CHAPTER V

ON THE STRUCTURE OF P - RINGS

The materials of this chapter are drawn from references [3], [4] and [5].

It is well known that every Boolean ring is isomorphic to a subring of direct sum of rings $\mathbb{Z}_2$. (see reference [5]) In this chapter we will show that a p - ring is isomorphic to a subring of a direct sum of rings $\mathbb{Z}_p$. So to classify p - rings we need only classify subrings of a direct sum of $\mathbb{Z}_p$. The aim of this chapter is to study the problem of classifying those subrings. We do the complete classification for the finite direct sum case.

Definition 5.1. A ring R is called a p - ring if $x^p = x$ and $px = 0$ for every x in R i.e. a p - ring is just a p^k - ring with $k = 1$. Therefore, if $p = 2$ we call it a Boolean ring.

Definition 5.2. A ring R is said to be imbedded in a ring R' if there exists some subring S' of R' such that $R \cong S'$

Definition 5.3. The prime radical of a ring R, denoted by Rad R, is the set Rad R = $\bigcap \{ P \mid P$ is a prime ideal of R $\}$.

If Rad R = $\{0\}$ we say that R is without prime radical or has zero prime radical.

Definition 5.4. Let I be an ideal of the ring R. The nil radical of I is the set $\{ r \in R \mid r^n \in I \text{ for some } n \in \mathbb{Z}_+ \}$

The nil radical of the zero ideal is refered to as the nil radical of the ring R .

Subring of direct sums.

For the theorem given here on subrings of direct sums neither of the rings considered need be commutative.

Theorem 5.5. A necessary and sufficient condition that a ring R be isomorphic to a subring of a direct sum of rings K_i $(i \in I)$ is that for every $b \neq 0$ in R there is a family of homomorphisms $(h_i)_{i \in I}$ where h_i takes R into a subring of K_i such that $h_i(b) \neq 0$ for at least one i .

proof. Consider first the necessity of the condition. Assume that R is isomorphic to a subring of a direct sum of rings K_i $(i \in I)$. Then we may assume that the elements of R are functions f defined on I such that $f(i) \in K_i$. If f in R is not zero, there is some i such that $f(i) \neq 0$. We obtain a homomorphism h_i of R into a subring of K_i by taking correspond to any f in R the value f(i) . So we get $h_i : R \to K_i$ defined by

$$h_i(f) = f(i)$$

Thus h_i is homomorphism and satisfies the condition of the theorem.

Turning now to the sufficiency of the condition, let

$$H = \{ h : R \longrightarrow K_i' \mid h \text{ is homomorphism, } K_i' \text{ is subring of } K_i \}$$

Let $K_h = h(R) \leqslant K_i'$, $i \in I$

Corresponding to each element b of R we define on H the function Y_b with values in K_i $(i \in I)$, as follows :

$$Y_b(h) = h(b)$$

Since h is homomorphism, it follows at once that

$$\begin{aligned} Y_{a+b}(h) &= h(a+b) \qquad a,b \in R \\ &= h(a) + h(b) \\ &= Y_a(h) + Y_b(h) \end{aligned}$$

and

$$\begin{aligned} Y_{ab}(h) &= h(ab) \\ &= h(a)\, h(b) \\ &= Y_a(h)\, Y_b(h) \end{aligned}$$

Let $\phi : R \rightarrow \Sigma \oplus K_i$ defined by

$$\phi(a) = Y_a$$

Thus ϕ is a homomorphism of R into a subring of a direct sum of rings K_i. To prove that this is actually an isomorphism onto its image, we need only show that the function Y_a vanishes identically on H only if a = 0. This follows almost at once, for we have assumed that if $a \neq 0$ there is an h on H such that

$$h(a) = Y_a(h) \neq 0$$

Thus R is isomorphic to a subring of direct sum of rings K_i.

Imbedding Theorem

Theorem 5.6 A p-ring R may be imbedded in a p-ring R^* which contains identity element.

Finite p-rings

To prove the main theorem, we need the following lemmas which the proof can be seen in references [4] and [5].

Lemma 5.7. Let I be an ideal of the ring R, and $S \subsetneq R$ closed under multiplication and disjoint from I then there exist an ideal P which is maximal in the set of ideals which contain I and do not meet S, any such ideal is prime.

Lemma 5.8. The intersection of all prime ideals of R which contain a given ideal I is pricisely the mil radical of I .

Corolly 5.9 The prime radical of a ring R coincides with the nil radical of R that is, the prime radical of R is simply the ideal of all nilpotent elements.

Lemma 5.10. If $\{A_i\}$ is a set of ideals in R having $\{0\}$ as intersection then R is isomorphic to a subring of the direct sum of the rings R/A_i

Theorem 5.11. A commutative ring R with more than one element is isomorphic to a direct sum of a finite number of fields if and only if it has zero prime radical and contains a finite number of ideals.

proof. To show sufficiency, assume that R has zero prime radical and only a finite number of ideals.

Case (1) If R has no zero divisor, by theorem 2.8, any integral domain with more than one element and only a finite number of ideals is a field, so the conclusion of the theorem is immediate.

Case (2) If R has zero divisors; that is (0) is not a prime ideal in R. Since R has zero prime radical, there exists a set of prime ideals in R having $\{0\}$ as intersection. Furthermore, since this set is necessarily finite, we may assume that if any one of these prime ideals is omitted, the intersection of the others is different from $\{0\}$. Since if

$$A_1 \cap A_2 \cap \ldots \cap \widehat{A_i} \ldots \cap A_n = \{0\},$$

we can find a set say $\{A_1, A_2, \ldots A_k\}$ s.t. this set is the smallest set such that $A_1 \cap A_2 \ldots \cap A_k = \{0\}$, That is

$$A_1 \cap A_2 \ldots \cap \widehat{A_i} \ldots \cap A_k \neq \{0\}.$$

So we may obtain a set of prime ideals A_j $(j = 1, \ldots k)$ having $\{0\}$ as intersection, s.t. none of them is $\{0\}$ or R and having the property that if A_i is any ideal of this set, there is an element of R which is not in A_i but in all A_j for $j \neq i$.

Since $A_i \neq R$, and is a prime ideal, R/A_i is an integral domain with more than one element. Furthermore, under the usual homomorphism $x \rightarrow \bar{x}$ of R onto R/A_i, different ideals in R/A_i have different inverse images in R. Since R has only a finite number of ideals, R/A_i also has a finite number of ideals, and by theorem 2.8 shows that R/A_i is a field. By lemma 5.10, the correspondence

$$x \longleftrightarrow (\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_k) \qquad \text{———— (1)}$$

defines an isomorphism of R with a subring of a direct sum of the fields R/A_i, $\bar{x}_i$ being the residue class to which x belongs modulo A_i. We now show that by this correspondence every element of the direct sum of the fields R/A_i appears as the image of an element of R, and hence that R is isomorphic to the direct sum of the fields R/A_i.

Let $(\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_k)$ be any element of this direct sum and let b_i be an element of R which is not in A_i but in all A_j for $j \neq i$. Such an element exists since if any one of those prime ideals is omitted, the intersection of the others is different from zero. Then $b_i \neq 0$, and since R/A_i is a field there is an element $\bar{x}_i$ of R/A_i such that $\bar{b}_i \bar{x}_i = \bar{a}_i$. Futhermore by the correspondence (1)

$$b_i \longleftrightarrow (0, \ldots \bar{b}_i, 0, \ldots 0)$$

b_i corresponds to an element with $\bar{b}_i$ in the i-th place and zero elsewhere.

If then x_i is any element of R in the residue class $\bar{x}_i$ modulo A_i we see that

$$b_1 x_1 + b_2 x_2 + \ldots b_k x_k \longleftrightarrow (\bar{b}_1 \bar{x}_1, \ldots \bar{b}_k \bar{x}_k)$$

$$\longleftrightarrow (\bar{a}_1, \bar{a}_2, \ldots \bar{a}_k)$$

That is for every $(\bar{a}_1, \bar{a}_2, \bar{a}_3, \ldots \bar{a}_k)$ belonging to the direct sum of the field R/A_i $(i = 1, \ldots k)$.

To prove the other part of the theorem, suppose that R is isomorphic to the direct sum of a finite number of field F_i $(i = 1, \ldots k)$

First we must prove that R has no nonzero nilpotent element. Let $x \in R$ be any nilpotent element. So

$$x = (x_1, x_2, \ldots x_k) \qquad x_i \in F_i$$

And $x^n = (x_1^n, x_2^n, \ldots x_k^n) = 0$ for some $n \in \mathbb{Z}_+$

Then $x_i^n = 0 \quad \forall i$

Since $x_i \in F_i$ which is field, therefore $x_i = 0 \ \forall i$

Hence $x = 0$.

That is, R has no nonzero nilpotent element, so R has zero nil radical and by **corollary 5.9 R has zero prime** radical.

It remains to show that R has only a finite number of ideals. Claim that every ideal in $F_1 \oplus \ldots \oplus F_k$ is of the form $I_1 \oplus I_2 \oplus \ldots \oplus I_k$ where I_i is an ideal of F_i.
Consider the homomorphism

$$(s_1, s_2, \ldots, s_k) \longrightarrow s_i \qquad \text{——— (2)}$$

of $F_1 \oplus F_2 \oplus \ldots \oplus F_k$ onto F_i

Let I be an ideal of $F_1 \oplus \dots \oplus F_k$ and I_i be the image of I under the homomorphism in (2) , that is I_i consists of all element of F_i which are image of the element of I , then I_i is an ideal in F_i . Hence $I \subseteq I_1 \oplus I_2 \oplus \dots \oplus I_k$.

Consider the ideal I_1 in F_1 . If b_1 is any element of I_1 there exists an element of I with b_1 in the first position say $(b_1, b_2, \dots b_k)$. Since $(b_1, b_2, \dots b_k)(e_1, 0, \dots 0) = (b_1, 0, \dots 0) \in I$, I contains all elements of the form $(b_1, 0, \dots 0)$. Similarly I contains all element of the form $(0, b_2, \dots 0)$, $b_2 \in I_2$ and so on. Hence I contains all sum of these elements that is $I_1 \oplus I_2 \oplus \dots \oplus I_k \subseteq I$.

So $$I = I_1 \oplus I_2 \oplus \dots \oplus I_k .$$

Since the only ideals in F_i are (0) and F_i . It is clear that the number of ideals is finite. Hence the isomorphic ring R has only a finite number of ideals, and so the proof of the theorem is completed.

<u>Theorem 5.12.</u> Every finite p - ring contains an identity and is a direct sum of fields Z_p .

proof. Let R be a p - ring containing a finite number of elements. By theorem 3.19, theorem 3.4 and theorem 5.6, R is commutative ring, R has no non zero nilpotent elements and R contains an identity respectively. Thus R is commutative ring with more than one element has zero prime radical and contains a finite number of ideals. By theorem 5.11 R is a direct sum of a finite number of fields. These fields, being subrings of R, are clearly p - rings also.

We will be done if we can show that $\mathbb{Z}_p$ is the only field which is a p - ring. Suppose S is such a field, the unit element of S being denote by e . Let

$$S^* = \{ m e \mid m = 0, 1, \dots p-1 \}$$

Clearly S^* is subfield of S. The mapping $f : S^* \longrightarrow \mathbb{Z}_p$ defined by

$$f(me) = m \qquad \text{for all } m \in \mathbb{Z}_p$$

is an isomorphism of S^* onto $\mathbb{Z}_p$. Since any finite field with p^n elements is a splitting field of the polynomial $f(x) = x^{p^n} - x \in \mathbb{Z}_p[x]$, therefore the finite field $\mathbb{Z}_p$ is the splitting field of the polynomial

$$x^p - x = \prod_{r_i \in \mathbb{Z}_p} (x - r_i)$$

or

$$x^p - x \equiv x(x-1)(x-2)(x-3) \dots (x-(p-1)) \mod p$$

Since S is a p - ring, every a belonging to S satisfies the equation

$$x^p - x = 0$$

Thus $x^p - x = x(x-e)(x-2e) \dots [x-(p-1)e] = 0$.

There exists a unique monic irreducible polynomial $f(x) \in S^*[x]$ s.t. $f(a) = 0$ and $f(x)$ divides $x^p - x$. Therefore $f(x)$ is one of its linear factors, and thus a is an element of S^* . So $S \subseteq S^*$, hence $S = S^* \cong \mathbb{Z}_p$.

<u>Remark</u> Let R be any p - ring containing an identity e and let a be any element in R. We denote by $< a, e >$ the ring generated by a and e consisting of all polynomials in a and e. Since $a^p = a$ and $pa = 0$, this ring is finite, and since it is a p - ring with identity it is expressible as a direct sum of field $\mathbb{Z}_p$. Thus there exists a set of non - zero elements $e_1, e_2, \dots e_r$ of $< a, e >$ such that

$$e = e_1 \oplus e_2 \oplus \dots \oplus e_r \quad \text{and}$$

$$e = eoe = e_1^2 + e_2^2 + \dots + e_r^2 .$$

Thus $e_i^2 = e_i$ and $e_i \cdot e_j = 0 \quad (i \neq j)$ ——— (3)

Let $x \in \langle a, e \rangle$, thus

$$x = x_1 \oplus \dots \oplus x_r \qquad x_i \in \mathbb{Z}_p$$

$$= x_1 e_1 \oplus x_2 e_2 \oplus \dots \oplus x_r e_r .$$

Therefore every element of $\langle a, e \rangle$ is expressible as a linear combination of the elements e_i $(i = 1, \ldots r)$ with coefficients in $\mathbb{Z}_p$. Furthermore the elements e_i are linearly independent over $\mathbb{Z}_p$. We shall call this set a basis of $\langle a, e \rangle$

Infinite p - rings.

Existence of homomorphism.

Let R be an arbitrary p - ring containing an identity e and S be a subring of R with contain e. If a is an element of R not in S, denote by S(a) the subring generated by S and a. The elements of the ring S(a) are expressible as polynomials in a having coefficients in S with degree at most p-1. Now let $e_i (i = 1, \ldots n)$ be a basis of $\langle a, e \rangle$ as in the remark. Each integral power of a is a linear combination of the e_i's with coefficients in $\mathbb{Z}_p$, and since e is also such a linear combination, each element b of S(a) may be written in the form

$$b = b_1 e_1 \oplus b_2 e_2 \oplus \cdots \oplus b_n e_n \qquad (4)$$

the coefficients b_i being elements of S .

If $c = c_1 e_1 \oplus c_2 e_2 \oplus \cdots \oplus c_n e_n$ is another element of S(a) it follows that

$$b + c = (b_1 + c_1)e_1 \oplus (b_2 + c_2)e_2 \oplus \cdots \oplus (b_n + c_n)e_n$$

$$bc = (b_1 c_1)e_1 \oplus \cdots \oplus (b_n c_n)e_n .$$

If $b = 0$, **it follows** from (3), (4) that

$$0 = e_i b = e_i b_i \quad \text{and thus}$$

$$b_1 b_2 \cdots b_n = b_1 b_2 \cdots b_n (e_1 \oplus \cdots \oplus e_n) = 0 .$$

So $e_i b = 0 \Longrightarrow b_1 b_2 \cdots b_n = 0$ ——— (5)

We use this part to prove the following lemma.

Lemma 5.13. Let S be subring of R containing the identity e of R, and let h be a given homomorphism $S \longrightarrow \mathbb{Z}_p$. Then there exists a homomorphism $h' : S(a) \longrightarrow \mathbb{Z}_p$ extending h. $\forall a \in R$.

proof. If $a \in S$, we done since $S(a) = S$. So assume that $a \notin S$. The symbol P_r will be used to represent the direct sum of the given ring S r times, the elements of P_r being denoted by $(b_1, b_2, \ldots b_r)$, where each b_i is an element of S. In like manner C_r will be used to represent the direct sum of the ring $\mathbb{Z}_p$ r times. Let

$$K = \{(b_1, b_2, \ldots, b_r) \in P_r \text{ s.t. } b_1 e_1 \oplus b_2 e_2 \oplus \cdots \oplus b_r e_r = 0$$

Claim that K is an ideal in P_r. To prove this let $b \in K$, $c \in P_r$

$$bc = (b_1, b_2, \dots b_r)(c_1, c_2, \dots, c_r)$$

$$= (b_1c_1, b_2c_2, \dots b_rc_r)$$

$$(b_1e_1 \oplus b_2e_2 \oplus \dots \oplus b_re_r)(c_1e_1 \oplus \dots \oplus c_re_r) = 0$$

$$b_1c_1e_1 \oplus \dots \oplus b_rc_re_r = 0$$

Thus $bc = (b_1c_1, b_2c_2, \dots b_rc_r) \in K$

Now h induced a homonorphism $(b_1, b_2, \dots b_r) \longrightarrow (b_1^*, b_2^*, \dots b_r^*)$ from P_r to C_r, where $b_i \longrightarrow b_i^*$ by h.

Denote by L the ideal in C_r which is the image of K under the induced homomorphism. Claim that the ideal L cannot contain $(1, 1, \dots 1)$. For if $(b_1, b_2, \dots b_r) \longrightarrow (1, 1, \dots 1)$.

Then $(h(b_1), h(b_2), \dots h(b_r)) = (1, 1, \dots 1)$

$$h(b_1) . h(b_2) \dots . h(b_r) = 1$$

$$h(b_1 b_2 \dots b_r) = 1$$

Thus $b_1 b_2 \dots b_r \neq 0$

From (5) $b_ie_i \neq 0 \quad \forall i = 1, \dots r$.

Hence $b_1e_1 \oplus \dots \oplus b_re_r \neq 0$, therefore $(b_1, b_2, \dots b_r) \notin K$ which is a contradiction. The ideal L cannot contain $(1, 1, 1, \dots 1)$, therefore L does not include all of C_r. Claim that L consists of all elements $(x_1, x_2, \dots x_r)$ such that for a certain fixed set of i's, $x_i = 0$, and for the remaining i's, x_i may take any value in $\mathbb{Z}_p$.

For if $L = \{(x_1, x_2, \dots x_r) \mid x_i \neq 0 \ \forall \ i = 1, \dots r\}$.

Let $K \ni (b_1, \dots b_r) \longrightarrow (x_1, x_2, \dots x_r) = (h(b_1), h(b_2), \dots h(b_r))$

$$0 \neq x_1 x_2 \dots x_r = h(b_1)\, h(b_2) \dots h(b_r)$$

$$= h(b_1 b_2 \dots b_r)$$

Thus $b_1 \dots b_r \neq 0$ which is impossible.

Since L is not identical with C_r, we may assume that L consists of all elements $(0, \dots 0, x_k, \dots x_r)$ where $k > 1$ and $x_k, x_{k+1}, \dots x_r$ are arbitrary elements of $\mathbb{Z}_p$. We now set up the homomorphism

$$b = b_1 e_1 \oplus b_2 e_2 \oplus \dots \oplus b_r e_r \longrightarrow b_1^* \qquad \text{——— (6)}$$

for any $b \in S(a)$.

Claim that this is the required homomorphism. $h' : S(a) \longrightarrow \mathbb{Z}_p$. First to prove that h' is well - defined. For any given element b of S(a), if b can also expressed as $c_1 e_1 \oplus \dots \oplus c_r e_r$, it follows that

$$(b_1 - c_1) e_1 \oplus (b_2 - c_2)\, e_2 \oplus \dots \oplus (b_r - c_r) e_r = 0$$

Therefore $[(b_1-c_1), (b_2-c_2), \ldots (b_r-c_r)] \in K$, that implies $[(b_1-c_1)^*, (b_2-c_2)^*, \ldots (b_r-c_r)^*] \in L$ or $[(b_1^*-c_1^*), (b_2^*-c_2^*), \ldots, (b_r^*-c_r^*)] \in L$.

From the form we have assumed L to have, it follows that $b_1^*-c_1^* = 0$ and hence $b_1^* = c_1^*$

Thus (6) defines a homomorphism $S(a) \to Z_p$. If x is any element of S, then from (6) we find

$$x = xe = x(e_1 \oplus e_2 \oplus \ldots \oplus e_r) \longrightarrow x^*$$

and the homomorphism h' coincide with h on S. This completes the proof.

To prove the main theorem for infinite p - rings, we need some definitions and lemmas as follows :

Definition 5.14. Let S be a subring of a ring R. For any $b \in R - S$, we shall denote the subring generated by S and b by S(b), i.e. $S(b) = \langle S \cup \{b\} \rangle$

Definition 5.15. Let γ be an ordinal. By a γ - sequence in a ring R we mean a one - to - one function a on γ into $R - \{0, e\}$ where e is identity of R. Given a γ - sequence in R and $\beta < \gamma$, we define a subring S_β as follows :

$$S_\beta = \langle e \rangle \qquad \text{if } \beta = 0$$

$$S_\beta = \langle S_0 \cup \{a_\alpha \mid \alpha < \beta\} \rangle$$

$\{S_\beta\}_{(\beta<\gamma)}$ will be called the γ - sequence of subrings determined by the γ - sequence $\{a_\alpha\}_{(\alpha<\gamma)}$.

Lemma 5.16. Let R be a ring containing an identity e and γ be an ordinal. Let $\{S_\alpha\}_{(\alpha<\gamma)}$ be a family of subrings of R such that for each $\alpha < \beta < \gamma$, $S_\alpha \subset S_\beta$. For each α such that $\alpha + 1 < \gamma$, let a_α be an element of $S_{\alpha+1}$ such that $a_\alpha \notin \bigcup_{\eta<\alpha} S_\eta$. If $\xi \leq \gamma$ is a cardinal number then $\xi \leq \overline{\overline{\bigcup_{\alpha<\xi} S_\alpha}}$, where $\overline{\overline{\bigcup_{\alpha<\xi} S_\alpha}}$ denotes the cardinal number of $\bigcup_{\alpha<\xi} S_\alpha$

proof. If ξ is finite then

$$\{0, e, a_0, a_1, \ldots a_{\xi-3}\} \subseteq S_{\xi-1}$$

$$= \bigcup_{\alpha<\xi} S_\alpha$$

Hence $\xi \leq \overline{\overline{\bigcup_{\alpha<\xi} S_\alpha}}$

If ξ is infinite cardinal by theorem 2.27, ξ is limit ordinal.

Since $\{a_\alpha\} \subseteq S_{\alpha+1}$

$$\bigcup_{\alpha<\xi}\{a_\alpha\} \subseteq \bigcup_{\alpha<\xi} S_{\alpha+1}$$

Since ζ is limit ordinal, $\bigcup_{\alpha<\zeta} S_{\alpha+1} = \bigcup_{\alpha<\zeta} S_\alpha$,

hence $\bigcup_{\alpha<\zeta} \{a_\alpha\} \subseteq \bigcup_{\alpha<\zeta} S_\alpha$

Therefore $\overline{\overline{\bigcup_{\alpha<\zeta} \{a_\alpha\}}} \leq \overline{\overline{\bigcup_{\alpha<\zeta} S_\alpha}}$

Since $\{a_\alpha\}_{(\alpha<\zeta)}$ is equipotent to ζ , hence

$$\zeta = \overline{\overline{\bigcup_{\alpha<\zeta} \{a_\alpha\}}}$$

Thus $\zeta \leq \overline{\overline{\bigcup_{\alpha<\zeta} S_\alpha}}$

<u>Theorem 5.17</u>, Given a ring R containing an identity e, then there exists an ordinal γ and a γ - sequence $\{a_\alpha\}_{(\alpha<\gamma)}$ in R such that the γ - sequence $\{S_\alpha\}_{(\alpha<\gamma)}$ of subrings of R determined by $\{a_\alpha\}_{(\alpha<\gamma)}$ has the property that $\bigcup_{\alpha<\gamma} S_\alpha = R$

<u>proof</u>. In the case that $R = \langle e \rangle$, take the ordinal $\gamma = 1$.

$$S_0 = \langle e \rangle = R .$$

Assume that $R \neq \langle e \rangle$. First we shall show that there exists an ordinal γ and a family of subrings $\{S_\alpha\}_{(\alpha<\gamma)}$ such that if $\alpha < \beta < \gamma$ then $S_\alpha \subset S_\beta$ and $\bigcup_{\alpha<\gamma} S_\alpha = R$

Let C be a choice fn. for R. Let β be any nonzero ordinal such that the subrings S_α have been defined for all $\alpha < \beta$ and $R - \bigcup_{\alpha<\beta} S_\alpha$ is not empty.

Case 1 $\beta = \delta + 1$ for some ordinal δ,

then $b_\delta = C(R - \bigcup_{\alpha<\beta} S_\alpha)$

and we define $S_\beta = \langle S_0 \cup \{b_\alpha \mid \alpha < \beta\} \rangle$.

Case 2 β is a limit ordinal. Define

$$S_\beta = \bigcup_{\alpha<\beta} S_\alpha$$

$$b_\beta = C(R - S_\beta) .$$

We claim that there exists an ordinal γ such that

$$R - \bigcup_{\alpha<\gamma} S_\alpha = \emptyset .$$

Suppose the contrary, i.e. for all γ, $\bigcup_{\alpha<\gamma} S_\alpha \subset R$

Take $\gamma' = \overline{\overline{\mathcal{P}R}}$ where $\mathcal{P}R$ is the power set of R.

Hence $\bigcup_{\alpha<\gamma'} S_\alpha \subset R$

Therefore $\overline{\overline{\bigcup_{\alpha<\gamma'} S_\alpha}} \leq \overline{\overline{R}}$

By lemma 5.16 we have $\overline{\overline{\bigcup_{\alpha<\gamma'} S_\alpha}} \geq \gamma'$

Hence $\overline{\overline{R}} \geq \overline{\overline{\mathcal{P}R}}$, which is contradiction.

Therefore the assumption is false, hence there exists an ordinal γ and a family $\{S_\alpha\}(\alpha<\gamma)$ of subrings of R such that $\bigcup_{\alpha<\gamma} S_\alpha = R$

Let

$$a_\beta = \begin{cases} C(R - \bigcup_{\alpha<\beta+1} S_\alpha) & \text{if } \beta \text{ is a non limit ordinal.} \\ C(R - \bigcup_{\alpha<\beta} S_\alpha) & \text{if } \beta \text{ is a limit ordinal .} \end{cases}$$

Observe that $a_\beta = b_\beta$ by the above construction, we see that $\{a_\alpha\}(\alpha<\gamma)$ is a γ- sequence and γ- sequence $\{S_\alpha\}(\alpha<\gamma)$ of subrings of R determined by $\{a_\alpha\}(\alpha<\gamma)$ has the property that $\bigcup_{\alpha<\gamma} S_\alpha = R$

<u>Theorem 5.18</u> If R is any p - ring containing identity e and if a is any non zero element of R then there exists a homomorphism h of R into Z_p such that $h(a) \neq 0$.

<u>proof.</u> From lemma 5.17 there exists an ordinal γ and a γ- sequence $\{a_\alpha\}(\alpha<\gamma)$ in R such that $a_0 = a$ and the γ sequence $\{S_\alpha\}(\alpha<\gamma)$ of subrings of R determined by $\{a_\alpha\}(\alpha<\gamma)$ has the property that $\bigcup_{\alpha<\gamma} S_\alpha = R$.

If $R = \langle e \rangle$, then R is a finite p - ring, thus it is isomorphic to a direct sum of $\mathbb{Z}_p$. Thus there exists an homomorphism $h_o : R \longrightarrow \mathbb{Z}_p$ such that $h_o(a) \neq 0$ for $a \neq 0$ in R.

If $R \neq \langle e \rangle$. Let $S_o = \langle e \rangle$ and $S_1 = \langle a_o , e \rangle$, S_1 is finite p - ring, it is isomorphic to direct sum of rings $\mathbb{Z}_p$. Thus there exists an homomorphism h_1 of S_1 onto $\mathbb{Z}_p$ such that $h_1(a_o) \neq 0$.

For each $1 < \alpha < \gamma$ we shall define h_α on S_α so that if $\alpha' < \alpha$ then h_α is an extension of $h_{\alpha'}$ we already have $h_{\alpha'}(a_o) \neq 0$.

This will be done by transfinite induction.

Let $P(\alpha)$ be the statement "h_α is an extension of $h_{\alpha'}$ for $\alpha' < \alpha$"

Let $\beta < \gamma$ be any ordinal number such that h_α is defined so that $P(\alpha)$ holds for all $\alpha < \beta$.

<u>Case 1</u> $\beta = \delta + 1$ for some ordinal δ.

Since h_δ has been defined on S_δ, hence by lemma 5.13 there exists h_δ' on $S_\delta(a_\delta)$ such that $h_{\delta'}(a_o) \neq 0$ and $h_{\delta'}|_{S_\delta} = h_\delta$.

Put $h_\beta = h_\delta'$ and $S_\beta = S_\delta(a_\delta)$. Then h_β is defined on S_β such that $P(\beta)$ holds.

Case 2 β is limit ordinal.

Note By $h = \bigcup_{\alpha<\beta} h_\alpha$ we mean that

$$h(a) = h_\alpha(a) \qquad\qquad a \in S_\alpha$$

This is well - defined since h_α is well - defined.

In this case we put $S_\beta = \bigcup_{\alpha<\beta} S_\alpha$ and $h_\beta = \bigcup_{\alpha<\beta} h_\alpha$.

Hence h_β is defined on S_β.

Therefore for each $\beta < \gamma$, h_β can be defined on S_β such that $P(\beta)$ holds.

Define $h = \bigcup_{\beta<\gamma} h_\beta$ Hence h is well-defined on $R = \bigcup_{\beta<\gamma} S_\beta$ and $h(a_0) \neq 0$.

We are now in a positicen to prove our principal theorem.

Theorem 5.19. If R is any p-ring, it is isomorphic to a subring of direct sum of $\mathbb{Z}_p$

proof. Apply theorem 5.5, 5.6 and 5.18

Classification of Subrings of direct sum $\mathbb{Z}_p$.

Theorem 5.20. Let $R = \underbrace{\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p}_{n\text{-times}}$ and K be a subring of R then $K = S_1 \oplus S_2 \oplus \cdots \oplus S_n$ where S_i be subring of $\mathbb{Z}_p$ or K is of type $\triangle$ where by this we mean that there exist at least two indicies i, j such that

$x_i = x_j \ \forall \ (x_1, x_2, \ldots x_n) \in K$.

proof. We prove this by induction. For $n = 1$ obvious, so we shall prove it for $n = 2$.

For $n = 2$. i.e. $R = \mathbb{Z}_p \oplus \mathbb{Z}_p$ and K be subring of R then we want to show that $K = S_1 \oplus S_2$ or $K = \{(x, x) \mid x \in \mathbb{Z}_p\}$ where S_1 and S_2 are subrings of $\mathbb{Z}_p$.

Let $\pi_i : R \longrightarrow \mathbb{Z}_p$ defined by

$$\pi_i(x_1, x_2) = x_i \quad (i = 1, 2)$$

Then π_i is homomorphism from R to $\mathbb{Z}_p$. $\pi_i(K)$ is subring of $\mathbb{Z}_p$ hence $\pi_i(K)$ is $\mathbb{Z}_p$ or $\{0\}$ since K is a subring of R and the only subrings of $\mathbb{Z}_p$ are $\mathbb{Z}_p$ and $\{0\}$.

<u>Case 1</u> If $\pi_1(K) = \{0\}$ and $\pi_2(K) = \{0\}$.

Then $K = \{0\} \oplus \{0\}$.

<u>Case 2</u> If $\pi_1(K) = \{0\}$ and $\pi_2(K) = \mathbb{Z}_p$.

Then $K = \{0\} \oplus \mathbb{Z}_p$.

<u>Case 3</u> If $\pi_1(K) = \mathbb{Z}_p$ and $\pi_2(K) = \{0\}$.

Then $K = \mathbb{Z}_p \oplus \{0\}$.

<u>Case 4</u> If $\pi_1(K) = \mathbb{Z}_p$ and $\pi_2(K) = \mathbb{Z}_p$.

Then claim that $K = \mathbb{Z}_p \oplus \mathbb{Z}_p$ or $K = \{(x;x) \mid x \in \mathbb{Z}_p\}$

<u>4.1</u> $p = 2$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 = \{(0,0),(0,1),(1,0),(1,1)\} .$$

The order of a subring K must divide 4, so the order order of K is 1,2, or 4.

If the order of K is 1, $K = \{(0,0)\}$ which is not in this case .

If the order of K is 2, $K = \{(0,0),(0,1)\}$, $K = \{(0,0),(1,0)\}$ and $K = \{(0,0),(1,1)\}$

If $K = \{(0,0),(0,1)\}$ or $K = \{(0,0),(1,0)\}$ again K can't be this case. So $K = \{(0,0),(1,1)\}$

Then K is of type of Δ, so we're done.

If the order of K is 4, clearly $K = \mathbb{Z}_2 \oplus \mathbb{Z}_2$ so done.

4.2 for $p > 2$

Assume that K is not type of Δ. We must prove that $K = \mathbb{Z}_p \oplus \mathbb{Z}_p$.

To do this we first want to show that $\exists$ $(x_1, x_2) \in K$ such that $x_1 \neq 0$, $x_2 \neq 0$ and $x_1 \neq x_2$.

Since $\pi_1(K) = \mathbb{Z}_p$ and $\pi_2(K) = \mathbb{Z}_p$, it follows that there exist α, $\beta \in \mathbb{Z}_p$ such that $(1, \alpha)$ and $(\beta, 1) \in K$. If $\alpha \neq 0, 1$ or $\beta \neq 0, 1$, then we're done.

4.2.1 If $\alpha = 0$, $\beta = 0$ we have

$(1, 0) + (0, 1) = (1, 1) \in K$ and

$(1, 1) + (1, 0) = (2, 1) \in K$, so done

4.2.2 If $\alpha = 0$, $\beta = 1$

$(1, 0) + (1, 1) = (2, 1) \in K$, so done

4.2.3 If $\alpha = 1$, $\beta = 0$, then use the same argument above.

4.2.4 If $\alpha = 1$, $\beta = 1$, so we can find $(x, y) \in K$ such that $x \neq y$.

If $x \neq 0$, and $y \neq 0$, then done.

If $x = 0$ or $y = 0$, (assume that $x = 0$) we have $(1, 1 + y) \in K$.

if $1 + y = 0$, we are back to case 4.2.2

If $1 + y \neq 0$, then $1 + y \neq 1$, so done.

So we can let $(x_1, x_2) \in K$ such that $x_1 \neq 0$, $x_2 \neq 0$ and $x_1 \neq x_2$.

Now, to prove that $K = \mathbb{Z}_p \oplus \mathbb{Z}_p$. Let $(x_1, x_2) \in K$ as mention above, then for any $(x_1', x_2') \in \mathbb{Z}_p \oplus \mathbb{Z}_p$ we shall show that $(x_1', x_2') \in$ the ring generated by (x_1, x_2), i.e. to prove that $\exists\ a_1, a_2 \in \mathbb{Z}$ such that $(x_1', x_2') = \sum_{i=1}^{2} a_i\ (x_1, x_2)^i$.

By letting

$$b_1 = \frac{\begin{vmatrix} x_1' & x_1^2 \\ x_2' & x_2^2 \end{vmatrix}}{\begin{vmatrix} x_1 & x_1^2 \\ x_2 & x_2^2 \end{vmatrix}} = \frac{c_1}{A}$$

$$b_2 = \frac{\begin{vmatrix} x_1 & x_1' \\ x_2 & x_2' \end{vmatrix}}{\begin{vmatrix} x_1 & x_1^2 \\ x_2 & x_2^2 \end{vmatrix}} = \frac{c_2}{A}$$

where

c_1 is the determinant $\begin{bmatrix} x_1' & x_1^2 \\ x_2' & x_2^2 \end{bmatrix}$

c_2 is the determinant $\begin{bmatrix} x_1 & x_1^2 \\ x_2 & x_2' \end{bmatrix}$ and

A is the determinant $\begin{bmatrix} x_1 & x_1^2 \\ x_2 & x_2^2 \end{bmatrix}$

b_1, b_2 exist and belong to $\mathbb{Z}_p$ since $A = x_1\, x_2\, (x_2 - x_1) \neq 0$. So b_1, b_2 satisfy

$$b_1 x_1 + b_2 x_1^2 = x_1'$$

$$b_1 x_2 + b_2 x_2^2 = x_2'$$

Let η be the natural homomorphism on $\mathbb{Z}$ onto $\mathbb{Z}_p$ by a lifting we mean a mapping μ from $\mathbb{Z}_p$ to $\mathbb{Z}$ such that $\eta \cdot \mu$ is the identity on $\mathbb{Z}_p$. We know that such a lifting always exist

$$\text{Let } a_1 = \mu\,(b_1)$$

$$a_2 = \mu\,(b_2)$$

Therefore $a_1 x_1 + a_2 x_1^2 = x_1' \mod p$

$$a_1 x_2 + a_2 x_2^2 = x_2^1 \mod p$$

For any $(x_1', x_2') \in \mathbb{Z}_p \oplus \mathbb{Z}_p$, $(x_1', x_2') \in$ the ring generated by (x_1, x_2) so we conclude that $K = \mathbb{Z}_p \oplus \mathbb{Z}_p$. The proof is completed for the case $n = 2$.

Assume that the theorem is true for $n = k - 1$ $(k - 1 \geqslant 2)$. To prove for $n = k$, let

$$\pi_k : R \longrightarrow \mathbb{Z}_p \quad \text{defined by}$$

$$\pi_k (x_1, x_2 \ldots\ldots , x_k) = x_k$$

Clearly π_k is a homomorphism and $\pi_k (K)$ is subring of $\mathbb{Z}_p$ so $\pi_k (K) = \{0\}$ or $\mathbb{Z}_p$. Consider any k-1 subscripts $i_1, i_2, \ldots\ldots, i_{k-1}$.

Let $\pi_{i_1 i_2 \ldots, i_{k-1}} : R \rightarrow \underbrace{\mathbb{Z}_p \oplus \ldots\ldots \oplus \mathbb{Z}_p}_{k-1 \text{ times}}$ defined by

$$\pi_{i_1 i_2 \ldots, i_{k-1}} (x_1, x_2, \ldots, x_k) = (x_{i_1}, x_{i_2}, \ldots, x_{i_{k-1}})$$

Then $\pi_{i_1 i_2 i_3 \ldots, i_{k-1}} (K)$ is subring of $\mathbb{Z}_p \oplus \ldots \oplus \mathbb{Z}_p$

<u>Case 1</u> If $\pi_{i_1 i_2 \ldots, i_{k-1}} (K)$ is of type Δ then K is of type Δ, so done.

<u>Case 2</u> If $\pi_{i_1 i_2 \ldots i_{k-1}}(K)$ is of type $S_1 \oplus \ldots \oplus S_{k-1}$ and $\pi_k(K) = 0$, then $K = S_1 \oplus \ldots \oplus S_{k-1} \oplus \{0\}$, so done.

<u>Case 3</u> If $\pi_{i_1 i_2 \ldots i_{k-1}}(K)$ is of type $S_1 \oplus \ldots \oplus S_{k-1}$ and some $S_j = \{0\}$, then choose new subcripts $\ell_1 \ldots \ell_{k-1}$ so that $\ell_k = j$.

$$\pi_{\ell_1 \ell_2 \ldots \ell_{k-1}}(K) = S_1 \oplus \ldots \oplus S_{k-1} \quad \text{and}$$

$\pi_{\ell_k}(K) = 0$. So we are back to case 2.

<u>Case 4</u> If $\forall\, i_1 i_2 \ldots i_{k-1}$, $\pi_{i_1 i_2 \ldots i_{k-1}}(K) = \underbrace{\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \ldots + \mathbb{Z}_p}_{k-1 \text{ times}}$ and $\pi_k(K) = \mathbb{Z}_p$ then claim that $K = \underbrace{\mathbb{Z}_p \oplus \ldots + \mathbb{Z}_p}_{k\text{-times}}$.

Let $x_1, x_2, \ldots x_k \in \mathbb{Z}_p$ be arbitrary. We have that $\exists\, \alpha \in \mathbb{Z}_p$ s.t. $(x_1, x_2, \ldots x_{k-1}, \alpha) \in K$, because $\pi_{12\ldots k-1}(K) = \underbrace{\mathbb{Z}_p \oplus \ldots \oplus \mathbb{Z}_p}_{k-1 \text{ times}}$

Similarly we have that $\exists \delta \in \mathbb{Z}_p$ such that

$$(\underbrace{1,0,0,\ldots 0}_{k-1 \text{ times}}, \delta) \in K .$$

If $\delta \neq 0, 1$,

$$(\underbrace{1,0,0,\ldots 0}_{k-1 \text{ times}}, \delta)^2 = (\underbrace{1,0,0,\ldots 0}_{k-1 \text{ times}}, \delta^2) ,$$

Thus $$(\underbrace{1,0,0,\ldots 0}_{k-1 \text{ times}}, \delta^2) - (\underbrace{1,0,0,\ldots 0}_{k-1 \text{ times}}, \delta) = (\underbrace{0,0,\ldots 0}_{k-1 \text{ times}}, a) \in K$$

where $a = \delta^2 - \delta \neq 0$.

Therefore we can find $(0,0,\ldots 0,x_k - \alpha) \in K$,

and $$(x_1, x_2, \ldots x_{k-1}, \alpha) + (0,0,\ldots 0,x_k - \alpha)$$

$$= (x_1, x_2,\ldots x_k) \in K$$

Since $x_1, x_2,\ldots x_k$ $\mathbb{Z}_p$ is arbitrary and we can find $(x_1, x_2,\ldots x_k) \in K$, we conclude that $K = \underbrace{\mathbb{Z}_p \oplus \ldots + \mathbb{Z}_p}_{k\text{-times}}$.

If $\delta = 0$, we have $(\underbrace{1,0,\ldots,0}_{k\text{ times}},0) \in K$, so done, because $\pi_{2\ldots k}(K) = \underbrace{\mathbb{Z}_p \oplus \ldots \oplus \mathbb{Z}_p}_{k-1 \text{ times}}$. and we have $(\alpha , x_2,\ldots x_k) \in K$

and also have

$(x_1 - \alpha'\ , 0, 0, \ldots, 0) \in K$. So their sum $\in K$.

If $\delta = 1$, we have $(\underbrace{1,0,0,\ldots 0,1}_{k\text{-times}}) \in K$.

For $p-1,\ 0 \in \mathbb{Z}_p$, $(p-1, 0, 0, \ldots 0) \in \pi_{12\cdots k-2,k}(K)$

and $(p-1, 0, 0, \ldots \underset{k-1^{th}}{\beta}, 0) \in K$.

If $\beta = 0$. So done, since we have that $\exists\ \eta \in \mathbb{Z}_p$ such that $(\eta, x_2, \ldots x_k) \in K$ and we can find $(x_1, x_2, \ldots x_k) \in K$ as before.

So assume that $\beta \neq 0$,

$(1,0,0,\ldots 0,1) + (p-1, 0, \ldots 0, \beta, 0) = (0,0,\ldots 0, \underset{k-1^{th}}{\beta}, 1) \in K$

and $(0,0,0,\ldots \underset{k-1^{th}}{\beta}, 1)^{p-1} = (0,0,\ldots \underset{k-1^{th}}{1}, 1)$.

Then $(1,0,0,\ldots 0,1) \cdot (0,0,\ldots 0,1,1) = (0,0,\ldots 0,1) \in K$.

So done.

Therefore $K = \underbrace{\mathbb{Z}_p \oplus \ldots \oplus \mathbb{Z}_p}_{k\text{-times.}}$

Hence the theorem is true for all $n \in \mathbb{Z}_+$.