ON THE COMMUTATIVITY OF *J*-RINGS

JIANG LUH

1. Introduction. A ring R is called a J-ring if there exists an integer $n > 1$ such that $x^n = x$ for every $x \in R$. The following beautiful theorem due to Jacobson **(4, 5)** is a generalization of Wedderburn's theorem, which asserts that every finite division ring must be a field.

THEOREM (Jacobson). *Every J-ring is commutative.*

This theorem was established by essential use of Zorn's lemma. Raymond and Christine Ayoub **(1)** have proved this theorem for a certain class of exponents n without recourse to transfinite methods. Herstein **(2, 3)** recently supplied an elegant but elementary proof of the Wedderburn theorem and the Jacobson theorem in the division case.

The purpose of this note is to give an elementary proof of the Jacobson theorem for any value of n. The technique of the present work is somewhat similar to that of Herstein in the division case.

2. Preliminaries. In preparation for the proof of the theorem, we shall first recall the basic concepts and results involved.

A ring R is called a p^k-ring if a prime p and a positive integer k exist such that $x^{p^k} = x$ and $px = 0$ for every $x \in R$.

LEMMA 1. *If x is an element of a ring R such that $x^n = x$ for some integer $n > 1$ and if h and k are positive integers, $h \equiv k \pmod{n-1}$, then $x^h = x^k$.*

This result can be obtained easily by induction; see **(1)**.

LEMMA 2. *Let R be a J-ring. Then R has no nilpotent elements other than zero and every idempotent element is in the centre of R.*

Proof. That R has no nilpotent elements other than zero is obvious. Now, if $e = e^2$ and x are elements of R, then

$$(ex - exe)^2 = (ex - exe)e(x - xe) = (exe - exe)(x - xe) = 0.$$

By noting that R has no nilpotent elements $\neq 0$, we have $ex = exe$. Also, by a precisely similar argument, we obtain that $xe = exe$. Thus, for every $x \in R$, $ex = xe$, i.e. e is in the centre.

LEMMA 3. *Let R be a ring and $a \in R$. If $a^{p^m} = a$ for some prime p and positive integer m, then $a^{p^m - 1}$ is idempotent.*

Received April 6, 1966.

https://doi.org/10.4153/CJM-1967-117-4 Published online by Cambridge University Press

Proof. It is an immediate consequence of Lemma 1 and the fact

$$(p^m - 1)|(2p^m - 2) - (p^m - 1).$$

LEMMA 4. *Let R be a finite p^k-ring. Then R is isomorphic to a direct sum of finitely many division rings.*

Proof. It is easy to see that there are minimal ideals $I_1, I_2, \ldots, I_n$ of R such that

$$R = I_1 + I_2 + \ldots + I_n \quad \text{(direct sum)}.$$

Each I_i is generated by any non-zero element a_i in I_i and hence is generated by an idempotent element, namely, $e_i = a_i^{p^k-1}$. In fact, $I_i = \{re_i | r \in R\} = Re_i$. We need only show that I_i ($i = 1, 2, 3, \ldots, n$) are division rings. Indeed, for any $r \in R$, $e_i(re_i) = (re_i)e_i = re_i^2 = re_i$, so e_i is a left unity of the ring I_i. Moreover, for any $s \in R$ and any non-zero element $re_i \in I_i$, re_i is a generator of the ideal I_i and $re_i s = rse_i = rsr^{p^k-1}e_i = rsr^{p^k-2}e_i re_i \in Re_i re_i$. Hence $I_i = Re_i re_i = I_i re_i$, so I_i is a division ring.

By Wedderburn's theorem and Lemma 4 we immediately have the following lemma.

LEMMA 5. *A finite ring R is a p^k-ring if and only if it is isomorphic to a direct sum of fields of characteristic p.*

LEMMA 6. *A ring R is a J-ring if and only if it is isomorphic to a direct sum of finitely many p^k-rings.*

This lemma has been recently proved by the author of this note. The proof can be found in **(6)**.

3. Proof of the theorem of Jacobson. By virtue of Lemma 6, we need only show that every p^k-ring is commutative.

Let R be a p^k-ring and let a be an arbitrary non-zero element in R. Denote by C the centralizer of a, i.e. $C = \{r | r \in R, ra = ar\}$. To show that R is commutative it will be sufficient to show that $C = R$.

Assume contrarily that $C \neq R$. Then there exists $b \in R$ such that $b \notin C$. Let $e = a^{p^k-1}$ and

$$P = \{0, e, 2e, \ldots, (p-1)e\}.$$

It is easy to see that P is a field isomorphic to the field Z_p of integers modulo the prime number p. Since, by Lemma 3, e commutes with every element in R and $b^{p^k} = b$, the ring $P(b)$ obtained by adjoining b to P is a finite p^k-ring. More precisely,

$$P(b) = \left\{ \sum_{j=1}^{p^k-1} n_j eb^j \,\middle|\, n_j \in Z_p \right\}.$$

From Lemma 5, $P(b)$ is isomorphic to a direct sum of subfields of $P(b)$. Since $eb \in P(b)$ but $eb \notin C$, there exists a direct summand F containing elements which do not commute with a. The multiplicative group of non-zero elements of F must be cyclic generated by f, say. Clearly, $f \notin C$. Suppose that F contains precisely p^m elements. Then $f^{p^m} = f$ and f^{p^m-1} is the unity element of F.

Now, we define a mapping π on R by $\pi(y) = yf - fy$, for all $y \in R$. By a trivial verification we have that

$$\pi^{p^m}(y) = yf^{p^m} - f^{p^m}y = yf - fy = \pi(y)$$

for all $y \in R$. Thus, $\pi^{p^m} = \pi$.

For any $g \in F$, $y \in R$, we obtain

$$\pi(gy) = (gy)f - f(gy) = gyf - gfy = g(yf - fy) = g\pi(y),$$

since g commutes with f.

Now, if we define mapping gI on R by $(gI)(y) = gy$ for all $y \in R$, then $\pi(gI) = (gI)\pi$ for all $g \in R$.

Consider the polynomial $f^{p^m-1}X^{p^m} - f^{p^m-1}X$ over the field F. It has all its p^m roots as the elements of F. Hence

$$f^{p^m-1}X^{p^m} - f^{p^m-1}X = \prod_{g \in F} (f^{p^m-1}X - g).$$

Thus, we get

$$0 = (f^{p^m-1}I)\pi^{p^m} - (f^{p^m-1}I)\pi = \prod_{g \in F} ((f^{p^m-1}I)\pi - gI).$$

If, for every non-zero element $g \in F$, $(f^{p^m-1}I)\pi - gI$ annihilates no non-zero element in $f^{p^m-1}R$, we would have $(f^{p^m-1}I)\pi(y) = 0$, or $yf - fy = 0$ for every $y \in f^{p^m-1}R$. Particularly, for $y = f^{p^m-1}a$, we would have

$$(f^{p^m-1}a)f - f(f^{p^m-1}a) = 0,$$

or $af = fa$. This contradicts the assumption that f does not commute with a. Therefore, there exist $g \neq 0$ in F and $x \neq 0$ in $f^{p^m-1}R$ such that

$$((f^{p^m-1}I)\pi - gI)(x) = 0,$$

or

$$\text{(A)} \qquad xf = fx + gx \in Fx.$$

Here $g = f^t$ for some positive integer $t < p^m$ since the multiplicative group of non-zero elements of F is cyclic generated by f.

Set

$$W = \left\{ \sum_{j=1}^{p^k-1} \sum_{i=1}^{p^m-1} p_{ij} f^i x^i \,\middle|\, p_{ij} \in Z_p \right\}.$$

Obviously, W is closed under addition. W is also closed under multiplication according to (A). Thus, W is a finite p^k-ring and hence by Lemma 5 is commutative.

Since fx^{p^k-1} and xf^{p^m-1} are in W, we have

$$fx^{p^k-1} \cdot xf^{p^m-1} = xf^{p^m-1} \cdot fx^{p^k-1},$$

or $fx = xf$. Thus, from (A), $gx = 0$. But f^{p^m-1} is the unity element of the field F and there is $g' \in F$ such that $g'g = f^{p^m-1}$. We obtain $f^{p^m-1}x = g'gx = 0$. Since $x \in f^{p^m-1}R$, $x = f^{p^m-1}x_1$ for some $x_1 \in R$. It follows that

$$0 = f^{p^m-1}x = f^{p^m-1}x_1 = x,$$

a contradiction. Therefore, $C = R$, and R is commutative.

References

1. R. Ayoub and C. Ayoub, *On the commutativity of rings*, Amer. Math. Monthly, *71* (1965), 267–271.
2. I. N. Herstein, *Wedderburn's theorem and a theorem of Jacobson*, Amer. Math. Monthly, *68* (1961), 249–251.
3. ——— *Topics in algebra* (New York, 1964).
4. N. Jacobson, *Structure theory for algebraic algebras of bounded degree*, Ann. of Math., *46* (1945), 695–707.
5. ——— *Structure of rings*, Amer. Math. Soc. Colloquium Publications, No. 37, rev. ed. (Providence, 1964).
6. J. Luh, *On the structure of J-rings*, Amer. Math. Monthly, *74* (1967), 164–166.

Wright State University,
Dayton, Ohio

https://doi.org/10.4153/CJM-1967-117-4 Published online by Cambridge University Press