Can. J. Math., Vol. XXVI, No. 4, 1974, pp. 794–799

ON RINGS WITH INVOLUTION

I. N. HERSTEIN

This paper is dedicated in memory of Adrian Albert.

In this note we prove some results which assert that under certain conditions the involution on a prime ring must satisfy a form of positive definiteness. As a consequence of the first of our theorems we obtain a fairly short and simple proof of a recent theorem of Lanski [**3**]. In fact, in doing so we actually generalize his result in that we need not avoid the presence of 2-torsion. One can easily adapt Lanski's original proof, also, to cover the case in which 2-torsion is present. This result of Lanski has been greatly generalized in a joint work by Susan Montgomery and ourselves [**2**].

Let R be a ring, and let $*$ be an involution on R. We let

$$S = \{x \in R | x^* = x\} \quad \text{and} \quad K = \{x \in R | x^* = -x\},$$

and refer to the elements of S and K as the symmetric and skew elements, respectively, of R. We shall also use the notation Z, or sometimes $Z(R)$, to denote the center of R. Finally, we call a ring R a *domain*, even when it is not commutative, if $ab = 0$ in R forces $a = 0$ or $b = 0$.

LEMMA 1. *Let R be a ring with involution $*$, and let $U \neq 0$ be an ideal of R such that $U^* = U$. If $U \cap S = 0$, that is, U has no non-zero symmetric elements, then $U^3 = 0$.*

Proof. If $0 \neq x \in U$ then $x^* \in U^* = U$, hence $x + x^* \in U \cap S = 0$. Thus $x^* = -x$ for every $x \in U$. In particular, since $U \cap S = 0$, we have that $2x = 0$, for x in U, forces $x = 0$. Now if $x \in U$, $x^* = -x$ whence $(x^2)^* = x^2$. By our hypothesis $U \cap S = 0$ we are led to $x^2 = 0$ for every $x \in U$. Since U is without 2-torsion, we get that $U^3 = 0$.

We now prove

THEOREM 1. *Let R be a prime ring with involution $*$ such that no non-zero element of S is nilpotent. Then either*

(1) *$xx^* = 0$ in R implies $x = 0$, or*

(2) *$S \subset Z$ and R is an order in F_2, the ring of all 2×2 matrices over a field F.*

Proof. Suppose that $xx^* = 0$ for some $x \neq 0$ in R; we want to show that $S \subset Z$ and R is an order in F_2.

Now $x^*Sx \subset S$, and from $xx^* = 0$ every element in x^*Sx has square 0. Consequently, from the hypothesis on R, we have $x^*Sx = 0$. If $r \in R$ then

Received October 12, 1972 and in revised form, November 3, 1973. This research was supported by NSF Grant GP-29269.

https://doi.org/10.4153/CJM-1974-074-5 Published online by Cambridge University Press

$x^*(r^* + r)x = 0$, hence $x^*r^*x = -x^*rx$, which is to say, x^*rx is skew for every $r \in R$. Because R is a prime ring, for some $r \in R$, $k = x^*rx \neq 0$. The element k is skew, and $k^2 = 0$. Thus k cannot be symmetric, in consequence of which the characteristic of R is not 2.

Since $0 = k^2 = -kk^*$, as above, we have that $kSk = 0$. If $s \in S$, then $ks - sk \in S$. Moreover, since $k^2 = 0$, and since s, s^2 are both in S, and since $kSk = 0$, we see that $(ks - sk)^2 = 0$. By our hypothesis on S we must have that $ks - sk = 0$ for all $s \in S$. Therefore k commutes with every element in $\bar{S}$, the subring of R generated by S.

By its definition, $\bar{S}$ is a subring of R. Moreover, if $s \in S$ and $y \in R$ then $sy - ys = sy + y^*s - (y + y^*)s$ is in $\bar{S}$. From this it follows that $\bar{S}$ is a Lie ideal of R. Since R is 2-torsion free and has no nilpotent ideals, by [**1**, Lemma 1.3], either $S \subset Z$ or $\bar{S}$ contains a non-zero ideal U or R. This latter possibility implies that k centralizes the non-zero ideal U; in a prime ring this forces k to be in Z. However, since $k \neq 0$ and $k^2 = 0$, this is in contradiction to the fact that k is an element in the center of a prime ring. Hence we are left with the possibility $S \subset Z$.

We claim that in this situation R must be an order in F_2. Since $S \subset Z$ and the elements of Z are not zero divisors in R, we can localize R at the non-zero elements of S to obtain a ring

$$T = \{r/s | r \in R, s \neq 0 \in S\}.$$

T is clearly a prime ring with involution; moreover, its non-zero symmetric elements are invertible in T. We assert that T is simple. If $V \neq 0$ is an ideal of T, then $U = VV^* \neq 0$, and $U^* = U$. By Lemma 1, U has a non-zero symmetric element; this element being invertible in T, we obtain that $U = T$. Since $V \supset U$, we have that $V = T$. In short, T is simple. Since the symmetric elements of T lie in the center of T, by [**1**, Theorem 1.6] we have that T is 4-dimensional over its center. Since T has zero divisors—recall that $xx^* = 0$— it is not a division ring. Thus $T = F_2$, the 2×2 matrices over a field F. By construction, R is an order in T. This completes the proof of Theorem 1.

Before proceeding to a skew analogue of Theorem 1, we use Theorem 1 to derive a result of Lanski [**3**]. First we dispose of the prime case for his theorem.

LEMMA 2. *Let R be a prime ring with involution in which $ab \neq 0$ if $a \neq 0$ and $b \neq 0$ are in S. Then either*

(1) *R is a domain, or*

(2) *$S \subset Z$ and R is an order in F_2, the 2×2 matrices over a field F.*

Proof. Suppose that R is not an order in F_2. By Theorem 1, if $xx^* = 0$ then $x = 0$ in R. Suppose that $uv = 0$, $u, v \in R$. Then $(u^*u)(vv^*) = 0$; since both u^*u and vv^* are in S, either $u^*u = 0$ or $vv^* = 0$. Hence either $u = 0$ or $v = 0$. Thus R must be a domain.

We wish to push Lemma 2 further, to characterize semi-prime rings with involution in which $ab \neq 0$ if $a \neq 0$ and $b \neq 0$ are in S. We already know the story if R is prime—this is Lemma 2. So we may assume that there are ideals $A \neq 0$ and $B \neq 0$ in R such that $AB = 0$.

We claim that $A^*A = 0$. We certainly do have $A^*AB = 0$, hence $0 = (A^*AB)^* = B^*A^*A$. Since R is semi-prime, this relation implies that $A^*AB^* = 0$. Thus $(A^*A)(B + B^*) = 0$. If $A^*A \neq 0$, then, since R is semi-prime, by Lemma 1 there is an element $u \neq 0 \in A^*A$ such that $u^* = u$. Likewise, in B $+ B^*$ there is an element $v \neq 0$ such that $v^* = v$. From $(A^*A)(B + B^*) = 0$ we have $uv = 0$, contradicting our hypothesis on the elements of S. In short, whenever $AB = 0$ with A, B non-zero ideals of R, then $A^*A = 0$. Note that since R is semi-prime, from $A^*A = 0$ we get $A \cap A^* = 0$.

Let $M = \{x \in R | xA = 0\}$; M is an ideal of R and $M \supset A^*$. Since $MA = 0$, by the argument above, $M^*M = 0$. Because R is semi-prime, this yields that $MM^* = 0$. If $Mx = 0$ then $A^*x = 0$ since $M \supset A^*$, hence $x^*A = 0$, and so $x^* \in M$. In other words, M^* is *precisely* the annihilator in R of M.

We claim that R/M^* is a domain. First note that M has no non-zero nilpotent elements. For if $u^2 = 0$, where $u \in M$, then since $uu^* \in MM^* = 0$, and $u^*u \in M^*M = 0$, we get $(u + u^*)^2 = 0$. Since S has no nilpotent elements, $u + u^* = 0$, and so $u = -u^*$ is in $M \cap M^* = 0$. We assert further that M is a domain. For if $uv = 0$ with $u, v \in M$, then since $(vu)^2 = 0$, $vu = 0$. Now $(u + u^*)(v + v^*) = 0$ results because $uv = 0$, $u^*v^* = (vu)^* = 0$ and $uv^* = 0$ and $u^*v = 0$ since they lie in $MM^* = 0$ and $M^*M = 0$ respectively. Our hypothesis on S forces $u + u^* = 0$ or $v + v^* = 0$. Because $M \cap M^* = 0$ these latter relations yield $u = 0$ or $v = 0$. In short, M is a domain.

Suppose that $xy \in M^*$. If m_1, m_2 are in M, then $(m_1x)(ym_2) \in M \cap M^* = 0$. However, M is a domain and m_1x, ym_2 are in M; therefore $m_1x = 0$ or $ym_2 = 0$. This immediately leads to $Mx = 0$ or $yM = 0$; but if $yM = 0$ then, by the semi-primeness of R, $My = 0$. In other words, $xy \in M^*$ implies $Mx = 0$ or $My = 0$; since M^* is the annihilator of M these translate into: $xy \in M^*$ implies $x \in M^*$ or $y \in M^*$, which is to say, R/M^* is a domain. Similarly, R/M is a domain.

Since $M \cap M^* = 0$, R is a subdirect sum of R/M and R/M^*; moreover, the involution $*$ on R interchanges the components of this subdirect sum. We have proved all the pieces of

THEOREM 2 (Lanski). *If R is a semi-prime ring with involution such that $ab \neq 0$ for $a \neq 0$, $b \neq 0$ in S, then*

(1) *R is a domain, or*

(2) *$S \subset Z$ and R is an order in F_2, the 2×2 matrices over a field F, or*

(3) *R is a subdirect sum of a domain and its opposite, with the involution being the exchange involution.*

Note that if R is any ring with involution satisfying the hypotheses of Theorem 2 on S, then the nil radical N of R must satisfy $N^3 = 0$ (Lemma 1). So we could describe R via $N^3 = 0$ and the structure of R/N given in Theorem

2. However, a little more can be said. In order to do this, however, we must strengthen the hypothesis a little. Instead of insisting that certain elements are not zero divisors in appropriate subsets we need that they are not zero divisor on R.

THEOREM 3. *Let R be a ring with involution, and suppose N, the maximal nil ideal of R, is not* 0. *Then, if either*

(1) *$x - x^*$ is not a zero divisor in R for any x such that $x - x^* \neq 0$ or*

(2) *$x + x^*$ is not a zero divisor in R for any x such that $x + x^* \neq 0$, then R/N is commutative.*

Proof. Since $N^* = N$, if $x \in N$ then $x \pm x^* \in N$, so is nilpotent. So if condition (1) is satisfied, $x = x^*$ for all $x \in N$; if condition (2) is satisfied, then $x = -x^*$ for all $x \in N$. In both cases we get that $ay = y^*a$ for all $a \in N$, $y \in R$.

Thus if $y, z \in R$, then $ayz = (yz)^*a = z^*y^*a = z^*ay = azy$, which is to say, $a(zy - yz) = 0$. Hence N annihilates C, the commutator ideal of R. If $C = 0$, R must be commutative, hence so is R/N. If $C \neq 0$, then since $NC = 0$, every element of C is a zero divisor in R. Then, as we did for N, we easily derive that $c(yz - zy) = 0$ for all $c \in C$, $y, z \in R$. This leads to $C^2 = 0$. Hence $C \subset N$ and so R/N is commutative.

We now prove the skew analogue of Theorem 1—actually the hypothesis we use is a little less restrictive than that of Theorem 1.

THEOREM 4. *Let R be a prime ring with involution $*$ such that no non-zero element of the form $x - x^*$ is nilpotent. Then either*

(1) *R is an order in F_2, the 2×2 matrices over a field F, or*

(2) *$xx^* = 0$ in R implies that $x = 0$.*

Proof. Let

$$K_0 = \{x - x^* | x \in R\};$$

if $K_0 = 0$ then every element of R must be symmetric; hence R must be commutative. As a commutative prime ring, R would be an integral domain, hence conclusion 2 of the theorem would hold. Thus we may assume that $K_0 \neq 0$.

Suppose that $xx^* = 0$ for some $x \neq 0$ in R. Then every element in x^*K_0x has square 0; however, since $x^*K_0x \subset K_0$, by our hypothesis on K_0 we have $x^*K_0x = 0$. Thus if $r \in R$, then $x^*rx = x^*r^*x$, that is, $x^*Rx \subset S$. Since R is prime, there is an $r \in R$ such that $s = x^*rx \neq 0$.

Because $s \in S$ and $s^2 = 0$, as above, we arrive at $sK_0s = 0$. Let $k \in K_0$; then $ks + sk \in K_0$. However,

$$(ks + sk)^2 = ksks + sksk + sk^2s + ks^2k = sk^2s$$

since $sK_0s = 0$ and $s^2 = 0$. Thus $(ks + sk)^4 = (sk^2s)^2 = 0$. Since $ks + sk \in K_0$, we conclude that $ks + sk = 0$ for all $k \in K_0$.

https://doi.org/10.4153/CJM-1974-074-5 Published online by Cambridge University Press

At this point we divide the argument according as the characteristic of R is or is not 2.

If the characteristic of R is 2, the above discussion tells us that the element s commutes with all elements $x + x^*$, x arbitrary in R. From [**4**, Theorem 21], it follows easily that either $s \in Z$ or R is an order in a simple algebra Q which is 4-dimensional over its center F. Since s is nilpotent, it cannot be in the center of a prime ring. Thus R is an order in Q which is simple and 4-dimensional over its center F. Since Q has zero divisors, we have that Q is isomorphic to F_2, the 2×2 matrices over the field F. Hence the characteristic 2 case is settled.

Suppose, then, that the characteristic of R is not 2. In this case, since $sk + ks = 0$ for all $k \in K_0$, we immediately also have that $sk + ks = 0$ for all $k \in K$. From this we have that s commutes with all k_1k_2 where $k_1, k_2 \in K$, that is, s centralizes K^2.

Now K^2 is a Lie ideal of R (in fact, so is $K_0{}^2$) for if $k_1, k_2 \in K$ and $y \in R$ then $(k_1k_2)y - y(k_1k_2) = k_1(k_2y + y^*k_2) - (k_1y^* + yk_1)k_2$ and so is in K^2. Thus $\overline{K^2}$, the subring of R generated by K^2, is both a subring and a Lie ideal of R. By, [**1**, Lemma 1.3], either $K^2 \subset Z$ or $\overline{K^2}$ contains a non-zero ideal of R. In this latter possibility, we would have s centralizing a non-zero ideal of R; in a prime ring this forces s to be in Z. Since $s^2 = 0$, this is not possible. Therefore, $K^2 \subset Z$.

Since $K^2 \subset Z$ we immediately have that if $a, b \in K$ then $\lambda a = \mu b \neq 0$ for some $\lambda, \mu \in S \cap Z$.

Localize R at $S \cap Z$; if Q is this localization, then Q is prime, has an involution and the non-zero skew elements of Q are invertible in Q. From this and the paragraph above, the skew elements of Q are central multiples of $a \neq 0$ in K. We claim that Q is simple. For, if $U \neq 0$ is an ideal of Q, then $V = UU^*$ $\neq 0$ satisfies $V^* = V$. If V contains a skew element $b \neq 0$, since b is invertible in Q we get $V = Q$, and so $U = Q$. Thus V contains no non-zero skew elements; thus V is commutative. However, a commutative ideal in a prime ring must be in the center. Hence again we end up with an invertible element in V, whence $V = Q$ and so $U = Q$. Thus Q is simple. Since its skew elements are 1-dimensional over $Z(Q)$, they cannot generate Q. By [**1**, Theorem 2.2], Q must be 4-dimensional over a field. Because R is an order in Q, we have shown the theorem to be correct.

We close the paper with an immediate corollary to Theorem 3. The result is a sharpening of Theorem 1.

COROLLARY. *Let R be a prime ring with involution $*$ such that no non-zero element of the form $x + x^*$ is nilpotent. Then either*

(1) *$xx^* = 0$ in R implies $x = 0$, or*

(2) *$S \subset Z$ and R is an order in F_2, the ring of all 2×2 matrices over a field F.*

Proof. If the characteristic of R is not 2, the hypothesis of the corollary implies that of Theorem 1, and so the corollary is true merely by applying Theorem 1.

On the other hand, if the chacteristic of R is 2, the hypothesis of the corollary reduces to that of Theorem 4, and the result follows as a consequence of Theorem 4.

References

1. I. N. Herstein, *Topics in ring theory* (Univ. of Chicago Press, Chicago, 1969).
2. I. N. Herstein and Susan Montgomery, *Invertible and regular elements in rings with involution*, J. Algebra *25* (1973), 390–400.
3. Charles Lanski, *Rings with involution whose symmetric elements are regular*, Proc. Amer. Math. Soc. *33* (1972), 264–270.
4. Charles Lanski and S. Montgomery, *Lie structure of prime rings of characteristic 2* (to appear).

University of Chicago,
Chicago, Illinois;
Weizmann Institute of Science,
Rehovot, Israel