

## A PROOF OF A CONJECTURE OF VANDIVER

I. N. HERSTEIN

The Wedderburn theorem that every finite division ring is commutative has been extended by several authors [1].<sup>1</sup> Vandiver, in his paper *The  $p$ -adic representation of rings* [2] conjectured the following generalization of Wedderburn's theorem: every finite, non-commutative ring contains an element which is a divisor of zero and is not in the centrum.

In this paper we give a short and simple proof of this conjecture. We also exhibit one generalization of it which was pointed out to us by the referee.

**THEOREM.** *A finite non-commutative ring contains an element which is a divisor of zero and is not in the centrum of the ring.*

**PROOF.** Let  $R$  be the ring,  $C$  its centrum and  $N$  its radical. If every element of  $R$  is a divisor of zero, then the theorem is trivially true. So we may assume that  $D$ , the set of elements in  $R$  which are not divisors of zero, is not empty. We claim that  $D$  is a multiplicative group. For if  $x, y, z \in D$ , then  $xy \in D$ ; and if  $xy = zy$  or  $yx = yz$ , then  $x = z$ . Hence, since  $D$  is finite, it forms a group under multiplication, and so contains a two-sided unit element, 1. We assert that 1 is a unit element for  $R$ . For if  $r \in R$ , then it can be written as  $r = xd$  where  $d \in D$  (since all the left multiples of  $d$  are distinct and so cover all of  $R$ ). Thus  $r1 = (xd)1 = x(d1) = xd = r$ . Similarly 1 is a left unit.

Now if  $R$  contains a nonzero idempotent  $e \neq 1$ , then for all  $x \in R$ ,  $xe(1-e) = x(1-e)e = 0$ , and so if the theorem were false, both  $xe$  and  $x(1-e)$  would be in  $C$ ; hence  $xe + x(1-e) = x$  would be in  $C$ . And thus  $R = C$ , contradicting that  $R$  is non-commutative. Hence we may assume that 1 is the only nonzero idempotent in  $R$ .

Since  $1 \notin N$ ,  $N \neq R$ . Let  $x \notin N$ . Then  $Rx$  is a non-nilpotent left ideal, and so contains a nonzero idempotent [3]; thus  $Rx$  contains 1. That is, if  $X \notin N$ , then  $x$  is regular. Hence  $R - N$  is a finite division ring, which by the Wedderburn theorem is commutative. But the multiplicative group of a finite field is cyclic; that is, there exists an  $\bar{a} \in R - N$  such that for every  $\bar{x} \neq 0$  in  $R - N$ , there exists an integer  $s$  so that  $\bar{x} = \bar{a}^s$ . Let  $a \in R$  map an  $\bar{a} \in R - N$ . Whence for every  $x \in R$ ,  $x \notin N$  we can find an integer  $S$  so that  $a^S - x \in N$ . If  $N$  is not contained

Presented to the Society, February 26, 1949; received by the editors February 17, 1949 and, in revised form, April 25, 1949.

<sup>1</sup> Numbers in brackets refer to the bibliography at the end of the paper.

in  $C$ , then there exists an element  $b \in N$ ,  $b \notin C$  such that  $b^n = 0$ , in which case the theorem would be true. So we may assume that  $N \subset C$ . Since for every  $x \in R$ ,  $x \notin N$  we can find an  $S$  so that  $a^s - x \in N \subset C$ ,  $(a^s - x)a = a(a^s - x)$ ; thus  $ax = xa$ . Also if  $x \in N$ , since  $N \subset C$ ,  $ax = xa$ . Thus  $a \in C$ . Since  $R$  is non-commutative, we can find an  $x \notin C$ . Thus, since  $x \notin N$ , for some integer  $s$ ,  $a^s - x \in N \subset C$ . And so, since  $a \in C$ ,  $a^s \in C$ , we conclude that  $x \in C$ . This is a contradiction; and so we have the theorem.

We are greatly indebted to the referee for pointing out to us the following generalization of the theorem proved above.

**THEOREM.** *Let  $R$  be a ring with the property that every element generates a finite subring. Then  $R$  is commutative if all the divisors of zero of  $R$  are in the centrum.*

**PROOF.** Without loss of generality we may assume that every element has characteristic some power of a fixed prime  $p$ . Let  $A$  be the set of divisors of zero of  $R$  and  $C$  the centrum; by assumption  $A \subset C$ . If  $x \in R$ ,  $x \notin A$ , then  $x = x^{r+1}$  for some integer  $r > 0$ ; and as  $x(x^r b - b) = (bx^r - b)x = 0$  for all  $b \in R$ ,  $x^r = 1$ , the identity of  $R$ . If  $A = (0)$  the theorem follows as a corollary of a theorem of Jacobson [4, Theorem 11, p. 702].

Let us now assume that  $A \neq (0)$ . If  $a \neq 0$  is in  $A$ ,  $c \in R$ , then  $ca \in A$ . Since  $A \subset C$ ,  $(bc - cb)a = 0$  for all  $b, c \in R$ ,  $a \in A$ . Thus  $bc - cb \in A$ , and so  $(bc - cb)^2 = 0$ . For any  $b \in R$ ,  $pb \in A$ , so that  $p(bc - cb) = 0$  for all  $b, c \in R$ . If  $bc - cb = e$ , then  $bc = cb + e$ ,  $e \in A$ ,  $pe = 0$ ,  $e^2 = 0$  and  $(bc)^p = (cb + e)^p = (cb)^p$ . If for  $b, c \in R$ ,  $bc \in A$ , then  $bc = cb$ . If  $bc \notin A$ , then  $(bc)^r = 1$  for some  $r > 0$ . Let  $r = np^k$ ,  $(n, p) = 1$ . Then  $((bc)^n - 1)^q = 0$  for  $q$  some power of  $p$ . Thus  $(bc)^n - 1 \in A$ , and so  $(bc)^n \in C$ . Hence  $b(bc)^n = (bc)^n b$ , and so  $(bc)^n = (cb)^n$ . As  $sn + tp = 1$ ,  $bc = (bc)^{sn}(bc)^{tp} = (cb)^{sn}(cb)^{tp} = cb$ , and the theorem follows.

#### BIBLIOGRAPHY

1. G. E. Forsythe and N. H. McCoy, *On the commutativity of certain rings*, Bull. Amer. Math. Soc. vol. 52 (1946) pp. 523-526.
2. H. S. Vandiver, *The  $p$ -adic representation of rings*, Ann. of Math. vol. 48 (1947) pp. 22-28.
3. R. Brauer, *On the nilpotency of the radical of a ring*, Bull. Amer. Math. Soc. vol. 48 (1942) pp. 752-758.
4. Nathan Jacobson, *Structure theory for algebraic algebras*, Ann. of Math. vol. 46 (1945) pp. 695-707.

UNIVERSITY OF KANSAS