# A CONDITION FOR THE COMMUTATIVITY OF RINGS

I. N. HERSTEIN

A well-known theorem of Jacobson **(1)** asserts that if every element $a$ of a ring $A$ satisfies a relation $a^{n(a)} = a$ where $n(a) > 1$ is an integer, then $A$ is a commutative ring. Thus the condition used in Jacobson's theorem is a sufficient condition for commutativity. However the condition is by no means a necessary one, as it is satisfied by a very restricted class of commutative rings.

In this paper we weaken Jacobson's condition by insisting that it applies only to commutators, and prove that the final result, namely that the ring is commutative, still remains true. In this way, we modify the assumptions used in Jacobson's theorem and produce a condition which is both necessary and sufficient.

The result might be of interest from, possibly, another point of view. The restrictions heretofore used have applied to subrings of the ring whereas the set we consider here is not even an additive subgroup. This suggests a variety of related problems which might be considered. The result may also play a role in the theory of restricted Lie algebras.

We follow the pattern which has become standard by now of ascending from the case of division rings to the general case of arbitrary rings via the Jacobson structure theory.

We begin with

THEOREM 1. *Let $D$ be a division ring in which $(xy - yx)^{n(x,y)} = (xy - yx)$ for all $x,y \in D$ where $n(x,y) > 1$ is an integer. Then $D$ is a commutative field.*

*Proof.* If $xy - yx = 0$ for all $x,y \in D$ there is, of course, nothing that needs proving. So we assume that for some $a,b \in D$, $ab - ba \neq 0$. Let $Z$ be the center of $D$. If $\lambda \in Z$, then $\lambda(ab - ba) = (\lambda a)b - b(\lambda a)$, so is again a commutator. Thus by hypothesis

$$(1) \qquad (ab - ba)^n = ab - ba, \qquad n > 1,$$

$$(2) \qquad [\lambda(ab - ba]^m = \lambda(ab - ba), \qquad m = m(\lambda) > 1.$$

If we put $S(\lambda) = S = (n - 1)(m - 1) + 1$ then $S > 1$ and we have

$$(1.1) \qquad (ab - ba)^S = (ab - ba)$$

$$(2.1) \qquad [\lambda(ab - ba)]^S = \lambda(ab - ba).$$

Received November 30, 1956. This paper was supported in part by the ONR contract number SAR/Nonr-609(19) with Yale University.

Since $ab - ba \neq 0$ and since $D$ is a division ring, we deduce from (1.1) and (2.1) that $\lambda^{S(\lambda)} = \lambda$ where $S(\lambda) > 1$ for every $\lambda \in Z$. But then $Z$ must be a field of characteristic $p \neq 0$; moreover, $Z$ is algebraic over its prime field $P$, which has $p$ elements.

Let $u = ab - ba \neq 0$. Since $u^n = u$, $u$ is algebraic over $P$, *a fortiori* it is algebraic over $Z$. Without loss of generality we may assume that $u \notin Z$, for if $u \in Z$ then

$$au = a(ab - ba) = a(ab) - (ab)a$$

is not in $Z$ (for otherwise $a \in Z$ and so $ab - ba = 0$ would follow) and we could carry the argument on for the commutator $au$ rather than for $u$. Consequently $u$ satisfies a minimal polynomial over $Z$ of degree

$$t > 1, \quad x^t + \lambda_1 x^{t-1} + \ldots + \lambda_t, \qquad \lambda_i \in Z.$$

Let $F = P(\lambda_1, \lambda_2, \ldots, \lambda_t)$ be the field obtained by adjoining $\lambda_1, \lambda_2, \ldots, \lambda_t$ to $P$. Because the $\lambda_i$ are algebraic over $P$ and commute with each other, $F$ is a finite field and has, say, $q$ elements. Clearly if $w \in F$ then $w^q = w$. Consider the field $F(u)$. The polynomial $x^q - x$ already has $q$ roots in $F$, and since it can have at most $q$ roots in $F(u)$, since $u \notin F \subset Z$, we can conclude that $u^q \neq u$. However,

$$u^t + \lambda_1 u^{t-1} + \ldots + \lambda_t = 0$$

so

$$0 = (u^t + \lambda_1 u^{t-1} + \ldots + \lambda_t)^q = u^{qt} + \lambda_1^q u^{q(t-1)} + \ldots + \lambda_t^q$$
$$= (u^q)^t + \lambda_1 (u^q)^{t-1} + \ldots + \lambda_t.$$

Thus $u$ and $u^q$ are both roots of the same minimal polynomial over $Z$. This implies that there is an element $r \in D$ so that $u^q = rur^{-1}$; that is, $ru = u^q r$. Consequently, $ur \neq ru$ and $(ru - ur)u = u^q(ru - ur)$. Let $y = ur - ru \neq 0$. From the above, $yu = u^q y$. Since $y$ is a commutator, by hypothesis $y^l = y$ for some $l > 1$.

Let

$$T = \left\{ \sum_{i=0}^{l-1} \sum_{j=0}^{n-1} p_{ij} y^i u^j \mid p_{ij} \in P \right\}.$$

$T$ is clearly finite and is an additive subgroup of $D$; by virtue of $yu = u^q y$, $T$ is also closed under multiplication. Hence $T$ is a finite division ring. By Wedderburn's theorem it follows that $T$ is a commutative field. But both $u$ and $y$ are in $T$, so $uy = yu$. Since $yu = u^q y$, $uy = yu$ we obtain $u^q = u$, which contradicts $u^q \neq u$. In this way the proof of Theorem 1 is complete.

We recall that a ring $A$ is a prime ring if $aAb = (0)$ implies that either $a = 0$ or $b = 0$. We now proceed to

LEMMA 2. *Let $A$ be a prime ring in which $(xy - yx)^{n(x,y)} = (xy - yx)$, $n(x,y) > 1$. Then $A$ has no non-zero nilpotent elements.*

https://doi.org/10.4153/CJM-1957-066-0 Published online by Cambridge University Press

*Proof.* If $A$ has nilpotent elements then it has an element $x \neq 0$ such that $x^2 = 0$. If $r \in A$ then $xrx = (xr)x - x(xr)$, so, being a commutator, $(xrx)^n = xrx$ for some $n > 1$. However, $(xrx)^2 \neq xrx^2rx = 0$; whence $0 = (xrx)^n = xrx$. That is, $xAx = (0)$. The primeness of $A$ then forces $x = 0$.

If $e^2 = e$, $e \in A$, it is readily verified that for any $x \in A$, $(xe - exe)^2 = 0$ and $(ex - exe)^2 = 0$. So by Lemma 2 we obtain

LEMMA 3. *If $A$ is as in Lemma 2 then any idempotent in $A$ is in the center of $A$.*

We now go to the next step in the Jacobson structure theory approach and prove

THEOREM 4. *If $A$ is a primitive ring in which $(xy - yx)^{n(x,y)} = (xy - yx)$ for all $x,y \in A$ where $n(x,y) > 1$ is an integer, then $A$ is a commutative field.*

*Proof.* Since $A$ is a primitive ring it possesses a maximal right ideal $\rho$ which contains no non-zero two-sided ideal of $A$. Thus $\rho \cap Z = (0)$ (where $Z$ is the center of $A$) for if $x \in \rho \cap Z$ then $xA = Ax \subset \rho$ is a two-sided ideal of $A$ which is located in $\rho$, so must be $(0)$; by the primitivity of $A$ we must conclude that $x = 0$.

Let $x,y \in \rho$. By the hypothesis, for some $n > 1$, $(xy - yx)^n = (xy - yx)$. But then $e = (xy - yx)^{n-1} \in \rho$ is an idempotent, so it must be in $Z$ by Lemma 3. That is $e \in \rho \cap Z$. By the above remarks this implies that $e = 0$; thus

$$0 = e(xy - yx) = (xy - yx)^n = xy - yx.$$

That is, any two elements of $\rho$ commute with each other. Suppose $a, b \in \rho$ and $r \in A$. Since $ar \in \rho$, $(ar)b = b(ar)$. However, $ab = ba$, so we deduce that $a(br - rb) = 0$ for all $a,b \in \rho$, $r \in A$. Thus $\rho(br - rb) = (0)$, which, in a primitive ring, means that either $\rho = 0$ or $br - rb = (0)$. Thus $b \in Z$, whence $b \in \rho \cap Z$ from which, as before, $b = 0$. But then $\rho = (0)$ is a maximal right ideal in the primitive ring $A$; in consequence $A$ must be a division ring, which, by Theorem 1, must in turn be a commutative field.

If $A$ is a ring semi-simple in the sense of Jacobson then $A$ is isomorphic to a subdirect sum of primitive rings. Each of these primitive rings is a homomorphic image of $A$, and so inherits the property that

$$(xy - yx)^{n(x,y)} = (xy - yx).$$

By Theorem 4 these primitive rings must all be commutative fields, and so we have

THEOREM 5. *If $A$ is a semi-simple ring in which $(xy - yx)^{n(x,y)} = (xy - yx)$ for all $x,y \in A$ then $A$ is commutative.*

We now have all the preliminaries needed to prove the main theorem of this paper, namely

THEOREM 6. *Let $A$ be a ring in which $(xy - yx)^{n(x,y)} = (xy - yx)$ for all $x,y \in A$ where $n(x,y) > 1$ is an integer. Then $A$ is a commutative ring.*

*Proof.* Let $N$ be the radical of $A$. Hence $A/N$ is semi-simple, and so, by Theorem 5, it is commutative. Thus $xy - yx \in N$ for all $x,y \in A$. However, $(xy - yx)^n = (xy - yx)$, so $e = (xy - yx)^{n-1}$ is an idempotent; moreover $e \in N$. But the only idempotent in the radical is 0. So $(xy - yx)^{n-1} = 0$ from which $0 = (xy - yx)^n = (xy - yx)$. Thus $A$ is commutative.

## REFERENCES

1. N. Jacobson, *Structure theory for algebraic algebras of bounded degree*, Ann. Math., *46* (1945), 695–707.

*Yale University*