A Decomposition Theory for Finite Groups with Applications to p-Groups

Thesis by

Paul Morris Weichsel

In Partial Fulfillment of the Requirements
For the Degree of
Doctor of Philosophy

California Institute of Technology
Pasadena, California

1960

ACKNOWLEDGEMENTS

The author wishes to express his thanks and appreciation to Professor Richard A. Dean who acted as adviser and friend during the preparation and writing of this thesis. His many helpful suggestions and patience were of invaluable assistance. Many thanks are also due to Miss Evangeline Gibson for her expert typing of the manuscript.

ABSTRACT

Let $\{G_\alpha\}$ be a set of finite groups and define $\overline{\{G_\alpha\}}$ to be the intersection of all sets of groups which contain $\{G_\alpha\}$ and are closed under the operations of subgroup, factor group and direct product. The equivalence relation defined by $G_1 \equiv G_2$ if $\overline{\{G_1\}} = \overline{\{G_2\}}$ is studied and it is shown that if Q_n and D_n are the generalized quaternion group of order 2^n and the dihedral group of order 2^n then $\overline{\{Q_n\}} = \overline{\{D_n\}}$.

A group G is called decomposable if $G \in \overline{\{A_\alpha\}}$ with $\{A_\alpha\}$ the set of proper subgroups and factor groups of G. It is shown that if G is decomposable then G must contain a proper subgroup or factor group whose class is the same as the class of G and one whose derived length is the same as the derived length of G. The set of indecomposable p-groups of class two are characterized and for $p \neq 2$ their defining relations are compiled. It is also shown that if the exponent of G is p and the class of G is greater than two then G is decomposable if $G/Z(G)$ is a direct product.

Finally the equivalence relation given above is modified and its connection with the isoclinism relation of P. Hall is investigated. It is shown that for a certain class of p-groups this relation is equivalent to isoclinism.

INTRODUCTION

This thesis introduces a notion of decomposition for finite groups which includes direct product and subdirect product as special cases. First a closure operator on sets of finite groups is introduced which embeds a given set of groups $\{G_\alpha\}$ into its "closure", denoted by $\overline{\{G_\alpha\}}$, which is the smallest set of groups containing $\{G_\alpha\}$ and closed under the operations of direct product, subgroup and factor group. A natural question which arises in studying this operator is: What are necessary and sufficient conditions for $\overline{\{G_1\}} = \overline{\{G_2\}}$? This question seems quite hard and is not answered in this thesis. One interesting result that is obtained along these lines is that the closure of the generalized quaternion group is equal to the closure of the dihedral group of the same order.

A group G is then defined to be decomposable if $G \in \overline{\{A_\alpha\}}$ where $\{A_\alpha\}$ is the set of all proper subgroups and factor groups of G. In classifying the various ways in which a group G may be decomposable a mode of decomposition which we call factordirect product and which is in many ways the dual of subdirect decomposition is introduced. It is also shown that simple groups are indecomposable in the sense defined above. In an attempt to obtain necessary conditions for a group G to be decomposable it is shown that if $G \in \overline{\{A_\alpha\}}$ then $G/Z(G) \in \overline{\{A_\alpha/Z(A_\alpha)\}}$ and if $G \in \overline{\{A_\alpha\}}$ then $G' \in \overline{\{A_\alpha\}}$. This provides important information concerning the kinds of subgroups and factor groups that a decomposable group must have. It tells for example that a decomposable p-group of class n must have a subgroup or factor group of class n. The remaining chapters are an attempt to apply the

ideas expressed above to finite p-groups.

Chapter II gives several characterizations of the set of indecomposable p-groups of class two. And in the case of $p \neq 2$ all the possible defining relations for such groups are enumerated. This enumeration allows one to assert that given any finite p-group G of class two, with $p \neq 2$ there exists a finite set of indecomposable groups $\{G_\alpha\}$ whose defining relations are given, such that G may be constructed in a finite number of steps from $\{G_\alpha\}$ by the application of the operations of subgroup, factor group and direct product.

In Chapter III an attempt is made to gain information about the decomposability of a p-group G from the knowledge that G/Z(G) is decomposable. If the class of G is greater than two and if the exponent of G is p it is shown that G is decomposable if G/Z(G) is a direct product. An example is given which shows that this decomposition is in general non-trivial. That is, G is neither a direct, subdirect or factordirect product.

The concluding chapter studies the connection between the closure operator and a group relation know as "isoclinism" which was introduced by P. Hall in 1940. It is easy to show that both of these ideas provide a partition of the set of finite groups into equivalence classes which share many numerical invariants. The connection between closure and isoclinism is made precise by introducing a restricted form of closure. It is then shown that for a certain class of p-groups these two concepts are equivalent.

Chapter I

Any algebraic decomposition theory specifies a certain set of algebras which may be called the "basis set" and a set of operations defined on the basis set. The basis theorem then states that any algebra of the type being considered may be obtained from the basis set by some applications of the given operations. In addition if a given algebra A is to be called decomposable then the basis elements required for its construction should be contained, in some sense, in A.

In the theory of finite abelian groups such a decomposition theory does indeed exist. The basis set is the set of all cyclic p-groups and the operation is that of direct product. In this case a group G may be constructed as a direct product of a certain subset of cyclic p-subgroups.

There exists a decomposition theory for all finite groups in the sense that every finite group may be obtained in a finite number of steps by applying the operation of group extension to a set of simple groups. That is, for an arbitrary finite group G there exists a finite set of simple groups, $\{A_\alpha\}$, the factors of a composition series of G, such that for some ordering of the $\{A_\alpha\}$, a sequence $\{B_i\}$ may be defined as follows: $B_1 = A_1$, B_i is an extension of A_i by B_{i-1} for $i = 1, \ldots, n$ and $G \cong B_n$.

One way of measuring the effectiveness of a given theory is its degree of "balance". A decomposition theory ought to divide the difficulty of understanding a class of algebras between the study of a fairly restricted set of them and the study of the effect of certain operations on the set. If the basis set is extremely easy to study but the operations

very complex then it may be said that the theory is unbalanced. In such a case the basis theorem that results will most likely not be very informative. Exactly such a state of affairs obtains if we restrict our attention to the set of finite p-groups for a particular prime p, and choose group extension as the operation. Here the basis set will be the set of all simple p-groups. But the only finite p-group which is simple is the group of order p. Hence all of the difficulty lies in understanding the operation of extending a p-group by a group of order p. On the other hand if we let the operation be direct product then the basis set becomes those finite p-groups which cannot be represented as a direct product. In this case little can be said concerning the basis set as such.

A decomposition theory for finite groups will here be developed which lies somewhere in between the two examples given above. That is, the basis set will contain all simple groups and will be contained in the set of all groups which are not direct products.

From this point on the word "group" will be used to mean "finite group".

Since it will be convenient to refer interchangeably to the notions of subgroup, factor group and factor group of a subgroup we define:

DEFINITION 1.1 A group A is said to be an ingroup of a group G if one of the following holds:

a) A is isomorphic to a subgroup of G.

b) A is isomorphic to a factor group of G.

c) A is isomorphic to a factor group of a subgroup of G.

The notation $A \leq G$ [1] will be used for the above with $A < G$ denoting that A is an ingroup of G but A is not isomorphic with G. In this case A is said to be a proper ingroup of G.

LEMMA 1.1 The relation $A \leq G$ is reflexive and transitive.

Proof $G \leq G$ since if $G = A$ then condition a) of Definition 1.1 is satisfied. Hence the relation is reflexive.

To demonstrate transitivity it must be shown that $A \leq B \leq C$ implies $A \leq C$. Denote the relation between A and B by I, the relation between B and C by II and that between A and C by III. It must now be shown that for all choices of I and II, III is one of the relations given in the definition. The following tabulation gives the results required.

	I	II	III
1)	a	a	a
2)	a	b	c
3)	a	c	c
4)	b	a	c
5)	b	b	b
6)	b	c	c
7)	c	a	c
8)	c	b	c
9)	c	c	c

---

1. For the convenience of the reader all symbols used in this thesis are collected in a glossary on page 62.

Note first that 1), 5), 6), and 7) follow from the fact that the relation "subgroup" and "factor group" are transitive relations. 4) is precisely the statement of alternative c) in Definition 1.1.

Now consider 2). Here B is a factor group of C and A is a subgroup of B. Hence $B = C/N$ and $A \subset B$. The inverse image of A in C, call it A_1, is a subgroup of C which contains N as a normal subgroup. Hence $A = A_1/N$ and $A_1 \subset C$. Therefore A is a factor group of a subgroup of C and hence III = c. Now 3) follows since A is a subgroup of a factor group of C. Hence A is a factor group of a subgroup of a subgroup of C and therefore alternative c) holds. Since it has been shown in the proof of 2) above that a subgroup of a factor group is a factor group of a subgroup 8) and 9) follow from the transitivity of the relations: subgroup and factor group.

We now define the notion of closure.

DEFINITION 1.2 Let $\{A_\alpha\}$ be a set of groups. A group G is said to be of rank 0 if $G \leq A$ for some $A \in \{A_\alpha\}$. G is of rank 1 if G is not of rank 0 and $G \leq A \times B$ with A and B of rank 0. In general G is of rank n if G has not been assigned rank $n-k$ for $k > 0$ and $G \leq C \times D$ with C and D both of rank less than n. The set of groups with assigned rank is called the closure of $\{A_\alpha\}$ and is denoted by $\overline{\{A_\alpha\}}$. [2]

The closure of a set of groups may also be described in a some-

---

2. Graham Higman, in a recent paper [1] has studied sets of groups with the property of being closed in the sense defined above.

what different manner.

LEMMA 1.2 If $\{A_\alpha\}$ is a set of groups then $\overline{\{A_\alpha\}}$ is closed under the operations of ingroup, factor group, and direct product. Furthermore, every set of groups which contains $\{A_\alpha\}$ and is closed under the operations given above contains $\overline{\{A_\alpha\}}$.

Proof If $G \in \overline{\{A_\alpha\}}$ then $G \leq C \times D$ with $C, D \in \overline{\{A_\alpha\}}$. Let $G \geq H$. Since the relation "$\leq$" is transitive it follows that $H \leq C \times D$. Hence $H \in \overline{\{A_\alpha\}}$. Suppose that $E, F \in \overline{\{A_\alpha\}}$. Then $E \times F \leq E \times F$ and therefore is contained in $\overline{\{A_\alpha\}}$.

Now suppose that $\mathfrak{A}$ is a set of groups closed under the operations of ingroup and direct product and $\mathfrak{A} \supseteq \{A_\alpha\}$. To show that $\overline{\{A_\alpha\}} \subseteq \mathfrak{A}$ consider $G \in \overline{\{A_\alpha\}}$ of rank 0. In this case $G \leq A \in \overline{\{A_\alpha\}} \subseteq \mathfrak{A}$ and since $\mathfrak{A}$ is closed under the operation of ingroup then $G \in \mathfrak{A}$. Suppose that all elements of $\overline{\{A_\alpha\}}$ of rank less than k are contained in $\mathfrak{A}$. Let $G \in \overline{\{A_\alpha\}}$ be of rank k. Therefore $G \leq C \times D$ where C, D are of rank less than k in $\overline{\{A_\alpha\}}$. Hence $C, D \in \mathfrak{A}$ and since $\mathfrak{A}$ is closed under direct product and ingroup $G \in \mathfrak{A}$. Therefore $\overline{\{A_\alpha\}} \subseteq \mathfrak{A}$.

The closure of a set of groups may therefore be thought of as the intersection of all sets containing the original set of groups and closed under the operations of ingroup and direct product.

If closure, as defined above, is regarded as a mapping defined on the set of all subsets of finite groups then it is a closure operator in the usual sense. That is:

LEMMA 1.3 If $\{A_\alpha\}$ and $\{B_\beta\}$ are sets of groups then:

a) $\{A_\alpha\} \subseteq \overline{\{A_\alpha\}}$,

b) $\overline{\{\overline{A_\alpha}\}} = \{\overline{A_\alpha}\}$ and

c) if $\{A_\alpha\} \subseteq \{B_\beta\}$ then $\{\overline{A_\alpha}\} \subseteq \{\overline{B_\beta}\}$.

Proof a) If $G \in \{A_\alpha\}$ then G is of rank 0 in $\{\overline{A_\alpha}\}$ and hence $\{A_\alpha\} \subseteq \{\overline{A_\alpha}\}$.

b) Clearly $\{\overline{A_\alpha}\} \subseteq \overline{\{\overline{A_\alpha}\}}$ since all elements of $\{\overline{A_\alpha}\}$ are of rank 0 in $\overline{\{\overline{A_\alpha}\}}$. Let $G \in \overline{\{\overline{A_\alpha}\}}$ be of rank 0. Then $G \leq B \in \{\overline{A_\alpha}\}$. But $\{\overline{A_\alpha}\}$ is closed under ingroups and therefore $G \in \{\overline{A_\alpha}\}$. Assume that every element of $\overline{\{\overline{A_\alpha}\}}$ whose rank is less than some integer k is contained in $\{\overline{A_\alpha}\}$. Let G be of rank k in $\overline{\{\overline{A_\alpha}\}}$. Then $G \leq E \times F$ with $E, F \in \{\overline{A_\alpha}\}$ of rank less than k. Therefore $E, F \in \{\overline{A_\alpha}\}$ and since $\{\overline{A_\alpha}\}$ is closed under direct products and ingroups $G \in \{\overline{A_\alpha}\}$. Therefore $\overline{\{\overline{A_\alpha}\}} \subseteq \{\overline{A_\alpha}\}$ and hence $\overline{\{\overline{A_\alpha}\}} = \{\overline{A_\alpha}\}$.

c) Since $\{\overline{B_\beta}\}$ is closed under the operations of ingroup and direct product, and since $\{\overline{B_\beta}\} \supseteq \{B_\beta\} \supseteq \{A_\alpha\}$, it follows from Lemma 1.2 that $\{\overline{B_\beta}\} \supseteq \{\overline{A_\alpha}\}$.

A natural question which arises from the definition of closure is: Can one give necessary and sufficient conditions for $\{\overline{G_1}\} = \{\overline{G_2}\}$, G_1 and G_2 arbitrary groups? The answer to this question is, in general, not easy. For certain classes of groups, however, a straightforward answer may be given.

It can easily be proved that: If G_1 and G_2 are abelian groups then $\{\overline{G_1}\} = \{\overline{G_2}\}$ if and only if the exponent of G_1 is equal to the exponent of G_2, written $e(G_1) = e(G_2)$.

One interesting fact that arises in this connection is given by:

THEOREM 1.1 Let Q_n be the generalized quaternion group[3] of order 2^n, and let D_n be the dihedral group of order 2^n with $n \geq 3$. Then $\{\overline{D_n}\} = \{\overline{Q_n}\}$.

Proof $Q_n = \langle a, b \rangle$ with $a^{2^{n-1}} = 1$, $b^2 = a^{2^{n-2}}$ and $bab^{-1} = a^{-1}$.

$D_n = \langle g, h \rangle$ with $g^{2^{n-1}} = h^2 = 1$, $hgh^{-1} = g^{-1}$. In both of these cases $n \geq 3$. The theorem will be proved by showing that $D_n \in \{\overline{Q_n}\}$ and $Q_n \in \{\overline{D_n}\}$. It will then follow from Lemma 1.3 that $\{\overline{D_n}\} = \{\overline{Q_n}\}$.

In order to show that $D_n \in \{\overline{Q_n}\}$ it suffices to form the direct product of Q_n with a cyclic group of order 4 and then consider an appropriate factor group of a subgroup of this direct product. Since Q_n contains a cyclic group of order 4 as a subgroup, the group which results will be contained in $\{\overline{Q_n}\}$. It will then be shown that this group is isomorphic to D_n.

A similar procedure will be adopted to show that $Q_n \in \{\overline{D_n}\}$.

Let $H = \langle c \rangle$ with $c^4 = 1$. Let $G = Q_n \times H$ and let $N = \langle [b^2, c^2] \rangle$. Clearly $N \lhd G$ since $b^2 \in Z(Q_n)$. Let $G_1 = G/N = \langle [a, 1] N, [b, 1] N, [1, c] N \rangle$. Now consider a subgroup of $G_1 \supset D = \langle [a, 1] N, [b, c] N \rangle$ and we will now show that $D \simeq D_n$.

It is clear that $([a, 1] N)^{2^{n-1}} = ([b, c] N)^2 = 1$. Also $[b, c] N [a, 1] N [b, c]^{-1} N = [b a b^{-1}, 1] N = [a^{-1}, 1] N = ([a, 1] N)^{-1}$. Hence the generators of D satisfy the same relations as to the generators of D_n. If it can be shown that the order of D equals the order of D_n then the isomorphism will follow.

---

3. Zassenhaus [2] p. 147.

Since $o(Q_n \times H) = 4 \cdot o(D_n)$ and $o(N) = 2$ it must be shown that $[G_1 : D] = 2$. We claim that $G_1 = D + ([b, c^2]N)D$.

Since any element of Q_n may be written as a word in a and b, it can be put in the form $b^{\beta} a^{\alpha}$. This follows from the fact that $ab = ba^{-1}$. Hence a general element of G_1 has the form $[b^{\beta} a^{\alpha}, c^{\gamma}]N$. Now it will be shown that $[b^{\beta} a^{\alpha}, c^{\gamma}]N$ is either in D or in $[b, c^2]ND$.

Since $D = \langle [a, 1] N, [b, c] N \rangle$, $[b, c]^{\beta} [a, 1]^{\alpha} N = [b^{\beta} a^{\alpha}, c^{\beta}] N \in D$. We must now consider the four cases: a) $\gamma \equiv \beta(4)$, b) $\gamma \equiv \beta + 1(4)$, c) $\gamma \equiv \beta + 2(4)$, and d) $\gamma \equiv \beta + 3(4)$.

In case a) $[b^{\beta} a^{\alpha}, c^{\gamma}]N = [b^{\beta} a^{\alpha}, c^{\beta}] N \in D$. In case b) notice that $[b^{-1}, c^{-1}]N \in D$ and so $[b^{-1}, c^{-1}] N [b^{\beta} a^{\alpha}, c^{\beta}] = [b^{\beta-1} a^{\alpha}, c^{\beta-1}]N \in D$. But $[b, c^2]N[b^{\beta-1} a^{\alpha}, c^{\beta-1}]N = [b^{\beta} a^{\alpha}, c^{\beta+1}]N = [b^{\beta} a^{\alpha}, c^{\gamma}]N \in [b, c^2]ND$. In case c) notice that $[a, 1]^{-2^{n-2}} N [b, c]^2 N = [1, c^2] N \in D$. Hence $[b^{\beta} a^{\alpha}, c^{\beta}] N [1, c^2]N = [b^{\beta} a^{\alpha}, c^{\beta+2}]N = [b^{\beta} a^{\alpha}, c^{\gamma}] N \in D$. Finally for case d) $[b, c]^{-1} N [1, c^2] N = [b^{-1}, c] N \in D$. Hence $[b, c^2]N[b^{-1}, c] N [b^{\beta} a^{\alpha}, c^{\beta}] N = [b^{\beta} a^{\alpha}, c^{\beta+3}] N = [b^{\beta} a^{\alpha}, c^{\gamma}]N$.

Therefore $o(D) = o(D_n)$ and $D \simeq D_n$.

Let H be defined as above and consider $R = D_n \times H$. Clearly $R \in \{\overline{D_n}\}$. Let $R \supset S = \langle [g, 1], [h, c] \rangle$. Let $M = \langle [g^{2^{n-2}}, c^2] \rangle$. Since $[h, c]^2 = [1, c^2]$ clearly $M \subset S$. And since $h g^{2^{n-2}} h^{-1} = g^{-2^{n-2}} = g^{2^{n-2}}$ it follows that $M \lhd S$. Let $Q = S/M$ and we will now show that $Q \simeq Q_n$.

As in the previous case the generators of Q satisfy the same relations as the corresponding generators of Q_n. For $([g, 1] M)^{2^{n-2}} = [g^{2^{n-2}}, 1] M = [1, c^2] M = ([h, c] M)^2$. Also $[h, c] M [g, 1] M ([h, c] M)^{-1}$

$= [h g h^{-1}, 1] M = [g^{-1}, 1] M = ([g, 1] M)^{-1}$.

Since $o(D_n \times H) = 4\, o(Q_n)$ and $o(M) = 2$, in order to show that $o(Q) = o(Q_n)$ we must show that the index of S in R is equal to 2. We claim that $R = S + [1, c]S$. For an arbitrary element of R is of the form $[h^{\beta} g^{\alpha}, c^{\gamma}]$. Clearly the element $[h^{\beta} g^{\alpha}, c^{\beta}] \in S$, and since $[1, c^2] \in S$ it follows that for $\gamma \equiv \beta(4)$ and $\gamma \equiv \beta + 2(4)$ $[h^{\beta} g^{\alpha}, c^{\gamma}] \in S$. If $\gamma \equiv 1 + \beta(4)$ or $\gamma \equiv 3 + \beta(4)$, $[h^{\beta} g^{\alpha}, c^{\gamma}] \in [1, c]S$. Therefore $Q \simeq Q_n$. Hence we have shown that $Q_n \in \{\overline{D_n}\}$ and $D_n \in \{\overline{Q_n}\}$ and therefore $\{\overline{D_n}\} = \{\overline{Q_n}\}$.

The closure of a set of groups can be regarded in a somewhat different light, namely as defining a rather special group-theoretic property. Any group property is determined by some set and conversely. The most familiar kinds of group properties have what can be called "inheritance". A property is said to be subgroup inherited if whenever a group has this property then so do all of its subgroups. In a similar way one defines factor group and direct product inheritance. It can be said that a property is considered important and interesting to study if it does have many inheritance characteristics. Commutativity, nilpotence and solubility are examples.

Therefore the closure of a set of groups is that set which defines the weakest property, which is subgroup, factor group and direct product inherited, that is shared by all the elements of the set. Weakest merely means that every other such property which is satisfied by all of the elements of the set is defined by a set of groups which contains the closure of the original set. Theorem 1.1 can thus be restated.

Every property satisfied by Q_n which is subgroup, factor group and direct product inherited is also satisfied by D_n and conversely.

Having now studied some properties of those operations which will be used to construct all finite groups from a given basis set we are now ready to define the notion of decomposability.

DEFINITION 1.3. Let G be a group and let $\{A_\alpha\}$ be the set of all proper ingroups of G. G is called decomposable if $G \in \overline{\{A_\alpha\}}$.

$G \in \overline{\{A_\alpha\}}$ implies that there exist $A, B \in \overline{\{A_\alpha\}}$ such that $G \leq A \times B$. This can happen in four ways.

I. First suppose that $G = A \times B$. Since A and B are subgroups of G and hence are contained in $\{A_\alpha\}$ it follows that G is of rank 1 in $\overline{\{A_\alpha\}}$.

II. Let $G \subset A \times B$. Since A and B are finite groups it certainly follows that A and B may be chosen so that for any choice of A_1 and B_1, proper subgroups of A and B respectively, $G \not\subseteq A_1 \times B$ and $G \not\subseteq A \times B_1$. With such a choice of A and $B \neq 1$, G is said to be a subdirect product of A and B. Subdirect products may be characterized in the following way:

A group G is a subdirect product of groups A and B if and only if there exist non-trivial subgroups $N_1, N_2 \lhd G$ such that $N_1 \cap N_2 = 1$ and $G/N_1 \simeq A$ and $G/N_2 \simeq B$.

The embedding of G into $A \times B$ is given by

$$g \longrightarrow [gN_1, gN_2] \in G/N_1 \times G/N_2 = A \times B$$

for all $g \in G$.

Thus if G is a subdirect product of A and B then since A and B are factor groups of G, A and B are contained in $\{A_\alpha\}$ and hence G is of rank 1 in $\overline{\{A_\alpha\}}$.

III. Let $G = (A \times B)/N$. In light of the definition of subdirect product it is natural to ask: Do there exist subgroups of G which are isomorphic with A and B?

THEOREM 1.2 Let $G = (A \times B)/N$. Then there exist subgroups A_1 and B_1 of G such that 1) $G \simeq (A_1 \times B_1)/N_1$ for some N_1,

2) A_1 and B_1 are isomorphic to factor groups of A and B respectively and

3) $G = A_2B_2$, with $A_2 \simeq A_1$, $B_2 \simeq B_1$ and A_2 and B_2 permute elementwise.

Proof For the sake of simplicity we will write $A \times B$ as AB, and ab in place of $[a, b]$.

Let $M = (A \cap N) \cup (B \cap N)$. Since $M \lhd G$ we may write $G = AB/N \simeq AB/M\big/N/M = AM/M \cdot BM/M\big/N/M$. This last equality holds because every element of AB/M is of the form $abM = aMbM \in AM/M \cdot BM/M$. Similarly a typical element of $AM/M \cdot BM/M$ is $am_1Mbm_2M = aMbM = abM$. We will now show that $AM/M \cdot BM/M$ is a direct product.

Suppose $AM/M \cap BM/M \supset M/M$. Then there exists $a_1 \in A$ and $b_1 \in B$ such that $a_1M = b_1M$. Hence $a_1 = b_1m = b_1ab$ and $a_1 = a$. But since $A \cap B = 1$, M is the direct product of $A \cap N$ and $B \cap N$ and so $ab \in M$ implies that $a, b \in N$. Hence $a \in M$ and $a_1M = M$.

Clearly AM/M, $BM/M \lhd AB/M$ and so $AM/M \cdot BM/M = AM/M \times BM/M$.

Let $A_1 = AM/M$ and $B_1 = BM/M$. Hence $G = (A_1 \times B_1)/N$ and A_1, B_1 are isomorphic to factor groups of A and B respectively. Further $A_1 \cap N_1 = B_1 \cap N_1 = 1$. Let $A_2 = A_1N_1/N_1$ and $B_2 = B_1N_1/N_1$. Then $G = A_2B_2$, $A_1 \simeq A_2$, $B_1 \simeq B_2$ and A_2 and B_2 permute elementwise. For $A_1 \cap B_1 = 1$ and hence permute elementwise. This completes the proof of the theorem.

In analogy with the notion of a subdirect product this theorem leads to the definition of factordirect product.

DEFINITION 1.4 A group G is called a factordirect product of A and B if for some N, $G \simeq (A \times B)/N$ and $1 \neq A$, $B \subset G$.

Thus Theorem 1.2 shows that if $G = (A \times B)/N$ then G is a factordirect product of two groups which are factor groups of A and B respectively.

It will now be shown that condition 3) of Theorem 1.2 implies that G is a factordirect product.

THEOREM 1.3 If $G = AB$ and $ab = ba$ for all $a \in A$ and all $b \in B$ then G is a factordirect product of A and B.

Proof Let $H = A \times B = \{[a, b] \; a \in A, \; b \in B\}$. Let $N = \{[c, c^{-1}] / \text{ for all } c \in A \cap B \text{ considered as subgroups of } G\}$. Since A and B permute elementwise in G it follows that $A \cap B \subseteq Z(G)$. Therefore $N \lhd A \times B$.

Consider the following mapping between G and $A \times B/N$.

$$G \ni g = a_1 b_1 \longleftrightarrow [a_1, b_1] \; N.$$

To show that it is one-one let $a_1b_1 = a_2b_2$. Then $b_1b_2^{-1} = a_1^{-1}a_2$. Since A and B permute elementwise and $a_1^{-1}a_2 \in B$, $a_1^{-1}a_2b_2 = b_2a_1^{-1}a_2 = b_1$. This implies that $a_1^{-1}a_2 = b_2^{-1}b_1$.

Now consider the images of a_1b_1 and a_2b_2 in $A \times B/N$. $[a_1, b_1]N = [a_1, b_1]\ N\ [a_1^{-1}a_2, b_1^{-1}b_2]\ N$ since $[a_1^{-1}a_2, b_1^{-1}b_2]\ N = N$. Therefore $[a_1, b_1]\ N = [a_2, b_2]\ N$.

Suppose that $[a_1, b_1]\ N = [a_2, b_2]\ N$. Then there exists $c \in A \cap B$ such that $[a_1, b_1] = [a_2, b_2]\ [c, c^{-1}]$. Hence $a_1 = a_2c$ and $b_1 = b_2c^{-1}$. Thus $a_2^{-1}a_1 = b_1^{-1}b_2$. But this implies that $a_2^{-1}a_1 = b_2b_1^{-1}$ and hence $a_1b_1 = a_2b_2$.

To show that it is a homomorphism suppose that

$$a_1b_1 \longleftrightarrow [a_1, b_1]\ N$$

and

$$a_2b_2 \longleftrightarrow [a_2, b_2]\ N.$$

Then $a_1b_1a_2b_2 = a_1a_2b_1b_2$ and similarly $[a_1, b_1]\ N\ [a_2, b_2]\ N = [a_1a_2, b_1b_2]\ N$. Hence the mapping is an isomorphism, and $G \simeq A \times B/N$. Since $A, B \subset G$, G is a factordirect product of A and B.

It is interesting to note that subdirect and factordirect products are dual in many respects. One illustration of this duality is the fact that the relation of "subdirect product" is transitive in some sense. And a similar result may also be stated for factordirect products.

First consider the subdirect case.

LEMMA 1.4 Let G be a subdirect product of A and B. If $H \subseteq G$ then either H is a subdirect product or else H is isomorphic to a

subgroup of A or B.

Proof Clearly $H \subseteq A \times B$. If $H \cap A \neq 1$ and $H \cap B \neq 1$ then H is a subdirect product, i.e. $H \subset (H/H \cap A) \times (H/H \cap B)$.

Suppose $H \cap A = 1$. Let $B_1 = \{b_i \mid [a_j, b_i] \in H\}$ and consider the mapping between H and B_1:

$$H \ni [a, b] \longleftrightarrow b \in B_1.$$

To show that this is one-one suppose that $[a_1, b_1] = [a_2, b_2]$ in H. Then $b_1 = b_2$. If $b_1 = b_2$ then consider $[a_2, b_2]$ and $[a_1, b_1]$. Clearly $[a_2, b_2]\,[a_1^{-1}, b_1^{-1}] = [a_2 a_1^{-1}, 1] \in H$. But $H \cap A = 1$. Hence $a_2 a_1^{-1} = 1$ and therefore $[a_2, b_2] = [a_1, b_1]$. Hence the mapping is one-one.

Since multiplication in H is carried out componentwise the mapping is clearly a homomorphism and under the assumption that $H \cap A = 1$, $H \simeq B_1 \subseteq B$.

If $H \cap B = 1$ then the argument above, applied to a subgroup of A shows that $H \simeq A_1 \subseteq A$. This completes the proof.

It is natural to ask whether a factor group of a subdirect product is always either a subdirect product or isomorphic to a factor group of one of the factors. The answer to this question is in the negative as may be demonstrated by the quaternion group of order 8. For it has been shown in Theorem 1.1 that the quaternion group is a factor group of a subdirect product of the dihedral group of order 8 and the cyclic group of order 4. Clearly the quaternion group is neither a factor group of either of these nor is it a subdirect product.

The dual result to Lemma 1.4 for factordirect products is as follows:

LEMMA 1.5 Let G be a factordirect product of A and B. If $H = G/N$ then either H is a factordirect product or else H is isomorphic to a factor group of A or B.

Proof Since G is a factordirect product $G = A_1B_1$ with $ab = ba$ for all $a \in A_1$ and $b \in B_1$. Let $N \lhd G$. Then $G/N = A_1N/N \cdot B_1N/N$. But $A_1N/N \simeq A_1/A_1 \cap N$ and $B_1N/N \simeq B_1/B_1 \cap N$, and these groups permute elementwise. If neither $A_1 \cap N$ or $B_1 \cap N = 1$ then H is a factordirect product. If $A_1 \cap N = A_1$ then $H \simeq B_1/B_1 \cap N$, and similarly for $A_1 \cap N$.

Analogous to the subdirect product situation a subgroup of a factordirect product need not be a subgroup of one of the factors or a factordirect product itself. In the proof of Theorem 1.1 the dihedral group of order 8 is constructed as a subgroup of a factordirect product of the quaternion group and the cyclic group of order 4. Clearly it is neither a factordirect product nor is it isomorphic to a subgroup of one of the factors.

IV. The final case in the enumeration of $G \leq A \times B$ is $G = H/N$ with $H \subset A \times B$. A very important distinction sets this case apart from the others. For up until now it has been the case that if $G < A \times B$ then $G \leq A_1 \times B_1$, with A_1, B_1 proper ingroups of G. No such conclusion will be possible here as is illustrated by Theorem 1.1. In other words, let $\{H_\alpha\}$ be a set of groups. Then if $G \in \overline{\{H_\alpha\}}$ by virtue of being a non-trivial direct product, subdirect product or

factordirect product then $G \in \overline{\{A_\alpha\}}$ where $\{A_\alpha\}$ is the set of proper ingroups of G.

In any event if $G = H/N$ with $H \subset A \times B$ then a special choice of the groups A, B, H, and N may be made.

LEMMA 1.6 Let $G = H_1/N_1$ with H_1 a subdirect product of A_1, B_1, $\neq 1$. Then there exist factor groups A, B, H and N of A_1, B_1, H_1, and N_1 respectively such that $G \simeq H/N$, $H \subset A \times B$ and there exist $R, S \lhd H$ such that:

$$R \cap S = R \cap N = S \cap N = 1.$$

Proof Since H_1 is a subdirect product it follows that there exist subgroups $R_1, S_1 \lhd H_1$ such that $R_1 \cap S_1 = 1$. Suppose that $(R_1 \cap N_1) \cup (S_1 \cap N) = M \supset 1$. Let $N = N_1/M$, $H = H_1/M$, $R = R_1M/M$ and $S = S_1M/M$. Clearly $R \cap N = 1$ since if $rmM = nm'M$ with $r \in R_1$, $m, m' \in M$ and $n \in N$, then $r = nm'' = nr's'$. This follows from the definition of M. But $r' \in R_1 \cap N_1 \subseteq M$ and $s' \in S_1 \cap N_1 \subseteq M$. Hence $r \in N_1$ and therefore $r \in R_1 \cap N_1 \subseteq M$, which implies that $rmM = M$. In a similar manner it can be shown that $S \cap N = 1$. Since $R_1 \cap S_1 = 1$ it is clear that $R \cap S = 1$ and since $R_1M/M \simeq R_1/R_1 \cap M$ the lemma is proved.

Since the case of $G \subset A \times B$ already has been considered we will assume now that $G \simeq H/N$ is not a subdirect product.

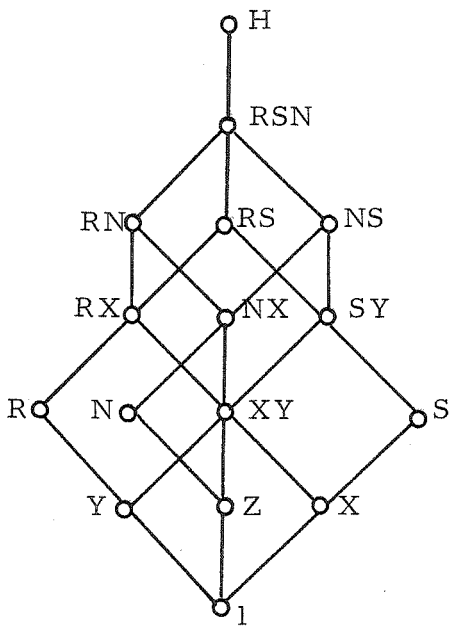
THEOREM 1.4 Let G, H, A, B, R, S be defined as in the lemma above. Assume in addition that G is not a subdirect product and that G is not isomorphic to a factor group of A or B. Then G contains

a normal abelian p-group.

Proof Consider the element $S \cap NR$. Since all of these subgroups are normal $R \cup N$ may be written as RN or NR.

Assume first that $NR \cap S = 1$. Since the lattice of normal subgroups of a group is modular it follows that $N \cup (NR \cap S) = NR \cap NS = N$. Now if $NR \neq N$ and $NS \neq N$ then $NR \neq NS$ and hence H/N is a subdirect product. If $NR = N$ then $G = H/N \simeq H/R \Big/ N/R$ and hence G is isomorphic to a factor group of A. If $NS = N$ then $G = H/N \simeq H/R \Big/ N/R$ and G is isomorphic to a factor group of B. Hence if $NR \cap S = 1$ then G is either a subdirect product or G is isomorphic to a factor group of A. But it is easy to see that $NR \cap S = 1$ if and only if $NS \cap R = 1$ which holds if and only if $RS \cap N = 1$. For if $RS \cap N \neq 1$ then there exist r, s, and n such that $rs = n \neq 1$, and hence $s = r^{-1}n$ and $r = ns^{-1}$. Note that $r \neq 1$ and $s \neq 1$ for otherwise $R \cap N \neq 1$ and $S \cap N \neq 1$ contrary to Lemma 1.6. Hence if $Y = NS \cap R$ and $Z = RS \cap N$ then $Y \neq 1$ and $Z \neq 1$.

The lattice diagram in Figure 1 below illustrates the relationships of the groups that have been discussed above. All of the argument above and some of the argument that follows will verify that the unions and intersections given in the diagram are indeed correct.



$X = NR \cap S$

$Y = NS \cap R$

$Z = RS \cap N$

FIGURE 1

$X \cap Y = (NR \cap S) \cap (NS \cap R) \subseteq R \cap S = 1$. Applying the same argument to $X \cap Z$ and $Y \cap Z$, (i) $X \cap Y = X \cap Z = Y \cap Z = 1$. By the use of the modular law we see: $XY = (NR \cap S) \cup (NS \cap R)$ $= NS \cap [(NR \cap S) \cup R] = NS \cap NR \cap RS$. By symmetry the same result holds for XZ and YZ. Hence

(ii) $XY = XZ = YZ = XYZ$.

Ore [3] has shown that under conditions (i) and (ii) the group XY is abelian.

Consider $XY \cup N = (NS \cap NR \cap RS) \cup N = NS \cap [N \cup (NR \cap S)]$ $= NS \cap [NR \cap (N \cup RS)] = NS \cap [NR \cap NRS] = NS \cap NR$. Also $XY \cap N$ $= [NS \cap NR \cap RS] \cap N = N \cap RS = Z$. Therefore $RN \cap SN/N$ $= XY \cap N/N \simeq XY/XY \cap N = XY/Z = XZ/Z \simeq X$. Hence we have exhibited a normal subgroup of $H/N = G$ isomorphic with X, which is abelian. Now if X had composite order then it would contain two characteristic

subgroups with trivial intersection. Since a characteristic subgroup of a normal subgroup is normal it would follow that G is not subdirectly indecomposable. Hence X is a p-group. This completes the proof of the theorem.

Using this theorem, a statement made earlier may now be verified. That is, the basis set of the decomposition theory presented here contains the set of all simple groups.

COROLLARY 1.4.1 If G is a simple group then G is indecomposable.

Proof Assume that G is decomposable. If $\{A_\alpha\}$ is the set of all proper ingroups of G then $G \in \overline{\{A_\alpha\}}$. Since G is simple it is clearly not a subdirect or factordirect product. Hence $G = H/N$ and H is a subdirect product of A and B, $A, B \in \overline{\{A_\alpha\}}$ and the ranks of A and B are less than the rank of G. Theorem 1.4 then shows that G is isomorphic to a factor group of A or B. This implies that the rank of G equals the rank of A or B, a contradiction. Hence $G \in \overline{\{A_\alpha\}}$ must be false and G is indecomposable.

The problem of determining whether or not a given group is indecomposable is a special case of the more general question: Given a group G and a set of groups $\{A_\alpha\}$, what are necessary and sufficient conditions for $G \in \overline{\{A_\alpha\}}$? Three necessary conditions are given below which in the decomposability problem, that is, in the case of $\{A_\alpha\}$ equal to the set of proper ingroups of G, prove to be sufficient for some cases.

THEOREM 1.5 Let $\{A_\alpha\}$ be a set of groups. If $G \in \overline{\{A_\alpha\}}$ then $G/Z(G) \in \overline{\{A_\alpha/Z(A_\alpha)\}}$.

Proof Let G be of rank 0 in $\overline{\{A_\alpha\}}$. This means that $G \leq A \in \{A_\alpha\}$. We now consider all the possibilities for $G \leq A$.

a) Let $G \subset A$. Clearly $G \cup [Z(A) \cup Z(G)] = G \cup Z(A)$. Since $Z(A)Z(G) = Z(G)Z(A)$ the modular law applies and since $Z(A) \cap G \subseteq Z(G)$, $G \cap [Z(A) \cup Z(G)] = Z(G) \cup [Z(A) \cap G] = Z(G)$. Hence $G/Z(G) \simeq G/G \cap [Z(A) \cup Z(G)] \simeq G \cup [Z(A) \cup Z(G)]/Z(A) \cup Z(G)$ $\simeq G \cup Z(A)/Z(A) \cup Z(G) \simeq G \cup Z(A)/Z(A) \Big/ Z(A) \cup Z(G)/Z(A)$. But $G \cup Z(A)/Z(A) \subset A/Z(A)$. Hence $G/Z(G)$ is isomorphic to a factor group of a subgroup of $A/Z(A)$ and $A \in \{A_\alpha\}$.

The proceeding argument may be illustrated by the lattice diagram in Figure 2.

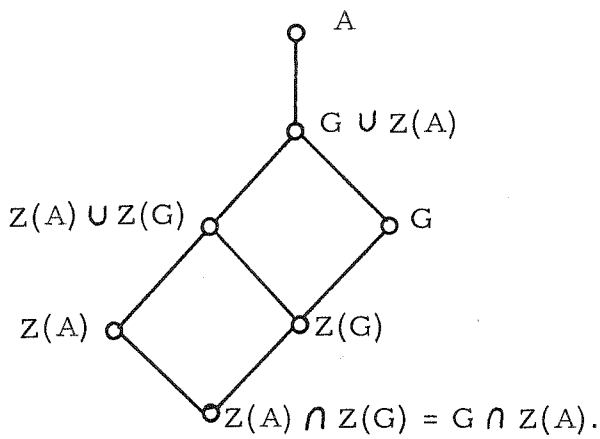


FIGURE 2

b) The second case to consider is $G = A/N$. Let $I_a = aZ(A)$ for $a \in A$ and $I_{aN} = aNZ(A/N)$. We will show that the mapping:

$$I_a \longrightarrow I_{aN} \qquad \text{of } A/Z(A) \qquad \text{into } G/Z(G)$$

is a homomorphism.

Suppose that $I_a = 1$ then $a\,Z(A) = Z(A)$ and $a \in Z(A)$. Consider $I_{aN} = aN\,Z(A/N)$. Since $a \in Z(A)$, $aN \in Z(A/N)$. Hence $I_{aN} = 1$.

Now let $I_{a_1} \longrightarrow I_{a_1 N}$ and

$$I_{a_2} \longrightarrow I_{a_2 N}.$$

$I_{a_1} I_{a_2} = a_1 Z(A)\, a_2 Z(A) = a_1 a_2 Z(A) = I_{a_1 a_2}$, and $I_{a_1 N} I_{a_2 N} = I_{a_1 a_2 N}$. Hence the mapping is a homomorphism and therefore $G/Z(G)$ is isomorphic to a factor group of $A/Z(A)$.

c) Finally if $G \simeq H/N$ and $H \subset A \in \{A_\alpha\}$ then $H/Z(H)$ is isomorphic to a factor group of a subgroup of $A/Z(A)$ and $G/Z(G)$ is isomorphic to a factor group of $H/Z(H)$. Hence $G/Z(G) \in \overline{\{A_\alpha/Z(A_\alpha)\}}$.

This completes the argument for G of rank 0. Notice that the above proves that if $G \leq A$ then $G/Z(G) \leq A/Z(A)$.

Now if G is of rank $n > 0$ then we assume that for all elements of $\overline{\{A_\alpha\}}$ of rank less than n the theorem holds. But $G \leq C \times D$ with C and D of rank less than n. Hence $C/Z(C)$, $D/Z(D) \in \overline{\{A_\alpha/Z(A_\alpha)\}}$. But $C \times D/Z(C \times D) \simeq C/Z(C) \times D/Z(D) \in \overline{\{A_\alpha/Z(A_\alpha)\}}$. Hence since $G/Z(G) \leq C \times D/Z(C \times D)$, $G/Z(G) \in \overline{\{A_\alpha/Z(A_\alpha)\}}$. The proof is then complete by induction.

If the set $\{A_\alpha\}$ is the set of proper ingroups of G and if G is a nilpotent group then the following holds.

COROLLARY 1.5.1 Let G be a nilpotent group. If G is decomposable then G contains a proper ingroup whose class (length of upper central series) is the same as the class of G.

Proof If the class of G is n, written $c(G) = n_1$ and $Z_r(G)$ is the r^{th} element of the upper central series, then $G/Z_n(G) = 1$ and $G/Z_{n-1}(G) \supset 1$. If $G \in \overline{\{A_\alpha\}}$ and the class of A is less than n, then $A/Z_{n-1}(A) = 1$ for all $A \in \{A_\alpha\}$. Therefore $\overline{\{A_\alpha/Z_{n-1}(A_\alpha)\}} = \{1\}$. But it follows from the theorem that if $G \in \overline{\{A_\alpha\}}$ then $G/Z_{n-1}(G) \in \overline{\{A_\alpha/Z_{n-1}(A_\alpha)\}}$. Since $G/Z_{n-1}(G) \supset 1$ this is a contradiction. Hence G is either not decomposable or it contains an ingroup with class n.

THEOREM 1.6 Let $\{A_\alpha\}$ be a set of groups. If $G \in \overline{\{A_\alpha\}}$ then $G' \in \overline{\{A'_\alpha\}}$.

Proof Let G be of rank 0 in $\overline{\{A_\alpha\}}$. Then $G \leq A \in \{A_\alpha\}$.

a) Suppose first that $G \subset A$. Then $G' \subseteq A'$ and hence $G' \in \overline{\{A'_\alpha\}}$.

b) If $G = A/N$ then $G' = (A/N)' = A'N/N \simeq A'/A' \cap N$. Hence $G' \in \overline{\{A'_\alpha\}}$.

c) If $G = H/N$ with $H \subset A$ then $H' \subseteq A'$ and $G' \simeq H'/H' \cap N$. But $H'/H' \cap N \in \overline{\{A'_\alpha\}}$ and hence $G' \in \overline{\{A'_\alpha\}}$.

Now assume that the lemma is true for all groups of rank less than n. Let G be of rank n. Then $G \leq A \times B$ where the ranks of A and B are less than n. But $(A \times B)' = A' \times B'$ and since $R' \leq S'$ if $R \leq S$ it follows that $G' \leq A' \times B' \in \overline{\{A'_\alpha\}}$. The theorem follows by induction.

COROLLARY 1.6.1 Let G be a soluble group. If G is decomposable then G contains a proper ingroup whose derived length equals that of G.

Proof Let $\{A_\alpha\}$ be the set of proper ingroups of G. If the derived length of G is d, then $G^{(d)} = 1$ but $G^{(d-1)} \neq 1$. But it follows from the theorem that $G^{(d-1)} \in \overline{\{A_\alpha^{(d-1)}\}}$, and if the derived length of every proper ingroup of G is less than d then $G^{(d-1)} \in \overline{\{A_\alpha^{(d-1)}\}} = \{\overline{1}\}$, a contradiction. Hence either G is indecomposable or it contains a proper ingroup whose derived length equals that of G.

THEOREM 1.7 Let $\{A_\alpha\}$ be a set of groups. If $G \in \{\overline{A_\alpha}\}$ then there exists a finite subset of $\{A_\alpha\}$, say $\{B_i\}$, such that the exponent of G divides the lcm of the exponents of $\{B_i\}$. That is $e(G) \mid \operatorname{lcm}_i \{e(B_i)\}$.

Proof Let G be of rank 0 in A. Then $G \leq A \in \{A_\alpha\}$.

a) If $G \subset A$ then clearly $e(G) \mid e(A)$.

b) If $G = A/N$ then $e(G) \mid e(A)$.

c) If $G = H/N$ and $H \subset A$ then $e(G) \mid e(H) \mid e(A)$. Hence for rank 0, $\{B_i\} = \{A\}$.

Assume the theorem is true for all groups of rank less than n. If G is of rank n then $G \leq A \times B$, and A and B are of rank less than n. By the induction assumption there exists subsets $\{R_j\}$ and $\{S_k\}$ of $\{A_\alpha\}$ such that $e(A) \mid \operatorname{lcm}_j \{e(R_j)\}$ and $e(B) \mid \operatorname{lcm}_k \{e(S_k)\}$. It follows that if $G \leq A \times B$ then $e(G) \mid \operatorname{lcm}_{j,k} \{e(R_j), e(S_k)\}$. Hence the theorem follows by induction.

From Theorems 1.5, 1.6, and 1.7 given above it appears that the decomposability question might be most accessible for p-groups. Since such groups always possess non-trivial central series and derived series. The next section is a first step in this direction.

Chapter II

In this chapter p-groups of class two will be considered. A group G is of class two if $1 \subset G' \subseteq Z(G)$. That is, G is non-abelian and $G/Z(G)$ is abelian. Since such groups are quite similar to abelian groups it is reasonable to expect that a decomposable group of class two will be decomposable in a rather simple way. This is indeed the case and a complete characterization of the indecomposable groups of class two is obtained. In case $p \neq 2$ all possible defining relations for the indecomposable p-groups of class two will be given.

The following lemmas concerning nilpotent groups will be needed in this section and in those that follow. The first three of these are given without proof and may be found in Zassenhaus [2] p. 114, and P. Hall [4] on p. 34 and 50 in that order.

LEMMA 2.1 If G is a nilpotent group then $G' \subseteq \Phi(G)$.

LEMMA 2.2 If G is nilpotent and $N \lhd G$ then $N \cap Z(G) \supset 1$.

LEMMA 2.3 If G is nilpotent and the class of G is n then $G_{(n)} \subseteq Z(G)$.

LEMMA 2.4 Let G be a p-group. G is a subdirect product if and only if $Z(G)$ is not cyclic.

Proof Assume that $Z(G)$ is not cyclic. Then $Z(G)$ is a non-cyclic abelian group and hence it contains subgroups N_1 and N_2 different from 1 such that $N_1 \cap N_2 = 1$. But since every subgroup of $Z(G)$ is normal in G it follows that $N_1, N_2 \lhd G$ and hence G is a subdirect

product.

Conversely, if G contains N_1, $N_2 \triangleleft G$ such that $N_1 \cap N_2 = 1$ then it follows from Lemma 2.2 that Z(G) contains subgroups M_1, M_2 different from 1 such that $M_1 \cap M_2 = 1$. Hence Z(G) is not cyclic.

LEMMA 2.5 If G is a non-abelian group and $Z(G) \not\subseteq \Phi(G)$ then G is a factordirect product.

Proof Since $\Phi(G)$ is the intersection of all maximal subgroups of G then there exists one maximal subgroup M of G such that $Z(G) \not\subseteq M$. Since M is maximal and Z(G) is normal in G, it follows that $G = MZ(G)$. But these groups permute elementwise and $Z(G) \subset G$, hence G is a factordirect product.

LEMMA 2.6 Let $a, b, c \in G$. If (a, b) and $(a, c) \in Z(G)$ then $(a, b)(a, c) = (a, bc)$ and $(a, b)(c, b) = (ac, b)$. Furthermore $(a, b)^n = (a^n, b) = (a, b^n)$.

Proof Since $(a, b) \in Z(G)$, $(a, bc) = a^{-1}c^{-1}b^{-1}abc = a^{-1}c^{-1}b^{-1}ba(a, b)c = a^{-1}c^{-1}a(a, b)c = a^{-1}c^{-1}ac(a, b) = (a, c)(a, b) = (a, b)(a, c)$. Similarly $(ac, b) = c^{-1}a^{-1}b^{-1}acb = c^{-1}a^{-1}b^{-1}abc(c, b) = c^{-1}(a, b)c(c, b) = (a, b)(c, b)$. The formula $(a, b)^n = (a^n, b) = (a, b^n)$ can be verified by a simple induction argument for $n \geq 0$. In order to show that the formula holds for $n < 0$, let $n = -1$ and consider (a^{-1}, b). There exists a positive integer r such that $(a^{-1}, b) = (a^r, b)$. But $(a^r, b) = (a, b)^r$ and $(a, b)^r(a, b) = (a, b)^{r+1} = (a^{r+1}, b) = (1, b) = 1$. Hence $(a, b)^r = (a, b)^{-1} = (a^{-1}, b)$, and the formula holds for all integers n.

LEMMA 2.7 Let G be a cyclic p-group and suppose that $G = \langle ab \rangle$ with $a, b \in G$. Then if $o(a) \geq o(b)$, $G = \langle a \rangle$.

Proof Since $ab = ba$, $(ab)^x = a^x b^x$. Since $a \in G$ there is some integer μ such that $a^\mu b^\mu = a$. Hence $b^\mu \in \langle a \rangle$. Clearly $p \nmid \mu$ since otherwise $o(a^\mu b^\mu) < o(a)$. But since $p \nmid \mu$, $\langle b^\mu \rangle = \langle b \rangle \subseteq \langle a \rangle$. Therefore $G = \langle a \rangle$.

LEMMA 2.8 Let G be a p-group. If G has two generators and $G = A \times B$ then A and B are cyclic and hence G is abelian.

Proof Consider $G/G' = A \times B/(A \times B)' \simeq A/A' \times B/B'$. If G has two generators then G/G' has two generators. Hence G/G' is the direct product of two cyclic groups. Hence A/A' and B/B' are cyclic. Therefore A and B are cyclic and G is abelian.

The main decomposition theorem for p-groups of class two may now be stated.

THEOREM 2.1 Let G be a p-group of class two. Then G is decomposable if and only if G is either a direct product, subdirect product, or factordirect product.

Proof Assume that G is decomposable but is not a direct or subdirect product. This implies that $Z(G)$ is cyclic and since $c(G) = 2$, $G' \subseteq Z(G)$ so that G' is cyclic. Let $Z(G) = \langle z \rangle$ with $z^{p^\alpha} = 1$. G' is generated by a product of commutators each of which is contained in G'. It follows from Lemma 2.7 that there exists a commutator, (a, b), such that $G' = \langle (a, b) \rangle$. Let $o((a, b)) = p^\beta$. Since G is decomposable it follows from Theorem 1.6 that $G' \in \{A'_\mu\}$ where $\{A_\mu\}$ is

the set of proper ingroups of G. Since G' is cyclic of order p^{β} there must be an element $A_1 \in \{A_\mu\}$ such that $e(A_1') \geq p^{\beta}$, and A_1' is cyclic. A_1 cannot be a factor group of G, for if $A_1 = G/N$ then $A_1' = (G/N)' = G'N/N \simeq G'/G' \cap N$. Lemma 2.2 states that all normal subgroups of G have a non-trivial intersection with Z(G) and hence with G'. Hence A_1' would have exponent properly smaller than e(G'). It follows from Theorem 1.7 that there exists A_1, a proper subgroup of G, such that $A_1' = G'$. For $A_1' \subseteq G'$ and since $e(A_1')$ $= e(G')$ and G' is cyclic, $A_1' = G'$. Hence there exist $u, v \in A_1$ such that $\langle (u, v) \rangle = A_1$. Since $A_1' = G'$ for some θ, $(u, v)^{\theta} = (u^{\theta}, v)$ $= (a, b)$. Let $c = u^{\theta}$, $d = v$ and $(c, d) = (a, b) = m$.

Let $A = \langle c, d \rangle$. It will now be shown that G must be a factor-direct product with A as one of the factors. Since A is a proper subgroup of G there exist elements $\{g_i\}$ such that $G = \langle c, d, g_1, \ldots g_k \rangle$, and such that none of the g_i's may be omitted. Consider $B = \langle g_1, \ldots, g_k \rangle$.

Let $(c, g_i) = m^{\alpha_i}$ for all $i = 1, \ldots, k$. It follows from Lemma 2.6 that $(c, d)^{-\alpha_i}(c, g_i) = (c, d^{-\alpha_i})(c, g_i) = (c, d^{-\alpha_i} g_i) = 1$. Let $g_i' = d^{-\alpha_i} g_i$. Hence $(c, g_i') = 1$ for all i. Suppose that $(d, g_i') = m^{\beta_i}$ for all i. Therefore $(d, c)^{-\beta_i}(d, g_i') = (d, c^{-\beta_i} g_i') = 1$. Now let $g_i'' = c^{-\beta_i} g_i'$. Hence $(d, g_i'') = 1$ for all i. But if $(c, g_i') = 1$ then $(c, g_i'') = (c, c^{-\beta_i} g_i') = 1$. Therefore A permutes elementwise with the group $B_1 = \langle g_1'', \ldots, g_k'' \rangle$. Since $A \cup B_1 = G$, $AB_1 = G$ and they permute elementwise.

Since A is a proper subgroup of G it remains to verify that

$B_1 \subset G$. If $B_1 = G$ then $c, d \in Z(G)$, a contradiction. Therefore G is a factordirect product. Hence if G is decomposable then G is either a direct product, subdirect product or factordirect product.

Conversely, if G is a direct, subdirect, or factordirect product then G is decomposable.

COROLLARY 2.1.1 Let G be a p-group of class two. If there exists a proper subgroup A of G such that $e(A') = e(G')$ then G is decomposable.

Proof If G is not a subdirect or direct product then G' is cyclic and hence $e(A') = e(G')$ implies that $A' = G'$. It has been shown in the proof of Theorem 2.1 that this implies that G is a factordirect product.

A further characterization of these groups is given by:

THEOREM 2.2 Let G be a p-group of class two. G is indecomposable if and only if $Z(G)$ is cyclic and G may be generated by two elements.

Proof Let G be indecomposable. Hence $Z(G)$ is cyclic and therefore G' is cyclic. It follows from Lemma 2.7 that there exists a commutator (a, b) such that $G' = \langle (a, b) \rangle$. If $\langle a, b \rangle$ were a proper subgroup of G then G would be decomposable by Corollary 2.1.1. Hence $G = \langle a, b \rangle$.

Conversely if $G = \langle a, b \rangle$ and $Z(G)$ is cyclic then G is certainly not a direct or subdirect product. Hence if G is decomposable it must be a factordirect product. Assume $G = AB$, $a_1 b_1 = b_1 a_1$ for

all $a_1 \in A$ and $b_1 \in B$. Clearly $G/A \cap B \simeq (A/A \cap B) \times (B/A \cap B)$ $= \bar{A} \times \bar{B}$. If G is generated by two elements then $G/A \cap B$ is also generated by two elements. But $G/A \cap B$ is the direct product of $\bar{A}$ and $\bar{B}$. Therefore it follows from Lemma 2.8 that $\bar{A}$ and $\bar{B}$ are cyclic, and since $A \cap B \subseteq Z(G)$, G is abelian, a contradiction.

If $p \neq 2$ the defining relations of an indecomposable p-group of class two can be shown to assume one of two distinct forms.

LEMMA 2.9 If G is a group of class two then for $a, b \in G$
$(ab)^u = a^u b^u (b, a)^{\frac{u(u-1)}{2}}$.

Proof The proof is by induction on u. It is trivially true for $u = 1$. If $(ab)^r = a^r b^r (b, a)^{\frac{r(r-1)}{2}}$ then since $(b, a) \in Z(G)$, $(ab)^{r+1}$ $= (ab)^r ab = a^r b^r (b, a)^{\frac{r(r-1)}{2}} ab = a^r b^r ab (b, a)^{\frac{r(r-1)}{2}}$. But $a^r b^r ab$ $= a^r a b^r (b^r, a) b = a^{r+1} b^{r+1} (b^r, a) = a^{r+1} b^{r+1} (b, a)^r$. Therefore $(ab)^{r+1}$ $= a^{r+1} b^{r+1} (b, a)^{\frac{r(r-1)}{2}+r} = a^{r+1} b^{r+1} (b, a)^{\frac{r(r+1)}{2}}$.

LEMMA 2.10 Let G be a p-group of class two, with $p \neq 2$, which is generated by two elements a_1, b_1 with $o(a_1) \geq o(b_1)$. Then there exist $a, b \in G$ such that $G = \langle a, b \rangle$ and $\langle a \rangle \cap \langle b \rangle = 1$.

Proof Suppose $a_1^{\theta} = b_1^{\phi} \neq 1$. Let $\theta = p^{\alpha} m$ and $\phi = p^{\beta} n$ with $(p, mn) = 1$. Clearly $\langle a_1^m \rangle = \langle a_1 \rangle$ and $\langle b_1^n \rangle = \langle b_1 \rangle$. Therefore we may as well assume that $a_1^{p^{\alpha}} = b_1^{p^{\beta}} \neq 1$ and $\alpha, \beta \neq 0$. For otherwise G would be cyclic. Since $o(a_1) \geq o(b_1)$ it follows that $\alpha \geq \beta$. Let $b = b_1 a_1^{-p^{\alpha-\beta}}$. Then $b^{p^{\beta}} = (b_1 a_1^{-p^{\alpha-\beta}})^{p^{\beta}} = b_1^{p^{\beta}} a_1^{-p^{\alpha}} (a_1^{-p^{\alpha-\beta}}, b_1)^{\frac{p^{\beta}(p^{\beta}-1)}{2}}$

$= (a_1^{-p^\alpha}, b_1)^{\frac{p^\beta - 1}{2}} = 1$ since $a_1^{-p^\alpha} = b_1^{-p^\beta}$. Notice that $\frac{p^\beta - 1}{2}$ is an integer only if $p \neq 2$. If $\langle b \rangle \cap \langle a_1 \rangle \supset 1$ then this process may be repeated and since $o(b) < o(b_1)$ it follows that there exists a choice of b such that $\langle b \rangle \cap \langle a_1 \rangle = 1$. Let $a = a_1$ and the lemma is proved.

If the condition $p \neq 2$ is removed then the quaternion group of order eight is a counterexample to the lemma.

THEOREM 2.3 Let G be an indecomposable p-group of class two with $p \neq 2$. Then G is generated by two elements and has defining relations either

I $a^{p^\alpha} = b^{p^\beta} = 1 \quad (a, b) = a^{p^{\alpha - \beta}}$ with $\alpha \geq 2\beta$, or

II $a^{p^\alpha} = b^{p^\beta} = 1 \quad (a, b)^{p^\gamma} = a^{p^\beta}, \ \gamma = 2\beta - \alpha \quad (a, b, a) = (a, b, b) = 1$ with $\beta \leq \alpha \leq 2\beta$.

Conversely any group defined by I or II is an indecomposable p-group of class two.

Proof Since G is indecomposable it follows from Theorem 2.2 and Lemma 2.9 that $Z(G)$ is cyclic, $G = \langle a, b \rangle$ with $a^{p^\alpha} = b^{p^\beta} = 1$, $\alpha \geq \beta$ and $\langle a \rangle \cap \langle b \rangle = 1$.

Suppose that $o((a, b)) = p^\omega$. Then $(a, b)^{p^\omega} = (a^{p^\omega}, b) = (a, b^{p^\omega}) = 1$ which implies that $a^{p^\omega}, b^{p^\omega} \in Z(G)$. Since $Z(G)$ is cyclic and $o(a) \geq o(b)$, $b^{p^\omega} \in \langle a^{p^\omega} \rangle$. But $\langle a \rangle \cap \langle b \rangle = 1$ and therefore $b^{p^\omega} = 1$. Hence $\beta \leq \omega$. But $(a, b)^{p^\beta} = (a, b^{p^\beta}) = 1$, and hence $\beta \geq \omega$. Therefore $o((a, b)) = p^\beta$, and $a^{p^\beta} \in Z(G)$.

Since G is of class two either $G' \subset Z(G)$ or $G' = Z(G)$.

Case I. Assume that $G' \subset Z(G)$ and let $Z(G) = \langle g \rangle$. Any element of G, in particular g, may be represented in the form $g = a^u b^v (a, b)^w$. Since $G' \subset Z(G)$ it follows that $\langle (a, b)^w \rangle \subset Z(G)$ and $a^u b^v \in Z(G)$. Hence by Lemma 2.7, $Z(G) = \langle a^u b^v \rangle$. But $(a^u b^v, b) = (a^u, b) = 1$, and $(a^u b^v, a) = (b^v, a) = 1$. Therefore a^u, $b^v \in Z(G)$. This implies that either $b^v = 1$ or $a^u = 1$. If $a^u = 1$ then $(a, b)^v = (a, b^v) = (a^v, b) = 1$, and a^v, $b^v \in Z(G)$ which would imply that $b^v = 1$. In any event $b^v = 1$ and $Z(G) = \langle a^u \rangle$.

Let $u = p^\delta m$ with $(p, m) = 1$. Since $Z(G) = \langle a^u \rangle$ it follows that $Z(G) = \langle a^{p^\delta} \rangle$. Since $a^{p^\beta} \in Z(G)$, $\beta \geq \delta$. But $(a, b)^{p^\delta} = (a^{p^\delta}, b) = 1$. Therefore $\delta \geq \beta$ so $\delta = \beta$ and $Z(G) = \langle a^{p^\beta} \rangle$.

If $a_1 = a^m$ then there exists θ such that $(a, b) = (a_1^{p^\beta})^\theta$ with $\theta = p^\epsilon n$, $(p, n) = 1$. Then if $a_2 = a_1^n$, $(a, b) = a_2^{p^{\beta+\epsilon}}$. But $o(a_2) = o(a)$ and hence $2\beta + \epsilon = \alpha$. Therefore $2\beta \leq \alpha$.

Case II. Assume that $Z(G) = G'$. Since $a^{p^\beta} \in Z(G)$, and $Z(G) = G'$ $(a, b)^u = a^{p^\beta}$. Let $u = p^\gamma m$ with $(m, p) = 1$. Hence $(a, b)^u = (a, b^m)^{p^\gamma}$ $= a^{p^\beta}$. Since $o(b^m) = o(b)$ we may replace b throughout by b^m and call it b. Now $(a, b)^{p^\gamma p^{\alpha-\beta}} = a^{p^\beta p^{\alpha-\beta}} = 1$ and $p^{\alpha-\beta}$ is the order of a^{p^β}. Hence $o((a, b)) = p^\beta = p^{\gamma+\alpha-\beta}$. Therefore $\gamma = 2\beta - \alpha$. Finally since $\gamma \geq 0$, $2\beta \geq \alpha$. The relations $(a, b, a) = (a, b, b) = 1$ follow from the fact that G is of class two.

It will now be shown that if a group G is defined by I or II then it is an indecomposable p-group of class two.

Suppose that $G = \langle a, b \rangle$ and is defined by $a^{p^\alpha} = b^{p^\beta} = 1$, $(a, b) = a^{p^{\alpha-\beta}}$ with $\alpha \geq 2\beta$. Since $(a, b) = a^{p^{\alpha-\beta}}$ it follows that $b^{-1}ab = a\,a^{p^{\alpha-\beta}}$. Hence $b^{-1}a^{p^\beta}b = a^{p^\beta}$ and therefore $a^{p^\beta} \in Z(G)$. But since $\alpha - \beta \geq \beta$ it follows that $\langle a^{p^\beta} \rangle \supseteq \langle a^{p^{\alpha-\beta}} \rangle$. Hence $(a, b) \in Z(G)$ and this implies that G is of class two. For any element of G may be written as $a^u b^v (a, b)^w$. Let g_1 and g_2 be two arbitrary elements of G. Then $(g_1, g_2) = (a^{u_1}b^{v_1}(a, b)^{w_1}, a^{u_2}b^{v_2}(a, b)^{w_2})$ $= (a^{u_1}b^{v_1}, a^{u_2}b^{v_2})$ since $(a, b) \in Z(G)$. But $Z(G) \ni (a,b)^{u_1v_2 - v_1u_2}$ $= (a, b)^{u_1v_2}(b, a)^{v_1u_2} = (a^{u_1}, b^{v_2})(b^{v_1}, a^{u_2}) = (a^{u_1}b^{v_1}, b^{v_2})(a^{u_1}b^{v_1}, a^{u_2})$ $= (a^{u_1}b^{v_1}, a^{u_2}b^{v_2}) = (g_1, g_2)$.

Since the generators of G have order a power of p and G is of class two, G is a p-group.

To show that $Z(G)$ is cyclic, let the element $a^u b^v (a, b)^w$ be an element of the center. Since $(a, b) \in Z(G)$, then $a^u b^v \in Z(G)$. Therefore $(a^u b^v, a) = (b^v, a) = 1$, and hence $b^v \in Z(G)$. But then (a, b^v) $= (a, b)^v = (a^{p^{\alpha-\beta}})^v = 1$, and since $o(a^{p^{\alpha-\beta}}) = p^\beta$, $b^v = 1$. Therefore $a^u b^v (a, b)^w = a^{u+wp^{\alpha-\beta}}$ for every element of the center and hence $Z(G)$ is cyclic. It follows from Theorem 2.2 that G is indecomposable.

Now suppose that $G = \langle a, b \rangle$ and is defined by $a^{p^\alpha} = b^{p^\beta} = 1$, $(a, b)^{p^\gamma} = a^{p^\beta}$, $(a, b, a) = (a, b, b) = 1$, and $\gamma = 2\beta - \alpha$, $\alpha \leq 2\beta$. Since $(a, b) \in Z(G)$ it follows from the argument given above that G is of class two.

G is clearly a p-group and it remains only to show that $Z(G)$

is cyclic.

Suppose that $a^u b^v (a, b)^w \in Z(G)$. Arguing as above $b^v \in Z(G)$ and $(a, b)^v = 1$. But $o((a, b)) = p^\beta$ and hence $b^v = 1$. Also $(a^u, b) = 1$ and hence $a^u \in Z(G)$. Therefore since $o((a, b)) = p^\beta$, it follows that $p^\beta \mid u$ and $a^u \in \langle a^{p^\beta} \rangle \subset \langle (a, b) \rangle$. Hence $a^u b^v (a, b)^w \in \langle (a, b) \rangle$ and $Z(G)$ is cyclic. Therefore G is indecomposable. This completes the proof of the theorem.

Notice that the condition $p \neq 2$ is used only in applying Lemma 2.9. If G is a 2-group which satisfies the conclusion of Lemma 2.9 then its defining relations are indeed of the form I or II above. An example of such a 2-group is the dihedral group of order eight.

The main results of this section may be summarized in the following manner:

Let G be an arbitrary p-group of class two with $p \neq 2$. If $e(G) = p^\mu$ then there exists a finite set of groups $\{H_i\}$ of type I and II given in Theorem 2.3 such that $G \in \{\overline{H_i}\}$. This follows from the fact that any group is contained in the closure of the set of its indecomposable ingroups and that the exponent of a group cannot exceed the largest of the exponents of its indecomposable ingroups.

Chapter III

The problem of determining when an arbitrary p-group G is decomposable can in some cases be solved by considering the decomposability of $G/Z(G)$. In the case of $e(G) = p$ it will be shown in this section that if $G/Z(G)$ is a direct product then G is decomposable. In general, this decomposition is non-trivial, i.e. G is neither a direct product, subdirect product, or factordirect product. An example will be given to illustrate this point. Two lemmas will be required before the main theorem can be proved.

LEMMA 3.1 Let G be a nilpotent group of class $n > 2$. Suppose that $G/Z(G) = \overline{G} = \overline{A}\overline{B}$ with $\overline{a}\,\overline{b} = \overline{b}\,\overline{a}$ for all $\overline{a} \in \overline{A}$ and $\overline{b} \in \overline{B}$. That is, $\overline{G}$ is a factordirect product of $\overline{A}$ and $\overline{B}$. Then if A and B are the inverse images of $\overline{A}$ and $\overline{B}$ respectively, $c(A) = n$ or $c(B) = n$.

Proof Let $\overline{A} = \langle \overline{a}_1, \ldots, \overline{a}_r \rangle$ and $\overline{B} = \langle \overline{b}_1, \ldots, \overline{b}_s \rangle$. Then $G = \langle a_1, \ldots, a_r, b_1, \ldots, b_s, Z(G) \rangle$. Since $\overline{G}$ is a factordirect product of $\overline{A}$ and $\overline{B}$ it follows that $(a_i, b_j) \in Z(G)$ for all i, j. Hence any element $g \in G$ may be put in the form $g = abz$ with $a \in A$, $b \in B$ and $z \in Z(G)$.

Since the factor z may be omitted as a multiplier of any entry in a commutator there exists a non-identity commutator of length n: $(c_1 d_1, \ldots, c_n d_n) \in Z(G)$ with $c_i \in \langle a_1, \ldots, a_r \rangle$ and $d_j \in \langle b_1, \ldots, b_s \rangle$. This follows from the fact that $c(G) = n$ and $G_{(n)} \subseteq Z(G)$. But $(c_1 d_1, \ldots, c_n d_n)$ $= (c_1 d_1, \ldots, c_{n-1} d_{n-1}, c_n)(c_1 d_1, \ldots, c_{n-1} d_{n-1}, d_n)$ since these three commutators are contained in $Z(G)$. Since $(c_i, d_j) \in Z(G)$

$(c_1d_1, c_2d_2) = (c_1, c_2)(d_1, d_2)z_1$ for some $z_1 \in Z(G)$ and hence by induction, $(c_1d_1, \ldots, c_{n-1}d_{n-1}) = (c_1, \ldots, c_{n-1})(d_1, \ldots, d_{n-1})z$ for some $z \in Z(G)$. Hence $(c_1d_1, \ldots, c_{n-1}d_{n-1}, c_n)$ $= ((c_1, \ldots, c_{n-1})(d_1, \ldots, d_{n-1}), c_n) = (c_1, \ldots, c_{n-1}, c_n)(d_1, \ldots, d_{n-1}, c_n)$. Now since $n > 2$ $(d_1, \ldots, d_{n-1}) = (u, v)$ with $u, v \in \langle b_1, \ldots, b_s \rangle$. Hence $(d_1, \ldots, d_{n-1}, c_n) = ((u, v), c_n) = (u^{-1}v^{-1}uv, c_n)$ $= (u^{-1}, c_n)(v^{-1}, c_n)(u, c_n)(v, c_n) = (u, c_n)^{-1}(v, c_n)^{-1}(u, c_n)(v, c_n) = 1$ since each of these commutators is in $Z(G)$. Therefore $(c_1d_1, \ldots, c_nd_n)$ $= (c_1d_1, \ldots, c_{n-1}d_{n-1}, c_n)(c_1d_1, \ldots, c_{n-1}d_{n-1}, d_n)$ $= (c_1, \ldots, c_n)(d_1, \ldots, d_n)$. If $c(A) < n$ and $c(B) < n$ it follows that $(c_1d_1, \ldots, c_nd_n) = 1$ and therefore $c(G) < n$, a contradiction. Hence either $c(A) = n$ or $c(B) = n$.

LEMMA 3.2 Let G be a p-group and let $G = \langle a_1, \ldots, a_r \rangle$ such that $\langle a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_r \rangle \subset G$ for all i. If $(a_i)^p = 1$ for all i then for all $g \in G$, g has a unique representation of the form $a_1^{\alpha_1} \ldots a_r^{\alpha_r} b$ with $b \in G'$.

Proof Since every element of G is a word in the a_i's it follows that every element has a representation of the form given above.

Suppose that $g = a_1^{\alpha_1} \ldots a_r^{\alpha_r} b_1 = a_1^{\beta_1} \ldots a_r^{\beta_r} b_2$ with $b_1, b_2 \in G'$. Therefore $a_1^{\alpha_1 - \beta_1} \ldots a_r^{\alpha_r - \beta_r} = b_3 \in G'$. Assume that for some i $p \nmid \alpha_i - \beta_i$. Then $G = \langle a_1, \ldots, a_{i-1}, b_3, a_{i+1}, \ldots, a_r \rangle$. For clearly $a_i^{\alpha_i - \beta_i}$ is generated by these elements and since $(\alpha_i - \beta_i, p) = 1$, $\langle a_i^{\alpha_i - \beta_i} \rangle = \langle a_i \rangle$. But $b_3 \in G'$ and hence is a non-generator. Therefore $G = \langle a_1, \ldots, a_{i-1}, a_{i+1} \ldots a_r \rangle$ contradicting

the hypothesis. Hence $p \mid \alpha_i - \beta_i$ for all i and thus $a_i^{\alpha_i} = a_i^{\beta_i}$ for all i. Therefore $b_1 = b_2$ and the lemma is proved.

THEOREM 3.1 Let G be a p-group of class greater than two and let $e(G) = p$. If $G/Z(G)$ is a direct product then G is decomposable.

Proof If $Z(G)$ is not cyclic then G is decomposable. Assume therefore that $Z(G)$ is cyclic and hence has order p. Let $G/Z(G) = \overline{A}\,\overline{B}_1$ with $\overline{a}\,\overline{b} = \overline{b}\,\overline{a}$ for all $\overline{a} \in \overline{A}$ and $\overline{b} \in \overline{B}_1$. Let $\{\overline{a}_1, \ldots, \overline{a}_r\}$ be an irredundant set of generators of $\overline{A}$. That is, if $\overline{A} = \langle \overline{a}_1, \ldots, \overline{a}_r \rangle$ then $\langle \overline{a}_1, \ldots, \overline{a}_{i-1}, \overline{a}_{i+1}, \ldots, \overline{a}_r \rangle \subset \overline{A}$ for all i. Choose $\{\overline{b}_1, \ldots, \overline{b}_s\}$ similarly for $\overline{B}_1$. If $c(G) = n > 2$ then according to Lemma 3.1 either $c(A) = n$ or $c(B_1) = n$. Let $c(A) = n$. Clearly $A_{(n)} \subseteq G_{(n)}$ and from Lemma 2.3 it follows that $1 \subset A_{(n)} \subseteq Z(G)$ and therefore $A_{(n)} = Z(G)$. Hence if $Z(G) = \langle z \rangle$ then $z \in A'$ and from Lemma 2.1 z is a non-generator of A. Therefore $A = \langle a_1, \ldots, a_r \rangle$ and this is an irredundant set of generators of A.

Let $B = \langle b_1, \ldots, b_s \rangle$. If $z \in B$ then $B = B_1$, but this may not necessarily be the case. In any event $G = AB_1$ and hence $G = AB$.

It can now be shown that $G \in \{A, B\}$. Since $(\overline{a}_i, \overline{b}_j) = 1$ it follows that $(a_i, b_j) = z^{\alpha_{ij}}$. Let $H = \underbrace{A \times \cdots \times A}_{r+1} \times B$. Since $Z(G) = A_{(n)}$ there exists $c, d \in A$ such that $(c, d) = z$. Let $\mathcal{A}$, $\mathcal{B}$ be subsets of H defined as follows:

$$\mathcal{A} = \{[a_i, c^{\delta_{1i}}, \ldots, c^{\delta_{ri}}, 1] \mid \delta_{ji} = 0 \text{ if } j \neq i,\ \delta_{ji} = 1 \text{ if } j = i \text{ and } i, j = 1, \ldots, r\}.$$

$$\mathcal{B} = \{[1, d^{\alpha_{1k}}, \ldots, d^{\alpha_{rk}}, b_k] \mid (a_i, b_j) = z^{\alpha_{ik}},\ k = 1, \ldots, s\}.$$

Let $H_1 = \langle \mathcal{A}, \mathcal{B} \rangle$. Notice that H could have been defined as $A \times A_1 \times \cdots \times A_1 \times B$ with $A_1 = \langle c, d \rangle$. That is, H may be defined as the direct product of A, B and r copies of a group of class two.

Let $N = \langle [z^{\alpha_{1i}}, z^{-\alpha_{1i}}, 1, \ldots, 1], [z^{\alpha_{2i}}, 1, z^{-\alpha_{2i}}, 1, \ldots, 1], \ldots [z^{\alpha_{ri}}, 1, \ldots, 1, z^{-\alpha_{ri}}, 1] \text{ for } i = 1, \ldots, s \rangle$. Since the commutator $([a_j, 1, \ldots, 1, c, 1, \ldots, 1], [1, d^{\alpha_{1k}}, \ldots, d^{\alpha_{rk}}, b_k]) = [1, \ldots, 1, z^{\alpha_{jk}}, 1, \ldots, 1]$ it follows that $N \subseteq H_1$ and clearly $N \triangleleft H_1$.

Let $G_1 = H_1/N$. It will now be shown that $G_1 \simeq G$ under the mapping induced by:

$$a_i \longleftrightarrow [a_i, c^{\delta_{1i}}, \ldots, c^{\delta_{ri}}, 1] N = g_i$$

$$b_j \longleftrightarrow [1, d^{\alpha_{1j}}, \ldots, d^{\alpha_{rj}}, b_j] N = h_j$$

where a word on the a_i and b_j corresponds to the same word on g_i and h_j. It will be shown that words are equal in G_1 if and only if they are equal in G. This will suffice to show isomorphism.

Let m be an arbitrary element of G. It appears as a word in the a_i's and b_j's as follows:

$$m = x_1 y_1 x_2 y_2 \cdots x_t y_t \quad \text{with } x_i \in A, \quad y_i \in B.$$

Under the mapping, the image of x_1 will be $[x_1, c^{\theta_{11}}, \ldots, \ldots, c^{\theta_{r1}}] N$ with θ_{i1} equal to the sum of the exponents of a_i in x_1. The image of y_1 will be $[1, d^{\phi_{11}}, \ldots, d^{\phi_{r1}}, y_1] N$ with $\phi_{i1} = \sum_{j=1}^{s} \alpha_{ij} \psi_{j1}$ and ψ_{j1} equal to the sum of the exponents of b_j in y_1. Therefore the image of m under the given mapping will be:

$$[x_1 x_2 \cdots x_t,\ c^{\theta_{11}} d^{\phi_{11}} \cdots c^{\theta_{1t}} d^{\phi_{1t}}, \ldots, c^{\theta_{r1}} d^{\phi_{r1}} \cdots c^{\theta_{rt}} d^{\phi_{rt}}, y_1 \cdots y_t] N.$$

Since $(a_i, b_j) = z^{\alpha_{ij}}$, x_i may be commuted to the left by adding suitable powers of z to the product. That is

$$b_i a_j = a_j b_i (b_i, a_j) = a_j b_i z^{-\alpha_{ji}}.$$

This operation is mirrored in G_1 by commuting powers of c to the left. That is $[1, d^{\alpha_{1i}}, \ldots, d^{\alpha_{ri}}, b_i]\ [a_j, 1, \ldots, 1, c, 1, \ldots, 1] N$
$= [a_j, d^{\alpha_{1i}}, \ldots, d^{\alpha_{j-1\,i}}, d^{\alpha_{ji}} c, d^{\alpha_{j+1\,i}}, \ldots, d^{\alpha_{ri}}, b_i] N$
$= [a_j, d^{\alpha_{1i}}, \ldots, d^{\alpha_{j-1\,i}}, c\, d^{ji} z^{-\alpha_{ji}}, d^{\alpha_{j+1\,i}}, \ldots, d^{\alpha_{ri}}, b_i] N$. But since the element $[z^{\alpha_{ji}}, 1, \ldots, 1, z^{-\alpha_{ji}}, 1, \ldots, 1] \in N$ the above expression may be written as $[a_j z^{-\alpha_{ji}}, 1, \ldots, 1, c, 1, \ldots, 1]\ [1, d^{\alpha_{1i}}, \ldots, d^{\alpha_{ri}}, b_i] N$. Hence every time some a_i is commuted with b_j in m, thereby introducing a power of z, the very same power of z is introduced in the image element in G_1 by commuting c with $d^{\alpha_{ij}}$. Therefore if $m = x_1 y_1 \cdots x_t y_t = x_1 \cdots x_t\ y_1 \cdots y_t\ z^{\alpha} = xyz^{\alpha}$ with $x = x_1 \cdots x_t$ and $y = y_1 \cdots y_t$ then the image of m, $n = [xz^{\alpha}, c^{\mu_1}, \ldots, c^{\mu_r}, 1]$ $[1, d^{\nu_1}, \ldots, d^{\nu_r}, y] N$ with μ_i equal to the sum of the exponents of a_i appearing in the product x and $\nu_i = \sum_{j=1}^{s} \alpha_{ij}\omega_j$, with ω_j equal to the sum of the exponents of b_j in y. Hence if an arbitrary element of G is put in the form xyz^{α} defined above then the image element can be put in the form $[xz^{\alpha}, c^{\mu_1} d^{\nu_1}, \ldots\ c^{\mu_r} d^{\nu_r}, y] N$.

By an argument similar to the one above it can be shown that an arbitrary element of G_1 may be put in the form

$[xz^{\alpha}, c^{\mu_1 d^{\vartheta_1}}, \ldots, c^{\mu_r d^{\vartheta_r}}, y]N$ and its image in the form xyz^{α}.

Suppose that $m, \bar{m} \in G$ and let n and $\bar{n}$ be their images in G_1. Let m be in the form $m = xyz^{\alpha}$ as defined above, and $\bar{m} = \bar{x}\bar{y}z^{\bar{\alpha}}$ similarly. Then if $m = \bar{m}$, $xyz = \bar{x}\bar{y}z^{\bar{\alpha}}$ implies that $x^{-1}\bar{x} \in Z(G)$ and $\bar{y}y^{-1} \in Z(G)$ since $A \cap B \subseteq Z(G)$. Hence $x^{-1}\bar{x} = z^{\gamma_1}$, $\bar{y}y^{-1} = z^{\gamma_2}$ and $\bar{\alpha} - \alpha \equiv -(\gamma_1+\gamma_2)(p)$. It follows from Lemma 3.2 that the sum of the exponents of a_i in $x^{-1}\bar{x}$ is equal to o mod p, and similarly for b_i in $\bar{y}y^{-1}$.

Now form $n^{-1}\bar{n}$ in G_1. If $n = [xz^{\alpha}, c^{\mu_1 d^{\vartheta_1}}, \ldots, c^{\mu_r d^{\vartheta_r}}, y]N$ and $\bar{n} = [\bar{x}z^{\bar{\alpha}}, c^{\bar{\mu}_1 d^{\bar{\vartheta}_1}}, \ldots, c^{\bar{\mu}_r d^{\bar{\vartheta}_r}}, \bar{y}]N$ then $n^{-1}\bar{n} =$

$$[x^{-1}z^{-\alpha}\bar{x}z^{\bar{\alpha}}, d^{-\vartheta_1}c^{-\mu_1}c^{\bar{\mu}_1}d^{\bar{\vartheta}_1}, \ldots, d^{-\vartheta_r}c^{-\mu_r}c^{\bar{\mu}_r}d^{\bar{\vartheta}_r}, y^{-1}\bar{y}]N$$

$$= [x^{-1}\bar{x}z^{\bar{\alpha}-\alpha}, c^{\bar{\mu}_1-\mu_1}d^{\bar{\vartheta}_1-\vartheta_1}z^{\vartheta_1(\bar{\mu}_1-\mu_1)}, \ldots, c^{\bar{\mu}_r-\mu_r}d^{\bar{\vartheta}_r-\vartheta_r}z^{\vartheta_r(\bar{\mu}_r-\mu_r)}, y^{-1}\bar{y}]N.$$

Since $x^{-1}\bar{x} = z^{\gamma_1}$ and $\bar{y}y^{-1} = y^{-1}\bar{y} = z^{\gamma_2}$ then $\mu_i \equiv \bar{\mu}_i \equiv o(p)$ and $\vartheta_i \equiv \bar{\vartheta}_i \equiv o(p)$ for $i = 1, \ldots, r$. Hence $n^{-1}\bar{n}$ $= [z^{\gamma_1-(\gamma_1+\gamma_2)}, 1, \ldots, 1, z^{\gamma_2}]N = [1, \ldots, 1]N$. Therefore if $m = \bar{m}$ in G then $n = \bar{n}$ in G_1.

Conversely let m and $\bar{m}$ in G have images n and $\bar{n}$ in G_1. Now suppose that $n^{-1}\bar{n} = 1$. This product will appear as above and hence $\bar{\mu}_i - \mu_i \equiv o(p)$, $\bar{\vartheta}_i - \vartheta_i \equiv o(p)$ for $i = 1, \ldots, r$. Hence $n^{-1}\bar{n} = [x^{-1}\bar{x}z^{\bar{\alpha}-\alpha}, 1, \ldots, 1, y^{-1}\bar{y}]N = [1, \ldots, 1]N$. Therefore $x^{-1}\bar{x} = z^{\gamma_1}$ and $y^{-1}\bar{y} = z^{\gamma_2}$ such that $-(\gamma_1 + \gamma_2) \equiv \bar{\alpha} - \alpha \equiv o(p)$. But then $x^{-1}\bar{x}z^{\bar{\alpha}-\alpha}y^{-1}\bar{y} = 1$. Hence $x^{-1}\bar{x}z^{\bar{\alpha}-\alpha}y^{-1}\bar{y} = y^{-1}yx^{-1}\bar{x}z^{\bar{\alpha}-\alpha}$ $= y^{-1}x^{-1}\bar{x}\bar{y}z^{\bar{\alpha}-\alpha} = 1$. Therefore $\bar{m} = \bar{x}\bar{y}z^{\bar{\alpha}} = xyz^{\alpha} = m$, and the mapping is one-one. Hence it is an isomorphism and therefore G is

decomposable.

In order to show that a group which is decomposable in the manner described above, i.e. $G/Z(G)$ is a direct product is not in general a direct, subdirect, or factordirect product consider the following example.

Let p be a prime greater than 3, and let $A = \langle a_1, a_2 \rangle$ with $a_1^p = a_2^p = y^p = z^p = 1$, $(a_1, a_2) = y$, $(a_1, y) = z$, $(a_2, y) = (a_1, z) = (a_2, z) = 1$. This group has order p^4 and class three. This group is discussed in Burnside [5] p. 146, and it is there shown that $o(A) = p^4$, $c(A) = 3$ and that $Z(A) = \langle z \rangle$. It is easy to see that $A' = \langle y, z \rangle$. Incidentally, A is indecomposable because all proper subgroups and factor groups have order at most p^3 and every group of order p^3 has class at most two.

Consider $A \times A \supset H = \langle [a_1, 1], [a_2, a_1], [1, y] \rangle$. First we show that $[A \times A : H] = p^2$.

Consider the set $\langle [1, a_1^u a_2^v] \rangle$ for all $u, v \leq p$. There are precisely p^2 elements in this set and we claim that these elements form a complete and irredundant set of coset representatives for H in $A \times A$.

A general element of $A \times A$ is $[a_1^\alpha a_2^\beta y^\gamma z^\delta, a_1^{\alpha'} a_2^{\beta'} y^{\gamma'} z^{\delta'}]$. Let $\alpha' \geq \beta$ and consider the coset $[1, a_1^{\alpha'-\beta} a_2^{\beta'}]H$. The element $[a_1^\alpha a_2^\beta, a_1^\beta] \in H$ and therefore $[a_1^\alpha a_2^\beta, a_1^{\alpha'} a_2^{\beta'}] \in [1, a_1^{\alpha'-\beta} a_2^{\beta'}]H$. But since $[y, 1]$, $[z, 1]$ and $[1, z] \in H$ it follows that $a_1^\alpha a_2^\beta y^\gamma z^\delta, a_1^{\alpha'} a_2^{\beta'} y^{\gamma'} z^{\delta'}$ is contained in the coset in question. Hence this set of coset representatives is complete.

Now suppose that two of these cosets are the same. Then

$[1, a_1^i, a_2^j] = [1, a_1^k a_2^\ell]\, h$ with $h \in H$. Let $h = [a_1^\alpha a_2^\beta y^\gamma z^\delta, a_1^\beta y^\theta z^\phi]$. Therefore $a_1^\alpha a_2^\beta y^\gamma z^\delta = 1$ and $a_1^i a_2^j = a_1^{k+\beta} a_2^\ell y^{\theta_1} z^{\phi_1}$. From Lemma 3.2 it follows that $\alpha \equiv \beta \equiv o(p)$ and hence $\gamma \equiv \delta \equiv o(p)$. Similarly $i - k \equiv j - \ell \equiv o(p)$ and hence $[1, a_1^i a_2^j] = [1, a_1^k a_2^\ell]$. Therefore the set of coset representatives is not redundant. Hence $[A \times A : H] = p^2$.

Now consider $N = \langle [z, z^{-1}] \rangle$. Clearly $N \lhd H$. Let $A_1 = H/N = \langle [a_1, 1]N,\ [a_2, a_1]N,\ [1, y]N \rangle$. Since $o(N) = p$ it follows that $o(A_1) = o(H)/p = p^5$.

It will now be shown that A_1 satisfies the hypothesis of Theorem 3.1.

a) It has already been shown that $o(A_1) = p^5$ and hence A_1 is not isomorphic to an ingroup of A.

b) A_1 has class three. Consider the triple commutator $([a_1,1]N, [a_2, a_1]N, [a_1,1]N) = ([y,1]N, [a_1,1]N) = [z^{-1}, 1]N \neq [1,1]N$. Hence $c(A_1) \geq 3$. But since A_1 is a factor group of a subdirect product of two groups of class three it follows that $c(A_1) \leq 3$. Hence $c(A_1) = 3$.

c) $Z(A_1)$ has order p and hence A_1 is neither a direct product or subdirect product. For suppose $\xi = [a_1^\alpha a_2^\beta y^\gamma z^\delta, a_1^\beta y^\theta z^\phi]N \in Z(A_1)$. Its commutator with $[a_1, 1]N$ is $[(a_1^\alpha a_2^\beta y^\gamma z^\delta, a_1), 1]N$. If this is N then $(a_1^\alpha a_2^\beta y^\gamma z^\delta, a_1) = (a_2^\beta y^\gamma, a_1) = 1$. But by direct calculation $(a_2^\beta y^\gamma, a_1) = (a_2^\beta, a_1)(a_2^\beta, a_1, y^\gamma)(y^\gamma, a_1) = y^{-\beta} z^{-\gamma} = 1$. Therefore $\beta \equiv \gamma \equiv o(p)$. Hence $\xi = [a_1^\alpha z^\delta, y^\theta z^\phi]N$. Its commutator with $[a_2, a_1]N$ is $([a_1^\alpha z^\delta, y^\theta z^\phi]N, [a_2, a_1]N) = [(a_1^\alpha z^\delta, a_2), (y^\theta z^\phi, a_1)]N = [(a_1^\alpha, a_2), (y^\theta, a_1)]N$. But one can easily show that $(a_1^\alpha, a_2) = y^\alpha z^{-\frac{\alpha(\alpha-1)}{2}}$, and $(y^\theta, a_1) = z^{-\theta}$.

Hence $(a_1^{\alpha}, a_2), (y^{\theta}, a_1)\ N = [y^{\alpha} z^{-\frac{\alpha(\alpha-1)}{2}}, z^{-\theta}] N = [1, 1]\ N$, $\alpha \equiv o(p)$ and $\theta \equiv o(p)$. Therefore $\xi = [z^{\delta}, z^{\phi}] N = [z^{\delta+\theta}, 1] N$ and $Z(A_1) = \langle [z, 1] N \rangle$. Thus $o(Z(A_1)) = p$.

d) Consider the subgroups $R = \langle [a_1, 1] N, [a_2, a_1] N \rangle$ and $S = \langle [1, y] N, [1, z] N \rangle$. It is easy to see that $A_1 = RS$, $R \cap S = Z(A_1)$ and $\{(r, s) \mid r \in R, s \in S\} = Z(A_1)$. Hence $A_1/Z(A_1)$ is a direct product.

It follows from the theorem that A_1 is decomposable.

If A_1 were a factordirect product then one of the factors would have to be a subgroup of class three. Since the smallest p-group of class three has order p^4, such a subgroup is of necessity maximal and hence must contain $A_1' = \langle [y, 1] N, [z, 1] N \rangle$. Now the intersection of the two factors of a factordirect product must be contained in the center of the whole group, and hence the factor group $A_1/Z(A_1)$ must be a direct product. Since $o(A_1) = p^5$ and $o(Z(A_1)) = p$, and $A_1/Z(A_1)$ is not abelian, it must be a direct product of a group of order p and one of order p^3. Hence the orders of the factors in the whole group must be p^4 and p^2. But the factor of order p^2 is abelian and hence in the center, contradicting the fact that $o(Z(A_1)) = p$. Therefore A_1 is not a factordirect product.

The decomposability of A_1 could also have been deduced from the fact that $A_1 \in \{\overline{A}\}$ and A is isomorphic to a proper subgroup of A_1. That is, the mapping $a_1 \longleftrightarrow [a_1, 1]\ N$

$a_2 \longleftrightarrow [a_2, a_1] N$ induces an isomorphism. Hence $A_1 \in \{\overline{A}\} \subseteq \{\overline{A_\alpha}\}$ where $\{A_\alpha\}$ is the set of proper ingroups of A.

It is easy to check that A_1 may be defined by:

$c^p = d^p = f^p = (c, d)^p = (c, c, d)^p = (c, c, c, d) = (d, c, c, d) = (f, c, c, d) = 1$

and $(d, f) = (c, c, d)$.

Chapter IV

The definition of closure given in Chapter I suggests an equivalence relation for finite groups. That is, $G_1 \equiv G_2$ if $\{\overline{G_1}\} = \{\overline{G_2}\}$. It is readily shown that this is indeed an equivalence relation and hence provides a partition of the set of all finite groups. This chapter will investigate the relation between this partition and a group relation introduced by P. Hall [6] known as isoclinism.

DEFINITION 4.1 The groups G_1 and G_2 are said to be isoclinic, $G_1 \sim G_2$ if:

1) $G_1/Z(G_1) \simeq G_2/Z(G_2)$,

2) $G_1' \simeq G_2'$,

3) if $a_1 Z(G_1) \leftrightarrow a_2 Z(G_2)$ and $b_1 Z(G_1) \leftrightarrow b_2 Z(G_2)$ under 1) then $(a_1, b_1) \leftrightarrow (a_2, b_2)$ under 2).

That is, there must exist isomorphisms 1) and 2) such that 3) is satisfied. Notice that 3) is unambiguous even though a particular choice of coset representatives has been made. For $(a_1, b_1) = (a_1 z_1, b_1 z_2)$ if z_1 and $z_2 \in Z(G_1)$.

Two groups are then said to be isoclinic if the first elements of their descending central series are isomorphic and if the first factor groups of their ascending central series are isomorphic and if the latter isomorphism induces the former.

Although the definition of isoclinism doesn't restrict the groups to p-groups, it becomes equivalent to isomorphism if G_1 and G_2 have trivial centers or if $G_1 = G_1'$, and $G_2 = G_2'$. For p-groups, of course, neither of these two possibilities can occur. The discussion

from this point on will be primarily restricted to p-groups.

It is quite easy to see that the relation of isoclinism is an equivalence relation and hence provides a partition of the set of groups being considered into isoclinic classes, or "families" as P. Hall denotes them. It follows from the definition that both the elements of the descending and ascending central series of one member of a given family is common to all members and hence is a family invariant. Similarly for the derived series. All groups of a given family will therefore have the same class and the same derived length.

Clearly all abelian groups belong to the family containing the element 1. And it is easy to see that if A is any abelian group then $G \times A \sim G$ for any G. This follows from the fact that $(G \times A)' = G'$ and $(G \times A)/Z(G \times A) \simeq G/Z(G)$. Using these properties Hall shows the following:

1) If $K \subseteq G$ then $G \sim K$ if and only if $G = KZ(G)$.

2) If $H = G/N$ then $G \sim H$ if and only if $N \cap G' = 1$.

The statements 1) and 2) may be restated as follows:

1') If $K \subseteq G$ then $G \sim K$ if and only if $G = KA$, A is abelian and A commutes with K elementwise.

2') If $H = G/N$ then $G \sim H$ if and only if there exists $M \lhd G$ with $N \cap M = 1$ and G/M abelian.

Another equivalent form is:

1'') If $K \subseteq G$ then $K \sim G$ if and only if G is a factordirect product of K with an abelian group.

2'') If $H = G/N$ then $H \sim G$ if and only if G is a subdirect product of H with an abelian group.

Hence the isoclinism of a group with an ingroup of itself is the statement that G is decomposable in a rather special way. This suggests that there may be some relation between $G_1 \sim G_2$ and $\{\overline{G_1}\} = \{\overline{G_2}\}$.

It is not true in general that $G_1 \sim G_2$ implies $\{\overline{G_1}\} = \{\overline{G_2}\}$. For $G_1 \sim G_1 \times A$ where A is an abelian group of arbitrarily large exponent whereas the exponent of any element of $\{\overline{G_1}\}$ is bounded by $e(G_1)$. Hence $G_1 \times A \notin \{\overline{G_1}\}$ if $e(A) > e(G_1)$. Similarly $\{\overline{G_1}\} = \{\overline{G_2}\}$ does not necessarily imply $G_1 \sim G_2$, since if $G_2 = G_1 \times G_1$ it is clear that $\{\overline{G_1}\} = \{\overline{G_1 \times G_1}\}$. But if G_1 is non-abelian $G_1/Z(G_1) \ncong (G_1 \times G_1)/Z(G_1 \times G_1) \cong G_1/Z(G_1) \times G_1/Z(G_1)$ and therefore $G_1 \not\sim G_1 \times G_1$. Hence if some statement concerning the relation between isoclinism and the equivalence induced by closure is to be formulated then either the domain of groups under consideration must be restricted or the definition of $\{\overline{G}\}$ must be modified, or both.

Before we can give the modification of closure that will be useful we define the notion of A-permissibility.

DEFINITION 4.2 If $H \subseteq G$ and A is a cyclic group then H is called an A-permissible subgroup of G if G is a factordirect product of H and A_1, with $A_1 \in \{\overline{A}\}$. If $H = G/N$ then H is called an A-permissible factor group of G if G is a subdirect product of H and $A_1 \in \{\overline{A}\}$.

Following are some of the elementary properties of this relation.

LEMMA 4.1 An A-permissible factor group of an A-permissible factor group of G is an A-permissible factor group of G.

Proof Let K be an A-permissible subgroup of G. Then $G = KA_1$, $A_1 \in \{\overline{A}\}$, and K commutes elementwise with the group A_1. If $K = HA_2$, $A_2 \in \{\overline{A}\}$, and H commutes elementwise with the group A_2 then $G = HA_2A_1$. $A_2A_1 \in \{\overline{A}\}$, it is abelian and commutes elementwise with H.

LEMMA 4.2 An A-permissible factor group of an A-permissible factor group of G is an A-permissible factor group of G.

Proof Let $K = G/N_1$ be an A-permissible factor group of G. Hence $G \subseteq G/N_1 \times G/R$ with $G/R \in \{\overline{A}\}$ and $N_1 \cap R = 1$. Let $H = K/M_1$ be an A-permissible factor group of K. Hence $K \subseteq K/M_1 \times K/S_1$ with $K/S_1 \in \{\overline{A}\}$ and $S_1 \cap M_1 = 1$. Let $H = K/M_1 = G/N_1 \big/ M/N_1 \simeq G/M$. It must now be shown that H is an A-permissible factor group of G. Let $S_1 = S/N_1$. Since G/R and $K/S_1 \simeq G/S$ are abelian $R, S \supseteq G'$ and hence $R \cap S \neq 1$. Since $S_1 \cap M_1 = 1$ and $S \cap M = N_1$ then $M \cap R \cap S = N_1 \cap R = 1$. Hence $G \subseteq G/M \times G/R \cap S$. It only remains to show that $G/R \cap S \in \{\overline{A}\}$. Since $G/R \in \{\overline{A}\}$ and $K/S_1 \simeq G/S \in \{\overline{A}\}$ and $G/S \cap R \subseteq G/R \times G/S$ it follows that $G/S \cap R \in \{\overline{A}\}$. Hence $H = K/M_1 \simeq G/S$ is an A-permissible factor group of G.

LEMMA 4.3 An A-permissible factor group of an A-permissible subgroup is an A-permissible subgroup of an A-permissible factor group.

Proof Let K be an A-permissible subgroup of G. That is, $G = KA_1$, with $(k, a) = 1$ for all $k \in K$ and $a \in A_1$ and $A_1 \in \{\overline{A}\}$. Let H be an A-permissible factor group of K. That is, $K \subseteq K/N_1 \times K/S$ with $H = K/N_1$, $N_1 \cap S = 1$ and $K/S \in \{\overline{A}\}$. It must now be shown that H

is an A-permissible subgroup of an A-permissible factor group of G.

Since N_1 and S are normal in K it follows that N_1, $S \triangleleft G$. Hence $G \subseteq G/N_1 \times G/S$ with $N_1 \cap S = 1$. But $G/S = KA_1/S = K/S \cdot A_1S/S$, with $A_1S/S \simeq A_1/A_1 \cap S \in \{\overline{A}\}$ and $K/S \in \{\overline{A}\}$. Hence $G/S \in \{\overline{A}\}$. Therefore G/N_1 is an A-permissible factor group of G. Now $G/N_1 = KA_1/N_1 = K/N_1 \cdot A_1N_1/N_1$. Clearly $(kN_1, aN_1) = 1$ for all $kN_1 \in K/N_1$ and all $aN_1 \in A_1N_1/N_1$ and since $A_1N_1/N_1 \simeq A_1/A_1 \cap N_1 \in \{\overline{A}\}$, $H = K/N_1$ is an A-permissible subgroup of G/N_1.

It is not difficult to show that if A is a priori chosen to be of order equal to the exponent of G then the converse of Lemma 4.3 is valid.

If now we define H to be an A-permissible ingroup of G if H is an A-permissible subgroup of an A-permissible factor group of G then the three lemmas above prove:

THEOREM 4.1 The relation "H is an A-permissible ingroup of G" is transitive.

We now define the notion of A-closure.

DEFINITION 4.3 Let $\{G_\alpha\}$ be a set of groups and let A be a cyclic group. A group G will be said to be of rank 0 if G is an A-permissible ingroup of some G_α. G is of rank 1 if it is an A-permissible ingroup of a direct product of a group of rank 0 with an element of $\{\overline{A}\}$, and it is not of rank 0. In general, G is of rank n if it is not of rank $k < n$, and it is an A-permissible ingroup of a direct product of a group of rank less than n with an element of $\{\overline{A}\}$. The set of

groups with an assigned rank number will be called the A-closure of $\{G_\alpha\}$, written $\{\overline{G_\alpha}\}_A$.

The A-closure of a set of groups may be described in another way:

LEMMA 4.4 Let $\{G_\alpha\}$ be a set of groups. Then $\{\overline{G_\alpha}\}_A$ satisfies:

1) $\{G_\alpha\} \subseteq \{\overline{G_\alpha}\}_A$,

2) if $H \in \{\overline{G_\alpha}\}_A$ and J is an A-permissible ingroup of H then $J \in \{\overline{G_\alpha}\}_A$ and

3) if $H \in \{\overline{G_\alpha}\}_A$ and $A_1 \in \{\overline{A}\}$ then $H \times A_1 \in \{\overline{G_\alpha}\}_A$.

Furthermore, if $\mathfrak{A}$ is a set of groups which satisfies the same conditions as $\{\overline{G_\alpha}\}_A$, above, then $\mathfrak{A} \supseteq \{\overline{G_\alpha}\}_A$.

Proof 1) $\{G_\alpha\} \in \{\overline{G_\alpha}\}_A$ since all elements of $\{G_\alpha\}$ are of rank 0 in $\{\overline{G_\alpha}\}_A$.

2) Trivially, J is an A-permissible ingroup of $H \times A_1$ for any $A_1 \in \{\overline{A}\}$, and is hence in $\{\overline{G_\alpha}\}_A$.

3) $H \times A_1$ is an A-permissible ingroup of itself.

Let $\mathfrak{A}$ be a set satisfying conditions 1), 2), and 3). If G is of rank 0 in $\{\overline{G_\alpha}\}_A$ then G is an A-permissible ingroup of some element of $\{G_\alpha\}$ and is hence in $\mathfrak{A}$. Assume the lemma to be true for all elements of $\{\overline{G_\alpha}\}_A$ of rank less than n. Let H have rank n in $\{\overline{G_\alpha}\}_A$. H is an A-permissible ingroup of $R \times A_1$ with R of rank less than n and $A_1 \in \{\overline{A}\}$. Then $R \in \mathfrak{A}$ and $R \times A_1 \in \mathfrak{A}$. Hence from 2) $H \in \mathfrak{A}$.

That is, $\{\overline{G_\alpha}\}_A$ is the intersection of all those sets of groups which contain $\{G_\alpha\}$ and which are "closed" under the operations of A-permissible ingroups, and direct product with elements of $\{\overline{A}\}$.

If $\{\overline{G_\alpha}\}_A$ is thought of as an operator on the lattice of subsets of the set of all finite groups then it is a closure operator. That is:

LEMMA 4.5 If $\{G_\alpha\}$ and $\{H_\beta\}$ are sets of groups and A is a cyclic group then:

1) $\{G_\alpha\} \subseteq \{\overline{G_\alpha}\}_A$ and,

2) $\overline{\{\{\overline{G_\alpha}\}_A\}}_A = \{\overline{G_\alpha}\}_A$ and,

3) if $\{G_\alpha\} \subseteq \{H_\beta\}$ then $\{\overline{G_\alpha}\}_A \subseteq \{\overline{H_\beta}\}_A$.

Proof 1) This has been demonstrated in Lemma 4.4.

2) From 1) it follows that $\{\overline{G_\alpha}\}_A = \overline{\{\{\overline{G_\alpha}\}_A\}}_A$. If $H \in \overline{\{\{\overline{G_\alpha}\}_A\}}_A$ is of rank 0 then H is an A-permissible ingroup of an element of $\{\overline{G_\alpha}\}_A$ and therefore $H \in \{\overline{G_\alpha}\}_A$. Assume the lemma true for $H \in \overline{\{\{\overline{G_\alpha}\}_A\}}_A$ of rank less than n. Let G be of rank n. Then G is an A-permissible ingroup of $J \times A_1$ with $J \in \overline{\{\{\overline{G_\alpha}\}_A\}}_A$ of rank less than n and $A_1 \in \{\overline{A}\}$. By the induction assumption $J \in \{\overline{G_\alpha}\}_A$. By Lemma 4.4, $J \times A_1 \in \{\overline{G_\alpha}\}_A$ and $G \in \{\overline{G_\alpha}\}_A$. Therefore $\overline{\{\{\overline{G_\alpha}\}_A\}}_A = \{\overline{G_\alpha}\}_A$.

3) It follows from 1) that $\{G_\alpha\} \subseteq \{H_\beta\} \subseteq \{\overline{H_\beta}\}_A$. Hence by Lemma 4.4 $\{\overline{G_\alpha}\}_A \subseteq \{\overline{H_\beta}\}_A$.

Now consider the special case in which $\{G_\alpha\}$ consists of a single group.

LEMMA 4.6 If $H \in \{\overline{G}\}_A$ then $\{\overline{H}\}_A = \{\overline{G}\}_A$.

Proof It is only necessary to show that $G \in \{\overline{H}\}_A$ for it follows from 3) and 2) above that if $H \in \{\overline{G}\}_A$ then $\{\overline{H}\}_A \subseteq \{\overline{G}\}_A$.

Assume that H is of rank n in $\{\overline{G}\}_A$. Hence H is an

A-permissible ingroup of $J \times A_1$, J a group of rank less than n and $A_1 \in \{\overline{A}\}$. By definition H is an A-permissible subgroup of an A-permissible factor group of $J \times A_1$, and it will first be shown that $J \times A_1 \in \{\overline{H}\}_A$.

Let $S = HA_2$ with $A_2 \in \{\overline{A}\}$ and $(h, a) = 1$ for all $h \in H$ and $a \in A_2$. Then $J \times A_1 \subseteq (J \times A_1)/N \times (J \times A_1)/R$ with $N \cap R = 1$, $(J \times A_1)/R \in \{\overline{A}\}$ and $S = (J \times A_1)/N$. First it must be shown that $J \times A_1 \in \{\overline{S}\}_A$. Clearly $S \times (J \times A_1)/R \in \{\overline{S}\}_A$. If $g \in J \times A_1$ then $(J \times A_1)/R \simeq \{[N, gR] \mid \text{all } g \in (J \times A_1)\}$. If $[g_1N, g_2R]$ is an arbitrary element of $(J \times A_1)/N \times (J \times A_1)/R$ then $[g_1N, g_2R]$ $= [g_1N, g_1R]\,[N, g_1^{-1}g_2R] = [N, g_1^{-1}g_2R]\,[g_1N, g_1R]$ since $R \supseteq (J \times A_1)'$. Hence $(J \times A_1)/N \times (J \times A_1)/R$ may be represented as a product of elementwise commuting subgroups one of which is $(J \times A_1)/R$ and the other a group isomorphic to $J \times A_1$. Hence $J \times A_1$ is an A-permissible subgroup of $(J \times A_1)/N \times (J \times A_1)/R = S \times (J \times A_1)/R \in \{\overline{S}\}_A$ and $J \times A_1 \in \{\overline{S}\}_A$. Therefore $J \in \{\overline{S}\}_A$.

In order to show that $S \in \{\overline{H}\}_A$ consider $(H \times A_2)/M$ with $M = \{[h, h^{-1}] \mid h \in H \cap A_2 \text{ in } S\}$. By Theorem 1.3 $S = (H \times A_2)/M$. To show that $(H \times A_2)/M$ is an A-permissible factor group of $H \times A_2$ consider $(H \times A_2)/M \times (H \times A_2)/(H \times 1)$. Since $M \cap (H \times 1) = 1$ and $(H \times A_2)/(H \times 1) \simeq A_2 \in \{\overline{A}\}$ it follows that $H \times A_2 \subseteq (H \times A_2)/M \times (H \times A_2)/(H \times 1)$ and $(H \times A_2)/M$ is an A-permissible factor group of $H \times A_2$. Hence $S \in \{\overline{H \times A_2}\}_A = \{\overline{H}\}_A$. Therefore $J \in \{\overline{H}\}_A$.

Now suppose that H is of rank 0 in $\{\overline{G}\}_A$; then H is an A-permissible ingroup of G. And the argument above, with $A_1 = 1$ and $J = G$ shows that $G \in \{\overline{H}\}_A$. If the lemma is assumed to be true for

all groups of rank less than n in $\{\overline{G}\}_A$ then the argument above shows that $G \in \{\overline{J}\}_A \subseteq \{\overline{H}\}_A$. Hence the lemma follows by induction.

The special case just treated actually represents the general situation since:

LEMMA 4.7 If $\overline{G} \stackrel{DEF.}{=} \{\overline{G}\}_A$ then $\{\overline{G_\alpha}\}_A = \bigvee_\alpha \{\overline{G_\alpha}\}$.

Proof Clearly $\bigvee_\alpha \{\overline{G_\alpha}\} \subseteq \{\overline{G_\alpha}\}_A$. If $H \in \{\overline{G_\alpha}\}_A$ is of rank 0 then H is an A-permissible ingroup of some element of $\{G_\alpha\}$, say G. Hence $H \in \overline{G}$. Assume that for all H of rank less than n in $\{\overline{G_\alpha}\}_A$, $H \in \{\overline{G}\}_A$ for some G in $\{G_\alpha\}$. If H is of rank n then H is an A-permissible ingroup of $J \times A_1$ with J of rank less than n and $A_1 \in \{\overline{A}\}$. But $J \times A_1 \in \overline{J}$ and by the induction assumption $J \in \overline{G}$ for some $G \in \{G_\alpha\}$. Therefore $H \in \overline{G}$ and the conclusion follows by induction.

It is quite evident that the definition of A-closure was formulated so as to preserve the relation of isoclinism. That is:

LEMMA 4.8 If $G_1 \in \{\overline{G_2}\}_A$ then $G_1 \sim G_2$.

Proof Let G_1 be of rank 0 in $\{\overline{G_2}\}_A$. Hence G is an A-permissible ingroup of G_2. Since isoclinism is a transitive relation it follows from 1") and 2") on page 47 that $G_1 \sim G_2$.

Suppose that the lemma is true for $G \in \{\overline{G_2}\}_A$ of rank less than n. If G_1 has rank n then G_1 is an A-permissible ingroup of $J \times A_1$ with J of rank less than n and $A_1 \in \{\overline{A}\}$. Hence $G_1 \sim J \times A_1 \sim J$. But $J \sim G_2$ by the induction assumption. Therefore $G_1 \sim G_2$.

Notice that from Lemma 4.8 it follows that $\{\overline{G_1}\}_A = \{\overline{G_2}\}_A$

implies $G_1 \sim G_2$.

The main theorem of this section will now be stated in the form of a corrected converse of Lemma 4.8 above.

THEOREM 4.2 If G_1 and G_2 are p-groups such that for $i = 1, 2$ $G_i/Z(G_i)$ may be generated by a set of elements of order p then $G_1 \sim G_2$ implies $\{\overline{G_1}\}_A = \{\overline{G_2}\}_A$ with $o(A) = \max_i \{e(G_i)\}$.

Proof Let $G_1/Z(G_1) = \langle \alpha_1 Z(G_1), \ldots, \alpha_k Z(G_k) \rangle$ be an irredundant set of generators of $G_1/Z(G_1)$ such that $o(\alpha_i Z(G_1)) = p$. Let $C = C_1 \times \cdots \times C_k$, $C_i = \langle c_i \rangle$ with $o(c_i) = o(\alpha_i)$ for all i. Consider $G_1 \times C \supseteq H = (\alpha_1 c_1), \ldots, (\alpha_k c_k)$. Since $e(C) \leq e(G_1)$ it follows that $C \in \{\overline{A}\}$. And since $G_1 \times C = HZ(G_1 \times C)$ it follows that H is an A-permissible subgroup of $G_1 \times C$. Hence $H \sim G_1 \times C \sim G_1$ and $\{\overline{H}\}_A = \{\overline{G_1 \times C}\}_A = \{\overline{G_1}\}_A$. It is easy to see that the mapping $\alpha_i c_i Z(H) \leftrightarrow \alpha_i Z(G_1)$ is the isomorphism required by the definition of isoclinism. Let $N = \langle (\alpha_1 c_1)^p, \ldots, (\alpha_k c_k)^p \rangle$. Since $\alpha_i^p \in Z(G_1)$, $N \lhd H$. Also $H' = (G_1 \times C)' = G_1'$ and therefore $N \cap H' = 1$. For if an element of N, $(\alpha_1 c_1)^{r_1 p} \ldots (\alpha_k c_k)^{r_k p}$, is contained in H' then $\alpha_1^{r_1 p} \ldots \alpha_k^{r_k p} c_1^{r_1 p} \ldots c_k^{r_k p}$ must be contained in G_1 and hence $c_1^{r_1 p} \ldots c_k^{r_k p} = 1$. Since all c_i are independent $o(c_i) \mid r_i p$. But $o(c_i) = o(\alpha_i)$ and therefore $\alpha_i^{r_i p} = 1$ for all i.

Let $M = H/N = \langle \alpha_1 c_1 N, \ldots, \alpha_k c_k N \rangle = \langle \beta_1, \ldots, \beta_k \rangle$. Since M is an A-permissible factor group of an A-permissible subgroup of $G_1 \times C$ it follows that $M \sim G_1$ and $\{\overline{M}\}_A = \{\overline{G_1}\}_A$. In addition $o(\beta_i) = p$ for all i. The isomorphism between $M/Z(M)$ and $G_1/Z(G_1)$

required by the definition of isoclinism is induced by the correspondence $\beta_i Z(M) \leftrightarrow \alpha_i Z(G_1)$ since the mapping $(\beta_i, \beta_j) \leftrightarrow (\alpha_i, \alpha_j)$ induces an isomorphism between M' and G_1'.

Now consider $G_2/Z(G_2) = \langle \gamma_1 Z(G_2), \ldots, \gamma_k Z(G_k) \rangle$ and choose these cosets so that $\alpha_i Z(G_1) \leftrightarrow \gamma_i Z(G_2)$ gives the isomorphism required by the definition. The argument given above for G_1 may be reproduced identically for G_2. Hence we obtain a subgroup $R = \langle \vartheta_1, \ldots, \vartheta_k \rangle$ with $o(\vartheta_i) = p$, $\{\overline{R}\}_A = \{\overline{G_2}\}_A$, $R \sim G_2$ and such that the mapping

$$\vartheta_i Z(R) \leftrightarrow \gamma_i Z(G_2)$$

gives the required isomorphism.

If $\{\alpha_1 Z(G_1), \ldots, \alpha_k Z(G_k)\}$ was chosen as an irredundant set of generators it follows that $\{\beta_1, \ldots, \beta_k\}$ is irredundant, and similarly $\{\vartheta_1, \ldots, \vartheta_k\}$ is irredundant.

Since $o(\beta_i) = o(\vartheta_j) = p$ for all i, j it follows that every element of M has a unique representation of the form $\beta_1^{r_1} \ldots \beta_k^{r_k} \theta_1$ with $\theta_1 \in M'$, and similarly for R. If $\sigma((\beta_i, \beta_j)) = (\vartheta_i, \vartheta_j)$ then σ induces the isomorphism between M' and R' implied by the $M/Z(M) \simeq R/Z(R)$.

Consider the mapping:

$$\beta_1^{r_1} \ldots \beta_k^{r_k} \theta_1 \leftrightarrow \vartheta_1^{r_1} \ldots \vartheta_k^{r_k} \sigma(\theta_1).$$

Clearly it is well defined on all of M, and since σ^{-1} is uniquely defined the mapping is one-one. To show that it is an isomorphism consider $\beta_1^{d_1} \ldots \beta_k^{d_k} \theta_1 \cdot \beta_1^{e_1} \ldots \beta_k^{e_k} \theta_2 = \beta_1^{d_1+e_1} \ldots \beta_k^{d_k+e_k} \theta_3 \theta_1 \theta_2$, and

$$\vartheta_1^{d_1} \ldots \vartheta_k^{d_k} \sigma(\theta_1) \vartheta_1^{e_1} \ldots \vartheta_k^{e_k} \sigma(\theta_2) = \vartheta_1^{d_1+e_1} \ldots \vartheta_k^{d_k+e_k} \theta_4 \sigma(\theta_1)\sigma(\theta_2).$$

Clearly θ_4 is formally identical to θ_3 with β_i replaced by ϑ_i. Hence $\theta_4 = \sigma(\theta_3)$ and since σ is an isomorphism $\sigma(\theta_3)\sigma(\theta_1)\sigma(\theta_2)$ $= \sigma(\theta_3\theta_1\theta_2)$.

Therefore $R \simeq M$ and $\{\overline{G_1}\}_A = \{\overline{G_2}\}_A$.

Using an argument quite similar to the one above it will now be shown that:

THEOREM 4.3 If G_i are p-groups such that $c(G_i) = 2$ and G_i $= \langle a_i, b_i \rangle$ for $i = 1, 2$ then $G_1 \sim G_2$ implies that $\{\overline{G_1}\}_A = \{\overline{G_2}\}_A$ with $o(A) = \max_i \{e(G_i)\}$.

Proof Let $G_1 = \langle a_1, b_1 \rangle$ and hence $G_1/Z(G_1) = \langle a_1 Z(G_1), b_1 Z(G_1) \rangle$. Suppose $o(a_1 Z(G_1)) = p^{\alpha_1}$ and $o(b_1 Z(G_1)) = p^{\beta_1}$. Let C and D be two cyclic groups such that $C = \langle c \rangle$, $o(c) = o(a_1)$ and $D = \langle d \rangle$, $o(d)$ $= o(b_1)$. Clearly $C, D \in \{\overline{A}\}$. Consider $G_1 \times C \times D \supset H = \langle a_1 c, b_1 d \rangle$. Since $G_1 \times C \times D \in \{\overline{G_1}\}_A$ and $HZ(G_1 \times C \times D) = G_1 \times C \times D$ then $H \in \{\overline{G_1}\}_A$. Let $N = \langle (a_1 c)^{p^{\alpha_1}}, (b_1 d)^{p^{\beta_1}} \rangle$. Clearly $N \lhd H$, and $N \cap H' = 1$. Hence $H_1 = G_1/N \in \{\overline{H}\}_A = \{\overline{G_1}\}_A$ and $\{\overline{H_1}\}_A = \{\overline{G_1}\}_A$. Now $H_1 = \langle (a_1 c)N, (b_1 d)N \rangle = \langle \overline{a}_1, \overline{b}_1 \rangle$ and if $\overline{a}_1^{p^{\alpha}} \in Z(H_1)$ then $(\overline{a}_1)^{p^{\alpha}} = 1$. For if $(\overline{a}_1^{p^{\alpha}}, \overline{b}_1) = 1$, $((a_1 c)^{p^{\alpha}}, b_1 d)N = (a_1^{p^{\alpha}}, b_1)N = N$. But $(a_1^{p^{\alpha}}, b_1) \in H_1'$ and $N \cap H_1' = 1$. Therefore $(a_1^{p^{\alpha}}, b_1) = 1$ and since $G_1 = \langle a_1, b_1 \rangle$ $a_1^{p^{\alpha}} \in Z(G_1)$, $(a_1 c)^{p^{\alpha}} \in N$ and $(\overline{a}_1)^{p^{\alpha}} = 1$. Similarly for $\overline{b}_1$. Now let $G_2 = \langle a_2, b_2 \rangle$ where a_2 and b_2 are chosen such that: $a_1 Z(G_1) \leftrightarrow a_2 Z(G_2)$, $b_1 Z(G_1) \leftrightarrow b_2 Z(G_2)$, induces

the isomorphism required by the definition of isoclinism.

In an analagous manner form $H_2 = \langle (a_2 r)M, (b_2 s)M \rangle = \langle \bar{a}_2, \bar{b}_2 \rangle$, and $\{\overline{H_2}\}_A = \{\overline{G_2}\}_A$.

It will now be shown that every element of H_1 has a unique representation in the form $\bar{a}_1^{\alpha_1} \bar{b}_1^{\beta_1} \theta_1$ with $\theta_1 \in H_1'$. For if $\bar{a}_1^{\alpha_1} \bar{b}_1^{\beta_1} \theta_1 = \bar{a}_1^{\alpha_2} \bar{b}_1^{\beta_2} \theta_2$ then $\bar{a}_1^{\alpha_1 - \alpha_2} = \bar{b}_1^{\beta_2 - \beta_1} \theta_2 \theta_1^{-1}$ and therefore $\bar{a}_1^{\alpha_1 - \alpha_2} \in Z(H_1)$. But then $\bar{a}_1^{\alpha_1 - \alpha_2} = 1$ and so $\bar{a}_1^{\alpha_1} = \bar{a}_1^{\alpha_2}$. Similarly $\bar{b}_1^{\beta_1} = \bar{b}_1^{\beta_2}$ and hence $\theta_1 = \theta_2$.

The identical argument shows that every element of H_2 has a unique representation of the form $\bar{a}_2^{\gamma_1} \bar{b}_2^{\delta_1} \phi_1$, with $\phi_1 \in H_2'$.

Let $\sigma((\bar{a}_1^x, \bar{b}_1^y)) = (\bar{a}_2^x, \bar{b}_2^y)$. Then σ induces an isomorphism between H_1' and H_2'.

Consider the mapping:

$$\bar{a}_1^x \bar{b}_1^y \theta_1 \leftrightarrow \bar{a}_2^x \bar{b}_2^y \sigma(\theta_1).$$

By an argument identical to that given in Theorem 4.2 $H_1 \simeq H_2$ and hence $\{\overline{G_1}\}_A = \{\overline{G_2}\}_A$.

The detailed description which P. Hall gives of the isoclinism families involves a discussion of the so-called "stem" groups of the family. These are the family members of least order. Stem groups may also be characterized by the property: $Z(G) \subseteq G'$. In showing that there always are such groups the following construction is used: Form the direct product of a group in the family with a finitely generated free abelian group and consider an appropriate factor group of a subgroup of this direct product. In this manner a stem group can

always be constructed. Hence if A is allowed to be the free group of one generator then there always exists a stem group G_1 such that for any group $G \sim G_1$, $\{\overline{G}\}_A = \{\overline{G_1}\}_A$.

CONCLUSION

Several rather general questions have been raised in the preceding four chapters. In Chapter I the problem of determining necessary and sufficient conditions for $\{\overline{G_1}\} = \{\overline{G_2}\}$ was mentioned. The interesting case to examine is that for which G_1 and G_2 are indecomposable. Since G_1 is not an ingroup of G_2 this question is equivalent to whether or not the basis set of our decompositions theory is "independent". It was shown in Chapter I that independence does not hold, in general since both the quaternion and dihedral groups of order eight are indecomposable and yet have the same closure. Whether this is just a peculiarity of 2-groups or perhaps irregular p-groups is not clear. One certainly ought to be able to settle this question for indecomposable p-groups of class two with $p \neq 2$ since these are given explicitly in Chapter II.

One rather obvious direction in which to carry the technics here developed is to study the decomposition question for finite groups of composite order. It follows from Theorem 1.4 that a decomposable group is either a subdirect product or it contains a normal abelian p-group. At this stage, however, it is not clear how useful it is to know that groups with no normal abelian p-subgroup are either indecomposable or subdirect products. Certainly this question might be profitably pursued. One might begin with composite order groups which have abelian Sylow subgroups, for example.

The unanswered question in Chapter II concerns the defining relations for indecomposable 2-groups of class two. It is not very surprising that there is a greater variety of indecomposable 2-groups

of this type since almost any compilation of p-groups of certain orders invariably must deal with $p = 2$ in a special way. One strong possibility is that this greater variety of 2-groups is absorbed by considering the closure of a 2-group and not the group itself. For example, it is shown in Chapter II that the quaternion group of order eight doesn't fit in with either of the two general forms of defining relations given. But if D and Q are the dihedral and quaternion groups of order eight then $\{\overline{Q}\} = \{\overline{D}\}$ and the defining relations for D do fit one of these given forms. Hence it seems plausible that if G is an indecomposable 2-group of class two then there exists a group in the closure of G whose defining relations fall in one of the two given categories.

The main result of Chapter III provides a tool for handling a good part of the decomposability problem for p-groups of class three. A complete characterization of the indecomposable p-groups of class three seems quite accessible. The most difficult case arises when $G/Z(G)$ is a subdirect product.

The notion of A-closure which is linked up with the relation of isoclinism might be investigated directly as a classification procedure for p-groups. This assumes of course that all of the hypotheses of Theorem 4.2 are indeed necessary. It certainly would be desirable to settle this question.

GLOSSARY

$\{A_\alpha\}$	Set of elements A_α, α contained in some index set.
$A \leq B$	A is an ingroup of B.
$A < B$	A is a proper ingroup of B.
$A \subseteq B$	A is a subgroup (subset) of B.
$A \subset B$	A is a proper subgroup (subset) of B.
$\overline{\{A_\alpha\}}$	The closure of $\{A_\alpha\}$.
$\langle a_1, \ldots, a_n \rangle$	The group generated by the set $\{a_1, \ldots, a_n\}$.
$[a, b]$	An element in $A \times B$ with $a \in A$, $b \in B$.
$N \lhd G$	N is a normal subgroup of G.
$A \simeq B$	A and B are isomorphic.
$o(A)$	The order of the group (element) A.
$[A : B]$	The index of B in A.
$a \equiv b(n)$	a is congruent to b modulo n.
$A \cap B$	The intersection of A and B.
$A \cup B$	The group generated by the subgroups A and B.
$Z(G)$	The center of G.
$Z_i(G)$	$Z_i(G)/Z_{i-1}(G) = Z(G/Z_{i-1}(G))$ with $Z(G) = Z_1(G)$.
$c(G)$	The class of the nilpotent group G.
G'	The derived group of G.
$G^{(n)}$	The n^{th} derived group of G with $G^{(1)} = G'$.
$a \mid b$	The integer a divides the integer b.
$a \nmid b$	The integer a does not divide the integer b.
$\Phi(G)$	The Frattini subgroup of G.
$G_{(n)}$	The n^{th} higher commutator group of G with $G_{(2)} = G'$.
(a, b)	The commutator of a and b, i.e. $a^{-1} b^{-1} a b$.

$A \sim B$	A is isoclinic to B.
$\{\overline{G}\}_A$	The A-closure of G.
$\bigvee_\alpha \{\overline{G_\alpha}\}$	Set union of the sets $\overline{G_\alpha}$.

REFERENCES

1 G. Higman, Some remarks on varieties of groups, Quart. J. of Math. (Oxford) vol. 10 (1959) pp. 165-178.

2 H. Zassenhaus, The Theory of Groups, Chelsea Publishing Company, New York, 1949.

3 O. Ore, Structures and group theory I, Duke Math. J. vol. 3 (1937) pp. 149-174.

4 P. Hall, A contribution to the theory of groups of prime-power order, Proc. London Math. Soc. vol. 36 (1933) pp. 29-95.

5 W. Burnside, Theory of Groups of Finite Order, 2nd ed. Cambridge, 1911.

6 P. Hall, The classification of prime-power groups, J. Reine Angew. Math. vol. 182 (1940) pp. 130-141.