

A DECOMPOSITION THEORY FOR FINITE GROUPS WITH APPLICATIONS TO p -GROUPS⁽¹⁾

BY

PAUL M. WEICHSEL

Introduction. This note 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 $\{G_\alpha\}^*$, which is the smallest set of groups containing $\{G_\alpha\}$ and closed under the operations of taking finite direct products, subgroups and factor groups.

A group G is then called an in-direct product if $G \in \{A_\alpha\}^*$ where $\{A_\alpha\}$ is the set of all proper subgroups and factor groups of G . Some necessary conditions for decomposability are derived and it is shown, in particular, that an in-direct product which is not a subdirect product or a factor group of a direct product contains a normal subgroup which is an abelian p -group.

In §2 an attempt is made to gain information about the decomposability of a p -group G from the knowledge that $G/Z(G)$ is an in-direct product. It is shown that whenever the class of G is greater than two then G is an in-direct product if $G/Z(G)$ is a factor group of a direct product. An example is given which shows that this decomposition is in general nontrivial. That is, an in-direct product is given which is neither a subdirect product, or the factor group of a direct product.

In §3 several characterizations of those p -groups of class two which are not in-direct products are given.

The following notation will be used throughout without special definition: $A \subset B$, A is a proper subgroup (subset) of B . $\langle a_1, \dots, a_n \rangle$ is the group generated by the set $\{a_1, \dots, a_n\}$. The direct product $A \times B = \{[a, b] \mid a \in A, b \in B\}$. $o(A)$ is the order of the group (element) A . $Z(G)$ is the center of G . $Z_i(G)$ is defined by: $Z_i(G)/Z_{i-1}(G) = Z(G/Z_{i-1}(G))$ for $i = 2, 3, \dots$ with $Z(G) = Z_1(G)$. $c(G)$ is the class of G .

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

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

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

Presented to the Society, November 25, 1960 under the title *A decomposition theory for finite groups*; received by the editors December 21, 1960 and, in revised form, June 8, 1961.

(¹) The author wishes to express his gratitude to the referee for his thorough critique and many helpful suggestions.

- (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 $A \leq G$ 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.*

We now define the notion of closure.

DEFINITION 1.2. Let $\{A_\alpha\}$ be a set of groups. Denote by $\{A_\alpha\}^*$ a set of groups containing $\{A_\alpha\}$ and closed under the operations of taking ingroups and finite direct products such that if \mathfrak{G} is a set of groups which contains $\{A_\alpha\}$ and is closed under the operations of taking ingroups and finite direct products then \mathfrak{G} contains $\{A_\alpha\}^*$. We shall refer to $\{A_\alpha\}^*$ as the *closure* of $\{A_\alpha\}$ ⁽²⁾.

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 1.2. *If $\{A_\alpha\}$ and $\{B_\beta\}$ are sets of groups then:*

- (a) $\{A_\alpha\} \subseteq \{A_\alpha\}^*$,
- (b) $\{A_\alpha\}^{**} = \{A_\alpha\}^*$ and
- (c) if $\{A_\alpha\} \subseteq \{B_\beta\}$ then $\{A_\alpha\}^* \subseteq \{B_\beta\}^*$.

A natural question which arises from the definition of closure is: Can one give necessary and sufficient conditions for $\{G_1\}^* = \{G_2\}^*$, 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 for example that if G_1 and G_2 are abelian groups then $\{G_1\}^* = \{G_2\}^*$ 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 the following: Let Q_n and D_n be the generalized quaternion⁽³⁾ group of order 2^n and the dihedral group of order 2^n respectively.

THEOREM 1.1. $\{D_n\}^* = \{Q_n\}^*$.

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 $D_n \in \{Q_n\}^*$ and $Q_n \in \{D_n\}^*$. It will then follow from Lemma 1.2 that $\{D_n\}^* = \{Q_n\}^*$.

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

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

⁽³⁾ Zassenhaus [2, p. 147].

$N \triangleleft G$ 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 $D \cong D_n$.

It is clear that $([a, 1]N)^{2^{n-1}} = ([b, c]N)^2 = 1$. Also $[b, c]N[a, 1]N[b, c]^{-1}N = [bab^{-1}, 1]N = [a^{-1}, 1]N = ([a, 1]N)^{-1}$. Hence the generators of D satisfy the same relations as the generators of D_n , and the mapping

$$\begin{aligned} g &\rightarrow [a, 1]N \\ h &\rightarrow [b, c]N \end{aligned}$$

induces a homomorphism of D_n onto D . But suppose that for some element $h^\alpha g^\beta \in D_n$,

$$h^\alpha g^\beta \rightarrow [1, 1]N.$$

Then $[b^\alpha a^\beta, c^\alpha] \in N$. Hence $2 \mid \alpha$ and $2^{n-1} \mid \beta$. Therefore $h^\alpha g^\beta = 1$ and the mapping is an isomorphism. Hence $D_n \in \{Q_n\}^*$.

Let H be as above and consider $R = D_n \times H$. Clearly $R \in \{D_n\}^*$. Let $R \supset S = \langle [g, 1], [h, c] \rangle$ and $M = \langle [g^{2^{n-2}}, c^2] \rangle$. Clearly $M \triangleleft S$. Now let $Q = S/M$ and we will show that $Q \cong Q_n$.

As in the previous case the generators of Q satisfy the same relations as the corresponding generators of Q_n , and thus the mapping:

$$\begin{aligned} a &\rightarrow [g, 1]M \\ b &\rightarrow [h, c]M \end{aligned}$$

induces a homomorphism of Q_n onto Q . Let $b^\gamma a^\delta$ be an arbitrary element of Q_n , and suppose that $b^\gamma a^\delta \rightarrow [1, 1]M$. Then $[h^\gamma g^\delta, c^\gamma] \in M$, and therefore either $4 \mid \gamma$ and $2^{n-1} \mid \delta$ or $2 \mid \gamma$ and $2^{n-2} \mid \delta$. In either case $b^\gamma a^\delta = 1$ and so the mapping is an isomorphism. Hence $Q_n \in \{D_n\}^*$ which completes the proof.

REMARK 1. There is a close connection between the closure of a set of groups as defined above and sets of groups defined by a set of identical relations. G. Birkhoff [3] has shown that any set of groups closed under the operations of taking ingroups and unrestricted direct products satisfy a certain set of identities and conversely the set of groups which satisfy a given set of identities is closed under these operations. Our notion of closure differs from that considered by Birkhoff in that we take restricted direct products only. It is easy to see however that the finite groups contained in the closure (in the sense of Birkhoff) of a set of finite groups is precisely the closure (in our sense) of that set.

REMARK 2. We call a group-theoretic property *inherited* if, whenever a group G has the property, then so do all of its ingroups and if $G \times H$ has the property whenever G and H have it. Hence the closure of a set of groups can be thought of as the "Strongest" inherited property that is shared by all of

the members of the set. In these terms Theorem 1.1 may be restated as follows: The groups Q_n and D_n have identical inherited properties for each n .

DEFINITION 1.3. Let $\{A_\alpha\}$ be the set of proper ingroups of a group G . G is called an *in-direct product* if $G \in \{A_\alpha\}^*(4)$.

$G \in \{A_\alpha\}^*$ implies that there exist $A, B \in \{A_\alpha\}^*$ such that $G \leq A \times B$. The interesting case in this connection is $G = H/N$ with $H \subset A \times B$. The cases of G , a subdirect product or a factor group of a direct product are discussed in detail in [5, pp. 12-18].

LEMMA 1.3. Let $G = H_1/N_1$ with H_1 a subdirect product of A_1 and B_1 . Then there exist factor groups A, B, H and N of A_1, B_1, H_1 , and N_1 respectively such that $G \cong H/N, H \subset A \times B$ and there exist $R, S \triangleleft H$ 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 $R_1, S_1 \triangleleft H_1$ such that $R_1 \cap S_1 = 1$. Let $(R_1 \cap N_1) \cup (S_1 \cap N_1) = M$. 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 $R_1M/M \cong R_1/R_1 \cap M$ the lemma is proved.

THEOREM 1.2. Let G, H, N, 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 $G = H/N \cong H/R/N/R$ and hence G is isomorphic to a factor group of A . If $NS = N$ then $G = H/N \cong H/R/N/R$ 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 $NS \cap R = 1$ 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 1.3. 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

(4) The referee has pointed out that this notion is equivalent to the idea of a "noncritical" group given by D. C. Cross in [4].

of the argument that follows verify that the unions and intersections given in the diagram are indeed correct.

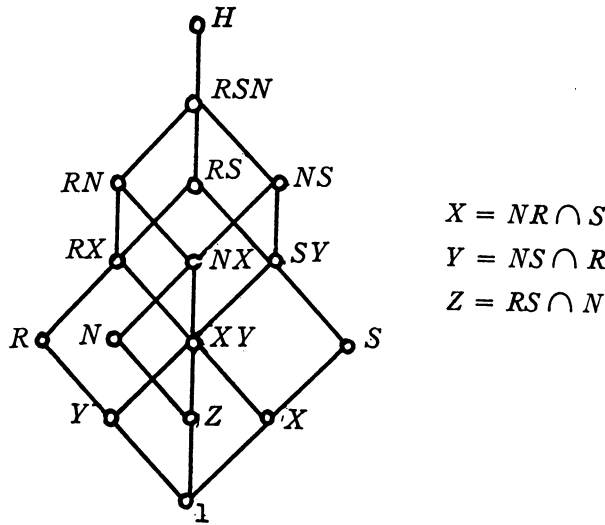


FIGURE 1

$X \cap Y = (NR \cap S) \cap (NS \cap R) \subseteq R \cap S = 1$. 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 [6] 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 $RN \cap SN / N = XY \cup N / N \cong XY / XY \cap N = XY / Z = XZ / Z \cong X$. 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.

The problem of determining whether or not a given group G is an indirect product is a special case of the more general question: Given a set of groups $\{A_\alpha\}$, and a group G , what are necessary and sufficient conditions for

$G \in \{A_\alpha\}^*$? Three necessary conditions are given below which follow directly from the definition of closure, or from the theorem quoted in Remark 1.

(1) If $G \in \{A_\alpha\}^*$ then $G/Z(G) \in \{A_\alpha/Z(A_\alpha)\}^*$. Hence if G is nilpotent and $\{A_\alpha\}$ is a set of proper ingroups, then the class of G is equal to the class of A_i for some $A_i \in \{A_\alpha\}$.

(2) If $G \in \{A_\alpha\}^*$ then $G' \in \{A'_\alpha\}^*$. If G is soluble, then the remark above holds with respect to the derived length of G .

(3) If $G \in \{A_\alpha\}^*$ 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, $e(G) \mid \text{lcm}_i \{e(B_i)\}$.

2. The problem of determining when an arbitrary group G is an in-direct product can in some cases be solved by considering $G/Z(G)$. The case of G , a p -group, will be interesting in this connection since then $Z(G) \neq 1$.

THEOREM 2.1. *Let G be a group, not of class two. If $G/Z(G)$ is a product of elementwise commuting proper subgroups, then G is an in-direct product.*

Proof. Let A and B be subgroups of G such that $G/Z(G) = [A/Z(G)][B/Z(G)]$ with $(a, b) \in Z(G)$ for all $a \in A, b \in B$. We will show that G is contained in the closure of the set of groups consisting of A, B and $\langle a, b \rangle$ for all $a \in A$ and $b \in B$.

Let $H = A \times B \times \prod_{a_i \in A, b_j \in B} \langle a_i, b_j \rangle$ and let G^* be the subgroup of H generated by the following elements: For each $a \in A$ choose the element $a^* \in H$ whose component in A is a , in B is 1, and in $\langle a_i, b_j \rangle$ is a if $a = a_i$ and 1 otherwise. Similarly choose b^* in H . We will now show that the mapping: $a^* \rightarrow a, b^* \rightarrow b$ induces a homomorphism of G^* onto G .

The mapping is clearly onto since $G = AB$. To demonstrate the homomorphism we must show that if $\omega(a^*, b^*)$ is any word on the elements of G^* and if $\omega(a^*, b^*) = 1$ then the corresponding relation $\omega(a, b) = 1$ holds in G . Since the commutators of the form (a, b) with $a \in A, b \in B$ are in the center of G it follows that any word $\omega(a^*, b^*)$ has $\omega_1(a)$ as its A component, $\omega_2(b)$ as its B component and $a^{e_i} b^{e_j} (a_i, b_j)^{f_{ij}}$ as its $\langle a_i, b_j \rangle$ component, with e_i and e_j the exponent sums of a_i and b_j in $\omega_1(a)$ and $\omega_2(b)$ respectively. Now consider the $\langle a_i, 1 \rangle$ component of $\omega(a^*, b^*)$. It must be $a_i^{e_i}$ and hence $a_i^{e_i} = 1$. Similarly $b_j^{e_j} = 1$ and therefore $(a_i, b_j)^{f_{ij}} = 1$. But $\omega(a, b) = \omega_1(a) \omega_2(b) \prod_{i,j} (a_i, b_j)^{f_{ij}}$. Therefore $\omega(a, b) = 1$.

In order to verify that G is an in-direct product it suffices to show that $\langle a_i, b_j \rangle$ is a proper subgroup of G for all i, j . But if $\langle a_i, b_j \rangle = G$ then $G/Z(G)$ is abelian and G has class two, contrary to hypothesis. This completes the proof of the theorem.

COROLLARY 2.2. *Let G be a p -group of class $n > 2$. If $G = AB$ with $(a, b) \in Z(G)$ for all $a \in A, b \in B$ then $c(A) = n$ or $c(B) = n$.*

Proof. It is clear that if $G \in \{A_\alpha\}^*$ then $c(G) \leq c(A_\alpha)$ for some α . Since

$G \in \{A, B, \langle a_i, b_j \rangle\}^*$ for all $a_i \in A, b_j \in B$ and $\langle a_i, b_j \rangle$ has class two for all i, j either A or B has class n .

In Theorem 2.1 G was obtained as a homomorphic image of a subgroup of a direct product. The following is an example of a group satisfying the hypothesis of the theorem and which cannot be obtained either as a subgroup of a direct product of proper ingroups or as a factor group of such a direct product.

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 3. Consider $A \times A \supset H = \langle [a_1, 1], [a_2, a_1], [1, y] \rangle$. Let $G = H/N$ with $N = \langle [z, z^{-1}] \rangle$. It is easy to see that G fulfills the conditions given above.

3. We will here consider p -groups of class two. A group G is of class two if $1 \subset G' \subseteq Z(G)$. That is, G is nonabelian and $G/Z(G)$ is abelian. Since such groups are quite similar to abelian groups it is reasonable to expect that an in-direct product of class two will be decomposable in a rather simple way. This is indeed the case and a complete characterization of class two groups which are not in-direct products is obtained.

The following lemmas concerning nilpotent groups will be needed in this and the following section.

LEMMA 3.1⁽⁵⁾. *If G is nilpotent and $N \triangleleft G$ then $N \cap Z(G) \supset 1$.*

LEMMA 3.2. *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 noncyclic 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 $N_1, N_2 \triangleleft G$ 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 3.1 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 3.3⁽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 $(a, b)^n = (a^n, b) = (a, b^n)$ for all integers n .*

LEMMA 3.4. *If a group G has two subgroups A, B such that $G = AB$ and $ab = ba$ for all $a \in A$ and $b \in B$ then $G \cong (A \times B)/N$ for some $N \triangleleft A \times B$.*

Proof. Consider the mapping $[a, b] \rightarrow ab$, from $A \times B$ into G . It is clearly a homomorphism since $a_1 b_1 a_2 b_2 = a_1 a_2 b_1 b_2$.

LEMMA 3.5. *Let G be a p -group of class two. If G is an in-direct product then*

⁽⁵⁾ P. Hall [4, p. 34].¹

⁽⁶⁾ H. Zassenhaus [2, p. 60].

G is either a direct product, subdirect product, or a factor group of a direct product.

Proof. Assume that G is an in-direct product but is not a direct or sub-direct 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 that there exists a commutator, (a, b) , such that $G' = \langle (a, b) \rangle$. Let $o((a, b)) = p^\beta$. Since G is an in-direct product it follows that $G' \in \{A_\mu\}^*$ where $\{A_\mu\}$ is the set of proper in-groups 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 $A_1' = (G/N)' = G'N/N \cong G'/G' \cap N$. Lemma 3.1 states that all normal subgroups of G have a nontrivial intersection with $Z(G)$ and hence with G' . Hence A_1' would have exponent properly smaller than $e(G')$. Therefore, 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 group of a direct product. Since A is a proper subgroup of G , there exist elements $\{g_i\}$ such that $G = \langle c, d, g_1, \dots, g_k \rangle$, and such that none of the g_i 's may be omitted. Consider $B = \langle g_1, \dots, g_k \rangle$.

Let $(c, g_i) = m^{\alpha_i}$ for all $i = 1, \dots, k$. It follows from Lemma 3.3 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 $B_1 = \langle g_1'', \dots, g_k'' \rangle$. 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 factor group of $A \times B$, completing the proof of the lemma.

THEOREM 3.1. *Let G be a p -group of class two. G is not an in-direct product if and only if $Z(G)$ is cyclic and G may be generated by two elements.*

Proof. If G is not an in-direct product then clearly $Z(G)$ is cyclic. The fact that G has two generators follows from a result of R. C. Lyndon which is given in all generality in [5]. This result states that a p -group of class c which is not an in-direct product may be generated by c elements.

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 an in-direct product it follows from Lemma 3.5 that $G = AB$, $ab = ba$ for all $a \in A$ and $b \in B$. Clearly $G/A \cap B \cong (A/A \cap B) \times (B/A \cap B) = \bar{A} \times \bar{B}$. 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 \bar{A} and \bar{B} are cyclic, and since $A \cap B \subseteq Z(G)$, G is abelian, a contradiction.

REFERENCES

1. G. Higman, *Some remarks on varieties of groups*, Quart. J. Math. Oxford Ser. 10 (1959), 165–178.
2. H. Zassenhaus, *The theory of groups*, Chelsea, New York, 1949.
3. G. Birkhoff, *On the structure of abstract algebras*, Proc. Cambridge Philos. Soc. 31 (1935), 433–454.
4. G. Higman, *Identical relations in finite groups*, Convegno Internazionale di Teoria dei gruppi finiti e applicazioni, Rome, 1960.
5. P. Weichsel, Doctoral dissertation, California Institute of Technology, Pasadena, California, (1960).
6. O. Ore, *Structures and group theory*. I, Duke Math. J. 3 (1937), 149–174.

CALIFORNIA INSTITUTE OF TECHNOLOGY,
PASADENA, CALIFORNIA
THE UNIVERSITY OF ILLINOIS,
URBANA, ILLINOIS