(x) = 0$, where $d(x) = xa - ax$, for all $x \in R$. Because $\text{char } R = 3$, we get from this that

$a^3x = xa^3$ for all $x \in R$, and so, $a^3 \in Z$. In particular, if $a \in A$ then $a^3 = 0$ or a must be invertible. Also, since $Z = 0$ or is an algebraically closed field, $a^3 = \mu^3$ for some $\mu \in Z$. Hence $(a - \mu)^3 = 0$.

Our aim is to show that if $b \in A$ and $b^2 = 0$ then $b = 0$. So, suppose that $b^2 = 0$ for some $b \in A$. As we saw earlier, this gives that $bKb = 0$. If $x \in R$, then $x - x^* \in K$, hence $bx b = bx^*b$ follows. Let $c \in A$, c nilpotent; thus $c^3 = 0$. Now $b(cx)b = b(cx)^*b = bx^*cb = bx^*bc$, whence $bcx b c^2 = bx^*bc^3 = 0$. Since R is simple, we get $bc^2 = 0$. But then $bcx b c = bx^*bc^2 = 0$; we are forced to $bc = 0$. Thus $bc = 0$ for all $c \in A$ which are nilpotent. If $a \in A$ then $(a - \mu)^3 = 0$ for some $\mu \in Z$, hence $b(a - \mu) = 0$, which is to say, $ba = \mu b$.

Let $c = (bk - kb)k - k(bk - kb)$ where $k \in K$. If c is nilpotent for every $k \in K$, by the above we have that $bc = 0$. Evaluating this, using $bkb = b^2 = 0$, we get $bk^2b = 0$. Since $\dim_Z R > 4$, the k^2 span S , hence $bSb = 0$. Together with $bKb = 0$, we end up with $bRb = 0$ and so $b = 0$. So, if $b \neq 0$, we may assume that $c = (bk - kb)k - k(bk - kb) = bk^2 + k b k + k^2b$ is not nilpotent for some $k \in K$. Since $c \in A$, and c is not nilpotent, c must be invertible. Thus, in particular, R must have a unit element.

We return to the relation $bx b = bx^*b$ for all $x \in R$. If $y \in R$ then $b(xby)b = b(xby)^*b = by^*bx^*b = bybxb$. This says that $((bx)(by) - (by)(bx))b = 0$. Let

$$\rho = bR \quad \text{and} \quad T = \{x \in \rho \mid x\rho = 0\}.$$

Thus ρ/T is commutative. From general theory, it is primitive. Hence ρ/T is a field. Again, from general ring theory, we get that R must then have a minimal right ideal, and the commuting ring of R on this right ideal is a field. Since R is simple, has a unit element and a minimal right ideal on which the commuting ring of R is a field we get that R is isomorphic to the $n \times n$ matrices over Z .

We know $bKb = 0$. Also, if $k \in K$ then $(bk - kb)k - k(bk - kb) \in A$ hence $b((bk - kb)k - k(bk - kb)) = \sigma b$ for some $\sigma \in Z$. Evaluating this, using $bkb = b^2 = 0$, we get $bk^2b = \sigma b$. Since the k^2 span S we get $bSb \subset Zb$. Hence $bRb \subset Zb$. This says that b , as a matrix, has rank at most 1. Now we know there is some element $c = bk^2 + k b k + k^2b$ which is invertible; on the other hand, the rank of c is at most 3. The net outcome of this is that $n \leq 3$. This contradicts $\dim_Z R > 9$.

Thus if $b \in A$ and $b^2 = 0$ then $b = 0$. In particular, this says that A has no nilpotent elements. But if $a \in A$ then $(a - \mu)^3 = 0$ for some $\mu \in Z$. Since $a - \mu \in A$ we get $a - \mu = 0$ and so $a = \mu \in Z$. Therefore $A \subset Z$ and the lemma is proved.

Having established the lemma we can pass to our first theorem.

THEOREM 1. *Let R be a simple ring with involution $*$ of characteristic not 2. Suppose that A is a subring of R such that $[A, K] \subset A$. Then:*

- (1) *if A is non-commutative and $\dim_Z R > 16$, $A = R$;*

- (2) if A is commutative, $\dim {}_Z R > 4$ and $\text{char } R \neq 3$, $A \subset Z$;
 (3) if A is commutative, $\text{char } R = 3$ and $\dim {}_Z R > 9$, $A \subset Z$.

Proof. We first argue out the case $A^* = A$, wherein $a^* \in A$ for every $a \in A$.

Let $A^- = A \cap K$. If $A^- = 0$ then every element in A is symmetric, for $a - a^* \in A^-$ if $a \in A$. Thus A is a commutative ring. By Lemma 1 and Lemma 2 we obtain the result. So we may suppose that $A^- \neq 0$.

Certainly $[A^-, K] \subset K$ and $[A^-, K] \subset A$, therefore $[A^-, K] \subset A^-$. Thus A^- is a Lie ideal of K . If $A^- \subset Z$ and if $\lambda \neq 0 \in A^-$ then for every $s \in S \cap A$, $\lambda s \in A^- \subset Z$. This would put $s \in Z$ and so $A = A^- + A \cap S \subset Z$. Hence we may suppose that $A^- \not\subset Z$.

If $\dim {}_Z R > 16$ then, as a non-central Lie ideal of K , by [1, Theorem 2.12], A^- must contain $[K, K]$, hence $A \supset [K, K]$. But $[K, K]$ generates R if $\dim {}_Z R > 4$ [1, Theorem 2.13], resulting in $A = R$. So we may suppose that $\dim {}_Z R \leq 16$. By our assumption on A , A must be commutative in this case.

So, suppose that A is commutative, $\dim {}_Z A > 4$ and $A^- = A \cap K \not\subset Z$. By [1, Theorem 2.9], $a^2 \in Z$ for all $a \in A^-$, hence $a(ak - ka) + (ak - ka)a = 0$ for all $k \in K$. But $ak - ka \in A$ so must commute with a . The net result is that $a(ak - ka) = 0$. If $a^2 \neq 0$ then since $a^2 \in Z$, a is invertible. But then $ak = ka$ for all $k \in K$; because K generates R , we get $a \in Z$. On the other hand, if $a^2 = 0$ then from $a(ak - ka) = 0$ we get $aKa = 0$. If $s \in S$ then $sas \in K$ hence $asasa = 0$. This leads, from $R = S + K$, to $(ax)^3 = 0$ for all $x \in R$. By Levitzki's Theorem [1, Lemma 1.1] this cannot happen in a simple ring. We thus end up with $A \subset Z$.

We have now disposed of the case $A^* = A$. Suppose that $A^* \neq A$. Let $B = A \cap A^*$. Then certainly $B^* = B$ and $[B, K] \subset B$. If A is commutative and $\dim {}_Z R > 4$ or $\dim {}_Z R > 9$ according as $\text{char } R \neq 3$ or $\text{char } R = 3$, or if A is not commutative and $\dim {}_Z R > 16$, by the discussion in the first part of the proof, we have $B \subset Z$ if $A \neq R$.

Let $a \in A$, $k = a^* - a \in K$. Then $ka - ak = a^*a - aa^* \in A$. But since $a^*a - aa^*$ is symmetric, it is also in A^* , hence in B . Thus $\mu = a^*a - aa^* \in Z$. Using the skew element $(a^*)^2 - a^2$, we get $(a^*)^2a - a(a^*)^2 \in A$. But $(a^*)^2a - a(a^*)^2 = 2\mu a^*$; since $(2\mu)^* = 2\mu$, we have $2\mu a^* \in A^*$. Since $2\mu a^* \in A \cap A^* = B \subset Z$ we have $a^* \in Z$ if $\mu \neq 0$, and so $a \in Z$, whence $\mu = a^*a - aa^* = 0$. In other words, $\mu = 0$ and $a^*a = aa^*$ for all $a \in A$.

Linearize $a^*a = aa^*$; this results in $a^*b + b^*a = ab^* + ba^*$ for all $a, b \in A$. Hence $a^*b - ba^* = ab^* - b^*a = -(a^*b - ba^*)^*$; in other words, the element $a^*b - ba^*$ is skew. But $a^*b - ba^* = (a^* - a)b - b(a^* - a) + (ab - ba)$, so is in A . Being skew, it is also in A^* , hence in $A \cap A^* = B \subset Z$. Let $\nu = a^*b - ba^*$; if $\nu \neq 0$ then $S = \nu K$ and $[A, S] = [A, \nu K] = \nu[A, K] \subset A$ since $\nu \in A$ and $[A, K] \subset A$. Therefore $[A, R] \subset A$. Since $\text{char } R \neq 2$ and A is a subring and a Lie ideal of R , by [1, Theorem 1.2], $A \subset Z$ or $A = R$; since $A \neq R$ we get that $A \subset Z$, the desired result. Hence we may assume that $\nu = 0$, which is to say, $a^*b = ba^*$ for all $a, b \in A$.

If A is commutative, then $C = A + A^* + AA^*$ is a subring of R , $C^* = C$ and $[C, K] \subset C$. Since C is commutative we have, under our assumptions, that $C \subset Z$ and so, $A \subset Z$. Thus we may suppose that A is not commutative and $\dim_Z R > 16$.

Let $a, b \in A$ such that $ab - ba \neq 0$. The ring $C = A + A^* + AA^*$ is not commutative, $[C, K] \subset C$ and $C^* = C$, hence $C = R$. Now $k = a^*b - b^*a \in K$, hence $(a^*b - b^*a)a - a(a^*b - b^*a) \in A$; since A^* centralizes A this yields $a^*(ab - ba) \in A$. Therefore, if $c \in A$ we must have $(a^*(ab - ba))c^* = c^*(a^*(ab - ba))$; this results in $(a^*c^* - c^*a^*)(ab - ba) = 0$ for all $a, b, c \in A$. Since $R = A + A^* + AA^*$, given $x \in R$, we can write x as $x = a_1 + a_2^* + \sum u_i v_i^*$ with all of a_1, a_2, u_i, v_i in A . Thus

$$(a^*x - xa^*)(ab - ba) = (a^*a_2^* - a_1^*a^*)(ab - ba) + \sum u_i(a^*v_i^* - v_i^*a^*)(ab - ba) = 0$$

from the above. Let $T = \{y \in R | (a^*x - xa^*)y = 0 \text{ for all } x \in R\}$. T is an ideal of R and, since $ab - ba \neq 0$ is in T , $T \neq 0$. Therefore $T = R$. Since all $a^*x - xa^*$ now must annihilate R , we have $a^*x = xa^*$ for all $x \in R$. This puts a^* , and so a , in Z . However this contradicts that $ab - ba \neq 0$. With this, the proof is complete.

We now continue with a study of subsets of a simple ring with involution which are invariant with respect to other operations with the skew or symmetric elements. The remaining theorems are very much easier than Theorem 1.

THEOREM 2. *Let R be a simple ring with involution, of characteristic not 2, such that $\dim_Z R > 4$. If A is an additive subgroup of R such that $[A, S] \subset A$ then either $A \subset Z$ or $A \supset [R, R]$. In particular, if A is a subring of R such that $[A, S] \subset A$ then either $A \subset Z$ or $A = R$.*

Proof. Since $[A, S] \subset A$, by use of the Jacobi identity we easily get $[A, [S, S]] \subset A$. Since S generates R , by the argument given on [1, p. 43], $[R, S] = [R, R]$. This gives $[R, R] = [S, K] + [S, S] \subset S + [S, S]$. Hence $[A, [R, R]] \subset [A, S] + [A, [S, S]] \subset A$. By [1, Theorem 1.14], we get $A \subset Z$ or $A \supset [R, R]$. If A is a subring and $A \supset [R, R]$ then $A = R$, since $[R, R]$ generates R [1, Corollary to Theorem 1.5]. This proves the theorem.

We now turn to invariance relative to the circle product $a \circ b = ab + ba$. If A and B are additive subgroups of R , by $A \circ B$ we mean the additive subgroup of R generated by all $ab + ba$ where $a \in A$ and $b \in B$.

THEOREM 3. *Let R be a simple ring with involution of characteristic not 2, with $\dim_Z R > 4$. If A is an additive subgroup of R such that $A \circ K \subset A$, then either $A = 0$ or $A = R$.*

Proof. Suppose that $A \neq 0$. If $a \in A$ and $k \in K$ then $(ak + ka)k +$

$k(ak + ka) \in A$, that is, $ak^2 + 2kak + k^2a \in A$. Linearizing this on k , we obtain

$$(1) \quad a(k_1k_2 + k_2k_1) + (k_1k_2 + k_2k_1)a + 2k_1ak_2 + 2k_2ak_1 \in A$$

for $a \in A, k_1, k_2 \in K$.

On the other hand since $k_1k_2 - k_2k_1 \in K$,

$$(2) \quad a(k_1k_2 - k_2k_1) + (k_1k_2 - k_2k_1)a \in A.$$

Adding (1) and (2) yields, using $2K = K$,

$$(3) \quad ak_1k_2 + k_1k_2a + k_1ak_2 + k_2ak_1 \in A.$$

But $(ak_1 + k_1a)k_2 + k_2(ak_1 + k_1a) \in A$, that is

$$(4) \quad ak_1k_2 + k_2k_1a + k_1ak_2 + k_2ak_1 \in A.$$

Subtracting (4) from (3) we obtain $(k_1k_2 - k_2k_1)a \in A$ for all $a \in A, k_1, k_2 \in K$ that is, $[K, K]A \subset A$. However, from this we get that the subring T , generated by $[K, K]$, satisfies $TA \subset A$. Since $\dim_z R > 4$, $[K, K]$ generates R , hence $T = R$ and $RA \subset A$. Also, since $(RA) \circ K \subset A$, we obtain $RAK \subset A$, whence $RAK \subset RA \subset A$. Because K generates R we have $RAR \subset A$. But since $A \neq 0$ and R is simple, $RAR = R$. Thus we get $A = R$.

The final result of the paper concerns invariance relative to circle multiplication with S .

THEOREM 4. *Let R be a simple ring with involution of characteristic not 2, with $\dim_z R > 4$. If A is a subring of R such that $A \circ S \subset A$, then $A = 0$ or $A = R$.*

Proof. Suppose that $A \neq 0$. If $a \neq 0 \in A$ then $(a^* + a)a + a(a^* + a) \in A$, hence $a^*a + aa^* \in A$. Since $a^*a + aa^*$ is symmetric, it must be in A^* hence in $B = A \cap A^*$. Now $B^* = B$ is a subring of R and $B \circ S \subset B$. If $B^+ = B \cap S$, we get that B^+ is a Jordan ideal of S , hence by [1, Theorem 2.6], $B^+ = 0$ or $B^+ = S$. If $B^+ = S$ then B contains the subring generated by S , that is, B contains R . Hence $A \supset R$ and so $A = R$. Thus we may suppose that $B^+ = 0$.

If $B^- = B \cap K$ then $B^- \circ S \subset B^-$; by [2] we get that $B^- = 0$ or $B^- = K$. If $B^- = K$ then $A \supset B \supset R$, since R is generated by K . Thus $B^- = 0$. But $B = B^+ + B^- = 0$. Thus $A \cap A^* = 0$ and so $aa^* + a^*a = 0$ for all $a \in A$.

Linearize $aa^* + a^*a = 0$; this gives $b^*a + ab^* + a^*b + ba^* = 0$ for all $a, b \in A$. Thus $b^*a + ab^* = -(a^*b + ba^*) = -(b^*a + ab^*)^*$ is skew. However, $b^*a + ab^* = (b^* + b)a + a(b^* + b) - (ab + ba)$ so is in A . Being skew, it is also in A^* , hence in $A \cap A^* = 0$. Thus we have $b^*a + ab^* = 0$ for all $a, b \in A$. Thus b^* anti-commutes with a . If $c \in A$ then c^*b^* must commute with a ; but $c^*b^* = (bc)^* \in A^*$, so anti-commutes with a . The net result of this is that $c^*b^*A = 0$ for all $c, b \in A$.

Thus, if $a \in A$, $s \in S$, we have $c^*b^*(as + sa) = 0$. This gives $c^*b^*SA = 0$. Repeating, we get $c^*b^*TA = 0$ where T is the subring generated by S ; since $T = R$ we have $c^*b^*RA = 0$. Because R is simple and $A \neq 0$ this yields $c^*b^* = 0$, hence $bc = 0$ for all $b, c \in A$. Thus $A^2 = 0$.

Since $A(as + sa) \subset A^2 = 0$ for $a \in A$, $s \in S$ we get $ASA = 0$. Repeating, and using that S generates R we end up with $ARA = 0$. Because R is simple, this forces the contradiction $A = 0$. With this the theorem is proved.

A few final remarks might be in order. To begin with, some analogous theorems to the ones we proved here can undoubtedly be proved in the wider context of semi-prime rings which are 2-torsion free. Also, even in this wider setting, one could insist on weaker hypotheses on A in some of these results. Instead of insisting that A be a subring, as we do in Theorems 1 and 4, we should be able to characterize all additive subgroups satisfying $[A, K] \subset A$ or $A \circ S \subset A$ for semi-prime, 2-torsion free rings. Also, one should be able to extend Theorem 1, even in this more general case, to the situation $[A, [K, K]] \subset A$. We shall return to these things another time.

REFERENCES

1. I. N. Herstein, *Topics in ring theory* (University of Chicago Press, Chicago, 1969).
2. ——— *Certain submodules in simple rings with involution*, *Duke Math. J.* 24 (1957), 357–364.
3. ——— *A unitary version of the Brauer-Cartan-Hua Theorem* (to appear).

*University of Chicago,
Chicago, Illinois*