CHAPTER III

PROPERTIES OF J - RINGS

The materials of this chapter are drawn from references [4] and [5].

In this chapter, we shall prove two important properties of J - rings that are used in the following chapter. The two properties of J - rings are J - ring has no nonzero nilpotent elements and J - ring is a commutative ring.

Definition 3.1. A ring R with identity is called a J - ring if there exist an integer $n > 1$ such that $x^n = x$ for all $x \in R$.

Definition 3.2. The Jacobson radical of a ring R, denoted by rad R is defined as follows :

$$\text{rad } R = \bigcap \{ M \mid M \text{ is maximal ideal of } R \}.$$

Definition 3.3. An element x of a ring R is said to be an idempotent if $x^2 = x$ and nilpotent if $x^m = 0$ for some positive integer m.

Theorem 3.4. If R is J - ring, then R has no nonzero nilpotent elements.

proof. Let x be a nilpotent element of R, therefore there

exists a positive integer m such that $x^m = 0$. Since R is J - ring, there exists a positive integer $n > 1$ such that $x^n = x$.

Case (1) : $n \geq m$

$$x = x^n = x^m . x^{n-m} = 0$$

Hence $x = 0$

Case (2) : $n < m$

$$0 = x^m = x^n . x^{m-n} = x . x^{m-n}$$

$$= x^{m-n+1}$$

If $m-n+1 \leq n$, then as in case (1) we get $x = 0$.

If $m-n+1 > n$, continue this process until we are in case (1). Thus we conclude that $x = 0$

Theorem 3.5. If the ring R is finitely generated, then each proper right ideal of R is contained in a maximal right ideal.

proof. Let I be any proper right ideal of R, a finitely generated ring, say $R = (a_1, a_2, \ldots a_n)$. We define a family of ideals of R by taking

$$\mathcal{A} = \{ J \mid I \subseteq J \quad J \text{ is a proper right ideal of } R \}$$

This family is obviously nonempty, for I itself belongs to $\mathcal{A}$. Now consider an arbitrary chain $\{I_i\}$ of ideals in $\mathcal{A}$ Claim that $\bigcup I_i$ is again a member of $\mathcal{A}$. To prove this, let the elements a, b $\in \bigcup I_i$ and r $\in$ R. Then there exist indices i and j for which a $\in I_i$, b $\in I_j$. As the collection $\{I_i\}$ forms a chain, either $I_i \subseteq I_j$ or $I_j \subseteq I_i$. Suppose that $I_i \subseteq I_j$, so that both a, b $\in I_j$. But I_j is in right ideal of R, hence a - b $\in I_j \subseteq \bigcup I_i$ and br $\in I_j \subseteq \bigcup I_i$. Therefore $\bigcup I_i$ is a right ideal of R.

Next we must verify that $\bigcup I_i$ is a proper right ideal of R. Suppose not, i.e. assume that $\bigcup I_i = R = (a_1, a_2, \ldots a_n)$. Then, each generated a_k would belong to some right ideal I_{i_k}, there exists right ideal $I_{i'}$ containing all I_{i_k}'s. Thus $a_1, a_2, \ldots a_n$ all lie in $I_{i'}$. Consequently, $I_{i'} = R$. Which is cleary impossible. Therefore $\bigcup I_i \in \mathcal{A}$ and $I \subseteq \bigcup I_i$.

By Zorn's Lemma, the family $\mathcal{A}$ contains a maximal elements M. It follows directly from the definition of $\mathcal{A}$ that M is proper right ideal of the ring R with $I \subseteq M$.

Claim that M is a maximal right ideal. To prove this, suppose that J is any right ideal of R with $M \subset J \subseteq R$. Since M is a maximal element of the $\mathcal{A}$, J can not belong to $\mathcal{A}$. Accordingly, the right ideal J must be improper, which is to say that $J = R$. We can thus conclude that M is a maximal right ideal of R, completing the proof.

Theorem 3.6 In a ring R with identity each proper right ideal is contained in a maximal right ideal.

proof Use theorem 3.5, since $R = (1)$.

Theorem 3.7 Every right ideal I of J - ring R is a two sided ideal of R.

proof By theorem 3.4, R has no nonzero nilpotent element. Indeed, if $x \neq 0$, the condition $x^n = x$ necessarily implies that $x^m \neq 0$, for all $m > 1$. Suppose that e is any idempotent element of R ; then for any $x \in R$.

$$(xe - exe)^2 = (ex - exe)^2 = 0 ,$$

so that $$xe - exe = 0 = ex - exe .$$

Therefore, $$ex = exe = xe ,$$

consequently $e \in \text{cent } R$.

It follows that every idempotent of R must be in the center. Given any $a \in I$, with $a^n = a$, claim that $e = a^{n-1}$ is an idempotent element of R :

$$(a^{n-1})^2 = a^{2n-2} = a^n . a^{n-2}$$

$$= aa^{n-2} = a^{n-1}$$

Hence, $a^{n-1} \in$ cent R and so, for every r in R we get

$$ra = ra^{n-1}a = a^{n-1}ra$$

$$= a(a^{n-2}ra) = ar'$$

where $r' = a^{n-2}ra$.

Let I be a right ideal and $a \in I$, then $ar \in I$, this shows that $ra \in I$, also making I a two - sided ideal of R.

Theorem 3.8. An element of a J-ring is invertible if and only if it belongs to no maximal ideal.

proof. Suppose a is invertible and $a \in M$ a maximal ideal. So there exists $a^{-1} \in R$ such that $a.a^{-1} = 1 \in M$, which implies that M = R, contradict to the maximality of M. Hence $a \notin M$.

To prove the converse, assume that $a \notin M$, for every maximal ideal M. Let I be the right ideal generated by a, by theorem 3.6 I is not a proper right ideal.

Hence $I = R = (a)$. Since $1 \in R$,

therefore $1 = ar$ for some $r \in R$. I

Let J be the left ideal generated by a. Claim that $I = J$.

Since $I = \{ax \mid x \in R\}$, and by theorem 3.7 I is also left ideal, therefore $J \subseteq I$. Similarly we can prove that $I \subseteq J$. Hence $I = J = R$. There exist $s \in R$ such that $sa = 1 = ra$. Obviously $r = s = a^{-1}$. So a is invertible.

We get the following result . The proof of this result is obtained by applying theorem 3.8

Theorem 3.9. Let I be an ideal of J - ring. Then $I \subseteq$ rad R if and only if each element of the coset 1+I has an inverse in R .

proof. We assume that $I \subseteq$ rad R and there is some element $a \in I$ for which 1+a is not invertible. By theorem 3.8 , the element 1+a must belong to some maximal ideal M of the ring R. Since $a \in$ rad R, a is also contained in M, therefore $1 = (1+a) - a$ lies in M.

But this means that M = R , which is clearly impossible.

To prove the converse, suppose that each member of 1+I has an inverse in R, but $I \not\subseteq$ rad R. By definition of rad R, there exists a maximal ideal M of R with $I \not\subseteq M$. Now if a is any element of I which is not in M.

Therefore (M, a) = R .

Then the identity element 1 can be expressed in the form $1 = m+ra$ for suitable choice of $m \in M$ and $r \in R$.

Thus $m = 1 - ra \in 1+I$,

so that m possesses an inverse, which is impossible, since no proper ideal contains an invertivle element.

Therefore $I \subseteq$ rad R .

Corollary 3.10. In J - ring, an element $a \in \text{rad } R$ if and only if $1-ra$ is invertible for each $r \in R$.

proof. Apply theorem 3.9, by letting $I = (a)$.

Corollary 3.11. If R is a J - ring then the only idempotent element in rad R is 0

proof. Let the element $a \in \text{rad } R$ with $a^2 = a$. Taking $r = 1$ in the preceding corollary, we see that $1 - a$ has an inverse in R ; say $(1 - a)b = 1$, where $b \in R$. This leads immediately to

$a = a(1-a)b = (a-a^2)b = 0$, which completes the proof.

Theorem 3.12 Let D be a division ring of characteristic $p > 0$ p a prime. Suppose that $a \in R - \text{cent } (R)$ is such that $a^{p^m} = a$ for some $m > 0$. Then there exists an $x \neq 0 \in R$ for which

1. $xax^{-1} \neq a$

2. $xax^{-1} \in \mathbb{Z}_p(a)$, the extension field obtained by adjoining a to $\mathbb{Z}_p$ the prime subfield.

proof Since $a^{p^m} - a = 0$, a is algebraic over $\mathbb{Z}_p$. The extension field $\mathbb{Z}_p[a]$ is finite field and therefore has p^n elements for some $n \in \mathbb{Z}_+$. Furthermore, each $r \in \mathbb{Z}_p(a)$ satisfies $r^{p^n} = r$. Now, define the function $f : R \longrightarrow R$ by setting

$f(x) = xa - ax$ for all x in R.

Using induction we can prove that

$$f^k(x) = \sum_{i=o}^{k} (-1)^i \binom{k}{i} a^i x\, a^{k-i} \qquad k \geq 1 .$$

When $k = p$ we get

$$f^p(x) = xa^p - a^p x$$

because $p \mid \binom{p}{i}$ for $0 < i < p$. Similarly we get

$$f^{p^n}(x) = xa^{p^n} - a^{p^n} x$$

But $a^{p^n} = a$, $f^{p^n}(x) = xa - ax = f(x)$ for all $x \in R$, i.e. $f^{p^n} = f$.

For each element $r \in \mathbb{Z}_p(a)$, consider the function l_r on R defined by

$$l_r(x) = rx$$

Claim that f commutes with all such l_r.

$$(f \circ l_r)(x) = f(rx) = rxa - a(rx)$$

$$= rxa - rax$$

$$= (l_r \circ f)(x)$$

Therefore $fol_r = l_r of$ for every r in $\mathbb{Z}_p(a)$. From **theorem 2.13**. The polynamial $y^{p^n} - y \in \mathbb{Z}_p[y]$ factors completely in $\mathbb{Z}_p(a)$, we have

$$y^{p^n} - y = \prod_{r \in \mathbb{Z}_p(a)} (y - r)$$

$$= y \prod_{0 \neq r \in \mathbb{Z}_p(a)} (y - r) .$$

This identity requires only that y commute with all elements $r \in \mathbb{Z}_p(a)$. But $fol_r = l_r o f$ and $f^{p^n} = f$, we thereby obtain

$$f^{p^n} - f = f \circ \prod_{0 \neq r \in \mathbb{Z}_p(a)} (f - l_r)$$

If, for every $r \neq 0$ in $\mathbb{Z}_p(a)$, it happens that

$$(f - l_r)(x) = 0$$

implies $x = 0$, this leads $f = 0$. This means that $xa - ax = 0$ for all $x \in R$, hence a lies in the center of R, contrary to hypothesis. Consequently there must exists some $0 \neq r \in \mathbb{Z}_p(a)$ and some $x \neq 0$ in R for which $(f-l_r)(x) = 0$, that is

$$xa - ax = rx \quad \text{and so}$$

$$xax^{-1} = r+a \in \mathbb{Z}_p(a)$$

Since $r \neq 0$, certainly the product $xax^{-1} \neq a$.

Corollary 3.13 As in theorem 3.12, $xax^{-1} = a^k \neq a$ for some integer $k \in \mathbb{Z}_+$.

proof. Since $a^{p^n - 1} = 1$, the element a has finite order as a member of the multiplicative group R^*. Let s be the order of a, then, in the field $\mathbb{Z}_p(a)$, each of the s elements $1, a, a^2, \ldots a^{s-1}$ is a root of the polynamial $y^s - y \in \mathbb{Z}_p(a)$.

This polynomial can possess at most s roots in $\mathbb{Z}_p(a)$ and $1, a, \ldots a^{s-1}$ are all distinct. But $xax^{-1} \in \mathbb{Z}_p(a)$ and clearly

$$(xax^{-1})^s = xa^s x^{-1} = xx^{-1} = 1$$

Consequently $xax^{-1} = a^k$ for some k with $2 \leq k \leq s-1$.

Lemma 3.14. If F is a finite field and $0 \neq \alpha \in F$, then there exist elements $a, b \in F$ such that $\alpha = a^2 + b^2$.

proof. First we consider the case where characteristic $F = 2$. F has 2^n elements and any element of F satisfies the equation

$$x^{2^n} = x$$

so $$\alpha = \alpha^{2^n} = \left(\alpha^{2^{n-1}}\right)^2 .$$

Therefore the lemma is proved by letting $a = \alpha^{2^{n-1}}$ and $b = 0$.

If the characteristic of F is odd prime p, then F will contain p^n elements. Let f be the mapping of F^* into itself defined by

$$f(x) = x^2$$

where F^* denotes the multiplicative group of F.

Then f is a group homomorphism, with

$$\ker f = \{x \in F^* \mid x^2 = 1\} = \{1, -1\} .$$

Since char F $\neq$ 2, 1 and -1 are necessarily distinct. This implies that, for each $\beta \in f(F^*)$ there exist exactly two elements α_1, α_2 in F^* which $\alpha_1^2 = \alpha_2^2 = \beta$, in fact $\alpha_2 = -\alpha_1$. Hence, half of the elements of F^* will be square, call these $\beta_1, \beta_2, \ldots, \beta_k$ where the integer $k = (p^n - 1)/2$. For these elements we are done since $\beta_i = \alpha_i^2 + 0^2$. Given $0 \neq \alpha \in F$, assume that α is not a square and consider the set

$$S = \{\alpha - \beta_i \mid i = 1, 2, \ldots, k\} .$$

If $\alpha - \beta_i$ is not a square for any value of i, then the set S which contains k distinct elements, must coincide with the k non - squares of F^*. But $\alpha \in F^*$, yielding

$$\alpha = \alpha - \beta_i \quad \text{for some choice of } i .$$

Therefore $\beta_i = 0$, contradiction since $\beta_i \in F^*$.

So we can conclude that $\alpha - \beta_i$ is square for some i therefore $\alpha - \beta_i = \beta_j$ for suitable integers i and j.

i.e. $\alpha = \beta_i + \beta_j$.

Thus, α is the sum of two squares in F.

Corollary 3.15 If F is a finite field and $0 \neq \alpha \in F$, then there exist elements a, b in F such that $1 + a^2 - \alpha b^2 = 0$.

proof. From lemma 3.14, there exist elements $c, d \in F$ such that $\alpha = c^2 + d^2$ and either $c \neq 0$ or $d \neq 0$, suppose $c \neq 0$. Since the element $c \in F$, $c^{-1} \in F$ and also $c^{-2} \in F$, let $b^2 = c^{-2}$ and $a = c^{-1}d$. So $a^2 = c^{-2}d^2$.

Therefore $$\alpha b^2 = (c^2 + d^2)\, c^{-2} = 1 + c^{-2}d^2 = 1 + a^2$$

So $$1 + a^2 - \alpha b^2 = 0 .$$

Theorem 3.16 (Wedderbern). Every finite division ring is a field.

proof. Suppose that the theorem is not true for all finite division rings. Let R has minimal order among the set of non commutative division rings, so that any division ring with fewer elements than R will be commutative.

Claim that if there exist elements $a, b \in R$ satisfying $ab^k = b^k a$ and $ab \neq ba$, then $b^k \in$ center of R. To prove this, consider the centralizer of b^k in R.

$$C(b^k) = \left\{ x \in R \mid xb^k = b^k x \right\} .$$

$C(b^k)$ is a division subring of R. If $C(b^k) \subsetneq R$, then by our hypothesis $C(b^k)$ would necessarily be commutative. But a, b both lie in $C(b^k)$ and a, b do not commute. This entails that $C(b^k) = R$ therefore $b^k \in \text{cent } R$

Now, to prove the theorem, since the multiplicative group R^* is finite, every non - zero element of R must have finite order, as a result, the set

$$S = \{ m \in \mathbb{Z}_+ \mid \text{for some } c \notin \text{cent } R \ , \ c^m \in \text{cent } R \}$$

is not empty. Let n be the minimal integer in S. Then there exists an element $a \notin \text{cent } R$ such that $a^n \in \text{cent } R$. We assert that n is a prime number. To prove this, suppose that

$$n = n_1 n_2 \qquad \text{with} \quad 1 < n_1, \ n_2 < n .$$

It would follow that $a^{n_1} \notin \text{cent } R$,

$$(a^{n_1})^{n_2} = a^n \in \text{cent } R ,$$

which implies that $n_2 \in S$, contradicting the minimality of n. Hence n is a prime number.

Apply theorem 3.12 and corollary 3.13 to obtain an element $x \in R^*$ (theorem 3.12) an integer $k > 1$ such that

$$xax^{-1} = a^k \neq a .$$

Observe that

$$x^2ax^{-2} = x(xax^{-1})\,x^{-1} = xa^kx^{-1}$$

$$= (xax^{-1})^k = a^{k^2}$$

so, by induction, $x^{n-1}a\,x^{-(n-1)} = a^{k^{n-1}}$.

Since we know that n is prime, from the Little Fermat Theorem, we know that there exists an integer u satisfying

$k^{n-1} = 1 + un$. Therefore,

$$a^{k^{n-1}} = a^{1+un} = a.a^{un}$$

$$= ar = ra$$

where $r = (a^n)^u \in \text{cent } R$.

Setting $b = x^{n-1}$, we get $ba\,b^{-1} = ra$

and $x \notin \text{cent } R$. Since $xax^{-1} \neq a$, we see that $b \notin \text{cent } R$. Since $ab \neq ba$ implies that $r \neq 1$.

On the other hand, since r and a^n both lie in cent R, thus

$$r^na^n = (ra)^n = (bab^{-1})^n$$

$$= ba^nb^{-1}$$

$$= a^n$$

By the same reasoning $r^n = 1$. Because n is prime, the order of r must be n. Since

$$b^n = r^n b^n = (rb)^n = (a^{-1}ba)^n = a^{-1}b^n a ,$$

we conclude that $ab^n = b^n a$. By our note, since a commutes with b^n but not with b, necessarily $b^n \in \text{cent}R$.

We now assert that whenever an element y of R satisfying $y^n = 1$, then it must be of the form $y = r^i$, where $0 \leq i \leq n-1$. Indeed, the extension field cent R(y) contains at most n roots of the polynomial $z^n - 1$. But, since r is of prime order n, the elements $1, r^2, \ldots . r^{n-1}$ comprise n distinct roots of $z^n - 1$ in this field. Therefore $y = r^i$ for some i. Because $y \in \text{cent}R$, cent R(y) = cent R . Since the multiplicative group of a finite field is cyclic, thus centR is cyclic, say with generator s . Accordingly,

$$a^n = s^j , \quad b^n = s^l$$

for suitable j and l .

Furthermore claim that, n divides neither j nor l . To see this, suppose that $j = nk$; then

$$a^n = s^j = s^{nk}$$

Thus $$a^n(s^{-k})^n = 1 .$$

As the element s lies in cent R we would have $(as^{-k})^n = 1$. Therefore $as^{-k} = r^i$ for some integer i, or $a = r^i s^k \in$ cent R, which is impossible. Therefore n does not divide j, in a similar fashion, one is able to establish that n does not divide l.

Set $c = a^l$, $d = b^j$, then

$$c^n = a^{nl} = s^{jl} = b^{nj} = d^n.$$

From $ba\,b^{-1} = ra$

we get $(ba\,b^{-1})^l = (ra)^l = r^l a^l$

so $ba^l b^{-1} = r^l a^l$

but $a^l = c$

hence $bc\,b^{-1} = r^l c$

and $br^{-l} = cb\,c^{-1}$

$(br^{-l})^j = cb^j c^{-1}$

$b^j r^{-jl} = cb^j c^{-1}$

but $b^j = d$

so $r^{-jl} d = cd\,c^{-1}$

$r^{-jl} dc = cd$.

Let $t = r^{-jl} \in \text{cent}\, R$, therefore $cd = tdc$.

Claim that $t \neq 1$, to prove this, suppose that $r^{-jl} = 1$. This implies that $n \mid jl$, since n is a prime number, either $n \mid j$ or $n \mid l$, resulting in a contradiction. We can also show that

$$t^n = (r^{-jl})^n = (r^n)^{-jl} = 1 .$$

So we produce two elements $c, d \in R$ with the following properties :

1) $c^n = d^n = \alpha \in \text{cent}\, R$

2) $cd = tdc$ with $t \in \text{cent}\, R$

3) $t \neq 1$ but $t^n = 1$.

From the relations, we shall prove by induction that

$$(c^{-1}d)^m = t^{1+2+\cdots+m-1}\, c^{-m} d^m \quad , \quad m \geqslant 2$$

For $m = 2$, $(c^{-1}d)^2 = c^{-1}d\, c^{-1}d = c^{-1}tc^{-1}dd = tc^{-2}d^2$

Assume that it is true for $m = k-1$, $k \geqslant 3$, consider $m = k$

$$(c^{-1}d)^m = (c^{-1}d)^{k-1}(c^{-1}d)$$

$$= t^{1+2+\cdots k-2}\, c^{-(k-1)}\, d^{k-1}\, c^{-1}d$$

$$= t^{1+2+\cdots k-2}\, c^{-(k-1)}\, d^{k-2}\, t\, c^{-1}dd$$

$$= t^{1+2+\cdots k-2}\, t^{k-1}\, c^{-k}\, d^k \quad .$$

Therefore we have $(c^{-1}d)^m = t^{1+2+\ldots m-1} c^{-m} d^m$

$= t^{m(m-1)/2} c^{-m} d^m$

So $(c^{-1}d)^n = t^{n(n-1)/2}$

If n is odd prime, then $(n-1)/2$ is an integer, so

$$t^{n(n-1)/2} = (t^n)^{n-1/2} = 1,$$

which implies that $(c^{-1}d)^n = 1$. Being a solution of the equation $y^n = 1$, it follows as before that $c^{-1}d = r^i \in \text{cent}\, R$ for some choice of i. But then $d^{-1}c = (c^{-1}d)^{-1} \in \text{cent}\, R$ and so using (2) above we get

$$t = c^{-1}tc = (dc^{-1}d^{-1})c$$

$$= dc^{-1}cd^{-1} = 1$$

an obvious contradiction. Thus, the theorem is proved, at least when n is an odd prime.

If $n = 2$, then $t^2 = 1$ and, of course $t \neq 1$ so $t = -1$. Then $cd = -dc \neq dc$, that is $cd \neq -cd$, consequently, the characteristic of R is different from 2. Applying corollary 3.15 to the field cent R, we can find elements x_i $(i=1,2)$ in cent R satisfying

$$1 + x_1^2 - \alpha x_2^2 = 0 \qquad (\alpha = c^2 = d^2)$$

We have

$$(c+dx_1+ cdx_2)^2 = (c+dx_1+ cdx_2)(c+dx_1 + cdx_2)$$

$$= c^2+dx_1c + cdx_2c + cdx_1 + dx_1dx_1 + cdx_2dx_1$$

$$+ c^2dx_2 + dx_1cdx_2 + cdx_2cdx_2$$

$$= c^2 + dcx_1 - dc^2x_2 - dcx_1 + d^2x_1^2 + d^2cx_2x_1$$

$$+ dc^2x_2 - d^2cx_1x_2 - c^2d^2x_2^2$$

$$= c^2+ d^2x_1^2 - c^2d^2x_2^2$$

$$= c^2(1+x_1^2 - \alpha x_2^2)$$

$$= 0$$

which, because R is division ring, leads to $c+dx_1+cdx_2 = 0$.

And

$$c(c+dx_1+ cdx_2) + (c+ dx_1+ cdx_2)\, c = 0$$

$$c^2+ cdx_1+ c^2dx_2 + c^2+ dx_1c + cdx_2c = 0$$

$$2c^2- dcx_1+ c^2dx_2 + dcx_1 - c^2dx_2 = 0$$

Hence $2c^2 = 0$.

Which is a contradiction since char $R \neq 2$ was shown already. This completes the proof of Wedderburn's Theorem.

Theorem 3.17. Let R be a J - ring. If R forms a division ring, then R is commutative.

proof. As a first step, let us show that R is of characteristic $p > 0$, p a prime. If char $R = 2$, then there is nothing to prove; thus it may be assumed that char $R \neq 2$. Consider any element $a \neq 0$ in R, by hypothesis there exists an integer $n > 1$ for which $a^n = a$, hence $(2a)^n = 2a$. From this, we obtain $(2^n - 2)a = 0$, with $2^n - 2 \neq 0$. Therefore, there exists a least positive integer p such that $pa = 0$, which implies that char $R = p$, p a prime by remark 2.3.

Let $\mathbb{Z}_p$ be the prime subfield of R. Since $a^n = a$, the element a is algebraic over $\mathbb{Z}_p$ and hence, the extension $\mathbb{Z}_p(a)$ constitutes a finite field say with p^m elements. In particular, a itself lies in $\mathbb{Z}_p(a)$, so that $a^{p^m} = a$.

If we now assume that $a \notin$ cent R, then all hypothesises of **theorem 3.12** and corllory 3.13 will be satisfied ; thus there exists an element $b \in R$ and an integer $k > 1$ satisfying theorem 3.12

$bab^{-1} = a^k \neq a$. Similar reasoning applied to the extension $\mathbb{Z}_p(b)$ gives that $b^{p^l} = b$ for some integer $l > 1$.

$$\text{Let} \quad W = \left\{ \sum_{i=0}^{p-1} \sum_{j=0}^{p-1} r_{ij} a^i b^j \;\middle|\; r_{ij} \in \mathbb{Z}_p \right\}^{m \quad 1} .$$

Clearly W is a finite set which is closed under addition and multiplication. W is also subring of R, by remark 2.4 W is finite division ring. Hence by Wedderburn's Theorem W is commutative. We have

$$ab = ba \quad , \quad \text{for} \quad a, b \in W$$

contradicting the relation $ba\, b^{-1} = a^k \neq a$.

Hence for every $a \in R$, $a \in \text{cent } R$ so that R must be commutative.

Lemma 3.18. Let R be a J - ring. For all $a, b \in R$, the element ab - ba lies in rad R.

proof. Obviously R has proper ideals, and by theorem 3.6 R has a maximal ideal M. By remark 2.7 $R/_M$ has no nontrival ideals and by remark 2.5 $R/_M$ becomes a division ring. Being a homomorphic image of R, $R/_M$ inherits the property that $x^n = x$. Thus by theorem 3.17 $R/_M$ is commutative. In other words

..

$$(a+M)(b+M) = (b+M)(a+M) \qquad \text{for all } a, b \text{ in } R$$

Or equivalently $ab - ba \in M$. As this relation holds for every maximal ideal of R, it follows that $ab - ba \in \text{rad } R$

Theorem 3.19. (Jacobson) If R is a J - ring, then R is commutative.

proof. Suppose that the element $x \in \text{rad}R$ and $n > 1$ satisfies the property that $x^n = x$ for every x in R. As was shown in theorem 3.7, $e = x^{n-1}$ is an idempotent element. Since radR forms an ideal of R, the element e will be in radR . But according to corollary 3.11 , 0 is the only idempotent belonging to radR ; hence the element

$$e = x^{n-1}$$

$$= 0$$

and so

$$x = x^n$$

$$= x.x^{n-1}$$

$$= 0$$

This implies that $\text{rad}R = \{0\}$. Lemma 3.18 tells us that $ab - ba \in \text{rad } R = \{0\}$ for all a, b in R. The net result is that any two elements of R commute, thereby completing the proof.