Pacific Journal of Mathematics

ON UNIQUENESS OF GENERALIZED DIRECT DECOMPOSITIONS

FRANCIS C.Y. TANG

Vol. 23, No. 1 March 1967

PACIFIC JOURNAL OF MATHEMATICS
Vol. 23, No. 1, 1967

ON UNIQUENESS OF GENERALIZED DIRECT DECOMPOSITIONS

C. Y. TANG

Generalized direct products were introduced by B. H. Neuman and H. Neumann. In this paper we attempt to study some properties of generalized direct decompositions of groups. In general, decompositions of a given group into indecomposable generalized direct factors are not unique up to isomorphisms. The main result of this paper is that if the commutator subgroup of G is a cyclic p-group contained in the center $Z(G)$ then any two generalized direct decompositions of G into indecomposable generalized direct factors with respect to its center $Z(G)$ of G are isomorphic modulo $Z(G)$.

Generalized direct products with amalgamated subgroups were defined externally by B. H. Neumann and H. Neumann in [1]. Different existence theorems of such products for given amalgams of groups were given in [1], [2], [3], [4]. The main application so far has been in the construction of groups. It seems to us that it is of interest to study the internal structure of such products. In particular, we like to obtain some information concerning the decomposition of a given group relative to some $H \subset Z(G)$ into factors indecomposable relative to the same H. Examples can easily be constructed to show that such decompositions may not necessarily be unique up to isomorphisms. The main difficulty is due to the fact that intersections of the commutator subgroups of the factors may not be trivial. In the following investigation we shall restrict ourselves to the special case when the generalized direct product has only a single amalgamated subgroup.

In § 2 we shall develop some simple properties concerning the exchangeability of factors in different decompositions. In § 3 we obtain a characterization of groups which are generalized directly indecomposable with respect to their centers for the case of nilpotent groups of class two with cyclic commutator subgroups. With this result we are able to show that for a nilpotent group of class two with a finite cyclic commutator subgroup any decompositions into generalized direct indecomposable factors with respect to its center $Z(G)$ are isomorphic mod $Z(G)$. It is of interest to note that, applying a theorem of Weichsel [5], for $Z(G) = C(G)$ we can give a characterization of critical p-groups in terms of generalized direct indecomposability with respect to the center.

Since it is too difficult to study generalized direct decompositions with respect to more than one amalgamated subgroup we shall only attempt to define generalized direct decomposition with respect to a single amalgamated subgroup. Moreover in our investigation we shall always assume the double chain condition of Zassenhaus [6] so that only a finite number of factors is involved.

DEFINITION 1.1. A group G is said to have a generalized direct decomposition with respect to a subgroup H if there exist subgroups $G_1, \cdots, G_n$ such that,

(i) G is generated by $G_1, \cdots, G_n$,

(ii) G_i and G_j commute elementwise for all $i \neq j$,

(iii) G_i contains H for all i,

(iv) the intersection of G_i with the subgroup generated by

$$G_1, \cdots, G_{i-1}, G_{i+1}, \cdots, G_n$$

is exactly H for all i.

G_i will be called a generalized direct factor of G with respect to H, and we shall denote such a decomposition by $G = (G_1 \times \cdots \times G_n)_H$. If there does not exist such a set of subgroups other than G and H then we shall say that G is generalized directly indecomposable with respect to H.

It is to be noted that H must be contained in the center of G.

NOTATIONS AND TERMINOLOGY. For abbreviation we shall call a generalized direct decomposition with respect to H an H-decomposition. Correspondingly we shall also use the terms H-products, H-factors and H-indecomposable.

We shall adopt the following notations:

$$\prod_{i=1}^{n} G_i = G_1 \times \cdots \times G_n$$

$$\left(\prod_{i=1}^{n} G_i\right)_H = (G_1 \times \cdots \times G_n)_H$$

If $G = \prod_{i=1}^{n} G_i$ then $G_i' = \prod_{\nu\neq i}^{n} G_\nu$ and in the same way if $G = (\prod_{i=1}^{n} G_i)_H$ then $G_i' = (\prod_{\nu\neq i}^{n} G_\nu)_H$.

If $G = (\prod_{i=1}^{n} G_i)_H$ then $\bar{G}$ and $\bar{G}_i$ will always mean G/H and G_i/H respectively. Moreover if $x \in G$ then $\bar{x}$ will be the image of x in $\bar{G}$.

For $G = \prod_{i=1}^{n} G_i$ the G_i-decomposition operator is to be understood in the sense of Zassenhaus [6].

The commutator of the elements x and y is denoted by $[x, y]$.

$[A, B]$ denotes the subgroup generated by the set of all commutators $[x, y]$ where $x \in A$ and $y \in B$.

$\{x_1, \cdots, x_n\}$ and $\{x_1, \cdots, x_n, H)$ will mean the group generated by $x_1, \cdots, x_n$ and the group generated by $x_1, \cdots, x_n$ together with elements of H respectively.

$Z(G)$ and $C(G)$ will be the center and the commutator subgroup of G respectively.

DEFINITION 1.2. Every H-decomposition of G induces a direct decomposition of $\bar{G}$. Thus two H-decompositions of G are said to be isomorphic mod H if and only if their induced direct decompositions of $\bar{G}$ are isomorphic.

It is not difficult to establish the following results:

THEOREM 1.3. *If G is abelian then any H-decompositions into indecomposable H-factors are isomorphic* mod H.

THEOREM 1.4. *If G splits over H then any H-decompositions into indecomposable H-factors are isomorphic. Indeed if $Z(G) = H$ then the decomposition is unique.*

2. DEFINITION 2.1. Let $G = (\prod_{i=1}^{n} G_i)_H = (\prod_{i=1}^{m} F_i)_H$ be two H-decompositions of G. Then the factors G_i and F_j are said to be exchangeable if $(F_j \times G_i')_H$ and $(G_i \times F_j')_H$ are H-decompositions of G. Two H-decompositions of G are said to be exchangeable if each factor of one decomposition is exchangeable with some factor of the other decomposition.

The following lemma is well known.

LEMMA 2.2. *Let $G = \prod_{i=1}^{n} G_i = \prod_{i=1}^{m} F_i$ and let θ_i and ϕ_i denote the $F_i =$ and G_i-decomposition operators respectively. G_i is exchangeable with F_j if and only if θ_j and ϕ_i induce isomorphisms between G_i and F_j.*

LEMMA 2.3. *If $G = G_1 \times G_2 \times A = F_1 \times F_2 \times B$ where G_1 and G_2 are exchangeable with F_1 and F_2 respectively, then $(G_1 \times G_2)$ is exchangeable with $(F_1 \times F_2)$.*

Proof. Since G_1 and F_1 are exchangeable we have

$$G = G_1 \times G_2 \times A = G_1 \times F_2 \times B .$$

Let θ map G onto $G\theta$ with ker $\theta = G_1$. Then

$$G\theta = G_2\theta \times A\theta = F_2\theta \times B\theta .$$

Now $G_1 \cap G_2 = G_1 \cap F_2 = 1$. Therefore, the $G_2\theta$- and $F_2\theta$-decomposition operators induce isomorphisms between $G_2\theta$ and $F_2\theta$. Hence

$$G\theta = G_2\theta \times B\theta = F_2\theta \times A\theta .$$

But this implies that $\ker \theta \cap (G_2 \times B) = 1$. It follows that

$$G = G_1 \times G_2 \times B .$$

In the same way we can show that $G = F_1 \times F_2 \times A$.

COROLLARY 2.4. *If* $G = \prod_{i=1}^{n} G_i = \prod_{i=1}^{m} F_i$ *such that* G_i *and* F_i *are exchangeable for* $1 \leqq i \leqq k$, *then*

$$\begin{aligned} G &= F_1 \times \cdots \times F_k \times G_{k+1} \times \cdots \times G_n \\ &= G_1 \times \cdots \times G_k \times F_{k+1} \times \cdots \times F_m . \end{aligned}$$

THEOREM 2.5. *If* $G = (\prod_{i=1}^{n} G_i)_H = (\prod_{i=1}^{m} F_i)_H$, *where* $H = Z(G)$, *are two exchangeable H-decompositions in which none of the factors is trivial, then the two H-decompositions are identical.*

Proof. Let G_1 and F_1, say, be two exchangeable factors. If $x \in G_1$ then $x = ab$ for some $a \in F_1$ and $b \in F_1'$. But the exchangeability of G_1 and F_1 implies that $b \in Z(F_1') \subset Z(G) = H$. Hence $G_1 \subset F_1$. In the same way $F_1 \subset G_1$, whence $F_1 = G_1$. Clearly each G_i coincides with one and only one F_j. Thus applying Lemma 2.4 to $\bar{G}$ we have $m = n$. This proves tne theorem.

Since any two Remak decompositions of a given group are exchangeable the following well-known result becomes an immediate consequence of this theorem.

COROLLARY 2.6. *If* $Z(G) = 1$ *then* G *admits a unique remark decomposition.*

3. In this section we shall be mainly concerned with nilpotent groups of class two since this is the simplest case after abelian groups. In particular we shall study the H-decompositions of G when $H = Z(G)$. H-products with $H = Z(G)$ are referred to as central products by P. Hall. Therefore, we shall call $G = (\prod_{i=1}^{n} G_i)_H$ a central decomposition of G whenever $H = Z(G)$. It is to be noted that in a central decomposition the center of each factor coincides with the center of the group. Thus in a central decomposition of G into centrally indecomposable factors each factor G_i is indeed indecomposable with respect to its center $Z(G_i)$. When G is nilpotent of class two with a cyclic commutator subgroup we are able to give a complete characterization of centrally indecomposable groups.

LEMMA 3.1. *Let* $G = (A \times B)_H = (C \times D)_H$. *If* x *is any element of* C *then there exist* $a \in A$ *and* $b \in B$ *with* a *and* b *respectively of the form* $a = cd$ *and* $b = c^*d^{-1}$ *where* $c, c^* \in C$ *and* $d \in D$ *such that*

$x = ab$.

Proof. Let $x \in C$. Then $x = ab$ for some $a \in A$ and $b \in B$. Now $a = cd$ and $b = c'd'$ for some $c, c' \in C$ and $d, d' \in D$. Thus $x = cc'dd'$, whence $dd' = h \in C \cap D = H$. Writing $c^* = c'h \in C$ we have $b = c^*d^{-1}$. This proves the lemma.

LEMMA 3.2. *Let $G = (A \times B)_H = (C \times D)_H$. If $a \in A$ and $a = cd$ with $c \in C$ and $d \in D$ then $[c, B] \subset H$ and also $[d, B] \subset H$.*

Proof. Consider $\bar{G} = \bar{A} \times \bar{B} = \bar{C} \times \bar{D}$. Then $\bar{a} = \bar{c}\bar{d}$ centralizes $\bar{B}$. Since $\bar{C} \cap \bar{D} = 1$ this implies that $\bar{c}$ and $\bar{d}$ centralize $\bar{B}$, whence $[c, b] = [b, d] \in H$ for all $b \in B$.

DEFINITION 3.3. Let $G = (\prod_{i=1}^{n} G_i)_H$ and θ be the homomorphism mapping G onto $\bar{G}$. Then the H-projection of $x \in G$ in G_i is defined to be the set of all preimages of $\bar{x}\theta_i$ under θ, where θ_i is the $\bar{G}_i$-decomposition operator of $\bar{G} = \prod_{i=1}^{n} \bar{G}_i$. We shall denote this set by $P_{G_i}(x)$.

It is easy to see that the H-projection of any subgroup of G in G_i is a subgroup of G_i containing H.

From now on, unless otherwise specified, we shall always take $H = Z(G)$.

LEMMA 3.4. *Let $G = (A \times B)_H = (C \times D)_H$. Let M be a subgroup of A containing H such that $M \subset P_A(C)$ and $P_C(M) = C$. Then $A = (M \times N)_H$ where $N = A \cap D$.*

Proof. Let x be any element of A. Then $x = cd$ for some $c \in C$ and $d \in D$. Since $P_C(M) = C$ this implies that there exists $u \in M$ such that $u = cd_1$, $d_1 \in D$. Therefore $x = ud_1^{-1}d$, whence $d_1^{-1}d = u^{-1}x \in A \cap D$. Hence $A = \{M, N\}$.

Now $M \subset P_A(C)$ implies that $M \subset CB$. But this implies that $[M, N] = 1$.

Finally $\{M, N\} = A$ together with $[M, N] = 1$ implies that

$$M \cap N \subset Z(A) \subset Z(G) = H .$$

Since $H \subset M \cap N$, it follows that $A = (M \times N)_H$.

COROLLARY 3.5. *Let $G = (A \times B)_H = (C \times D)_H$ where A is H-indecomposable. If M is a subgroup of A containing H such that $M \subset P_A(C)$ and $P_C(M) = C$ then $M = A$.*

As it was pointed out in §1 that the main difficulty in the study of such decompositions is due to the fact that, in general, $C(G_i)$ and $C(G_i')$ will not intersect trivially. If, however, $C(G_i) \cap C(G_i') = 1$ for all i then we have the following strong result.

THEOREM 3.6. *If $G = (\prod_{i=1}^{n} G_i)_H$ is a central decomposition of G into centrally indecomposable factors such that $C(G_i) \cap C(G_i') = 1$ for all i, then G admits a unique central decomposition into centrally indecomposable factors.*

Proof. Let $G = (\prod_{i=1}^{m} F_i)_H$ be a central decomposition of G into centrally indecomposable factors. Thus $\bar{G} = \prod_{i=1}^{n} \bar{G}_i = \prod_{i=1}^{m} \bar{F}_i$. Let θ_i and ϕ_i be the $\bar{G}_i$- and $\bar{F}_i$-decomposition operators of $\bar{G}$ respectively. Since $\bar{G}_1 = \prod_{i=1}^{m} \bar{G}_{1i}\phi_i\theta_1$ and $\overline{P_{F_i}(G_1)} = \bar{G}_1\phi_i$ it follows that

$$Q_i = P_{G_1}(P_{F_i}(G_1))$$

is the set of all preimages of $\bar{G}_1\phi_i\theta_1$ under θ, where $G\theta = \bar{G}$, and that $G_1 = \{Q_1, \cdots, Q_m\}$.

Now let $x \in P_{F_i}(G_1)$ and $y \in P_{F_j}(G_1)$, $i \neq j$. Then $x = su$ and $y = tv$ where $s, t \in G_1$ aud $u, v \in G_1'$. Since $[x, y] = 1$ and $C(G_1) \cap C(G_1') = 1$ we have $[s, t] = [u, v] = 1$. This implies that $[Q_i, Q_j] = 1$ for $i \neq j$. Moreover, it is clear that

$$Q_i \cap \{Q_1, \cdots, Q_{i-1}, Q_{i+1}, \cdots, Q_m\} \subset Z(G_1) \subset H .$$

Hence $G_1 = (\prod_{i=1}^{m} Q_i)_H$. But G_1 is centrally indecomposable. Therefore there exists $i = 1$, say, such that $G_1 = Q_1$ and $Q_i = H$ for $i \neq 1$. Applying Lemma 3.4 and putting $M = P_{F_1}(G_1)$, $A = F_1$ and $C = G_1$ we have $F_1 = (P_{F_1}(G_1) \times (F_1 \cap G_1'))_H$, whence $F_1 = P_{F_1}(G_1)$. But

$$G_1 = Q_1 = P_{G_1}(P_{F_1}(G_1))$$

implies that $G_1 = P_{G_1}(F_1)$. Thus $F_1 = P_{F_1}(P_{G_1}(F_1))$ and $P_{F_1}(P_{G_i}(F_1)) = H$ for all i $\neq 1$.

Let $x \in F_1$ and $y \in F_1'$. Then $x = g_1u$ and $y = g_1^*v$ where $g_1, g_1^* \in G_1$ and $u, v \in G_1'$. Since $P_{G_1}(F_1) = G_1$ and $C(G_1) \cap C(G_1') = 1$, it follows that $g_1^* \in Z(G) = H$. Therefore $F_1' \subset G_1'$. Also $P_{F_1}(P_{G_i}(F_1)) = H$ for all $i \neq 1$ implies that $P_{G_1}(F_1) \subset F_1'$ for all $i \neq 1$, whence $u \in Z(G)$. Therefore $F_1 \subset G_1$ and by Corollary 3.5 $F_1 = G_1$. This implies that

$$G = (G_1 \times G_1')_H = (G_1 \times F_1')_H .$$

Thus $F_1' \subset G_1'$ implies that $F_1' = G_1'$. Hence by induction $m = n$ and with proper reindexing $F_i = G_i$ for all i.

LEMMA 3.7. *The congruences $x + y \equiv 1 \bmod n$ and $xy \equiv 0 \bmod n$ have solutions in x, y other than 0 and 1 mod n if and only if $n \neq p^\alpha$*

or ∞ *where* p *is a prime.*

Proof. We shall first show that if $n = p^\alpha$ or ∞ then the only solutions are 0 and 1 mod n. Let $n = \infty$. Then $xy = 0$ implies $x = 0$, say, whence $y = 1$. On the other hand if $n = p^\alpha$ then $xy \equiv 0 \bmod n$ and $x + y \equiv 1 \bmod n$ imply that $p^\alpha \mid x(x-1)$. Thus $p^\alpha \mid x$ or $p^\alpha \mid (x-1) \equiv -y$. Hence the only solutions are 0 and 1 mod n.

Suppose now $n \neq p^\alpha$ or ∞. Then there exist integers $\beta, \gamma \neq 1$ such that $n = \beta\gamma$ and $(\beta, \gamma) = 1$. This implies that there exists integers s and t such that $s\beta + t\gamma = 1$. Let $x = s\beta$ and $y = t\gamma = (1 - x)$. Clearly $\beta \mid x$ and $\gamma \mid (x - 1)$. On the other hand $n \nmid x$ or $(x - 1)$. For, if not, say, $n \mid x = s\beta$. This implies that $\gamma \mid s$, whence $\gamma \mid s\beta + t\gamma = 1$. Thus $s\beta$ and $t\gamma$ are solutions to the given congruences with neither of them congruent to 0 mod n.

THEOREM 3.8. *Let* G/H *be an abelian group of rank two.* G *is centrally indecomposable if and only if* $C(G)$ *is a cyclic p-group or an infinite cyclic group.*

Proof. Since G/H is an abelian group of rank two it implies that there exist $a, b \in G$ such that $G = \{a, b, H\}$ where $a, b \notin H$ and $1 \neq [a, b] \in H$. Let $[a, b] = h$ and ord $h = n$ where $n = p^k$ or ∞. It is clear that $C(G) = \{h\}$ and the orders of a and b must be either divisible by n or infinite. Indeed if $n = p^k$ then a^{p^k} and b^{p^k} are elements of H. Let $G = (A \times B)_H$. Then $a = xy$ and $b = x'y'$ where $x, x' \in A$ and $y, y' \in B$. But $x = a^\alpha b^\beta u$, $y = a^\gamma b^\delta v$, $x' = a^{\alpha'} b^{\beta'} u'$ and $y' = a^{\gamma'} b^{\delta'} v'$ where $u, v, u', v' \in H$. Since $[x, y] = 1$ we have $\alpha\delta - \beta\gamma \equiv 0 \bmod n$. Moreover $a = xy = a^{\alpha+\gamma} b^{\beta+\delta} h^{-\beta\gamma} uv$ implies $a^{\alpha+\gamma-1} b^{\beta+\delta} h^{-\beta\delta} uv = 1$. This This means $a^{\alpha+\gamma-1} b^{\beta+\delta} \in H$. But

$$[a, a^{\alpha+\gamma-1} b^{\beta+\delta}] = 1$$

implies $\beta + \delta \equiv 0 \bmod n$ and $[b, a^{\alpha+\gamma-1} b^{\beta+\delta}] = 1$ implies $\alpha + \gamma - 1 \equiv 0 \bmod n$ or $\alpha + \gamma \equiv 1 \bmod n$ Hence $0 \equiv \alpha\delta - \beta\gamma \equiv \delta(\alpha + \gamma) \equiv \delta \bmod n$. Applying the same argument to x' and y' we have $\beta' = \delta' = 1 \bmod n$ and $\alpha' \equiv -\gamma' \equiv 0 \bmod n$. But $\beta \equiv \delta \equiv \alpha' \equiv \gamma' \equiv 0 \bmod n$ implies b^β, b^δ, $a^{\alpha'}$ and $a^{\gamma'}$ are elements of H. Thus for $[x, y'] = [x', y] = 1$ we must have $\alpha\delta' \equiv 0$ and $\beta'\gamma \equiv 0 \bmod n$. It follows that $(\alpha\beta')(\gamma\delta') \equiv 0 \bmod n$. But $(\alpha + \gamma)(\beta' + \delta') \equiv 1 \bmod n$ implies $\alpha\beta' + \gamma\delta' \equiv 1 \bmod n$. Hence, by lemma 3.7, the congruences cannot have solutions other than 0 and 1 mod n. Suppose $\alpha\beta' \equiv 0$ and $\gamma\delta' \equiv 1 \bmod n$. Since $\gamma \equiv 1 - \alpha$ and $\delta' \equiv 1 - \beta' \bmod n$ we have $(1 - \alpha)(1 - \beta') \equiv 1 \bmod n$ which implies $\beta' \equiv -\alpha \bmod n$. Recalling the facts that $[x, y'] = [x', y] = 1$ and a^{p^k}, $b^{p^k} \in H$ we must have $\alpha(1 + \alpha) \equiv 0$ and $-\alpha(1 - \alpha) \equiv 0 \bmod n$. This means $2\alpha \equiv 0 \bmod n$. If $p \neq 2$ then $\alpha \equiv 0$, which will imply $a, b \in B$. If $p = 2$ then $2\alpha \equiv 0 \bmod 2^k$. Thus $\alpha \equiv 0$ or $t2^{k-1}$ for some odd t. Clearly both $(1 - t2^{k-1})$ and $(1 + t2^{k-1})$ are relatively prime to 2^k for $k \neq 1$. Since $y = a^{1-\alpha}z$ and $y' = b^{1+\alpha}z^*$ for some $z, z^* \in H$ we have $a, b \in B$. Thus $B = G$. If $k = 1$ and $\alpha \equiv 1$ then $G = A$. Similarly, if $\alpha\beta' = 1$ and $\gamma\delta' \equiv 0 \bmod n$ we have $G = A$ or B. Hence G is centrally indecomposable.

To prove the converse we shall show that if the order of $C(G)$ is not a prime power or infinity then G is centrally decomposable. Again let $G = \{a, b, H\}$ and $[a, b] = h$ with ord $h = n \neq p^k$ or ∞. By Lemma 3.7 there exist solutions other than 0 and 1 mod n to the congruences $x + y = 1$ and $xy \equiv 0 \bmod n$. Let α, β be such a pair solutions. Let $A = \{a^\alpha, b^\alpha, H\}$ and $B = \{a^\beta, b^\beta, H\}$. A simple check will show $G = (A \times B)_H$.

THEOREM 3.9. *Let G be a nilpotent group of class two with a cyclic commutator subgroup. If $G = (\prod_{i=1}^n G_i)_H$ is a central decomposition of G into centrally indecomposable factors then $\bar{G}_i = G_i/H$ is an abelian group of rank two.*

Proof. Clearly $\bar{G}_i$ cannot be of rank one since this will imply $G_i \subset Z(G) = H$. Hence G_i will not be a proper central factor. We shall therefore assume that $\bar{G}_i$ is of rank $r > 2$. Thus

$$G_i = \{\alpha_1, \cdots, \alpha_r, H\} .$$

Since $C(G)$ is cyclic we shall let $C(G) = \{h\}$ where $h \in H$. This implies $C(G_i) = \{h^\nu\}$. Therefore there exist $a, b \in G_i$ such that $[a, b] = h^\nu = c$. Let $A = \{a, b, H\}$. Clearly $A \neq G_i$ since A/H is of rank two. Let $\beta_1, \cdots, \beta_k \in G_i$ such that $G_i = \{a, b, \beta_1, \cdots, \beta_k, H\}$ and that k is minimal. Let $[a, \beta_i] = c^{\lambda_i}$ and $[b, \beta_i] = c^{\mu_i}$. Define $B = \{\beta_i a^{\mu_i} b^{-\lambda_i}, H; i = 1, \cdots, k\}$. Clearly $G_i = \{A, B\}$. Also $[a, \beta_i a_i^{\mu_i} b^{-\lambda_i}] = c^{\lambda_i} \cdot c^{-\lambda_i} = 1$ and $[b, \beta_i a_i^{\mu_i} b^{-\lambda_i}] = c^{\mu_i} \cdot c^{-\mu_i} = 1$. Therefore $[A, B] = 1$. Furthermore if $x \in A \cap B$ then

$$x \in Z(G_i) \subset H .$$

In fact this also says that A cannot be contained in B. Hence $G_i = (A \times B)_H$ contradicting the hypothesis that G_i is centrally indecomposable.

Applying Theorems 3.8 and 3.9 the following characterization of centrally indecomposable nilpotent groups of class two with cyclic commutator subgroups is immediate.

THEOREM 3.10. *Let G be a nilpotent group of class two with a cyclic commutator subgroup. G is centrally indecomposable if and* *only if G/H is of rank two and $C(G)$ is either a p-group or an infinite group.*

COROLLARY 3.11. *Let G be a nilpotent group of class two with a cyclic center. G is centrally indecomposable if and only if G/H is of rank two and $C(G)$ is either a p-group or an infinite group.*

It is of interest to note at this point that applying a theorem of Weichsel [5] we have a characterization of critical p-groups when their centers coincide with their commutator subgroups.

THEOREM 3.12. *Let G be a p-group with $Z(G) = C(G)$. G is critical if and only if $Z(G)$ is cyclic and G is centrally indecomposable.*

Proof. Let G be a critical group. Since G is a p-group this means $Z(G) \neq 1$. Therefore $C(G) = Z(G) \neq 1$. Hence G is nilpotent of class two. By Theorem 3.1 of [5], (noting that a critical group is equivalent to its not being an in-direct product), $Z(G)$ is cyclic and G may be generated by two elements. Let $G = \{a, b\}$. Since G is not abelian we must have $a, b \notin Z(G)$. Therefore $G/Z(G)$ is of rank two. But G is a p-group. It follows that $C(G)$ is a p-group. Hence, by Corollary 3.11 G is centrally indecomposable.

Conversely, let $Z(G)$ be cyclic and G be centrally indecomposable. By Corollary 3.11, we have $G/Z(G)$ is of rank two. Thus

$$G = \{a, b, Z(G)\} .$$

But $Z(G) = C(G)$. Therefore $G = \{a, b\}$. Hence, by Theorem 3.1 of [5], G must be critical.

LEMMA 3.13. *Let G be a nilpotent group of class two with a cyclic commutator subgroup. Let $G = (\prod_{i=1}^{n} G_i)_H = (\prod_{i=1}^{m} F_i)_H$ be two central decompositions of G into centrally indecomposable factors. If $F_i = \{s_i, t_i, H\}$ such that $\bar{F}_i = \{\bar{s}_i\} \times \{\bar{t}_i\}$ then for a given G_j there exist subgroups $A_j \subset G_j$ and $B_j \subset G'_j$ such that $A_j = \{s_i^{\alpha} u_i^{-1}, t_i^{\alpha} v_i^{-1}, H\}$ and $B_j = \{s^{1-\alpha} u_i, t_i^{1-\alpha} v_i, H\}$ where $u_i, v_i \in F'_i$.*

Proof. Consider $\bar{G} = \prod_{i=1}^{n} \bar{G}_i = \prod_{i=1}^{m} \bar{F}_i$. By Lemma 3.1, there exist $\bar{a} \in \bar{G}_j$ and $\bar{b} \in \bar{G}'_j$ with $\bar{a} = \bar{c}\bar{u}_i^{-1}$ and $\bar{b} = \bar{c}^* \bar{u}_i$ where $\bar{c}, \bar{c}^* \in \bar{F}_i$ and $\bar{u}_i \in \bar{F}'_i$ such that $\bar{s}_i = \bar{a}\bar{b}$. Let $\bar{c} = \bar{s}_i^{\alpha} \bar{t}_i^{\beta}$ and $\bar{c}^* = \bar{s}_i^{\varepsilon} \bar{t}_i^{\eta}$. This means $\bar{s}_i = \bar{s}_i^{\alpha+\varepsilon} \bar{t}_i^{\beta+\eta}$. Since $\bar{F}_i = \{\bar{s}_i\} \times \{\bar{t}_i\}$, it follows that $\bar{t}_i^{\eta} = \bar{t}_i^{-\beta}$ and $\bar{s}_i^{\varepsilon} = \bar{s}_i^{1-\alpha}$. Therefore G_j contains an element of the form $a = s_i^{\alpha} t_i^{\beta} u_i^{-1}$ and G'_j contains an element of the form $b = s_i^{1-\alpha} t_i^{-\beta} u_i$ such that for a suitable $k \in H$ we have $s_i = abk$. In the same way there exist $a^* = s_i^{\gamma} t_i^{\delta} v_i^{-1} \in G_j$ and $b^* = s_i^{-\gamma} t_i^{1-\delta} v_i \in G'_j$ such that $t_i = a^* b^* k^*$ for some suitable $k^* \in H$. Since $[G_j, G'_j] = [F_i, F'_i] = 1$, therefore, $[a, b] = 1$ implies that,

$$1 = [u_i, u_i] = [s_i^{\alpha} t_i^{\beta}, s_i^{1-\alpha} t_i^{-\beta}] = h^{-\alpha\beta+(\alpha-1)} = h^{-\beta}$$

where $h = [s_i, t_i]$. Thus $\beta \equiv 0 \mod q$ where $q = \text{ord } h$. In the same way $[a^*, b^*] = 1$ implies $\gamma \equiv 0 \mod q$. On the other hand $[a, b^*] = 1$ and $[a^*, b] = 1$ respectively imply:

$$[u_i, v_i] = [s_i^{\alpha} t_i^{\beta}, s_i^{-\gamma} t_i^{1-\delta}] = h^{\alpha(1-\delta)+\beta\gamma} = h^{\alpha(1-\delta)}$$

and $[u_i, v_i]^{-1} = [v_i, u_i] = [s_i^{\gamma} t_i^{\delta}, s_i^{1-\alpha} t_i^{-\beta}] = h^{-\beta\gamma+(\alpha-1)\delta} = h^{(\alpha-1)\delta}$. Therefore $\alpha(1-\delta) \equiv (1-\alpha)\delta \mod q$, or $\alpha \equiv \delta \mod q$. Since for any λ with $q \mid \lambda$ we have $s_i^{\lambda}, t_1^{\lambda} \in H$. It follows that $s_i^{\alpha} u_i^{-1}$ and $t_i^{\alpha} v_i^{-1}$ are elements of G_j and $s_i^{1-\alpha} u_i$ and $t_i^{1-\alpha} v_i$ are elements of G'_j. Hence

$$A_j = \{s_i^{\alpha} u_i^{-1}, t_i^{\alpha} v_i, H\} \subset G_j$$

and $B_j = \{s_i^{1-\alpha} u_i, t_i^{1-\alpha} v_i, H\} \subset G'_j$.

THEOREM 3.14. *If G is a nilpotent group of class two with a finite cyclic commutator subgroup, then any two central decompositions of G into centrally indecomposable factors are isomorphic* mod H.

Proof. Let $G = (\prod_{i=1}^{n} G_i)_H = (\prod_{i=1}^{m} F_i)_H$ be two central decompositions of G into centrally indecomposable factors. Since $C(G)$ is cyclic, by Theorem 3.9, $\bar{G}_i$ and $\bar{F}_i$ are abelian of rank two for all i. In particular we shall let $F_i = \{s_i, t_i, H\}$ such that $\bar{F}_i = \{s_s\} \times \{t_i\}$. Thus, by Lemma 3.13, and using the same notations, there exist $A_j \subset G_j$ and $B_j \subset G'_j$. Since $C(G)$ is finite and cyclic, by Theorem 3.8, $C(F_i)$ must be a cyclic p-group. Let $p^{\lambda} = \text{ord } C(F_i)$. Then either α or $(1-\alpha)$ must be relatively prime to p. Therefore either $\{s_i^{\alpha}, t_i^{\alpha}, H)$ or $\{s_i^{1-\alpha}, t_1^{1-\alpha}, H\}$ must give the group F_i.

CASE 1. $F_i = \{s_i^{\alpha}, t_i^{\alpha}, H\}$ for all j. (Note: α, u_i, v_i are dependent on G_j.) In particular we shall let $i = j$. Since G_i is centrally indecomposable, therefore, by Lemma 3.4, $G_i = A_i$. A simple check will show that F_i and $\bar{G}_i$ are exchangeable in the decompositions

$$\bar{G} = \prod_{\nu=1}^{n} \bar{G}_{\nu} = \prod_{\nu=1}^{m} \bar{F}_{\nu} .$$

Thus by Lemma 2.2, $\bar{F}_i \simeq \bar{G}_i$. Moreover, applying Lemma 2.3, we must have $m = n$. Hence the two central decompositions are isomorphic mod H.

CASE 2. There exists j such that $F_i = \{s_i^{1-\alpha}, t_i^{1-\alpha}, H\}$. We shall prove this case by induction on n. Clearly the theorem is true for $n = 1$. Consider $G = (G_j \times G'_j)_H = (F_i \times F'_i)_H$. Since $C(F_i)$ is a cyclic p-group therefore ord $[s_i, t_i]$ must be a power of p. Moreover

$$[u_i, v_i] \in \{[s_i, t_i]\} .$$

Therefore $C(B_j)$ must be a cyclic p-group. Hence by Theorem 3.8 B_j is centrally indecomposable. Moreover, by Lemma 3.4,

$$G'_j = (B_j \times N)_H$$

where $N = G'_j \cap F'_i$. Therefore, by induction, $\bar{B} \simeq \bar{G}_k$ for some $k \neq j$ and any central decompositions of N into centrally indecomposable factors are isomorphic mod H to $(\prod_{\nu \neq k j}^{n} G_\nu)_H$. A simple check will show that in the decompositions $\bar{G} = \bar{G}_j \times \bar{B}_j \times \bar{N} = \bar{F}_i \times \bar{F}'_i$, $\bar{B}_j$ and $\bar{F}_i$ are exchangeable. Thus $\bar{B}_j \simeq \bar{F}_i$. Furthermore by the construction of A_j and B_j we have $F_i \subset \{A_j, B_j\}$. Therefore $F_i \subset (G_j \times B_j)_H$. Let $U = F'_i \cap (G_j \times B_j)_H$. We shall show that $P = (G_j \times B_j)_H = (F_i \times U)_H$. It is clear that $[F_i, U] = 1$ and $F_i \cap U = H$. Let

$$x \in (G_j \times B_j)_H .$$

Then $x = gb$ for sme $g \in G_j$ and $b \in B_j$. But $g = fu$ and $b = f^*u^*$ for some $f, f^* \in F_i$ and $u, u^* \in F'_i$. Since $F_i \subset P$ we must have $u, u^* \in P$. Hence $x = (ff^*)(uu^*)$ where $ff^* \in F_i$ and $uu^* \in (F'_i \cap P) = U$. Thus we have,

$$G = (G_j \times B_j \times N)_H = (F_i \times U \times N)_H = (F_i \times F'_i)_H .$$

Since $(U \times N)_H \subset F'_i$ we must have $(U \times N)_H = F'_i$. We must now show that U is centrally indecomposable. Since G_j is centrally indecomposable there exist $g, g^* \in G_j$ such that $G_j = \{g, g^*, H\}$ and $\bar{G}_j = \{\bar{g}\} \times \{\bar{g}^*\}$. Let $g = fu$ and $g^* = f^*u^*$, where $f, f^* \in F_i$ and $u, u^* \in F'_i$. Thus if $x \in G_j$ and $x = yv$ where $y \in F_i$ and $v \in F'_i$ we have,

$$x = yv = w(g, g^*)h = w(f, f^*) \cdot w(u, u^*) \cdot h$$

where $h \in H$ and $w(g, g^*)$ is a word on g, g^* (we shall regard w as a function). Since y and $w(f, f^*)$ are elements of F_i, therefore, $v \in \{u, u^*, H\}$. In particular we note that u_i and v_i are elements of $\{u, u^*, H\}$. Since $F_i \subset P$ it is not difficult to see that $\{u, u^*, H\} \subset P$ and indeed $U = \{u, u^*, H\}$. Furthermore $C(G_j)$ is a cyclic p-group. Therefore $C(U)$ must be a cyclic p-group. Hence U is centrally indecomposable. Recalling that any central decomposition of N into centrally indecomposable factors is isomorphic mod H to $(\prod_{\nu \neq j,k}^{n} G_\nu)_H$ it follows that in the central decomposition of $F'_i = (U \times N)_H$ into indecomposable factors there will be exactly $(n - 1)$ indecomposable factors. Hence by induction $F_i' = (\prod_{\nu \neq i}^{m} F_\nu)_H$ is isomorphic mod H to $F_i' = (U \times \prod_{\nu=1}^{n-2} N_\nu)_H$, where $N = (\prod_{\nu=1}^{n-2} N_\nu)_H$ and N_ν centrally indecomposable and $m - 1 = n - 1$.

We now note that in the decompositions of $\bar{P} = (\bar{G}_j \times \bar{B}_j) = (\bar{F}_i \times \bar{U})$, $\bar{B}_j$ and $\bar{F}_i$ are exchangeable. This implies $\bar{G}_j$ and $\bar{U}$ are exchangeable in these two decompositions. Thus $\bar{G}_j$ and $\bar{U}$ are isomorphic. Hence with suitable re-indexing we can have $\bar{G}_\lambda \simeq \bar{F}_\lambda$ where G_λ and F_λ are re-indexed factors of G_k' and F_i' respectively. Recalling that $\bar{G}_k \simeq \bar{B}_j$ and $\bar{B}_j \simeq \bar{F}_i$ the theorem follows immediately.

The author wishes to thank the referee for his suggestions.

REFERENCES

1. B. H. Neumann and H. Neumann, *A remark on generalised free products*, J. London Math. Soc. **25** (1950), 202-204.

2. H. Neumann, *Generalised free sums of cyclical groups*, Amer. J. Math. **72** (1950), 671-685.

3. ———, *On an amalgam of abelian groups*, J. London Math. Soc. **26** (1951), 228-232.

4. C. Y. Tang, *An existence theorem for generalized direct products with amalgamated subgroups*, Canad. J. Math. **18** (1966), 75-82.

5. P. M. Weichsel, *A decomposition theory for finite groups with applications to p-groups*, Trans. Amer. Math. Soc. **102** (1962) 218-226.

6. H. Zassenhaus, *The theory of groups*, Chelsea, New York, 1958.

Received July 30, 1966.

UNIVERSITY OF WATERLOO
ONTARIO, CANADA

PACIFIC JOURNAL OF MATHEMATICS

Printed in Japan by International Academic Printing Co., Ltd., Tokyo, Japan

Pacific Journal of Mathematics

Vol. 23, No. 1 March, 1967