CHAPTER II

PRELIMINARIES

The materials of this chapter are drawn from references [1] , [2] , [5] , [6] .

To make this thesis essentially self contained, we recall some relevant notions and facts from group theory. However we first recall the all important Zorn's Lemma.

2.1 <u>Definitions</u>. A relation $\leq$ on a set S is said to be <u>transitive</u> if for any a, b, c in S with $a \leq b$ and $b \leq c$, we always have $a \leq c$. It is said to be <u>reflexive</u> if $a \leq a$ for each element a in S; and it is said to be <u>antisymmetric</u> if for any elements a, b of S, $a \leq b$ and $b \leq a$ implies $a = b$.

A <u>partially ordered set</u> is a pair $(S, \leq)$, where S is a set and where $\leq$ is a transitive, reflexive and antisymmetric relation on S. If no confusion can arise, we usually say that S is a partially ordered set.

A <u>linearly ordered subset</u> or <u>chain</u> of a partially ordered set $(S, \leq)$ is a subset T such that, if a and b are in T, then either $a \leq b$ or $b \leq a$. In connection with subgroups of a group, a chain is a set of subgroups linearly ordered by inclusion; and the union of the subgroups of such a chain is an <u>ascending union</u>.

An upper bound of a subset W of partially ordered set S is an element u of S such that $w \leq u$ for all w in W.

An element M of a partially ordered set S is maximal if $M \leq s$ for s in S, implies that M = s.

2.2 Zorn's Lemma . A non - empty partially ordered set X in which every linearly ordered subset of X has an upper bound contains a maximal element.

We now recall some concepts from Group Theory.

2.3 Notations. Let A be a non - empty subset of a group G. The set of finite products of elements of $A \cup A^{-1}$ is a subgroup of G; it is called the subgroup generated by A and is denoted by [A] . If A consists of a single element a, then $[\{a\}]$ is cyclic and will also be denoted by [a] .

2.4 Definitions. The subgroup of elements of finite order of an abelian group G is called the torsion subgroup of G, denoted by tG.

An element of finite order of any group (not necessarily abelian) is called a torsion element.

If all the elements of a subgroup are torsion elements, the subgroup is said to be torsion; if no element, other than the identity element 1, is torsion, the subgroup is said to be torsion - free.

2.5 Definition. A group G is said to be torsion - free in the strong sense or strongly torsion - free if for each non - zero integer n, and for any elements x, y of G, $x^n = y^n$ implies $x = y$.

2.6 Remark. (a) A group G is torsion - free if and only if for any non - zero integer n, and for any element x of G, $x^n = 1$ implies $x = 1$. Consequently, a group which is torsion - free in the strong sense is torsion - free.

(b) Torsion - free abelian groups are strongly torsion - free; for if $x^n = y^n$ holds in such a group, then $x^n \circ y^{-n} = 1$, and by the commutativity of the group, $(x \circ y^{-1})^n = 1$. Since the group is torsion - free, $x \circ y^{-1} = 1$; i.e., $x = y$.

(c) Let G be a torsion - free group, and $1 \neq g \in G$. Let

$$\langle g \rangle = \{ x \in G \ / \ x^m \in [g] \text{ for some non - zero integer } m \}.$$

For any x, y $\in \langle g \rangle - \{1\}$, there exist non - zero integers m and n such that $x^m = y^n$; for if x, y $\in \langle g \rangle$, then there exist non - zero integers r, s, t and u such that $x^r = g^s$, $y^t = g^u$ and therefore $x^{ru} = g^{su}$, $y^{st} = g^{su}$. Hence $x^{ru} = y^{st}$, i.e., $x^m = y^n$ for $m = ru$ and $n = st$.

Convention : For the remainder of the chapter, all groups are additive abelian.

2.7 Definitions. An abelian group G is said to be an (internal) direct sum of its subgroups A_k, where k ranges over some index set K, if

$$\text{i.} \quad G = \left[\bigcup_{k \in K} A_k \right]$$

and

$$\text{ii.} \quad A_t \cap \left[\bigcup_{k \in K^*} A_k \right] = \{0\},$$

for each $t \in K$, where $K^* = K \setminus \{t\}$ and 0 denotes the zero of G.

In this case, we write $G = \sum_{k \in K} A_k$ and call the A_k (direct) summands of G. If $K = \{1, 2, \ldots, n\}$, we shall write $G = A_1 \oplus A_2 \oplus \ldots \oplus A_n$.

A group G is said to be decomposable if it is a direct sum of some of its proper subgroups. Otherwise G is said to be indecomposable.

2.8 Definitions. The subgroup of elements of p-power order, p a fixed prime, of an abelian group G is called the p-component of G.

If each element of any group G (not necessarily abelian) has order a power of p, then G is called a p-group.

2.9 Theorem. An abelian torsion group is the direct sum of its p-components.

<u>Proof</u> : Let G be an abelian torsion group, and for each prime p, let

$$G_p = \{ g \in G \,/\, g \text{ has order a power of } p \}.$$

Then obviously $0 \in G_p$, and for any elements x, y of G_p, there exist non - zero integers m , n such that $p^n x = 0 = p^m y$. Hence $p^{n+m}(x \pm y) = 0$, that is the order of $(x \pm y)$ is a power of p, that is G_p is a subgroup of G. Moreover, G_p is a p-component.

We will show that $G = \sum_{p \in \mathbb{P}} G_p$, where $\mathbb{P}$ is the set of prime numbers.

a. Let g be a non - zero element of G. Since G is torsion, the order n of g is finite. Let

$$n = p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdots p_k^{\gamma_k},$$

where $p_i \in \mathbb{P}$ and let $n_i = n/ p_i^{\gamma_i}$, i = 1, 2, ... , k. Then the greatest common divisor of the $n_1, n_2, \ldots, n_k$ is 1, and therefore there exist integers $\alpha_1, \alpha_2, \ldots, \alpha_k$ such that $1 = \sum_{i=1}^{k} \alpha_i n_i$, then $g = \sum_{i=1}^{k} \alpha_i n_i g$. Now $p_i^{\gamma_i} \alpha_i n_i g = \alpha_i n g = 0$ so that the order of $\alpha_i n_i g$ devides $p_i^{\gamma_i}$, that is the order of $\alpha_i n_i g$ is a power of p_i, hence $\alpha_i n_i g$ belongs to G_{p_i}.

Thus g belongs to $\left[\bigcup_{p \in \mathbb{P}} G_p\right]$, that is G is a subgroup of $\left[\bigcup_{p \in \mathbb{P}} G_p\right]$. Since the reverse inclusion is obvious,

$$G = \left[\bigcup_{p\in\mathbb{P}} G_p\right].$$

b. We are left to show that for each $q \in \mathbb{P}$,

$$G_q \cap \left[\bigcup_{p\in\mathbb{P}^*} G_p\right] = \{0\}, \text{ where } \mathbb{P}^* = \mathbb{P} \setminus \{q\}.$$

Let $x \in G_q \cap \left[\bigcup_{p\in\mathbb{P}^*} G_p\right]$. Then $x = \sum_{i=1}^{n} \alpha_i g_i$, where $g_i \in G_{p_i}$ and α_i are integers. The order of x is a power of q, while the order of $\sum_{i=1}^{n} \alpha_i g_i$ is a product of powers of p_i, $i = 1, 2, \ldots, n$. Thus $q^{\alpha} = p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdots p_n^{\gamma_n}$ for some integers α, $\gamma_1, \ldots, \gamma_n$, which can not happen unless $\alpha = \gamma_i = 0$ for all $i = 1, 2, \ldots n$. Hence $x = 0$, that is

$$G_q \cap \left[\bigcup_{p\in\mathbb{P}^*} G_p\right] = \{0\} \text{ for all } q \in \mathbb{P} \text{ and } \mathbb{P}^* = \mathbb{P} \setminus \{q\}.$$

2.10 Example and Definition. It is easy to see that the group $\mathbb{Q}/\mathbb{Z}$ of the additive abelian group $\mathbb{Q}$ of rationals modulo the additive abelian group $\mathbb{Z}$ of integers is torsion so that, by Theorem 2.9, we have

$$\mathbb{Q}/\mathbb{Z} = \sum_{p\in\mathbb{P}} (\mathbb{Q}/\mathbb{Z})_p ,$$

where $\mathbb{P}$ is the set of all primes.

A group is said to be of type p^{∞} if it is isomorphic to $(\mathbb{Q}/\mathbb{Z})_p$ and the symbol $\sigma(p^{\infty})$ will be used to denote any such group.

For each $p \in \mathbb{P}$, let $A^{(p)}$ be the set of all rationals τ in $[0, 1[$ whose denominator is a power of p. Then clearly

$$A^{(p)} = (\mathbb{Q}/\mathbb{Z})_p \cap [0, 1[\; ;$$

i.e., $A^{(p)}$ is the set of representatives of the cosets of $(\mathbb{Q}/\mathbb{Z})_p$ which are in $[0, 1[$. Thus the map $\bar{x} \mapsto x - [\![x]\!]$, where $[\![x]\!]$ is the greatest integer less than or equals to x, from $(\mathbb{Q}/\mathbb{Z})_p$ onto $A^{(p)}$ induces an isomorphism of the group $(\mathbb{Q}/\mathbb{Z})_p$ and the group $A^{(p)}$ with the binary operation which is just the ordinary addition in $\mathbb{Q}$ modulo 1.

2.11 <u>Definition</u>. A group G is said to be <u>p- cocyclic</u> if and only if G is isomorphic to $\sigma(p^n)$ for some $n = 1, 2, \ldots, \infty$, where p is a prime and where $\sigma(k)$ denotes a cyclic group of order k.

2.12 <u>Remarks</u> : For each positive integer n, let

$$a_n = \frac{1}{p^n}$$

Then $pa_1 = 1 = 0 \pmod{\mathbb{Z}}$

and for $n > 1$, $pa_n = a_{n-1}$.

Hence a_n has order p^n so that $[a_n] = \sigma(p^n)$ for each positive integer n. (We identify isomorphic groups).

(a) $0 \subset [a_1] \subset [a_2] \subset \cdots \subset [a_n] \subset \cdots \subset \sigma(p^\infty)$;

in fact, $[a_k] \subset [a_n]$ for any integers k and n with $k \leq n$.

<u>Proof</u> : The case $k = n$ is obvious; assume $k < n$. It then follows that the element $p^{n-k} a_n = \frac{p^{n-k}}{p^n}$ of $[a_n]$ is just a_k

so that $[a_k] \subset [a_n]$ as required.

(b) $\sigma(p^{\infty}) = \bigcup_{n=1}^{\infty} \sigma(p^n)$

Proof : We only need to prove that $\sigma(p^{\infty}) \subset \bigcup_{n=1}^{\infty} [a_n]$, since the reverse inclusion follows from (a) .

Let $x \in \sigma(p^{\infty}) = A^{(p)}$ (see 2.10). Then $x = m/p^n$ for some non - negative integers m , n with $m < p^n$, so that $x \in [a_n]$.

(c) The only non - zero proper subgroups of $\sigma(p^{\infty})$ are the finite cyclic subgroups $\sigma(p^n)$, for n = 1, 2, 3, ...

Proof : Suppose A is a non - zero proper subgroup of $\sigma(p^{\infty})$. If A contains all the a_n, then

$$A \supset \bigcup_{n=1}^{\infty} [a_n] = \sigma(p^{\infty}) \text{ , (by (b))}$$

so that we must have an n such that $a_n \notin A$. Let m be the smallest integer which $a_{m+1} \notin A$. Then $a_m \in A$ so that $[a_m] \subset A$. To conclude, we will show that $A \subset [a_m]$; i.e., $\sigma(p^{\infty}) \setminus A \supset \sigma(p^{\infty}) \setminus [a_m]$.

First, note that it follows from (a) and the choice of m that

$$a_n \notin A$$

for all $n > m + 1$.

Suppose to the contrary that there is a y in $\sigma(p^{\infty}) \setminus [a_m]$ and in A. Then

$$y \in [a_k] \setminus [a_m]$$

for some $k > m + 1$ by (a) and (b). Thus

$$a_k \in [a_k] = [y] \subset A,$$

contradicting the above remark.

2.13 Theorem . The additive group $\mathbb{Q}/\mathbb{Z}$ of rationals modulo 1 is isomorphic to a direct sum of p-cocyclic groups, one for each prime. Moreover, group is isomorphic to a subgroup of $\mathbb{Q}/\mathbb{Z}$ if and only if it is a direct sum Of p-cocyclic groups.

Proof : The first statement of this theorem follows from 2.10 and definition 2.11.

Thus it remains to prove the second statement. We have already shown in 2.10 that $\mathbb{Q}/\mathbb{Z}$ is torsion; hence subgroups of $\mathbb{Q}/\mathbb{Z}$ are also torsion.

Then by Theorem 2.9, we have that $\mathbb{Q}/\mathbb{Z} = \sum_{p \in \mathbb{P}} \sigma(p^\infty)$ and that any subgroup H of $\mathbb{Q}/\mathbb{Z}$ is the direct sum of its p-components : $H = \sum_{p \in \mathbb{P}} H_p$, where $\mathbb{P}$ is the set of prime numbers. Hence each H_p is a subgroup of $\sigma(p^\infty)$ and, therefore, is p-cocyclic by 2.12 (c).

Conversely, if a group G is a direct sum of p-cocyclic groups G_p. Then $G_p \subset \sigma(p^\infty)$ by 2.12 (a). This inclusion map then induces an isomorphism of $G = \sum_{p \in \mathbb{P}} G_p$ onto a subgroup of $\sum_{p \in \mathbb{P}} \sigma(p^{\infty}) = \mathbb{Q}/\mathbb{Z}$.

Thus the theorem is completely proved.

2.14 Theorem. Let G be a decomposable p-group, for some prime p. Then no two elements, different from 0, from distinct summands (of the same direct sum decomposition) of G can belong to a common cyclic subgroup of G.

Proof : Let A and B be distinct summands of G, and $G = A \oplus B \oplus C$. Suppose there exist $0 \neq a \in A$ and $0 \neq b \in B$ with $a, b \in [g]$ for some $0 \neq g \in G$, where $[g]$ denotes the cyclic group generated by g. Let $g = a' + b' + c$, for some a' in A, b' in B and c in C. Since $a, b \in [g]$, then $a = mg$, $b = ng$, for some non-zero integers m and n. It then follows that $a = ma'$ and $b = nb'$; $O(b')$ divides m and $O(a')$ divides n, where $O(x)$ denotes the order of x. If $O(a') = O(b')$, then $O(a')$ divides m and $O(b')$ divides n so that $a = 0 = b$, contradicting the choice of a and b. Hence $O(a') \neq O(b')$. Without loss of generality we shall assume that $O(a') < O(b')$. Since both $O(a')$ and $O(b')$ are powers of a fixed prime p, $O(a')$ divides m also, thus $a = 0$, contradicting the choice of a. Hence in any case, we have a contradiction, and the theorem is proved.

Corollary. Any p-cocyclic group is indecomposable.

Proof : This is just a consequence of Theorem 2.14 with the aid of Remark 2.12 (b).

Moreover, the converse of this Corollary holds for p-primary group.

2.15 Theorem. A p-primary group is indecomposable if and only if it is p-cocyclic.

We shall devote the remainder of this chapter to complete the proof of this theorem.

Definitions. Let G be a group, an element x in G is divisible by an integer n if there exists an element y in G with ny = x.

A group G is divisible if for every x in G, x is divisible by every integer n.

A divisible subgroup is a subgroup which considered as a group is divisible.

A group is reduced if it contains no (non-zero) divisible subgroups.

Remarks. a) The element 0 of any group is divisible by any integer.

b) If x is an element of a group G of order m, then it is divisible by any integer prime to m; for if n and m are relatively primes, there exist integers a, b such that $an + bm = 1$, hence $anx + bmx = x$ and we have $n(ax) = x$.

<u>Lemma A.</u> A divisible subgroup of a group G is a direct summand.

<u>Proof</u> : Let H be a divisible subgroup of G. We consider the set B of all subgroups L of G which satisfy $H \cap L = \{0\}$. B is not empty since $\{0\}$ is in B. We partially order B by set-theoretical inclusion. Suppose $\{L_i\}$ is a chain in B; let M be the set-theoretical union of the L_i's. Two things need to be verified.

a) M is a subgroup of G. We take x and y in M and have to show that $x - y$ is in M. Now x and y are in M so that x is, say, in L_i, and y in L_j. But L_i and L_j are comparable, say $L_i \leq L_j$. Then both x and y are in L_j, and so is $x - y$. Hence $x - y$ is in M.

b) $H \cap M = \{0\}$. This follows from the fact that every element of M is in one of the L_i's and $H \cap L_i = \{0\}$.

Hence M is a upper bound for $\{L_i\}$. By Zorn's Lemma, we conclude that B contains a maximal element, say K. We are left to prove that $[H \cup K] = G$. We suppose the contrary.

Then there exists an element x in G which is not in $[H \cup K]$, and it follows that x is not in K. Let $K' = [K \cup \{x\}]$. K' properly contains K, and in fact, K' consists of all elements $k + nx$ where k is in K and n is an integer. By the maximality of K we know that $H \cap K' \neq \{0\}$. Hence there exists a non-zero element h in $H \cap K'$ such that $h = k + nx$. Thus it follows that nx is in $[H \cup K]$. We may suppose that n is the smallest positive integer such that $nx \in [H \cup K]$. Hence $n > 1$, let p be a prime dividing n, and write $y = (n/p)x$. Thus y is not in $[H \cup K]$, but $py = nx = h - k$. By the divisibility of H we may write $h = ph_1$, for some $h_1 \in H$. Let $z = y - h_1$. Then z is not in $[H \cup K]$ which implies that z is not in K, but

(1) $\qquad pz = py - ph_1 = py - h = - K$

is in K. Since z is not in K, we then have $K'' = [K \cup \{z\}]$ properly contains K. Again $H \cap K'' \neq \{0\}$; hence we can find

(2) $$h_2 = k_2 + mz$$

with $h_2 \in H$, $h_2 \neq 0$, $k_2 \in K$, and m is an integer. It is impossible for m to be a multiple of p, for then $h_2 = k_2 + \ell pz$ for some integer ℓ, so that h_2 is a non-zero element in $H \cap K$. Hence m is prime to p; we may find integers a, b such that $am + bp = 1$. We have $z = amz + bpz$; by (1) and (2), z is in $[H \cup K]$, which is a contradiction. Hence $G = [H \cup K]$.

Lemma B Any group G can be written as a direct sum, $G = M \oplus N$, where N is reduced subgroup and M is a divisible subgroup of G.

Proof : Let M be the union of the divisible subgroups of G. Now $[M]$ consists of finite sum $x_1 + x_2 + \dots + x_k$ where each x_i lies in some divisible subgroup of G. Since each x_i is divisible by arbitrary n, so is the sum. Thus $[M]$ is itself a divisible subgroup. By Lemma A. $[M]$ is a direct summand of G; hence $G = [M] \oplus N$, where N is a subgroup of G. N can have no (non-zero) divisible subgroups, since such subgroups of N are also divisible subgroups of G; i.e., N is reduced.

Remark C. To classify all abelian groups it suffices, by Lemma B, to classify the divisible and reduced abelian groups.

Lemma D. A divisible indecomposable p-group G_p is isomorphic to $\sigma(p^{\infty})$.

Proof : We select in G_p an element x_1 of order p. Using the divisibility of G_p, we find in succession elements $x_2, x_3, \dots$ with $px_2 = x_1$, $px_3 = x_2$, ..., and in general $px_{i+1} = x_i$. Now map x_1 into $1/p$, x_2 into $1/p^2, \dots$, x_i into $1/p^i, \dots$. This gives rise to an isomorphism between the subgroup H generated by the x_i's , and the group $\sigma(p^{\infty})$.

Since every element of H is of order a power of p, it is divisible by every integer prime to p. On the other hand, every element of H can be divided by arbitrary powers of p. On putting these two statements together, we establish that H is divisible. By Lemma A, $G_p = H \oplus R$, but G_p is indecomposable; thus $R = \{0\}$. Hence we have proved that G_p is isomorphic to $\sigma(p^\infty)$.

Definition. A subgroup H of a group G is pure if for any $h \in H$ and for any integer n, $h = ny$ for some $y \in G$ implies $h = nh_1$ for some h_1 in H.

Lemma E. Let G be a group, H a pure subgroup of G, and y an element of G/H. Then there exists an element x in G, having the same order as y, and $x^* = y$, where x^* is the image of x under the natural quotient map from G onto G/H.

Proof : If y has infinite order, then any choice of an element mapping on y will do. So suppose y has finite order n. First choose any z in G with $z^* = y$. Then nz is in H. By the purity of H, there exists an element $h \in H$ with $nh = nz$ Set $x = z - h$. Then $x^* = y$, and has order n.

Lemma F. Let G be a group and H a pure subgroup of G such that G/H is a direct sum of cyclic groups. Then H is a direct summand of G.

Proof : For each cyclic summand of G/H pick a generator y_i, by Lemma E, we can choose element x_i in G such that $x_i^* = y_i$ and x_i has the same order as y_i ($z^* = z + H = \{z + h / h \in H\}$). Let K be the subgroup of G generated by the elements x_i's. We claim that $G = H \oplus K$.

(a) $G = [H \cup K]$: Let t be any element in G. Then t^* is a finite sum $\sum a_i y_i$ where a_i are integers. Then $t - \sum a_i x_i$ maps on 0 in G/H, and so is in H. Since $\sum a_i x_i \in K$, we have $t \in [H \cup K]$.

(b) $H \cap K = \{0\}$: Let $w \in H \cap K$. Then $w \in K$ so that

$$w = \sum_{k=1}^{n} a_{i_k} x_{i_k}$$

where the a_{i_k} are integers. Since $w \in H$ also, we have

$$0 = w^* = \sum_{k=1}^{n} a_{i_k} x_{i_k}^*$$

$$= \sum_{k=1}^{n} a_{i_k} y_{i_k}$$

Since $a_{i_k} y_{i_k}$ comes from distinct summands of G/H, $a_{i_k} y_{i_k} = 0$ for $k = 1, 2, \ldots, n$. If the order of y_{i_k} is infinite, $a_{i_k} = 0$; if the order of y_{i_k} is n_k, then n_k divides a_{i_k} so that $a_{i_k} x_{i_k} = 0$ since n_k is also the order of x_{i_k} by choice. Hence, in any case,

$$w = \sum_{k=1}^{n} a_{i_k} x_{i_k} = 0$$

so that $H \cap K = \{0\}$

Lemma G. Let G be a group, S a pure subgroup of G, and T a subgroup of G containing S such that T/S is pure in G/S. Then T is pure in G.

Proof : Suppose $t \in T$ and $t = nx$ with $x \in G$. We have to prove that t is a multiple of n in T. Let t^* and x^* be the homomorphic images of t and x in G/S. Then $t^* = nx^*$. Since T/S is pure in G/S, there exists $y \in T$ such that $y^* \in T/S$ and $t^* = ny^*$. It follows that $t = ny + s$ for a suitable element $s \in S$. Since $s = t - ny = nx - ny$, and since S is pure in G, we conclude that $s = ns_1$ = for some $s_1 \in S$. This gives us that $t = ny + ns_1 = n(y + s_1)$ where $y + s_1 \in T$, as desired.

Lemma H. Let S be a pure subgroup of G with $nS = \{0\}$, where n is an integer and $nS = \{ns / s \in S\}$. Then $[S \cup nG]/nG$ is pure in G/nG.

Proof : Suppose $x = my$ where $x \in [S \cup nG]/nG$, $y \in G/nG$, and m is an integer. We have to prove that x is a multiple of m within $[S \cup nG]/nG$. Let us take representatives s in S of x and t in G of y. Then s and mt differ by an element of nG:

$$s = mt + nz$$

for some $z \in G$. Let r be the greatest common divisor of m and n. Then $m = rm_1$, $n = rn_1$, with m_1 and n_1 relatively prime; we can then find integers a and b such that $am_1 + bn_1 = 1$. We have $s = rm_1t + rn_1z$. Since S is pure in G, we have $s = rs_1$ with s_1 in S. Hence

$$s = rs_1 = r(am_1 + bn_1)s_1 = mas_1 + nbs_1,$$

and $ns_1 \in nS = \{0\}$, so we have $s = mas_1$.

Passing to the quotient $[S \cup nG]/nG$ with the notation

$$z^* = z + nG,$$

we have

$$x = s^* = (mas_1)^*$$
$$= m(as_1)^*$$

with $(as_1)^* = as_1^* \in [S \cup nG]/nG$, as to be proved.

Definition. A group G is of bounded order if there exists a (positive) integer n such that $nx = 0$ for all x in G.

Lemma I. Let G be a p-primary group satisfying $p^rG = \{0\}$ for some integer r. Let x be an element of order p^r in G. Then the cyclic subgroup K generated by x is pure.

<u>Proof</u> : As remarked earlier, in a p-primary group, every element is divisible by any integer which is prime to p; thus to check the purity of K, we only have to deal with powers of p.

First we deal with elements in K which are of the form $p^i x$. Suppose $p^i x = p^j y$ for $i \nless r$ and y in G. If $j > i$, then

$$0 = p^r y = p^{r-j}(p^i x)$$

so that the order of x is $p^{r-j+i} < p^r$, contradicting the assumption that the order of x is p^r. Hence $j \leq i$ and, therefore,

$$p^i x = p^j (p^{i-j} x)$$

with $p^{i-j}x \in K$. Hence $p^i x$ is divisible by p^j in K, whenever $p^i x$ is divisible by p^j in G. Note that the important fact used is that the order of x is p^r.

Now for the general case, let nx be an arbitrary non-zero element of K. Then we can write $n = mp^i$ for $i < r$ and m relatively prime to p. Suppose

$$nx = mp^i x = p^j y$$

for $y \in G$ and some non-negative integer j. Since m is relatively prime to p, the orders of mx and x are the same. By the above case, we can find an $\alpha(mx)$ in the cyclic subgroup $[mx]$ such that $p^i(mx) = p^j \alpha(mx)$ and nx is divisible by p^j in K.

Hence K is pure in G.

Lemma J. Let G be a group, S a subgroup of G, and x an element of G. Suppose that x and y = x + S have the same order. Let K be the cyclic subgroup generated by x. Then $[S \cup K]$ is a direct sum.

Proof : We have to show that $S \cap K = \{0\}$. Suppose the contrary that there is a $rx \in K$ which is also in S. Since $rx \in S$, $ry = 0$. Thus r is a multiple of the order of y, so is also a multiple of the order of x; whence $rx = 0$.

Lemma K. A group G of bounded order is a direct sum of cyclic groups.

Proof : We may assume that G is p-primary by Theorem 2.9.

A subset L of G will be called pure-independent if the subgroup $[L]$ generated by L is pure in G and if

$$[L] = \sum_{x \in L} [x],$$

The direct sum of cyclic subgroups $[x]$ as x runs over L.

Let $\mathcal{B}$ be the set of all pure-independent subsets of G. Partially ordered $\mathcal{B}$ by inclusion. If $\{I_i\}$ is a chain in $\mathcal{B}$, then it can easily shown that $U = \bigcup I_i$ is an upper bound for $\{I_i\}$ in $\mathcal{B}$. It then follows from Zorn's Lemma that $\mathcal{B}$ contains a maximal element M. Suppose that

$[M] \neq G$ and let $S = [M]$. then G/S is again a p-primary group of bounded order. Let $x \in G$ be chosen so that $x^* = x + S$ is of maximal order in G/S. By Lemma I, $[x^*]$ is pure in G/S. Since S is pure in G it follows from Lemma E that we may and shall assume that x and x^* have the same order. Since x and $x^* = x + S$ have the same order, Lemma J says that $[S \cup \{x\}]$ is a direct sum. Moreover since S is pure and $[S \cup \{x\}] / S = [x^*]$ is pure in G/S, it follows from Lemma G that $[S \cup \{x\}]$ is pure in G. Since $[M \cup \{x\}] = [S \cup \{x\}]$, we have that $M \cup \{x\}$ is a pure-independent subset of G and $M \cup \{x\}$ properly contains M. The latter contradicts the maximality of M and, therefore, we must have that $[M] = G$.

The lemma is now completely proved.

Lemma L. Let S and T be subgroups of G with $S \cap T = \{0\}$ and suppose that $[S \cup T]/T$ is a direct summand of G/T. Then S is a direct summand of G.

Proof : Let R/T be such that $G/T = R/T \oplus [S \cup T] / T$. We have $[R \cup [S \cup T]] = G$, $R \cap [S \cup T] = T$. We want to show that $G = S \oplus R$. Since $R \supset T$, we have $[S \cup R] = [S \cup T \cup R] = G$. Moreover, $R \cap S \subset R \cap [S \cup T] = T$, and hence $R \cap S \subset T \cap S = \{0\}$ by the assumption. Hence $G = S \oplus R$

and the lemma is proved.

Lemma M. Let G be a group and S a pure subgroup of bounded order. Then S is a direct summand of G.

Proof : Suppose $nS = \{0\}$. Then by Lemma H, $[S \cup nG]/nG$ is pure in G/nG. Also, G/nG and all its homomorphic images are groups of bounded order. Hence it follows from Lemma K that the group

$$H = (G/nG)/([S \cup nG]/nG)$$

is a direct sum of cyclic groups. By Lemma F, $[S \cup nG]/nG$ is a direct summand of G/nG. We next note that $S \cap nG = \{0\}$ For if $x \in S \cap nG$, $x = ng$ for some integer n and for some g in G; by the purity of S, we have $x = ns_1$ for some $s_1 \in S$; but $nS = 0$ so that $x = 0$. Apply Lemma L with nG instead of T, we deduce that S is a direct summand of G.

Definition. Let G be a p-primary group, and $x \in G$. We say that x has height n if x is divisible by p^n but not by p^{n+1}, and that x has infinite height if x is divisible by p^m for every non-negative integer m. We will use the symbol $h_G(x)$ to denote the height of x.

If S is a subgroup of the p-primary group G and $x \in S$, then it is clear that $h_S(x) \leq h_G(x)$. However, if either the context of the height of x is clear or else all the heights, of x concerned are equal, we will simply use $h(x)$.

Note that $h(0) = +\infty$, therefore, when we say that a p-primary group G has no elements of infinite height we mean all non-zero elements of G has finite height.

Remarks. Let G be a p-primary group.

a) If $x, y \in G$ and if $h(x) \neq h(y)$, then

$$h(x+y) = \min \{ h(x), h(y) \}.$$

If $h(x) = h(y)$, then

$$h(x+y) \geq h(x).$$

b) G is divisible if and only if $h(x) = +\infty$ for all $x \in G$.

c) It follows from previous remarks that a subgroup S of G is pure in G if and only if $h_S(x) = h_G(x)$ for all $x \in S$.

Lemma N. Let G be a p-primary group and S a subgroup of G with $h_S(x) < +\infty$ for all $x \in S$. Suppose that $h_S(x) = h_G(x)$ for all $x \in S$ whose order is p. Then S is pure in G.

Proof : By Remark (c), we only need to prove that

$$h_S(x) = h_G(x)$$

for all $x \in S$. The proof is by induction on n. Assume that the above statement is true for all elements of S whose order are less than or equal to p^n. Let x be in S whose order is p^{n+1}. Then $px \in S$ has order p^n so that $h_S(px) = h_G(px) = r$, say; thus

$$px = p^r y$$

for some $y \in S$. If either $h_S(p^{r-1}y)$ or $h_G(p^{r-1}y)$ is larger than $r - 1$, then $h(px) > r$ so that both $h_S(p^{r-1}y)$ and $h_G(p^{r-1}y)$ are not larger than $r - 1$. Hence

$$r - 1 \leq h_S(p^{r-1}y) \leq h_G(p^{r-1}y) \leq r - 1$$

so that

$$h(p^{r-1}y) = h_S(p^{r-1}y) = h_G(p^{r-1}y).$$

$$= r - 1.$$

Consider $h_S(x)$ and $h_G(x)$. If either $h_S(x)$ or $h_G(x)$ is larger than $r - 1$, then $h(px) > r$. It follows that both $h_S(x)$ and $h_G(x)$ are not larger than $r - 1$. On the other hand, we can write

$$(*) \qquad x = (x - p^{r-1}y) + p^{r-1}y .$$

Since the element $x - p^{r-1}y$ is in S of order p, we have

$$k = h(x - p^{r-1}y) = h_S(x - p^{r-1}y)$$

$$= h_G(x - p^{r-1}y)$$

$$< +\infty .$$

If $k \neq r - 1$, then both $h_S(x)$ and $h_G(x)$ equal to min (k, r-1), which follows from equation (*) and Remark (a). Hence

$$h(x) = h_S(x) = h_G(x)$$

$$= \min(k, r - 1),$$

if $k \neq r - 1$. On the other hand, if $k = r - 1$, then it follows from Equation (*) and Remark (a) that

$$k = r - 1 \leq h_S(x) \; , \; h_G(x).$$
$$\leq r - 1,$$

where the last inequality had been observed earlier. Hence in any case, $h_S(x) = h_G(x)$.

The proof is now completed by induction.

Lemma 0 . Let G be a p-primary group and suppose that all elements of G of order p have infinite height. Then G is divisible.

Proof : It follows from Remark (b) that we only need to show that $h_G(x) = +\infty$ for all $x \in G$. The proof is by induction on n. Assume that the above statement is true for all elements of G of order less than or equal to p^n. Let $x \in G$ be of order p^{n+1} and assume that $h_G(x) = m < +\infty$. Then px has order p^n and, therefore, $h(px) = +\infty$ by the inductive assumption. Hence we can find a $y \in G$ such that

$$px = py.$$

where $h_G(y) > m$, then $h_G(x - y) = \min \{ h_G(x), \; h_G(y) \} = m$. On the other hand, we have $p(x - y) = 0$ so that $h_G(x - y) = +\infty$ by assumption. Thus the assumption that $h_G(x) < +\infty$ led to two contradictory statements so that we must have $h_G(x) = +\infty$.

The proof is completed by induction.

Lemma P. If G is a p-primary reduced group, then G contains a finite cyclic direct summand.

Proof : Since G is not divisible, it follows from Lemma O that there is an $x \in G$ of order p whose height, say m, is finite. Then

$$x = p^m y$$

for some y in G. Let H = [y] . Since px = 0, H is a finite cyclic subgroup of G. We will show that H is a direct summand. Since an element of H is of order p if and only if it is of the form kx , where k is relatively prime to p, and $kx = p^m(ky)$ with $ky \in H$, it is immediate that the elements of H of order p have the same height in H and in G. Moreover, since $h(x) < +\infty$, no element of H can have infinite height. Hence, it follows from Lemma N that H is pure in G. Finally, it follows from Lemma M that H is a direct summand of G, as to be proved.

Proof of Theorem 2.15

It remains to prove that if G is an indecomposable p-primary group, then G is p-cocyclic.

Suppose G is an indecomposable p-primary group. We consider two cases.

If G is reduced, then G is a finite cyclic p-primary group by Lemma P , i.e., G is a cyclic group of order a power of p.

If G is not reduced, then G is divisible since G is indecomposable. Hence G is isomorphic to $\sigma(p^{\infty})$ by Lemma D.

Hence, in any case, G is p-cocyclic and the theorem is proved.