ON A SPECIAL CLASS OF p-GROUPS

BY

N. BLACKBURN

Manchester, England

In the study of p-groups the chief difficulty lies in the fact that the number of such groups is very large. It is therefore of interest to study certain classes of p-groups, and the present paper is devoted to such a topic.

Let G be a group and let x, y be elements of G. We define the commutator $[x, y]$ and the transform x^y by the formulae:

$$[x, y] = x^{-1}y^{-1}xy, \qquad x^y = x[x, y] = y^{-1}xy.$$

For subsets U, V of G, $[U, V]$ denotes the group generated by all commutators $[u, v]$, where $u \in U$, $v \in V$. We define the *lower central series*

$$G \geqslant \gamma_2(G) \geqslant \gamma_3(G) \geqslant \ldots \geqslant \gamma_{i-1}(G) \geqslant \gamma_i(G) \geqslant \ldots$$

of G inductively as follows:

$$\gamma_2(G) = [G, G], \qquad \gamma_i(G) = [\gamma_{i-1}(G), G] \quad (i = 3, 4, \ldots).$$

If there exists an integer k such that $\gamma_k(G) = 1$, then G is said to be *nilpotent*, and if k is the smallest such integer, $k - 1$ is called the *class* of G.

p is to denote a prime number and a p-group is a group of order a power of p. It is well known that all p-groups are nilpotent, and we may therefore speak of the class of a p-group. If m, n are integers and $3 \leqslant m \leqslant n$, it is convenient to denote by CF (m,n,p) the set of all groups G of order p^n and class $m - 1$ in which

$$(\gamma_{i-1}(G) : \gamma_i(G)) = p \quad (i = 3, 4, \ldots m).$$

Similarly ECF (m, n, p) denotes the set of those groups G of CF (m, n, p) in which $G/\gamma_2(G)$ is elementary Abelian. These two classes of groups are to be investigated. Many of our earlier results can also be stated for another class of groups which we denote by NCF (m), and which consists of all nilpotent groups G of class $m - 1$ in which each of the groups $\gamma_{i-1}(G)/\gamma_i(G)$ $(i = 3, 4, \ldots, m)$ is an infinite cyclic group. The general considerations on which our investigation of these groups is founded are based on a paper of P. Hall [3] together with a few remarks which are developed in § 1.

Perhaps the most interesting groups considered are the p-groups of maximal class, that is, the p-groups of the greatest class which is compatible with their order. In § 2 we begin by discussing the most elementary properties of these groups and their generalizations to the classes of groups considered. Two characteristic subgroups are then introduced and these play a fundamental part in the discussion which follows. Our aim is to find what we call the degree of commutativity of our groups and, in particular, to find whether or not this is greater than 0. The main result is Theorem 2.11 which asserts that a considerable proportion of the groups in question have degree of commutativity greater than 0. We conclude § 2 by a result (Theorem 2.16) on the maximal number of generators of the derived group of a group of CF(m,n,p).

In § 3 we consider the groups of ECF(m,n,p) and show that their study reduces essentially to that of p-groups of maximal class. The problem of finding the degree of commutativity is continued and results in this direction are Theorems 3.8, 3.10, 3.12, 3.13 and 3.14. The power-structure of these groups is also investigated. In § 4 all groups of order p^6 and class 5 and all 3-groups of maximal class are found.

Apart from their intrinsic interest p-groups of maximal class are also of interest on account of certain applications. Thus it is sometimes the case that in characterizing all p-groups with a given simple property, we find that these groups generally have a simple structure but that exceptionally certain p-groups of maximal class also have the given property. The best-known instance of this is the problem of finding all p-groups with just 1 subgroup of order p: such a group is either cyclic or is a generalized quaternion group (which is a 2-group of maximal class). The consideration of such problems tends to take us outside the scope of the present work and is accordingly not discussed here. The author hopes, however, to return to this question in a later paper.

A paper on p-groups of maximal class has already appeared, namely by A. Wiman [12]. The discussion given in the present work is to some extent based on Wiman's ideas, and we wish to express our indebtedness to this author. Unfortunately the conclusions that we have reached do not coincide with those of Wiman, and so we have made the present work independent of [12]. A detailed comparison will not be made, but it may be said that it is in II and III of [12] that statements are made which seem to us to be in general untrue.

The author also wishes to express his deep gratitude to Prof. P. Hall, of King's College, Cambridge, whose suggestions and encouragement were of the greatest value to him when he was working on the material of this work.

1. We begin by stating some of the known results which are of fundamental importance for our purpose. Amongst these the following theorem plays an important part in the construction of nilpotent groups.

THEOREM 1.1. *Let G be a group generated by a set X of elements. If Y is a set of elements which together with $\gamma_{i+1}(G)$ generate $\gamma_i(G)$, then $\gamma_{i+1}(G)$ is generated by $\gamma_{i+2}(G)$ together with all commutators $[x,y]$, where x,y run through X, Y respectively. This is true for $i=1$, $2,\dots,$ provided that $\gamma_1(G)$ is interpreted to mean G.*

For the proof we refer the reader to P. Hall [3], Theorem 2.81.

The following result is due to L. Kaloujnine [7] and [8].

THEOREM 1.2. *Let G be a group, and let*

$$H = H_0 \geqslant H_1 \geqslant H_2 \geqslant \dots \geqslant H_i \geqslant \dots$$

be a series of normal subgroups of G. If L is any subgroup of G such that $[L, H_{i-1}] \leqslant H_i$ $(i=1,2,\dots)$, then

$$[\gamma_j(L), H_i] \leqslant H_{i+j} \quad (i=0,1,\dots;\ j=2,3,\dots).$$

We shall need an application of this involving another characteristic subgroup. For any group G, we define $\eta_i(G)$ to be that subgroup of G for which $\eta_i(G)/\gamma_i(G)$ is the centre of $G/\gamma_i(G)$ $(i=2,3,\dots)$. Thus $\eta_2(G)=G$, and for $i>2$ $\eta_i(G) \geqslant \gamma_{i-1}(G)$.

If in Theorem 1.2 we put $L=G$, $H=\eta_i(G)$, and define the subgroups H_k inductively by the rules $H_0=H$, and $H_{k+1}=[H_k, G]$ for $k \geqslant 0$, we find that $[\gamma_j(G), H_k] \leqslant H_{j+k}$. But by the definition of η_i, $H_1 \leqslant \gamma_i(G)$; hence, $H_j \leqslant \gamma_{i+j-1}(G)$, for $j \geqslant 1$. Thus,

$$[\gamma_j(G), \eta_i(G)] = [\gamma_j(G), H_0] \leqslant H_j \leqslant \gamma_{i+j-1}(G).$$

COROLLARY 1. *In any group G, $[\gamma_j(G), \eta_i(G)] \leqslant \gamma_{i+j-1}(G)$ $(i,j=2,3,\dots)$.*

Using $\gamma_i(G) \leqslant \eta_{i+1}(G)$ we obtain the well known result:

COROLLARY 2. *In any group G, $[\gamma_i(G), \gamma_j(G)] \leqslant \gamma_{i+j}(G)$ $(i,j=2,3,\dots)$.*

We shall also need the *upper central series*,

$$1=\zeta_0(G) \leqslant \zeta_1(G) \leqslant \dots \leqslant \zeta_{i-1}(G) \leqslant \zeta_i(G) \leqslant \dots,$$

of a group G, which is defined inductively by the rules: $\zeta_0(G)=1$, $\zeta_i(G)/\zeta_{i-1}(G)$ is the centre of $G/\zeta_{i-1}(G)$ $(i=1,2,\dots)$. Then G is nilpotent of class $m-1$ if and only if $\zeta_{m-1}(G) = G$, $\zeta_{m-2}(G) \neq G$, and in such a group $\gamma_i(G) \leqslant \zeta_{m-i}(G)$, but $\gamma_i(G) \nleqslant \zeta_{m-i-1}(G)$. It follows that for $i=1,2,\dots,m-1$,

$$[G, \eta_{i+1}(G)] \leqslant \gamma_{i+1}(G) \leqslant \zeta_{m-i-1}(G),$$

and so $\eta_{i+1}(G) \leqslant \zeta_{m-i}(G)$.

In Theorem 1.2 we may put $L = G$, $H_l = \zeta_{k-l}(G)$ $(l = 0,1, \ldots, k)$ and $H_l = 1$ $(l > k)$. We find that for $0 \leqslant j + l \leqslant k$,

$$[\gamma_j(G), \zeta_{k-l}(G)] \leqslant \zeta_{k-j-l}(G),$$

or, putting $i = k - l$:

COROLLARY 3. *In any group G, $[\gamma_j(G), \zeta_i(G)] \leqslant \zeta_{i-j}(G)$ $(2 \leqslant j \leqslant i)$.*

Further, for any group G we denote by

$$G \geqslant G' \geqslant G'' \geqslant \ldots \geqslant G^{(i-1)} \geqslant G^{(i)} \geqslant \ldots$$

the *derived series* of G, which is defined inductively by

$$G' = [G, G] = \gamma_2(G), \quad G^{(i)} = [G^{(i-1)}, G^{(i-1)}] \quad (i = 2, 3, \ldots);$$

also we denote by $\Phi(G)$ the Frattini subgroup of G.

If $x_1, x_2, \ldots, x_n$ are elements of G we define the *simple commutator* $[x_1, x_2, \ldots, x_n]$ by induction on n; for $n = 2$ it is already defined, and for $n > 2$ we put

$$[x_1, x_2, \ldots, x_n] = [[x_1, x_2, \ldots, x_{n-1}], x_n].$$

In the sequel we shall only be concerned with one of the subgroups $\eta_i(G)$, namely $\eta_3(G)$, and we shall therefore put $\eta(G) = \eta_3(G)$. This subgroup possesses the following property.

THEOREM 1.3. *Suppose that G is a nilpotent group and that H is a subgroup of G with the property that $H\eta(G) = G$. Then H is normal in G and $\gamma_i(H) = \gamma_i(G)$, for $i = 2, 3, \ldots$.*

It is obvious that $\gamma_i(H) \leqslant \gamma_i(G)$. Let $m - 1$ be the class of G: we prove that $\gamma_i(H) = \gamma_i(G)$ by induction on $m - i$. For $i = m$ it is trivial, since $\gamma_i(H)$, $\gamma_i(G)$ are then both equal to the unit subgroup. For $i < m$ it follows from the inductive hypothesis that $\gamma_{i+1}(H) = \gamma_{i+1}(G)$. Now by hypothesis, G is generated by the elements of $\eta(G)$ and H; hence by Theorem 1.1, $\gamma_i(G)$ is generated by $\gamma_{i+1}(G)$ and all commutators

$$y = [y_1, y_2, \ldots, y_i],$$

where each component y_j of y is either an element of $\eta(G)$ or of H. But by Theorem 1.2 Corollary 1, $[\eta(G), \gamma_j(G)] \leqslant \gamma_{j+2}(G)$ $(j = 2, 3, \ldots, m - 2)$, and so any commutator y, one of whose components is an element of $\eta(G)$, is an element of $\gamma_{i+1}(G)$. Hence $\gamma_i(G)$ is generated by $\gamma_{i+1}(G) = \gamma_{i+1}(H)$ and all commutators of the form of y, where $y_j \in H$. Since each of these commutators belongs to $\gamma_i(H)$, it follows that $\gamma_i(G) \leqslant \gamma_i(H)$, and therefore $\gamma_i(G) = \gamma_i(H)$, as required. In particular $H \geqslant \gamma_2(H) = \gamma_2(G)$, and so H is a normal subgroup of G.

In the manipulation of commutators the following formulae are largely used:

$$[xy, z] = [x, z]^y [y, z], \qquad [x, yz] = [x, z]\,[x, y]^z, \tag{1}$$

where x, y, z are any elements of any group. We also note that

$$[x^{-1}, y] = [y, x]^{x^{-1}}, \qquad [x, y^{-1}] = [y, x]^{y^{-1}}. \tag{2}$$

By (1), it follows that if one of the components x or y is multiplied by an element of the centre of the group in which they lie, then the value of $[x, y]$ remains unaltered.

We shall also require results on the powers of a product of elements, of which the simplest is the following.

THEOREM 1.4. *If G is a group, $x \in G$ and $y \in \gamma_r(G)$, then for any integer n,*

$$[x^n, y] \equiv [x, y^n] \equiv [x, y]^n \pmod{\gamma_{r+2}(G)},$$

$$(xy)^n \equiv x^n y^n [x, y]^{-\binom{n}{2}} \pmod{\gamma_{r+2}(G)}.$$

This is true for $r = 1, 2, \ldots$, if $\gamma_1(G)$ is interpreted to mean G.

This is proved by a simple induction on n, using (1) and (2).

We shall require the following consequences of Theorem 1.4.

THEOREM 1.5. *Let G be a p-group.*

(i) *If $n_1, n_2, \ldots, n_r$ are the invariants of the Abelian p-group $G/\gamma_2(G)$, and $n_1 \geqslant n_2 \geqslant \cdots \geqslant n_r$, then the exponent of $\gamma_2(G)/\gamma_3(G)$ is at most p^{n_2}.*

(ii) *If for some $i \geqslant 2$ $\gamma_i(G)/\gamma_{i+1}(G)$ is of exponent p^m, then the exponent of $\gamma_{i+1}(G)/\gamma_{i+2}(G)$ is at most p^m.*

(iii) *If $G/\gamma_2(G)$ is an Abelian group with two invariants λ, μ, where $\lambda \geqslant \mu$, then $\gamma_2(G)/\gamma_3(G)$ is a cyclic group of order at most p^μ.*

To prove (i), suppose that $G/\gamma_2(G)$ is the direct product of the cyclic groups generated by the elements $x_i\gamma_2(G)$ $(i = 1, 2, \ldots, r)$, where p^{n_i} is the order of x_i modulo $\gamma_2(G)$. Then G is generated by $x_1, x_2, \ldots, x_r$ together with the elements of $\gamma_2(G)$, and it is easily deduced from Theorem 1.1 that $\gamma_2(G)$ is generated by $\gamma_3(G)$ and all the commutators $[x_i, x_j]$ $(1 \leqslant i < j \leqslant r)$. In such a commutator $j \geqslant 2$ and so $n_j \leqslant n_2$; hence $x_j^{p^{n_2}} \in \gamma_2(G)$, and by Theorem 1.4

$$[x_i, x_j]^{p^{n_2}} \equiv [x_i, x_j^{p^{n_2}}] \equiv 1 \pmod{\gamma_3(G)}.$$

$\gamma_2(G)/\gamma_3(G)$ is therefore of exponent at most p^{n_2}.

The proof of (ii) is very similar: if G is generated by $y_1, y_2, \ldots, y_s$ and $\gamma_i(G)$ is generated by $z_1, z_2, \ldots, z_t$ and $\gamma_{i+1}(G)$, so that by hypothesis $z_i^{p^m} \in \gamma_{i+1}(G)$, then by Theorem 1.1 $\gamma_{i+1}(G)$ is generated by all commutators $[y_i, z_j]$ and $\gamma_{i+2}(G)$, whilst by Theorem 1.4,

$$[y_i, z_j]^{p^m} \equiv [y_i, z_j^{p^m}] \equiv 1 \pmod{\gamma_{i+2}(G)}.$$

To prove (iii), we observe as in (i) that if x, y and $\gamma_2(G)$ generate G, then $[x, y]$ and $\gamma_3(G)$ generate $\gamma_2(G)$, so that $\gamma_2(G)/\gamma_3(G)$ is cyclic. The bound on the order of this group follows from (i).

We conclude the present paragraph by a remark on a formula of P. Hall for a power of a product (see [3], § 3). If x, y are elements of a group, we define elements $\sigma_i(x, y)$ of this group inductively by the rules.

$$\sigma_1(x, y) = y, \quad \sigma_i(x, y) = [\sigma_{i-1}(x, y), x] \quad (i = 2, 3, \dots).$$

Also, if G is a p-group, we denote by $P_i(G)$ $(i = 0, 1, \dots)$ the subgroup of G generated by all p^i-th powers of elements of G. In this notation we have the following result.

THEOREM 1.6. *Let G be a p-group, and let x, y be elements of G. Denote by Y the group generated by y and $\gamma_2(G)$. Then*

$$(xy)^p \equiv x^p \sigma_1^p \sigma_2^{\binom{p}{2}} \dots \sigma_i^{\binom{p}{i}} \dots \sigma_p \pmod{P_1(Y')[Y, \gamma_{p-1}(G)] \prod_{i=2}^{p-2} [\gamma_i(G), \gamma_{p-i}(G)]},$$

where $\sigma_i = \sigma_i(x, y)$. (For $p = 2$ we interpret $\gamma_{p-1}(G)$ to mean $\gamma_2(G)$).

For $p = 2$ this is trivial, since

$$(xy)^2 = x^2\sigma_1{}^2\sigma_2[\sigma_2, \sigma_1],$$

and so we need only consider the case when p is odd. The proof in this case is a slight modification of the proof given by Hall for his formula. According to this proof, it is necessary first of all to arrange the various distinct commutators of x and y in an order. Let $c_{w1}, c_{w2}, \dots, c_{wa_w}$ be the commutators of x and y of weight w, other than σ_w. The order that we take is

$$\sigma_2, \sigma_3, c_{31}, \dots c_{3a_3}, \dots, \sigma_w, c_{w1}, c_{w2}, \dots, c_{wa_w}, \dots .$$

If G is of class $m - 1$, all commutators of weight m are equal to 1, and we only consider those σ_w, c_{wj} for which $w < m$.

The proof proceeds by stages, each stage being attained by a number of steps. At the 0th stage, we have

$$(xy)^p = x\sigma_1 x\sigma_1 \dots x\sigma_1,$$

and the only point at which we wish to refine the procedure of Hall is in passing to the 1st stage. This is done by collecting all the elements x in the expression $x\sigma_1 x\sigma_1 \dots x\sigma_1$ over on the left. To do this we may begin with the following steps:

$$\begin{aligned}(x\sigma_1)^p &= x^2\sigma_1[\sigma_1,x]\sigma_1 x\sigma_1 \dots x\sigma_1\\ &= x^2\sigma_1[\sigma_1,x]x\sigma_1[\sigma_1,x]\sigma_1 \dots x\sigma_1\\ &= x^2\sigma_1 x[\sigma_1,x]\,[\sigma_1,x,x]\sigma_1[\sigma_1,x]\sigma_1 \dots x\sigma_1\\ &= x^3\sigma_1[\sigma_1,x]^2\,[\sigma_1,x,x]\sigma_1[\sigma_1,x]\sigma_1 \dots x\sigma_1\\ &= \dots .\end{aligned}$$

Here we have collected the first three elements x and obtained

$$(xy)^p = x^3\sigma_1\sigma_2{}^2\sigma_3\sigma_1\sigma_2\sigma_1 \dots x\sigma_1.$$

Suppose that after collecting the first i elements x, where $1 \leqslant i \leqslant p$, we have an expression of the form

$$(xy)^p = x^i d_1 d_2 \dots d_k\, x\sigma_1 x\sigma_1 \dots x\sigma_1, \tag{3}$$

in which $n_w(i)$ of the d_l are equal to σ_w, for $w = 1, 2, \dots, m-1$. Then

$$n_1(1) = 1 \qquad n_w(1) = 0\,(w = 2, 3, \dots, m-1). \tag{4}$$

If $i < p$ we can collect another x over on the left, and obtain from (3)

$$(xy)^p = x^{i+1}d_1[d_1, x]d_2[d_2, x] \dots d_k[d_k, x]\sigma_1 x\sigma_1 \dots x\sigma_1.$$

Therefore
$$n_1(i+1) = n_1(i) + 1 \quad (i = 1, 2, \dots, p-1), \tag{5}$$

$$n_w(i+1) = n_w(i) + n_{w-1}(i) \quad (i = 1, 2, \dots, p-1; \ \ w = 2, 3, \dots, m-1). \tag{6}$$

By induction on i, (4), (5) and (6) show that

$$n_w(i) = \binom{i}{w} \quad (i = 1, 2, \dots, p; \ w = 1, 2, \dots, m-1).$$

Thus at the end of the first stage, that is, when all the p elements x have been collected on the left, we have an equation of the form

$$(xy)^p = x^p e_1 e_2 \dots e_l, \tag{7}$$

where $\binom{p}{w}$ of the e_j are equal to σ_w. In particular, just one of the e_j is equal to σ_p.

The next stage is to collect the elements σ_1 which occur in (7), then the elements σ_2, and so on. At each step in each stage a new commutator is introduced, which can be written as a commutator in $\sigma_1, \sigma_2, \dots, \sigma_p$. All commutators of weight less than m are collected after a finite number of stages, and this is the end of the process. The exponent with which each of the commutators appears is calculated by Hall, and using his result, we find that

$$(xy)^p = x^p \sigma_1^p \sigma_2^{\binom{p}{2}} \sigma_3^{\binom{p}{3}} c_{31}^{n_{31}} \ldots c_{3q_3}^{n_{3q_3}} \ldots \sigma_w^{\binom{p}{w}} c_{w1}^{n_{w1}} c_{w2}^{n_{w2}} \ldots c_{wq_w}^{n_{wq_w}} \ldots, \tag{8}$$

where, for $3 \leqslant w < p$, n_{wj} is divisible by p.

Now since each commutator c_{wj} which occurs with positive exponent in (8) can be written as a commutator of weight greater than 1 in $\sigma_1, \sigma_2, \ldots, \sigma_p$, it follows that such a c_{wj} lies in Y', and so, for $3 \leqslant w < p$,

$$c_{wj}^{n_{wj}} \in P_1(Y').$$

For $w \geqslant p$, we can write $c_{wj} = [a, b]$ say, where a and b are also commutators in $\sigma_1, \sigma_2, \ldots \sigma_p$. If a is of weight i in x and y, then b is of weight at least $p - i$ in x and y. Thus if $2 \leqslant i \leqslant p - 2$, $a \in \gamma_i(G)$, $b \in \gamma_{p-i}(G)$, and

$$c_{wj} \in [\gamma_i(G), \gamma_{p-i}(G)].$$

If $i = 1$, then a is either x or y, and since it can be expressed as a commutator in $\sigma_1, \sigma_2, \ldots, \sigma_p$, it follows that $a = y = \sigma_1$, and so $a \in Y$. Also $b \in \gamma_{p-1}(G)$, since p is odd, and

$$c_{wj} \in [Y, \gamma_{p-1}(G)].$$

If $i \geqslant p - 1$, then $a \in \gamma_{p-1}(G)$, and b is a commutator in $\sigma_1, \sigma_2, \ldots, \sigma_p$, and therefore lies in Y. Thus we again obtain

$$c_{wj} \in [Y, \gamma_{p-1}(G)].$$

Since $P_1(Y')$, $[Y, \gamma_{p-1}(G)]$ and all $[\gamma_i(G), \gamma_{p-i}(G)]$ $(i = 2, 3, \ldots, p-2)$ are normal subgroups of G, the theorem follows from (8).

2. We begin by finding the maximal class of a p-group of given order. For this we need the following remark.

LEMMA 2.1. *If G is a group and N is a normal subgroup of G for which G/N is cyclic, then $G' = [G, N]$.*

It is obvious that $[G, N] \leqslant G'$, and so in order to prove the lemma we may assume that $[G, N] = 1$, that is, that N is contained in the centre of G. But then it follows that G is Abelian, since G/N is cyclic (see [13], Kap. IV, p. 104), and so $G' = 1$ as required.

Now in a non-Abelian nilpotent group G, $\gamma_2(G) = G'$ and $\gamma_3(G)$ cannot coincide, and so by taking $N = \gamma_2(G)$ in Lemma 2.1, we see that $G/\gamma_2(G)$ cannot be cyclic. In particular, in a non-Abelian p-group G, $\gamma_2(G)$ is of index greater than p, and if $G/\gamma_2(G)$ is of order p^2, then it is elementary Abelian. Also, if G is a p-group of class $m - 1$ where $m \geqslant 3$, then each of the groups $\gamma_{i-1}(G)/\gamma_i(G)$ is of order at least p $(i = 3, 4, \ldots, m)$, and so G is of order at least p^m. Thus a group of order p^m is of class at most $m - 1$.

We shall refer to groups of order p^m and class $m-1$ for some $m \geqslant 3$ as *p-groups of maximal class*. If G is such a group,

$$(G:\gamma_2(G))=p^2, \quad (\gamma_{i-1}(G):\gamma_i(G))=p \ \ (i=3,4,\ldots,m).$$

Thus G has just $p+1$ maximal subgroups, and these are all normal in G. The remaining normal subgroups are determined in the simple result:

LEMMA 2.2. *If G is a p-group of maximal class and N is a normal subgroup of G of index p^r where $r \geqslant 2$, then $N=\gamma_r(G)$.*

The group G/N is of order p^r, and therefore of class at most $r-1$; that is, $\gamma_r(G/N)=1$. But

$$\gamma_j(G/N)=\gamma_j(G)N/N \ \ (j=2,3,\ldots),$$

and so $\gamma_r(G)\leqslant N$. But

$$(G:\gamma_r(G))=p^r=(G:N),$$

and so $\gamma_r(G)$ and N, being both of the same order, are equal.

As stated in the introduction we shall consider more general classes of groups. For $\mathrm{CF}(m,n,p)$ we may generalize Lemma 2.2 as follows:

LEMMA 2.3. *If $G\in\mathrm{CF}(m,n,p)$ and N is a normal subgroup of G of order p^i which is contained in $\gamma_2(G)$, then $N=\gamma_{m-i}(G)$.*

Obviously, $\gamma_j(G)$ is of order p^{m-j}. Thus if $i=m-2$, the result is obvious, and for $m-i>2$ we may use induction on $m-i$. Since $N<\gamma_2(G)$, there exists a normal subgroup M of G of order p^{i+1}, such that

$$N<M\leqslant\gamma_2(G),$$

(see [13], Kap. IV, p. 104), and by the inductive hypothesis, $M=\gamma_{m-i-1}(G)$. But M/N is a normal subgroup of G/N of order p, and is therefore contained in the centre of G/N, that is, $[G,M]\leqslant N$. Hence

$$N\geqslant[G,\gamma_{m-i-1}(G)]=\gamma_{m-i}(G).$$

But N and $\gamma_{m-i}(G)$ are both of order p^i, and are therefore equal.

Lemma 2.2 shows that in a p-group of maximal class the terms of the upper central series are the same as those of the lower central series, but in the reverse order. We now state the corresponding result for the groups of $\mathrm{CF}(m,n,p)$ and $\mathrm{NCF}(m)$.

THEOREM 2.4. *If $G\in\mathrm{CF}(m,n,p)$ or $G\in\mathrm{NCF}(m)$, then*

$$\zeta_i(G)\cap\gamma_2(G)=\gamma_{m-i}(G) \ \ (i=0,1,\ldots,m-2).$$

In the case when $G \in \mathrm{CF}(m, n, p)$, this is most easily proved as follows. By a remark made in § 1, $\zeta_i(G) \geqslant \gamma_{m-i}(G)$, but $\zeta_i(G) \ngeqslant \gamma_{m-i-1}(G)$. Hence $\zeta_i(G) \cap \gamma_2(G) \geqslant \gamma_{m-i}(G)$, since $i \leqslant m-2$. But if $\zeta_i(G) \cap \gamma_2(G)$ were of greater order than $\gamma_{m-i}(G)$, it would follow from Lemma 2.3 that $\zeta_i(G) \cap \gamma_2(G)$ contains $\gamma_{m-i-1}(G)$, and this is not possible.

If $G \in \mathrm{NCF}(m)$, we must adopt a different procedure, for Lemma 2.3 has no direct analogue for these groups. In this case we proceed by induction on i: for $i=0$ it is trivial. For $i>0$, we observe first that $\zeta_i(G) \cap \gamma_2(G) \geqslant \gamma_{m-i}(G)$, just as above. Now suppose that the theorem is not true: then there exists an element a of $\zeta_i(G) \cap \gamma_2(G)$, which does not belong to $\gamma_{m-i}(G)$. If $i \leqslant m-3$, there exists an integer r, such that a is an element of $\gamma_r(G)$, but not of $\gamma_{r+1}(G)$, where $2 \leqslant r \leqslant m-i-1$. Since $\gamma_r(G)/\gamma_{r+1}(G)$ is cyclic, we may choose an element x which together with $\gamma_{r+1}(G)$ generates $\gamma_r(G)$, and since a does not lie in $\gamma_{r+1}(G)$, there exists a non-zero integer, α, such that $a = x^\alpha y$, where $y \in \gamma_{r+1}(G)$. Now let z be any element of G. By Theorem 1.4, using (1),

$$[z, a] = [z, x^\alpha y] \equiv [z, y]\, [z, x^\alpha]^y \equiv [z, x]^\alpha \pmod{\gamma_{r+2}(G)}.$$

But $a \in \zeta_i(G)$, and so $[z, a] \in \zeta_{i-1}(G) \cap \gamma_2(G)$. By the inductive hypothesis $\zeta_{i-1}(G) \cap \gamma_2(G) = \gamma_{m-i+1}(G)$. Since $m-i+1 \geqslant r+2$, it follows that $[z, a] \in \gamma_{r+2}(G)$, and so

$$[z, x]^\alpha \equiv 1 \pmod{\gamma_{r+2}(G)}.$$

But by Theorem 1.1, $\gamma_{r+1}(G)$ is generated by $\gamma_{r+2}(G)$ and all elements $[z, x]$ as z runs through G. Hence $\gamma_{r+1}(G)/\gamma_{r+2}(G)$ is a group of exponent at most α. Since $r+1 \leqslant m-1$, this contradicts the definition of $\mathrm{NCF}(m)$, and so the theorem is proved for $i \leqslant m-3$. For $i = m-2$, it is, of course, trivial.

For the groups under consideration, the case $m=3$ is not without interest: for example, O. Schreier [9] determined all types of groups in $\mathrm{ECF}(3, n, p)$. However the considerations of the present work do not apply to this case, and we shall henceforth assume that $m>3$. In this case the basic step is the introduction of another characteristic subgroup which we shall denote by $\gamma_1(G)$ (cf. Wiman [12]). This is defined for a group G of $\mathrm{CF}(m, n, p)$ or $\mathrm{NCF}(m)$, where $m>3$, by the property that $\gamma_1(G)/\gamma_4(G)$ is the centraliser in $G/\gamma_4(G)$ of $\gamma_2(G)/\gamma_4(G)$; that is, $\gamma_1(G)$ is the largest subgroup of G such that

$$[\gamma_1(G),\ \gamma_2(G)] \leqslant \gamma_4(G).$$

Thus it is clear that $\gamma_1(G)$ is a characteristic proper subgroup of G which contains $\gamma_2(G)$. In order to see how $\gamma_1(G)$ is situated in G, we prove the following.

LEMMA 2.5. *Let G be a nilpotent group of class $m-1$, where $m>3$, and suppose that for $i = 3, 4, \ldots, m$, $\gamma_{i-1}(G)/\gamma_i(G)$ is cyclic. For $i = 3, 4, \ldots, m-1$, let K_i be the subgroup of*

G defined by the fact that $K_i/\gamma_{i+1}(G)$ is the centraliser in $G/\gamma_{i+1}(G)$ of $\gamma_{i-1}(G)/\gamma_{i+1}(G)$. Then G/K_i is a cyclic group of the same order as $\gamma_i(G)/\gamma_{i+1}(G)$.

To prove this suppose that a is an element which together with $\gamma_i(G)$ generates $\gamma_{i-1}(G)$, and that b is an element which together with $\gamma_{i+1}(G)$ generates $\gamma_i(G)$. If x is any element of G, then $[a, x]$ lies in $\gamma_i(G)$, and so there exists an integer ξ such that

$$[a, x] \equiv b^{\xi} \pmod{\gamma_{i+1}(G)},$$

or

$$a^x \equiv ab^{\xi} \pmod{\gamma_{i+1}(G)}.$$

If n is the order of $\gamma_i(G)/\gamma_{i+1}(G)$, and we map x into the residue class of integers modulo n containing ξ, we obtain a homomorphism of G into the additive group of residue classes modulo n. K_i is the kernel of this homomorphism. The image is the whole group of residue classes, for as x runs through G, by Theorem 1.1 the elements $[a, x]$ and $\gamma_{i+1}(G)$ generate $\gamma_i(G)$, and so the elements b^{ξ} together with $\gamma_{i+1}(G)$ generate $\gamma_i(G)$. Hence G/K_i is cyclic of order n.

It follows from Lemma 2.5 that if $G \in \mathrm{CF}(m, n, p)$ $(m > 3)$, then $\gamma_1(G)$ is of index p, whilst if $G \in \mathrm{NCF}(m)$ $(m > 3)$, then $G/\gamma_1(G)$ is an infinite cyclic group.

THEOREM 2.6. *If $G \in \mathrm{CF}(m, n, p)$ or $G \in \mathrm{NCF}(m)$ $(m > 3)$, then the derived group $\gamma_1'(G)$ of $\gamma_1(G)$ is contained in $\gamma_3(G)$.*

To prove this we may argue modulo $\gamma_4(G)$, and may therefore assume that $m = 4$. $\gamma_1'(G)$ is generated by all elements $[u, v]$, as u, v run through $\gamma_1(G)$, and so we have to prove that $[u, v] \in \gamma_3(G)$. By the above remarks, there exists an element s of G which together with $\gamma_1(G)$ generates G. If $[u, s] = x$, $[v, s] = y$, then

$$[u, v]^s = [u^s, v^s] = [ux, vy].$$

But x, y are elements of $\gamma_2(G)$, and it follows from the definition of $\gamma_1(G)$ that they commute with u, v. Since also $\gamma_2(G)$ is Abelian, we find, using (1), that

$$[ux, vy] = [u, v].$$

Thus $[u, v]$ commutes with s. But again $[u, v]$, being an element of $\gamma_2(G)$, commutes with each element of $\gamma_1(G)$, and so $[u, v]$ lies in the centre of G. It follows from Theorem 2.4 that $[u, v] \in \gamma_3(G)$, as required.

Next we discuss the position of $\eta(G) = \eta_3(G)$, as defined in § 1.

THEOREM 2.7. *If $G \in \mathrm{CF}(m, n, p)$ $(m > 3)$, then $\eta(G)$ is a subgroup of $\gamma_1(G)$ of index p. If $G \in \mathrm{NCF}(m)$ $(m > 3)$, then $\eta(G)$ is a subgroup of $\gamma_1(G)$, and $\gamma_1(G)/\eta(G)$ is an infinite cyclic group.*

In both cases we prove that $\gamma_1(G)/\eta(G)$ is cyclic as follows. If s is as defined in the proof of Theorem 2.6, we deduce from Theorem 1.1 that $\gamma_2(G)$ is generated by $\gamma_3(G)$ together with the elements $[u, s]$ and $[u, v]$, as u, v run through $\gamma_1(G)$. By Theorem 2.6 the elements $[u, v]$ lie in $\gamma_3(G)$, and may therefore be disregarded. Let a be an element which together with $\gamma_3(G)$ generates $\gamma_2(G)$. Then there exists a finite set of elements $u_1, u_2, \ldots, u_r$ of $\gamma_1(G)$, such that

$$a \equiv \prod_{i=1}^{r} [u_i, s]^{\lambda_i} \quad (\text{mod } \gamma_3(G)),$$

where $\lambda_1, \lambda_2, \ldots, \lambda_r$ are suitable integers. Let

$$s_1 = u_1^{\lambda_1} u_2^{\lambda_2} \ldots u_r^{\lambda_r},$$

so that if $[s_1, s] = s_2$, then by (1) and Theorem 1.4, $s_2 \equiv a$ (mod $\gamma_3(G)$). Thus $\gamma_2(G)$ is generated by $\gamma_3(G)$ and s_2.

For any element u of $\gamma_1(G)$, we may therefore write $[u, s] \equiv s_2^{\alpha}$; we then define $\bar{u} = u s_1^{-\alpha}$ Thus $\gamma_1(G)$ is generated by s_1 and the elements $\bar{u}$. Now $\bar{u} \in \gamma_1(G)$, and so by Theorem 2.6 $\bar{u}$ commutes modulo $\gamma_3(G)$ with each element of $\gamma_1(G)$. But also $\bar{u}$ commutes modulo $\gamma_3(G)$ with s, for

$$[\bar{u}, s] = [u s_1^{-\alpha}, s] \equiv [u, s]\,[s_1^{-\alpha}, s] \equiv s_2^{\alpha-\alpha} \equiv 1 \quad (\text{mod } \gamma_3(G)),$$

and so $\bar{u}$ lies in the centre of G modulo $\gamma_3(G)$, that is, $\bar{u} \in \eta(G)$. By Theorem 1.2, Corollary 1, $[\eta(G), \gamma_2(G)] \leqslant \gamma_4(G)$, and so $\eta(G) \leqslant \gamma_1(G)$. Hence $\gamma_1(G)$ is generated by s_1 and $\eta(G)$, and $\gamma_1(G)/\eta(G)$ is cyclic.

To find the order of $\gamma_1(G)/\eta(G)$, we use the fact that according to Theorem 1.4, for any integer r

$$[s_1^r, s] \equiv s_2^r \quad (\text{mod } \gamma_3(G)).$$

By Theorem 2.6 s_1^r commutes modulo $\gamma_3(G)$ with each element of $\gamma_1(G)$, and so $s_1^r \in \eta(G)$ if and only if s_1^r and s commute modulo $\gamma_3(G)$, that is, if $s_2^r \in \gamma_3(G)$. If $G \in \mathrm{CF}(m, n, p)$, it follows that $s_1^p \in \eta(G)$, $s_1 \notin \eta(G)$, and therefore $\gamma_1(G)/\eta(G)$ is of order p. If $G \in \mathrm{NCF}(m)$, it follows that no positive power of s_1 lies in $\eta(G)$, and so $\gamma_1(G)/\eta(G)$ is infinite.

Corollary. *If* $G \in \mathrm{CF}(m, n, p)$ *or* $G \in \mathrm{NCF}(m)$, *then* $\eta(G) = \zeta_{m-2}(G)$.

By a remark in § 1, $\eta(G) \leqslant \zeta_{m-2}(G)$. Also, by Theorem 1.2, Corollary 3 and Theorem 2.4, for $m > 3$,

$$[\zeta_{m-2}(G), \gamma_2(G)] \leqslant \zeta_{m-4}(G) \cap \gamma_2(G) = \gamma_4(G)$$

and so $\zeta_{m-2}(G) \leqslant \gamma_1(G)$. Suppose that $\zeta_{m-2}(G) > \eta(G)$; then $\zeta_{m-2}(G)$ is of finite index r in $\gamma_1(G)$. Hence $s_1^r \in \zeta_{m-2}(G)$, and by Theorem 2.4

$$[s_1^r, s] \in \zeta_{m-3}(G) \cap \gamma_2(G) = \gamma_3(G).$$

But by Theorem 1.4 $[s_1^r, s] \equiv s_2^r \pmod{\gamma_3(G)}$, and so $s_2^r \in \gamma_3(G)$. If $G \in \mathrm{NCF}(m)$ this is impossible since r is finite, and if $G \in \mathrm{CF}(m, n, p)$ this implies that $r \geqslant p$. In both cases, we have a contradiction, and so $\zeta_{m-2}(G) = \eta(G)$. For $m = 3$ the corollary is trivial.

In future, instead of $\eta(G)$ we shall speak of the more familiar group $\zeta_{m-2}(G)$. We are now therefore considering groups with the following series of characteristic subgroups.

$$G > \gamma_1(G) > \zeta_{m-2}(G) \geqslant \gamma_2(G) > \gamma_3(G) > \dots > \gamma_{m-1}(G) > \gamma_m(G) = 1.$$

In this series all factor groups of successive terms are cyclic of equal order, except for $\zeta_{m-2}(G)/\gamma_2(G)$. This group is arbitrary, as is seen by considering the direct product of a group in which it is the unit subgroup with an arbitrary Abelian group.

Now according to Theorem 1.2, Corollary 2, in any group G,

$$[\gamma_i(G), \gamma_j(G)] \leqslant \gamma_{i+j}(G) \quad (i, j = 2, 3, \dots).$$

This is in general the best possible result, as, for example, the Sylow p-subgroups of the symmetric groups show (see [6]). In a particular group however, it may happen that a much stronger commutation law holds. Thus, if $G \in \mathrm{CF}(m, n, p)$ or $G \in \mathrm{NCF}(m)$ $(m > 3)$, and

$$[\gamma_i(G), \gamma_j(G)] \leqslant \gamma_{i+j+k}(G) \quad (i, j = 1, 2, \dots),$$

we say that G has *degree of commutativity* k. (We do not assume that k is the greatest such number).

The aim of the present paragraph is to find conditions under which a group G has degree of commutativity greater than 0, that is,

$$[\gamma_i(G), \gamma_j(G)] \leqslant \gamma_{i+j+1}(G) \quad (i, j = 1, 2, \dots).$$

In particular, this requires that

$$[\gamma_1(G), \gamma_i(G)] \leqslant \gamma_{i+2}(G) \quad (i = 1, 2, \dots, m-2). \tag{9}$$

For $i = 1$ this is always true by Theorem 2.6, and for $i = 2$ it is always true on account of the definition of $\gamma_1(G)$. For $2 \leqslant i \leqslant m-2$, (9) simply asserts that $\gamma_1(G)/\gamma_{i+2}(G)$ is the centraliser of $\gamma_i(G)/\gamma_{i+2}(G)$ in $G/\gamma_{i+2}(G)$, for, in the case of the p-groups this centraliser cannot be larger than a maximal subgroup, and in the case of the groups of $\mathrm{NCF}(m)$ this centraliser must have infinite index by Lemma 2.5. Our next result shows that whether (9) holds or not is the crux of the matter.

THEOREM 2.8. *If $G \in \mathrm{CF}(m, n, p)$ or $G \in \mathrm{NCF}(m)$ $(m > 3)$, and*

$$[\gamma_1(G), \gamma_i(G)] \leqslant \gamma_{i+2}(G) \quad (i = 1, 2, \dots, m-2),$$

then G has degree of commutativity greater than 0.

This is proved by means of the following lemma.

5 − 583801. *Acta mathematica* 100. Imprimé le 26 septembre 1958.

LEMMA 2.9. *Suppose that $G \in \mathrm{CF}(m, n, p)$ or $G \in \mathrm{NCF}(m)$ $(m > 4)$, and that $G/\gamma_{m-1}(G)$ has degree of commutativity greater than 0. Let elements s, s_1 of G be defined by the properties that s and $\gamma_1(G)$ generate G, s_1 and $\zeta_{m-2}(G)$ generate $\gamma_1(G)$. Write $s_i = \sigma_i(s, s_1)$ $(i = 1, 2, \ldots, m-2)$. Then for $i = 2, 3, \ldots, m-2$, s_i and $\gamma_{i+1}(G)$ generate $\gamma_i(G)$, and*

$$[s_1, s_{m-2}] = [s_2, s_{m-3}]^{-1} = \cdots = [s_i, s_{m-i-1}]^{(-1)^{i-1}} = \cdots = [s_{m-2}, s_1]^{(-1)^{m-1}}.$$

Note that there is no ambiguity in the definition of s_1. By Theorem 1.1 $\gamma_2(G)$ is generated by $\gamma_3(G)$, $[s_1, s] = s_2$, and certain other commutators, one of whose components lies in $\zeta_{m-2}(G)$, for G is generated by s, s_1 and $\zeta_{m-2}(G)$. Since $\zeta_{m-2}(G) = \eta(G)$, these other commutators already lie in $\gamma_3(G)$, and so for $i = 2$, s_i and $\gamma_{i+1}(G)$ generate $\gamma_i(G)$. For $i > 2$ we prove this by induction on i: thus by the inductive hypothesis s_{i-1} and $\gamma_i(G)$ generate $\gamma_{i-1}(G)$. Hence by Theorem 1.1 $\gamma_i(G)$ is generated by $\gamma_{i+1}(G)$, $[s_{i-1}, s] = s_i$, and certain other commutators, one of whose components lies in $\gamma_1(G)$. But since $G/\gamma_{m-1}(G)$ has degree of commutativity greater than 0 and $i \leqslant m-2$,

$$[\gamma_{i-1}(G), \gamma_1(G)] \leqslant \gamma_{i+1}(G),$$

and so these other commutators already lie in $\gamma_{i+1}(G)$, and the result is proved.

For $2 \leqslant i \leqslant m-2$,

$$[s_i, s_{m-i-1}] = s_i^{-1} s_i^{s_{m-i-1}} = s_i^{-1}[s_{i-1}, s]^{s_{m-i\ 1}} = s_i^{-1}[s_{i-1}^{s_{m-i-1}}, s^{s_{m-i-1}}].$$

Since $G/\gamma_{m-1}(G)$ has degree of commutativity greater than 0, $[s_{i-1}, s_{m-i-1}] \in \gamma_{m-1}(G)$, and so $s_{i-1}^{s_{m-i-1}}$ is the product of s_{i-1} and an element of the centre of G. Also $s^{s_{m-i-1}} = s s_{m-i}^{-1}$, and so

$$[s_i, s_{m-i-1}] = s_i^{-1}[s_{i-1}, s s_{m-i}^{-1}].$$

Working out the right-hand side by means of (1) and (2), and using the fact that $[s_{i-1}, s_{m-i}]$ lies in the centre of G, we obtain

$$[s_i, s_{m-i-1}] = [s_{i-1}, s_{m-i}]^{-1},$$

as required.

Theorem 2.8 is trivial for $m = 4$, and we prove it for $m > 4$ by induction on m. Applying the inductive hypothesis to $G/\gamma_{m-1}(G)$, we find that $G/\gamma_{m-1}(G)$ has degree of commutativity greater than 0. Thus we have only to prove that $[\gamma_i(G), \gamma_{m-i-1}(G)] = 1$ $(i = 1, 2, \ldots, m-2)$. The conditions of Lemma 2.9 are satisfied, and so in the notation there adopted,

$$[s_i, s_{m-i-1}] = [s_1, s_{m-2}]^{(-1)^{i-1}}.$$

But by hypothesis, $[\gamma_1(G), \gamma_{m-2}(G)] = 1$, and so s_i and s_{m-i-1} commute. It is clear from

Theorem 1.2, Corollary 2 that s_i commutes with all s_j for which $j \geqslant m-i$, and that s_{m-i-1} commutes with all s_j for which $j \geqslant i+1$, and so $[\gamma_i(G), \gamma_{m-i-1}(G)] = 1$, as required.

Lemma 2.9 also has the following consequence.

THEOREM 2.10. *Suppose that* $G \in \mathrm{CF}(m, n, p)$ *or* $G \in \mathrm{NCF}(m)$ $(m \geqslant 5)$, *and that* $G/\gamma_{m-1}(G)$ *has degree of commutativity greater than* 0. *Then*

(i) *if* m *is odd,* G *has degree of commutativity greater than* 0;

(ii) *if* m *is even,* G *has degree of commutativity greater than* 0 *if and only if* $\gamma_{\frac{1}{2}m-1}(G)$ *is Abelian.*

By Theorem 2.8 G has degree of commutativity greater than 0 if and only if $[\gamma_1(G), \gamma_{m-2}(G)] = 1$, and in the notation of Lemma 2.9 this is equivalent to $[s_1, s_{m-2}] = 1$. By Lemma 2.9 this is so if and only if $[s_{\frac{1}{2}m-1}, s_{\frac{1}{2}m}] = 1$ when m is even, or $[s_{\frac{1}{2}(m-1)}, s_{\frac{1}{2}(m-1)}] = 1$ when m is odd. This condition is always satisfied when m is odd, and when m is even it is satisfied if and only if $[\gamma_{\frac{1}{2}m-1}(G), \gamma_{\frac{1}{2}m}(G)] = 1$, which is the condition for $\gamma_{\frac{1}{2}m-1}(G)$ to be Abelian, according to Lemma 2.1.

COROLLARY. *If* $G \in \mathrm{CF}(m, n, p)$ *or* $G \in \mathrm{NCF}(m)$ $(m \geqslant 5)$, *and* $\gamma_2(G)$ *is Abelian, then* G *has degree of commutativity greater than* 0.

This follows by a very simple induction on m.

We now reach the main result of this paragraph.

THEOREM 2.11. *If* $G \in \mathrm{CF}(m, n, p)$, *where* m *is odd and* $5 \leqslant m \leqslant 2p+1$, *or if* $G \in \mathrm{NCF}(m)$, *where* m *is odd and* $m \geqslant 5$, *then* G *has degree of commutativity greater than* 0.

For $m = 5$, this is a direct consequence of Theorem 2.10 (i), for $G/\gamma_4(G)$ necessarily has degree of commutativity greater than 0. For $m > 5$ we proceed by induction on m. Applying the inductive hypothesis to $G/\gamma_{m-2}(G)$ we see that this group has degree of commutativity greater than 0. Hence we may apply Lemma 2.9 to $G/\gamma_{m-1}(G)$, and defining $s, s_1, s_2, \ldots, s_{m-3}$ as in this lemma we find that

$$[s_i, s_j] \in \gamma_{i+j+1}(G) \quad (i+j \leqslant m-3), \tag{10}$$

$$[s_i, s_{m-i-2}] \equiv [s_1, s_{m-3}]^{(-1)^{i-1}} \quad (\mathrm{mod}\ \gamma_{m-1}(G)) \quad (i = 1, 2, \ldots, m-3). \tag{11}$$

Now if $G/\gamma_{m-1}(G)$ has degree of commutativity greater than 0, we can apply Theorem 2.10, and since m is odd, we obtain at once the required result. We shall therefore assume that $G/\gamma_{m-1}(G)$ does not have degree of commutativity greater than 0 and obtain a contradiction. By Theorem 2.8 it follows from this assumption that (9) does not hold for $i = m-3$, and thus that $\gamma_1(G)/\gamma_{m-1}(G)$ is not the centraliser of $\gamma_{m-3}(G)/\gamma_{m-1}(G)$. But $\gamma_1(G)$ is generated by s_1 and $\zeta_{m-2}(G)$: thus s_1 cannot lie in this centraliser, since $\zeta_{m-2}(G)$ certainly does lie in it. And since $\gamma_{m-3}(G)$ is generated by s_{m-3} and $\gamma_{m-2}(G)$ it follows that $[s_{m-3}, s_1] = s_{m-2}$ say lies in $\gamma_{m-2}(G)$ but not in $\gamma_{m-1}(G)$.

By (11) $$[s_2, s_{m-4}] \equiv s_{m-2} \pmod{\gamma_{m-1}(G)},$$

and so $$[s_{m-2}, s_1] \equiv [s_2, s_{m-4}]^{-1} [s_2, s_{m-4}]^{s_1}.$$

But $$[s_2, s_{m-4}]^{s_1} = [s_2^{s_1}, s_{m-4}^{s_1}] = [s_2[s_2, s_1], s_{m-4}[s_{m-4}, s_1]].$$

Also $[s_2, s_1]$ lies in $\gamma_4(G)$ and thus commutes with any element of $\gamma_{m-4}(G)$: hence by (1)

$$[s_2, s_{m-4}]^{s_1} = [s_2, s_{m-4}[s_{m-4}, s_1]].$$

Similarly $[s_{m-4}, s_1] \in \gamma_{m-2}(G)$ and thus commutes with s_2. Hence

$$[s_2, s_{m-4}]^{s_1} = [s_2, s_{m-4}],$$

and $$[s_{m-2}, s_1] = 1. \tag{12}$$

Since s_1 and $\zeta_{m-2}(G)$ generate $\gamma_1(G)$, it follows that s_{m-2} commutes with all elements of $\gamma_1(G)$. Now s_{m-2} lies in $\gamma_2(G)$ but not in $\gamma_{m-1}(G)$, and so by Theorem 2.4 s_{m-2} does not lie in $\zeta_1(G)$. Hence s_{m-2} cannot commute with s, and the element $s_{m-1} = [s_{m-2}, s]$ is not the unit element.

Next we prove by induction on i that

$$[s_i, s_{m-i-1}] = s_{m-1}^{(-1)^{i-1}(i-1)} \quad (i = 2, 3, \ldots, m-3). \tag{13}$$

For $i = 2$ we have

$$[s_2, s_{m-3}] = s_2^{-1} s_2^{s_{m-3}} = s_2^{-1}[s_1, s]^{s_{m-3}} = s_2^{-1}[s_1^{s_{m-3}}, s^{s_{m-3}}] = s_2^{-1}[s_1[s_1, s_{m-3}], s[s, s_{m-3}]]. \tag{14}$$

Now $[s, s_{m-3}]$ lies in $\gamma_{m-2}(G)$ and thus commutes with s_1 and all elements of $\gamma_2(G)$ by (12). By (1) and (2) it follows from (14) that

$$[s_2, s_{m-3}] = s_2^{-1}[s_1 s_{m-2}^{-1}, s] = s_{m-1}^{-1},$$

as required. For $i > 2$ we have by the inductive hypothesis

$$[s_{i-1}, s_{m-i}] = s_{m-1}^{(-1)^i(i-2)}.$$

Now

$$[s_i, s_{m-i-1}] = s_i^{-1} s_i^{s_{m-i-1}} = s_i^{-1} [s_{i-1}, s]^{s_{m-i-1}} = s_i^{-1} [s_{i-1}^{s_{m-i-1}}, s^{s_{m-i-1}}]$$
$$= s_i^{-1} [s_{i-1} [s_{i-1}, s_{m-i-1}], s [s, s_{m-i-1}]] = s_i^{-1} [s_{i-1} s_{m-2}^{(-1)^{i-1}}, s s_{m-i}^{-1}]$$

by (11). Using (1) and (2) it follows that

$$[s_i, s_{m-i-1}] = [s_{i-1}, s_{m-i}]^{-1} [s_{m-2}, s]^{(-1)^{i-1}} = s_{m-1}^{(-1)^{i-1}(i-1)},$$

as required.

Putting $i = \frac{1}{2}(m-1)$ in (13) we obtain $s_{m-1}^{\frac{1}{2}(m-3)} = 1$, and from above $s_{m-1} \neq 1$. This is impossible if $G \in \mathrm{NCF}(m)$. If $G \in \mathrm{CF}(m, n, p)$, it implies that $\frac{1}{2}(m-3) \equiv 0 \pmod{p}$, and since $m > 3$, we have $m \geqslant 2p+3$. This contradicts the hypothesis of the theorem and so the result is proved.

Corollary. *If $G \in \mathrm{CF}(m, n, p)$, where m is even and $6 \leqslant m \leqslant 2p+2$, or if $G \in \mathrm{NCF}(m)$ where m is even and $m \geqslant 6$, then G has degree of commutativity greater than 0 if and only if $\gamma_{\frac{1}{2}m-1}(G)$ is Abelian.*

For we may apply Theorem 2.11 to $G/\gamma_{m-1}(G)$, which shows that this group has degree of commutativity greater than 0. The result therefore follows by Theorem 2.10.

We mention the following consequences of Theorem 2.11.

Theorem 2.12. *Suppose that G is a p-group and that there exists an even integer m satisfying $4 \leqslant m \leqslant 2p$, such that $G/\gamma_m(G) \in \mathrm{CF}(m, n, p)$ for some n. Then $(\gamma_m(G) : \gamma_{m+1}(G)) \leqslant p$.*

Theorem 2.13. *Suppose that G is a nilpotent group, and that there exists an even integer $m \geqslant 4$, such that $G/\gamma_m(G) \in \mathrm{NCF}(m)$. If $T/\gamma_{m+1}(G)$ is the torsion subgroup of $\gamma_m(G)/\gamma_{m+1}(G)$, then $\gamma_m(G)/T$ is cyclic.*

Let s, s_1 be defined in the usual way, and let x be an element defined by the property that x and $\gamma_m(G)$ generate $\gamma_{m-1}(G)$. By Theorem 1.1 and Theorem 1.2, Corollary 1, $\gamma_m(G)$ is generated by $\gamma_{m+1}(G)$ and the elements $[x, s]$, $[x, s_1]$. Let N be the subgroup of G generated by $[x, s]$ and $\gamma_{m+1}(G)$. Then $\gamma_m(G)/N$ is cyclic.

If G is a p-group, suppose that $\gamma_m(G)/N$ is of order p. Then $G/N \in \mathrm{CF}(m+1, n+1, p)$, and by Theorem 2.11 G/N has degree of commutativity greater than 0. Thus $[x, s_1] \in N$, which is a contradiction. Hence $N = \gamma_m(G)$, that is, $\gamma_m(G)$ is generated by $[x, s]$ and $\gamma_{m+1}(G)$. The result now follows at once from Theorem 1.5 (ii).

Similarly, for Theorem 2.13, we obtain a contradiction if we assume that $\gamma_m(G)/N$ is infinite, and so $\gamma_m(G)/\gamma_{m+1}(G)$ is an extension of a cyclic group by a finite cyclic group. Hence the result.

We shall not investigate further the conditions under which a general group of $\mathrm{CF}(m, n, p)$ has degree of commutativity greater than 0, but it will be proved later that the groups of $\mathrm{ECF}(m, n, p)$ for which $m > p+1$ have this property. We now wish to construct examples which show that nothing more can be proved in this direction; that is, we construct a p-group of maximal class of order p^{2r}, where $6 \leqslant 2r \leqslant p+1$, which does not have degree of commutativity greater than 0. Thus, for $p > 3$ and $3 \leqslant r \leqslant \frac{1}{2}(p+1)$, let E be an elementary Abelian group of order p^r, with generators $e_1, e_2, \dots e_r$. Let A be the subgroup of the holomorph of E consisting of all elements which induce in E an automorphism of the form

$$e_i \to e_i e_r^{\sigma_i} \quad (i = 1, 2, \ldots, r-1), \quad e_r \to e_r.$$

Let $a_1, a_2, \ldots, a_{r-1}$ be the automorphisms in A defined by

$$e_i^{a_j} = e_i e_r^{(-1)^{r+i-1}\binom{r-j-1}{i-1}} \quad (i = 1, 2, \ldots, r-1;\ j = 1, 2, \ldots, r-1),$$
$$e_r^{a_j} = e_r \quad (j = 1, 2, \ldots, r-1).$$

Now if b is any automorphism in A other than 1 and $e_i^b = e_i e_r^{\sigma_i}$ $(i = 1, 2, \ldots, r-1)$, define k to be the greatest of the integers $1, 2, \ldots, r-1$ such that $\sigma_k \not\equiv 0 \pmod p$; then $b a_{r-k}^{(-1)^{r+k}\sigma_k}$ leaves invariant all e_i for which $i \geqslant k$. It follows that the automorphism group A/E is generated by $a_1, a_2, \ldots, a_{r-1}$. We have

$$[a_i, a_j] = 1 \quad (1 \leqslant i < j \leqslant r-1),$$
$$a_i^p = 1 \quad (i = 1, 2, \ldots, r-1).$$

It is easily verified that A possesses an automorphism α for which

$$a_i^\alpha = a_i a_{i+1}^{-1} \quad (i = 1, 2, \ldots, r-2), \qquad a_{r-1}^\alpha = a_{r-1} e_1^{-1},$$
$$e_i^\alpha = e_i e_{i+1}^{-1} \quad (i = 1, 2, \ldots, r-2), \qquad e_{r-1}^\alpha = e_{r-1},\ e_r^\alpha = e_r.$$

α is of order p, and we may thus form an extension G of A, such that G/A is of order p, and an element of G induces the automorphism α in A (see [13], Kap. III, § 7). G is of order p^{2r} and class $2r-1$, but does not have degree of commutativity greater than 0, since $e_{r-1}^\alpha = e_{r-1}$.

The above considerations only make use essentially of relations between commutators and it is therefore to be conjectured that the calculations can be applied more generally. If for instance we consider nilpotent groups whose lower central factors are cyclic of arbitrary order, generalizations of the above theorems can be obtained. The results are, however, rather complicated; the price of generality is a very considerable loss of clarity, and we have therefore been content to state the results in their simplest forms.

We conclude the present paragraph by obtaining a result on the maximal number of generators of the derived group of a group of $\mathrm{CF}(m, n, p)$. With later aims in mind it will be convenient to work under slightly more general hypotheses than are necessary for this purpose. Thus we suppose that $G \in \mathrm{CF}(m, n, p)$ $(m > 3)$, and that if $m > 5$, $G/\gamma_{m-1}(G)$ has degree of commutativity greater than 0. By Lemma 2.5 the centraliser K of $\gamma_{m-2}(G)$ in G is of index p and contains $\zeta_{m-2}(G)$. There are therefore at least $p^{m-2}(p-1)^2$ elements of G which belong neither to K nor to $\gamma_1(G)$: let s be such an element, and let S be the centraliser of s in G. Clearly $\gamma_{m-1}(G) \leqslant S$, and we prove that $S \cap \gamma_2(G) = \gamma_{m-1}(G)$. If in fact there exists an element x of $S \cap \gamma_2(G)$ which does not belong to $\gamma_{m-1}(G)$, then there exists an integer i, with $2 \leqslant i \leqslant m-2$, such that x lies in $\gamma_i(G)$ but not in $\gamma_{i+1}(G)$. Thus x and $\gamma_{i+1}(G)$ generate $\gamma_i(G)$; but s was chosen so that it does not belong to the centraliser of $\gamma_i(G)$ modulo $\gamma_{i+2}(G)$, and so $[x, s]$ cannot lie in $\gamma_{i+2}(G)$. Since $i \leqslant m-2$, and $x \in S$, this is a contradiction.

LEMMA 2.14. *Suppose that $G \in \mathrm{CF}(m, n, p)$ $(m > 3)$ and that, if $m > 5$, $G/\gamma_{m-1}(G)$ has degree of commutativity greater than* 0. *Let s be an element of G which belongs neither to $\gamma_1(G)$ nor to the centraliser of $\gamma_{m-2}(G)$, and let S be the centraliser of s in G. Then $S \cap \gamma_2(G) = \gamma_{m-1}(G)$.*

Next we show that we can proceed from $\gamma_2(G)$ to $\zeta_{m-2}(G)$ by adjoining elements of S.

THEOREM 2.15. *Under the conditions of Lemma 2.14, a set T of elements of S can be chosen, which together with $\gamma_2(G)$ generate $\zeta_{m-2}(G)$. If $t, u \in T$, then $[t, u] \in \gamma_{m-1}(G)$.*

This may be proved by induction on m. Thus for $m > 4$, there exists a set $\overline{T}$ of elements which together with $\gamma_2(G)$ generate $\zeta_{m-2}(G)$, such that if $\bar{t} \in \overline{T}$, then $[s, \bar{t}] \in \gamma_{m-1}(G)$, as is seen by applying the inductive hypothesis to $G/\gamma_{m-1}(G)$. This is also true for $m = 4$, since $\zeta_{m-2}(G) = \eta(G)$. Let x be an element which together with $\gamma_{m-1}(G)$ generates $\gamma_{m-2}(G)$, so that by the definition of s, $y = [x, s] \neq 1$, that is, y generates $\gamma_{m-1}(G)$. Thus for each element $\bar{t} \in \overline{T}$, there exists an integer α such that $[s, \bar{t}] = y^\alpha$; we put $t = \bar{t} x^\alpha$, and denote by T the set of all elements t which arise in this way. Since $m \geqslant 4$, $t \in \zeta_{m-2}(G)$, and so $\zeta_{m-2}(G)$ is generated by T and $\gamma_2(G)$. Since also by (1) and Theorem 1.4

$$[s, t] = [s, \bar{t}\, x^\alpha] = [s, x^\alpha] y^\alpha = 1,$$

we see that T is contained in S. Finally, if $t, u \in T$, then $[t, u] \in S \cap \gamma_2(G)$, and so $[t, u] \in \gamma_{m-1}(G)$, by Lemma 2.14.

We shall need one or two consequences of Theorem 2.15.

COROLLARY 1. *Under the same conditions S is of order p^{n-m+2} and is of class at most* 2.

First of all we show that $S \cap \zeta_{m-2}(G)$ is generated by T and $\gamma_{m-1}(G)$, and is of order p^{n-m+1}. If $x \in S \cap \zeta_{m-2}(G)$, x can be written in the form yz, where y is a product of elements of T, and $z \in \gamma_2(G)$, for $\zeta_{m-2}(G)$ is generated by T and $\gamma_2(G)$. Since T is contained in S, it follows that $y \in S$: thus $z = y^{-1}x \in S$. Hence $z \in \gamma_{m-1}(G)$ by Lemma 2.14. Also, if $t \in T$ and t is of order p^α modulo $\gamma_2(G)$, then $t^{p^\alpha} \in \gamma_2(G) \cap S = \gamma_{m-1}(G)$. Thus, since $\zeta_{m-2}(G)/\gamma_2(G)$ is of order p^{n-m}, it follows that T and $\gamma_{m-1}(G)$ generate a group of order p^{n-m+1}, for $[T, T] \leqslant \gamma_{m-1}(G)$. This proves the assertions.

Next we show that $S \cap \gamma_1(G) = S \cap \zeta_{m-2}(G)$. If $x \in S \cap \gamma_1(G)$ and s_1 is an element of G so defined that s_1 and $\zeta_{m-2}(G)$ generate $\gamma_1(G)$, then we can write $x = s_1^\alpha y$ where $y \in \zeta_{m-2}(G)$ for a suitable integer α. Thus

$$1 = [s, x] = [s, s_1^\alpha y] = [s, y]\,[s, s_1^\alpha]^y.$$

But $[s, y] \in \gamma_3(G)$, since $\zeta_{m-2}(G) = \eta(G)$, and so $[s, s_1^\alpha] \in \gamma_3(G)$. Hence, modulo $\gamma_3(G)$ s_1^α commutes with every element of G; that is, $s_1^\alpha \in \eta(G) = \zeta_{m-2}(G)$. Thus $x \in \zeta_{m-2}(G)$, as required.

Finally, if $x \in S$, we can write $x = s^\alpha y$ where $y \in \gamma_1(G)$. Since x and s lie in S, we have $y \in S \cap \gamma_1(G) = S \cap \zeta_{m-2}(G)$. Thus S is generated by s, T and $\gamma_{m-1}(G)$. Also, since $s^p \in S \cap \gamma_1(G) = S \cap \zeta_{m-2}(G)$, S is of order p^{n-m+2}. S is of class 2, since $[T, T] \leqslant \gamma_{m-1}(G)$.

Corollary 2. *Under the same conditions the conjugacy class of G containing s is the coset $s\gamma_2(G)$.*

For by Corollary 1 s has p^{m-2} distinct conjugates in G. Since $s^x = s[s, x]$ for any element x of G, each of these conjugates is of the form sy where $y \in \gamma_2(G)$. And since $\gamma_2(G)$ has just p^{m-2} elements, it follows that each element of this form must be a conjugate of s.

Theorem 2.16. *Suppose that $G \in \mathrm{CF}(m, n, p)$ $(m > 3)$, and that r is the smallest positive integer such that there exists an element s of G, not belonging to $\gamma_1(G)$, for which s^{p^r} lies in $\gamma_2(G)$. Then $\gamma_2(G)$ can be generated by fewer than p^r elements.*

Suppose that this is not true. Then the index of the Frattini subgroup $\Phi(\gamma_2(G))$ of $\gamma_2(G)$ in $\gamma_2(G)$ is at least p^{p^r}, and so there exists a normal subgroup N of G, such that $\Phi(\gamma_2(G)) \leqslant N < \gamma_2(G)$, and $\gamma_2(G)/N$ is elementary Abelian of order p^{p^r}. By considering G/N we see that without loss of generality, it may be assumed that $\gamma_2(G)$ is an elementary Abelian group of order p^{p^r}, for by Lemma 2.3 $G/N \in \mathrm{CF}(p^r + 2, n', p)$ for some n'. By Theorem 2.10, Corollary, G has degree of commutativity greater than 0. Hence Lemma 2.14 may be applied, and since $s^{p^r} \in S \cap \gamma_2(G)$, it follows that $s^{p^r} \in \gamma_{m-1}(G)$.

If s_1 is an element which together with $\zeta_{m-2}(G)$ generates $\gamma_1(G)$, we define $s_i = \sigma_i(s, s_1)$ $(i = 2, 3, \ldots, m-1)$, so that as in Lemma 2.9, s_i and $\gamma_{i+1}(G)$ generate $\gamma_i(G)$ $(i = 2, 3, \ldots, m-1)$. We prove by induction on k that

$$s_1^{s^k} = s_1 s_2^k s_3^{\binom{k}{2}} \cdots s_i^{\binom{k}{i-1}} \cdots s_{k+1} \quad (k = 1, 2, \cdots, m-2).$$

For $k = 1$ this is clear; for $k > 1$ we assume the corresponding result for $k-1$ and transform by s, using $s_i^s = s_i s_{i+1}$. Since $\gamma_2(G)$ is Abelian, we may deduce the stated result at once. Putting $k = p^r = m-2$, and using the fact that $\gamma_2(G)$ is of exponent p, we obtain

$$s_1^{s^{p^r}} = s_1 s_{m-1}.$$

Thus s^{p^r} cannot belong to the centre of G. But we have shown that $s^{p^r} \in \gamma_{m-1}(G)$ and so we have a contradiction. Thus Theorem 2.16 is proved.

It is very easy to show that Theorem 2.16 is the best possible result. Thus let E be an elementary Abelian group of order p^{p^r} generated by elements $s_1, s_2, \dots, s_{p^r}$. Let σ be the automorphism of E defined by $s_i^\sigma = s_i s_{i+1}$ $(i = 1, 2, \dots, p^r - 1)$ and $s_{p^r}^\sigma = s_{p^r}$. Then σ is of order p^r and we may form an extension G of E, such that G/E is cyclic of order p^r and an element s of G induces the automorphism σ in E. Then $G \in \mathrm{CF}(p^r + 1, 2r, p)$, and $\gamma_2(G)$ cannot be generated by fewer than $p^r - 1$ elements. It is to be observed that in the case $r = 1$ the group that we have constructed is the Sylow p-subgroup of the symmetric group of degree p^2.

We mention two particular cases of Theorem 2.16.

Corollary 1. *If $G \in \mathrm{CF}(m, n, 2)$, and there exists an element s of G which does not belong to $\gamma_1(G)$, such that $s^2 \in \gamma_2(G)$, then $\gamma_2(G)$ is cyclic.*

Corollary 2. *If $G \in \mathrm{CF}(m, n, 3)$, and there exists an element s of G which does not belong to $\gamma_1(G)$, such that $s^3 \in \gamma_2(G)$, then $\gamma_2(G)$ is an Abelian group with at most two generators.*

The first corollary is obvious. To prove the second we observe first that $\gamma_2(G)$ can be generated by 2 elements, by Theorem 2.16. It follows that $[\gamma_2(G), \gamma_3(G)] = 1$ (see [1], Theorem 2). Since $\gamma_2(G)/\gamma_3(G)$ is cyclic, it follows from Lemma 2.1 that $\gamma_2(G)$ is Abelian.

3. The corollaries of Theorem 2.16 suggest that far deeper results will be obtainable if some condition is imposed on $G/\gamma_2(G)$, and we shall therefore assume henceforth that this group is elementary Abelian, that is, that $G \in \mathrm{ECF}(m, n, p)$. For $m > 3$ such a group always possesses a subgroup of order p^m and class $m - 1$ with the same lower central series as G. For by the results of the previous paragraph G can be generated by two elements x, y and $\eta(G)$. Thus, if H is the group generated by x, y, $H\eta(G) = G$, and so by Theorem 1.3, $\gamma_i(H) = \gamma_i(G)$. By hypothesis, x^p, y^p are elements of $\gamma_2(G) = \gamma_2(H)$, and so H is of order p^m, as required. Thus the study of the groups of $\mathrm{ECF}(m, n, p)$ reduces essentially to that of p-groups of maximal class, at least so far as the properties of the lower central series are concerned. The following lemma shows that the groups of ECF (m, n, p) possess other subgroups which are p-groups of maximal class.

Lemma 3.1. *Suppose that $G \in \mathrm{ECF}(m, n, p)$ $(m > 3)$ and that, when $m > 5$, $G/\gamma_{m-1}(G)$ has degree of commutativity greater than 0. Then G possesses a subgroup K which is of order $p^{m-1}$and class $m - 2$, and $\gamma_i(K) = \gamma_{i+1}(G)$ $(i = 1, 2, \dots, m - 2)$.*

One of our principal aims is to prove that if $G \in \mathrm{ECF}(m, n, p)$ and $m > p + 1$, then G has degree of commutativity greater than 0 (Theorem 3.8). This will be proved by induction on m and so, in Lemma 3.1 and a number of the following results, we shall work under the hypothesis that $G/\gamma_{m-1}(G)$ has degree of commutativity greater than 0. This hypothesis is of course shown to be unnecessary by Theorems 2.11 and 3.8. In such a group our notation will be as follows. s denotes an element which belongs neither to $\gamma_1(G)$ nor to the centraliser of $\gamma_{m-2}(G)$. s_1 denotes an element which belongs to $\gamma_1(G)$ but not to $\zeta_{m-2}(G)$. For $i = 2, 3, \ldots, m-1$ we write $s_i = \sigma_i(s, s_1)$. By Lemma 2.9 s_i and $\gamma_{i+1}(G)$ generate $\gamma_i(G)$ if $2 \leqslant i \leqslant m-2$. This is also true if $i = m-1$. For s_{m-2} and $\gamma_{m-1}(G)$ generate $\gamma_{m-2}(G)$, and s commutes with every element of $\gamma_{m-1}(G)$ but does not belong to the centraliser of $\gamma_{m-2}(G)$: thus s and s_{m-2} do not commute, that is, $s_{m-1} \neq 1$. It is also important to observe that $s^p \in \gamma_{m-1}(G)$. For since $G/\gamma_2(G)$ is elementary Abelian, $s^p \in \gamma_2(G)$; also s^p certainly belongs to the centraliser of s, and so by Lemma 2.14, $s^p \in \gamma_{m-1}(G)$.

To prove Lemma 3.1 we define K to be the group generated by s and $\gamma_2(G)$. Since $\gamma_2(G)$ is of order p^{m-2} and $s^p \in \gamma_{m-1}(G) \leqslant \gamma_2(G)$, K is of order p^{m-1}. Also s_2 and s are both elements of K and $\sigma_{m-2}(s, s_2) = s_{m-1} \neq 1$; thus K has class at least $m-2$. Since $m-2$ is the maximal class of a group of order p^{m-1}, K is a p-group of maximal class and $\gamma_i(K)$ is of order p^{m-i-1} $(i = 1, 2, \ldots, m-2)$. Since $K \geqslant \gamma_2(G)$, K is a normal subgroup of G, and so $\gamma_i(K)$ is normal in G. For $i \geqslant 2$ $\gamma_i(K) \leqslant \gamma_2(G)$, and so by Lemma 2.3, $\gamma_i(K) = \gamma_{i+1}(G)$. Also

$$[\gamma_2(G), \gamma_2(K)] = [\gamma_2(G), \gamma_3(G)] \leqslant \gamma_5(G) = \gamma_4(K),$$

and so $\gamma_2(G) \leqslant \gamma_1(K)$. But these groups have the same order, and are therefore equal: thus the result is proved.

We observe that any such subgroup K has degree of commutativity greater than 0, for

$$[\gamma_i(K), \gamma_j(K)] = [\gamma_{i+1}(G), \gamma_{j+1}(G)] \leqslant \gamma_{i+j+2}(G) = \gamma_{i+j+1}(K).$$

It is also to be observed that by repeated application of Lemma 3.1, if $2 \leqslant r \leqslant m-3$, we can construct a subgroup L of G of order p^{m-r+1} and class $m-r$, with degree of commutativity $r-1$, such that $\gamma_j(L) = \gamma_{r+j-1}(G)$ $(j = 1, 2, \ldots, m-r)$. This result is due to Wiman ([12], § 4).

Our next aim is to investigate the "power-structure" of the groups of ECF(m, n, p). For small values of m, we obtain the following result.

Theorem 3.2. *Suppose that $G \in$ ECF(m, n, p), where p is odd and $4 \leqslant m \leqslant p+1$. Then $G/\gamma_{m-1}(G)$ and $\gamma_2(G)$ are of exponent p. If $m \leqslant p$, the elements of G of order at most p form a characteristic subgroup of index at most p.*

By Theorem 2.11 $G/\gamma_{m-1}(G)$ has degree of commutativity greater than 0, and so there are at most 2 maximal subgroups of G which can be centralisers of the groups $\gamma_i(G)/\gamma_{i+2}(G)$ $(i = 2, 3, \ldots, m-2)$. G has $p+1$ maximal subgroups containing $\zeta_{m-2}(G)$, and so, since p is odd, we may select two such subgroups, neither of which is the centraliser of any $\gamma_i(G)/\gamma_{i+2}(G)$. Let s, s' be elements which together with $\zeta_{m-2}(G)$ generate these two subgroups: then G is generated by s, s' and $\zeta_{m-2}(G)$. Let S, T be defined as in Theorem 2.15. Thus G is generated by s, s', T and $\gamma_2(G)$, and it follows that G is generated by s, s' and T. Now s^p and, for each $t \in T$, t^p are elements of $S \cap \gamma_2(G)$, since $G/\gamma_2(G)$ is elementary Abelian. Hence by Lemma 2.14 s^p and t^p lie in $\gamma_{m-1}(G)$. Similarly, by considering the centraliser of s', s'^p lies in $\gamma_{m-1}(G)$. Hence $G/\gamma_{m-1}(G)$ is generated by a set of elements of order p. But $G/\gamma_{m-1}(G)$ is a regular p-group, since the class of this group is $m-2$, which is less than p (see [3], Corollary 4.13, p. 73). Hence $G/\gamma_{m-1}(G)$ is of exponent p (see [3], Theorem 4.26, p. 76).

For $m \leqslant p$ G is itself a regular p-group, since the class of G is less than p. It follows that the elements of G of order at most p form a subgroup E_1, the index of which in G is equal to the order of $P_1(G)$. But since $G/\gamma_{m-1}(G)$ is of exponent p, $P_1(G) \leqslant \gamma_{m-1}(G)$, and so E_1 is of index at most p in G. It follows that $\gamma_2(G) \leqslant E_1$, and so $\gamma_2(G)$ is of exponent p.

For $m = p+1$ we observe that by Theorem 2.6 $\gamma_2(\gamma_1(G)) \leqslant \gamma_3(G)$. It follows that $\gamma_i(\gamma_1(G)) \leqslant \gamma_{i+1}(G)$ by induction on i. Hence $\gamma_p(\gamma_1(G)) = 1$, and so $\gamma_1(G)$ is regular. Thus the elements of $\gamma_1(G)$ of order at most p form a subgroup F of index the order of $P_1(\gamma_1(G))$. But $P_1(\gamma_1(G)) \leqslant P_1(G) \leqslant \gamma_{m-1}(G)$, and so F is of index at most p in $\gamma_1(G)$, and at most p^2 in G. Thus G/F is Abelian, and so $\gamma_2(G) \leqslant F$. Hence $\gamma_2(G)$ is of exponent p.

The investigation of the power-structure in the case $m > p+1$ rests upon the following result.

LEMMA 3.3. *If $G \in \mathrm{ECF}(m, n, p)$ $(m > p+1)$, then $s_1{}^p s_p$ lies in $\gamma_{p+1}(G)$.*

Here we need not assume that $G/\gamma_{m-1}(G)$ has degree of commutativity greater than 0, for the lemma is essentially a result about $G/\gamma_{p+2}(G)$, and by Theorem 2.11 this group has degree of commutativity greater than 0. It is on the basis of this fact that we may use the notation described, so far as $s, s_1, s_2, \ldots, s_p$ are concerned.

For p odd we apply Theorem 1.6 to calculate $(ss_1)^p$. Since the group generated by s_1 and $\gamma_2(G)$ is contained in $\gamma_1(G)$, this yields

$$(ss_1)^p \equiv s^p s_1{}^p \ldots s_i^{\binom{p}{i}} \ldots s_p \pmod{P_1(\gamma_2(G)) \prod_{i=1}^{p-2} [\gamma_i(G), \gamma_{p-i}(G)]}.$$

Since $G/\gamma_{p+2}(G)$ has degree of commutativity greater than 0,

$$[\gamma_i(G), \gamma_{p-i}(G)] \leqslant \gamma_{p+1}(G) \quad (i = 1, 2, \ldots, p-2).$$

Also, by applying Theorem 3.2 to $G/\gamma_{p+1}(G)$, we see that $P_1(\gamma_2(G)) \leqslant \gamma_{p+1}(G)$.

Thus
$$(ss_1)^p \equiv s^p s_1{}^p \ldots s_i^{\binom{p}{i}} \ldots s_p \pmod{\gamma_{p+1}(G)}.$$

This is also true for $p = 2$, for

$$(ss_1)^2 = s^2 s_1{}^2 s_2 [s_2, s_1].$$

Now s and ss_1 are both elements of G which do not lie in $\gamma_1(G)$, and so, by an above remark applied to $G/\gamma_{p+2}(G)$, s^p and $(ss_1)^p$ lie in $\gamma_{p+1}(G)$. Also, for $i = 2, 3, \ldots, p-1$, $s_i^{\binom{p}{i}} \in P_1(\gamma_2(G)) \leqslant \gamma_{p+1}(G)$. Hence the equation reduces to

$$s_1{}^p s_p \equiv 1 \pmod{\gamma_{p+1}(G)},$$

as required.

Lemma 3.3 is not necessarily true if $m = p + 1$, as the Sylow p-subgroup of the symmetric group of degree p^2 shows (see below).

We deduce now a result on the power-structure which is most conveniently stated for p-groups of maximal class.

THEOREM 3.4. *If G is a group of order p^m and class $m - 1$, where $m > 3$, then $\gamma_1(G)$ is a regular p-group. If $m > p + 1$, and for each $i = 1, 2, \ldots, m - p + 1$, we write*

$$m - i = (p - 1)q_i + r_i \quad (0 \leqslant r_i < p - 1),$$

then $\gamma_i(G)$ has r_i invariants equal to $q_i + 1$, and $p - r_i - 1$ invariants equal to q_i.

Again the second sentence of this theorem is not true if $m = p + 1$. For if p is odd and G is the Sylow p-subgroup of the symmetric group of degree p^2, then $\gamma_1(G)$ is an elementary Abelian group of order p^p, as may be seen from the defining relations given for this group in § 2. Thus $\gamma_1(G)$ has p invariants, all of which are equal to 1. Thus Theorem 3.4 shows that *if p is odd, the Sylow p-subgroup of the symmetric group of degree p^2 cannot be a factor group of a p-group of maximal class of order greater than p^{p+1}*. In contrast, the Sylow 2-subgroup of the symmetric group of degree 4 (that is, the dihedral group of order 8) is always a factor group of a 2-group of maximal class of order greater than 8.

To prove Theorem 3.4 we observe first that since any p-group of order less than p^{p+1} is regular, it is clear that $\gamma_1(G)$ is regular if $m \leqslant p + 1$. For $m > p + 1$ we consider $P_1(\gamma_1(G))$, which is a characteristic subgroup of G. By Lemma 2.2 $P_1(\gamma_1(G)) = \gamma_\lambda(G)$, for some λ. By Theorem 3.2 applied to $G/\gamma_{p+1}(G)$, $P_1(\gamma_1(G)) \leqslant \gamma_p(G)$, or $\lambda \geqslant p$. But by Lemma 3.3 s_1^p does not belong to $\gamma_{p+1}(G)$, and so λ cannot be greater than p, for $s_1^p \in P_1(\gamma_1(G))$. Thus $\lambda = p$, and $P_1(\gamma_1(G)) = \gamma_p(G)$. Hence $P_1(\gamma_1(G))$ is of index p^{p-1} in $\gamma_1(G)$, and so $\gamma_1(G)$ is regular (see [4], Theorem 2.3, p. 477).

If X is any regular p-group, we denote by $E_i(X)$ the subgroup of X consisting of all elements of X of order at most p^i; thus

$$(E_i(X) : 1) = (X : P_i(X)).$$

If $p \leqslant j \leqslant m$, we apply this equality with $i = 1$ to the group $\gamma_1(G)/\gamma_j(G)$. Thus

$$(E_1(\gamma_1(G)/\gamma_j(G)):1) = (\gamma_1(G):\gamma_p(G)) = p^{p-1}.$$

Hence by applying Lemma 2.2 to $\gamma_1(G)/\gamma_j(G)$

$$E_1(\gamma_1(G)/\gamma_j(G)) = \gamma_{j-p+1}(G)/\gamma_j(G)$$

We deduce by induction on i that if $m-1 \geqslant i(p-1)$,

$$E_i(\gamma_1(G)) = \gamma_{m-i(p-1)}(G). \tag{15}$$

For $i = 1$, this follows at once by putting $j = m$. For $i > 1$, we need only observe that

$$\begin{aligned} E_i(\gamma_1(G))/E_{i-1}(\gamma_1(G)) &= E_1(\gamma_1(G)/E_{i-1}(\gamma_1(G))) \\ &= E_1(\gamma_1(G)/\gamma_{m-(i-1)(p-1)}(G)) \\ &= \gamma_{m-i(p-1)}(G)/E_{i-1}(\gamma_1(G)). \end{aligned}$$

If $i(p-1) \geqslant m$, then $E_i(\gamma_1(G)) = \gamma_1(G)$, as is seen by the same argument, using the fact that $\gamma_1(G)/\gamma_p(G)$ is of exponent p.

It follows from (15) that if $1 \leqslant j \leqslant m - i(p-1)$, then $\gamma_j(G) \geqslant E_i(\gamma_1(G))$, and so $E_i(\gamma_j(G)) = \gamma_{m-i(p-1)}(G)$, for $i = 1, 2, \ldots, q_j$. Again $E_{q_j+1}(\gamma_j(G)) = \gamma_j(G)$. Thus $(E_k(\gamma_j(G))$: $E_{k-1}(\gamma_j(G))) = p^{p-1}$ $(k = 1, 2, \ldots, q_j)$, whilst $(\gamma_j(G)$: $E_{q_j}(\gamma_j(G))) = p^{r_j}$. These indices give rise to the partition $((p-1)^{q_j}, r_j)$ of $m-j$. The invariants of $\gamma_j(G)$ are the parts of the conjugate partition, which are as stated.

COROLLARY 1. *If* $G \in \mathrm{ECF}(m, n, p)$ $(m > p+1)$, *then* $P_1(\gamma_j(G)) = \gamma_{j+p-1}(G)$, *for* $j = 1, 2, \ldots, m-p+1$.

As remarked at the beginning of this paragraph G possesses a subgroup H, such that H is a p-group of maximal class and $\gamma_i(H) = \gamma_i(G)$ $(i = 2, 3, \ldots, m-1)$. It follows from Theorem 3.4 that for $j = 1, 2, \ldots, m-p+1$, $\gamma_j(H)$ has $p-1$ invariants: thus $P_1(\gamma_j(H))$ is a characteristic subgroup of H of order $p^{m-j-p+1}$, and so $P_1(\gamma_j(H)) = \gamma_{j+p-1}(H)$, by Lemma 2.2. This gives the result at once if $j > 1$. For $j = 1$ we observe that

$$[\gamma_1(H), \gamma_2(G)] = [\gamma_1(H), \gamma_2(H)] \leqslant \gamma_4(H) = \gamma_4(G),$$

and so $\gamma_1(H) \leqslant \gamma_1(G)$. Hence $P_1(\gamma_1(G)) \geqslant P_1(\gamma_1(H)) = \gamma_p(H) = \gamma_p(G)$. But for p odd, we can apply Theorem 3.2 to $G/\gamma_{p+1}(G)$, and so $P_1(\gamma_1(G)) \leqslant \gamma_p(G)$; this is also true for $p = 2$, since $G/\gamma_2(G)$ is elementary Abelian. Hence $P_1(\gamma_1(G)) = \gamma_p(G)$, as required.

COROLLARY 2. *If* $G \in \mathrm{ECF}(m, n, p)$ $(m > p+1)$ and $G/\gamma_{m-1}(G)$ *has degree of commutativity greater than* 0, *then* $s_i^p s_{i+p-1} \in \gamma_{i+p}(G)$ $(i = 2, 3, \ldots, m-p)$.

Without loss of generality it may be assumed that G is a p-group of maximal class. By Lemma 3.3 the result holds for $i = 1$, and so we may use induction on i. By the inductive hypothesis $s_{i-1}^{p} s_{i+p-2} \in \gamma_{i+p-1}(G)$, and so

$$[s_{i-1}^{p}\, s_{i+p-2},\, s] \in \gamma_{i+p}(G).$$

This commutator is

$$s_{i+p-2}^{-1}\, s_{i-1}^{-p}\, (s_{i-1}^{s})^{p}\, s_{i+p-2}^{s} = s_{i+p-2}^{-1}\, s_{i-1}^{-p}\, (s_{i-1}\, s_{i})^{p}\, s_{i+p-2}\, s_{i+p-1}.$$

By Theorem 3.4 $\gamma_1(G)$ is regular, and so if H is the group generated by s_{i-1} and s_i,

$$(s_{i-1}\, s_i)^p \equiv s_{i-1}^{p}\, s_i^{p} \pmod{P_1(H')}.$$

Now $H \leqslant \gamma_{i-1}(G)$, and since $\gamma_{i-1}(G)/\gamma_{i+1}(G)$, being of order p^2, is Abelian, $H' \leqslant \gamma_{i+1}(G)$. Hence by Theorem 3.4 $P_1(H') \leqslant \gamma_{i+p}(G)$, and we obtain

$$s_{i+p-2}^{-1}\, s_i^{p}\, s_{i+p-2}\, s_{i+p-1} \equiv 1 \pmod{\gamma_{i+p}(G)}.$$

Also by Theorem 3.4 $s_i^p \in \gamma_{i+p-1}(G)$, and so s_i^p lies in the centre of G modulo $\gamma_{i+p}(G)$. Hence it commutes with s_{i+p-2}, and so the result follows.

We shall now investigate more closely the commutator-structure of the groups of ECF(m, n, p). We begin with the following lemma.

LEMMA 3.5. *Suppose that* $G \in \mathrm{CF}(m, n, p)$ $(m > 4)$, *that* $G/\gamma_{m-1}(G)$ *has degree of commutativity greater than* 0 *and that* G *has degree of commutativity* $k \geqslant 0$. *If*

$$[s_i, s_j] \equiv s_{i+j+k}^{\alpha_{ij}} \pmod{\gamma_{i+j+k+1}(G)} \quad (1 \leqslant i < j,\ i + j \leqslant m - k - 1),$$

then
$$\alpha_{i\,i+2} \equiv \alpha_{i\,i+1} \pmod{p} \quad (1 \leqslant i \leqslant [\tfrac{1}{2}(m - k - 3)]),$$

and
$$\alpha_{i\,j+1} + \alpha_{i+1\,j} \equiv \alpha_{ij} \pmod{p} \quad (1 \leqslant i \leqslant j - 2,\ i + j \leqslant m - k - 2).$$

(If x is any number, we denote by $[x]$ the greatest integer not greater than x, as usual.)

The hypothesis that $G/\gamma_{m-1}(G)$ has degree of commutativity greater than 0 is of course only necessary when $k = 0$, and in that case ensures that we may use the notation described.

To prove Lemma 3.5, we observe that for $1 \leqslant i < j$ and $i + j \leqslant m - k - 2$

$$[s_{i+1}, s_j] = s_{i+1}^{-1}\, s_{i+1}^{s_j} = s_{i+1}^{-1}\, [s_i, s]^{s_j} = s_{i+1}^{-1}\, [s_i^{s_j}, s^{s_j}].$$

Hence
$$[s_{i+1}, s_j] = s_{i+1}^{-1}\, [s_i\, s_{i+j+k}^{\alpha_{ij}},\, s s_{j+1}^{-1}] \pmod{\gamma_{i+j+k+2}(G)}.$$

We calculate the right-hand side by means of (1) and (2). Thus we have

$$[s_i\, s^{\alpha_{ij}}_{i+j+k},\, s\, s^{-1}_{j+1}] = [s_i\, s^{\alpha_{ij}}_{i+j+k},\, s^{-1}_{j+1}]\, [s_i\, s^{\alpha_{ij}}_{i+j+k},\, s]^{s^{-1}_{j+1}},$$

$$[s_i\, s^{\alpha_{ij}}_{i+j+k},\, s^{-1}_{j+1}] = [s_i, s^{-1}_{j+1}]^{s^{\alpha_{ij}}_{i+j+k}} [s^{\alpha_{ij}}_{i+j+k},\, s^{-1}_{j+1}],$$

$$[s_i\, s^{\alpha_{ij}}_{i+j+k},\, s] = [s_i, s]^{s^{\alpha_{ij}}_{i+j+k}}\, [s^{\alpha_{ij}}_{i+j+k},\, s].$$

Also $$[s_i,\, s^{-1}_{j+1}] = [s_i,\, s_{j+1}]^{-s^{-1}_{j+1}} \equiv s^{-\alpha_{ij+1}}_{i+j+k+1} \quad (\text{mod } \gamma_{i+j+k+2}(G)).$$

Thus $$[s_i\, s^{\alpha_{ij}}_{i+j+k},\, s^{-1}_{j+1}] \equiv s^{-\alpha_{ij+1}}_{i+j+k+1} \quad (\text{mod } \gamma_{i+j+k+2}(G)).$$

Again $$[s_i,\, s]^{s^{\alpha_{ij}}_{i+j+k}} = s_{i+1}\, [s_{i+1},\, s^{\alpha_{ij}}_{i+j+k}] \equiv\equiv s_{i+1} \quad (\text{mod } \gamma_{i+j+k+2}(G)),$$

and so by Theorem 1.4,

$$[s_i\, s^{\alpha_{ij}}_{i+j+k},\, s] \equiv s_{i+1}\, s^{\alpha_{ij}}_{i+j+k+1} \quad (\text{mod } \gamma_{i+j+k+2}(G)).$$

Hence $$[s_{i+1},\, s_j] \equiv s^{\alpha_{ij}-\alpha_{ij+1}}_{i+j+k+1} \quad (\text{mod } \gamma_{i+j+k+2}(G)).$$

This reduces to the result stated, whether $j = i + 1$ or $j > i + 1$.

The next lemma is of a similar nature, but uses the p-th power relationships that we have found.

LEMMMA 3.6. *Suppose that $G \in \mathrm{ECF}(m, n, p)$ $(m > p + 1)$, that $G/\gamma_{m-1}(G)$ has degree of commutativity greater than 0 and that G has degree of commutativity $k \geqslant 0$. Then $[s_1, s_p] \in \gamma_{p+k+2}(G)$, and if for $i = 2, 3, \ldots, m - k - p - 1$,*

$$[s_1,\, s_i] \equiv s^{\alpha_i}_{i+k+1} \quad (\text{mod } \gamma_{i+k+2}\, (G)),$$

then $$[s_p,\, s_i] \equiv s^{\alpha_i}_{i+k+p} \quad (\text{mod } \gamma_{i+k+p+1}(G)).$$

By Lemma 3.3 $s_1^p s_p$ is an element of $\gamma_{p+1}(G)$, and so for $i = 1, 2, \ldots, m - k - p - 1$,

$$[s_i,\, s_1^p s_p] \in [\gamma_i(G), \gamma_{p+1}(G)] \leqslant \gamma_{i+p+k+1}(G).$$

Thus by (1) $$[s_i,\, s_p] \equiv [s_1^p,\, s_i]^{s_p} \quad (\text{mod } \gamma_{i+p+k+1}(G)). \tag{16}$$

With $i = 1$ this gives $[s_1, s_p] \in \gamma_{p+k+2}(G)$, as required. For $i > 1$ we write

$$[s_1,\, s_i] = s^{\alpha_i}_{i+k+1}\, x,$$

so that $x \in \gamma_{i+k+2}(G)$. Hence by Theorem 3.4, Corollary 1, $x^p \in \gamma_{i+k+p+1}(G)$. Now

$$[s_1^p, s_i] = s_1^{-p}(s_1^{s_i})^p = s_1^{-p}(s_1 s_{i+k+1}^{\alpha_i} x)^p. \tag{17}$$

Let L be the group generated by s_1 and $\gamma_{i+k+1}(G)$, and let H be the group generated by s and s_1. By the argument at the beginning of this paragraph H is a p-group of maximal class, and $\gamma_i(H) = \gamma_i(G)$ $(i = 2, 3, \ldots, m-1)$. Clearly $s_1 \in \gamma_1(H)$, and so $L \leqslant \gamma_1(H)$. By Theorem 3.4 it follows that L is regular. Hence

$$(s_1 s_{i+k+1}^{\alpha_i} x)^p \equiv s_1^p s_{i+k+1}^{p\alpha_i} x^p \pmod{P_1(L')}.$$

By Lemma 2.1

$$L' = [L, \gamma_{i+k+1}(G)] \leqslant \gamma_{i+k+2}(G),$$

and so by Theorem 3.4, Corollary 1,

$$P_1(L') \leqslant \gamma_{i+k+p+1}(G).$$

Thus
$$(s_1 s_{i+k+1}^{\alpha_i} x)^p \equiv s_1^p s_{i+k+1}^{p\alpha_i} \pmod{\gamma_{i+k+p+1}(G)}.$$

But by Theorem 3.4, Corollary 2,

$$s_{i+k+1}^p \equiv s_{i+k+p}^{-1} \pmod{\gamma_{i+k+p+1}(G)},$$

and so
$$s_1^{-p}(s_1 s_{i+k+1}^{\alpha_i} x)^p \equiv s_{i+k+p}^{-\alpha_i} \pmod{\gamma_{i+k+p+1}(G)}.$$

Hence by (16) and (17)

$$[s_p, s_i] \equiv s_{i+k+p}^{\alpha_i} \pmod{\gamma_{i+k+p+1}(G)},$$

as required.

This brings us to the key lemma.

Lemma 3.7. *Suppose that $G \in \mathrm{ECF}(m, n, p)$ $(m > p+2)$, that $G/\gamma_{m-1}(G)$ has degree of commutativity k, where $1 \leqslant k \leqslant m-p-2$, and that*

$$[\gamma_i(G), \gamma_{m-k-i+1}(G)] = 1 \quad (i = 2, 3, \ldots, m-k-1). \tag{18}$$

Then G has degree of commutativity k.

Since it is assumed that $G/\gamma_{m-1}(G)$ has degree of commutativity k, it is only necessary to prove that

$$[\gamma_i(G), \gamma_{m-k-i}(G)] = 1 \quad (i = 1, 2, \ldots, m-k-1). \tag{19}$$

We begin by showing that (18) is true with $i = 1$, that is,

$$[\gamma_1(G), \gamma_{m-k}(G)] = 1. \tag{20}$$

For $i = m-k, m-k+1, \ldots, m-1$,

$$[s_1, s_i] = s_i^{-s_1} s_i = [s, s_{i-1}]^{s_1} s_i = [s^{s_1}, s_{i-1}^{s_1}] s_i = [s s_2^{-1}, s_{i-1}[s_{i-1}, s_1]] s_i.$$

But $[s_{i-1}, s_1] \in [\gamma_{m-k-2}(G), \gamma_1(G)]$, and by hypothesis this group is contained in $\gamma_{m-1}(G)$. Hence

$$[s_1, s_i] = [s s_2^{-1}, s_{i-1}] s_i = s_i^{-s_2^{-1}} [s_2^{-1}, s_{i-1}] s_i.$$

But $[s_2, s_i]$ and $[s_2, s_{i-1}]$ are both elements of $[\gamma_2(G), \gamma_{m-k-1}(G)]$, and by (18) this group is the unit subgroup. Hence $[s_1, s_i] = 1$, or, s_1 commutes with each of the elements s_{m-k}, $s_{m-k+1}, \ldots, s_{m-1}$. Thus s_1 is contained in the centraliser of $\gamma_{m-k}(G)$. Now s_1 was defined to be any element of $\gamma_1(G)$ which does not belong to $\zeta_{m-2}(G)$. Thus if $y \in \zeta_{m-2}(G)$, we could use $s_1 y$ instead of s_1, and prove the same. Hence $s_1 y$ and therefore y itself belong to the centraliser of $\gamma_{m-k}(G)$. Hence all elements of $\gamma_1(G)$ belong to this centraliser, and (20) is proved. It is to be observed that (18), (20) and the hypothesis on $G/\gamma_{m-1}(G)$ imply that G has degree of commutativity $k-1$.

To improve this to k we define T as in Theorem 2.15 and observe that for $t \in T$

$$[t, s_{m-k-1}] = s_{m-k-1}^{-t} s_{m-k-1} = [s, s_{m-k-2}]^t s_{m-k-1} = [s^t, s_{m-k-2}^t] s_{m-k-1}.$$

By the definition of T $s^t = s$, and

$$[s_{m-k-2}, t] \in [\gamma_{m-k-2}(G), \gamma_1(G)] \leqslant \gamma_{m-1}(G).$$

Hence $[t, s_{m-k-1}] = 1$. It follows that in order to prove (19) it is sufficient to prove that

$$[s_i, s_{m-k-i}] = 1 \quad (i = 1, 2, \ldots, m-k-1),$$

on account of (18). We already have $[s_i, s_{m-k-i}] \in \gamma_{m-1}(G)$, since G has degree of commutativity $k-1$, and we can therefore write

$$[s_i, s_{m-k-i}] = s_{m-1}^{\alpha_i} \quad (i = 1, 2, \ldots, m-k-1).$$

We now apply Lemma 3.5 and find that

$$\alpha_1 \equiv -\alpha_2 \equiv \alpha_3 \equiv \ldots \equiv (-1)^{m-k} \alpha_{m-k-1} \pmod p,$$

since $G/\gamma_{m-1}(G)$ has degree of commutativity k. Also we apply Lemma 3.6 and find that since $[s_1, s_{m-p-k}] \in \gamma_{m-p+1}(G)$, it follows that $[s_p, s_{m-k-p}] = 1$, and so $\alpha_p \equiv 0 \pmod p$. Hence $\alpha_i \equiv 0 \pmod p$, and

$$[s_i, s_{m-k-i}] = 1 \quad (i = 1, 2, \ldots, m-k-1),$$

as required.

THEOREM 3.8. *If $G \in \mathrm{ECF}(m, n, p)$ $(m \geqslant p+2)$, then G has degree of commutativity greater than* 0.

This is already known for $m = p+2$, (or, if $p = 2$, for $m = 5$), on account of Theorem 2.11. For greater values of m we use induction on m. Thus $G/\gamma_{m-1}(G)$ has degree of commutativity 1, and since $m \geqslant p+3$ and

$$[\gamma_i(G), \gamma_{m-i}(G)] = 1 \quad (i = 2, 3, \ldots, m-2),$$

we may apply Lemma 3.7 with $k = 1$. Thus the result follows at once.

Analogous to Theorem 2.12 we deduce the following consequence of Theorem 3.8.

THEOREM 3.9. *Let G be a p-group of class at least $p+1$, and suppose that $G/\gamma_{p+1}(G) \in \mathrm{ECF}(p+1, n, p)$. Then $G \in \mathrm{ECF}(m, n', p)$, for some m, n'.*

Let $m-1$ be the class of G. For p odd we proceed by induction on m: thus $G/\gamma_{m-1}(G) \in \mathrm{ECF}(m-1, n'', p)$ by hypothesis if $m = p+2$ and by the inductive hypothesis if $m > p+2$. The result is obtained by an exact repetition of the argument used to prove Theorem 2.12.

For $p = 2$ this argument does not quite suffice, and instead we prove that the hypothesis of Theorem 3.9 implies that $\gamma_2(G)$ is cyclic. If this were not so, then the Frattini subgroup $\Phi(\gamma_2(G))$ of $\gamma_2(G)$ is of index at least 4 in $\gamma_2(G)$. By hypothesis $\gamma_3(G)$ is a maximal subgroup of $\gamma_2(G)$, and so $\Phi(\gamma_2(G)) < \gamma_3(G)$. Hence there exists a normal subgroup N of G such that $\Phi(\gamma_2(G)) \leqslant N < \gamma_3(G)$, and $\gamma_2(G)/N$ is of order 4. It follows that $\gamma_2(G)/N$ is elementary Abelian and that $G/N \in \mathrm{ECF}(4, n, 2)$. But this implies by Theorem 2.16, Corollary 1 that $\gamma_2(G)/N$ is cyclic, which gives us a contradiction. Hence $\gamma_2(G)$ is cyclic, and each of the groups $\gamma_{i-1}(G)/\gamma_i(G)$ $(i = 3, 4, \ldots, m)$ is cyclic. But by Theorem 1.5 (i) and (ii), each of these groups is also elementary Abelian, and so is of order 2, as required.

COROLLARY. *If G is a 2-group, and $G/\gamma_2(G)$ is of order 4, then G is a 2-group of maximal class, and $\gamma_1(G)$ is cyclic.*

If G is non-Abelian it follows from Theorem 1.5 (i) that $\gamma_2(G)/\gamma_3(G)$ is of order 2, and so we may apply Theorem 3.9. Hence G is a 2-group of maximal class, and by Theorem 3.4 $\gamma_1(G)$ is cyclic. All 2-groups of maximal class have of course been known for a long time, and very simple direct proofs that $\gamma_1(G)$ is cyclic can be given (see [10], page 121).

We see from Theorem 2.10 that if $G \in \mathrm{ECF}(m, n, p)$ and $6 \leqslant m \leqslant p+1$, then G fails to have degree of commutativity 1 if and only if the maximal Abelian normal subgroup of G contained in $\gamma_2(G)$ is $\gamma_{[\frac{1}{2}(m+1)]}(G)$. We now propose to examine the properties of the lower central series of G under the hypothesis that a given term of this series is Abelian.

Suppose first that G is a metabelian p-group of maximal class of order p^m. By Theorem 2.10, Corollary G has degree of commutativity greater than 0. By Lemma 2.2 the centre of $\gamma_1(G)$ is of the form $\gamma_\lambda(G)$, where $1 \leqslant \lambda \leqslant m$. We shall show that $\lambda \leqslant p$. This is obvious if $m \leqslant p+1$. If $m > p+1$, then $s_1^p s_p$ is an element of $\gamma_{p+1}(G)$ by Lemma 3.3. Thus s_1^p is an element of $\gamma_p(G)$, but not of $\gamma_{p+1}(G)$, and it is therefore sufficient to show that s_1^p lies in the centre of $\gamma_1(G)$. Now $s_1^p \in \gamma_2(G)$, and so s_1^p commutes with each element of $\gamma_2(G)$, since G is metabelian. But also s_1^p commutes with s_1; hence s_1^p commutes with each element of $\gamma_1(G)$, as required. Thus

$$[\gamma_1(G), \gamma_p(G)] = 1.$$

More generally we prove by induction on $p - i$ that, if $m \geqslant p + 1$,

$$[\gamma_1(G), \gamma_i(G)] \leqslant \gamma_{m-p+i}(G) \quad (i = 2, 3, \ldots, p).$$

We have proved this for $p - i = 0$; if $p - i > 0$, then

$$[\gamma_1(G), \gamma_{i+1}(G)] \leqslant \gamma_{m-p+i+1}(G), \tag{21}$$

by the inductive hypothesis. Now

$$[s_1, s_i]^s = [s_1^s, s_i^s] = [s_1[s_1, s], s_i[s_i, s]] = [s_1 s_2, s_i s_{i+1}].$$

By (1) $$[s_1 s_2, s_i s_{i+1}] = [s_1 s_2, s_{i+1}]\,[s_1 s_2, s_i]\,[s_1 s_2, s_i, s_{i+1}].$$

Hence by (21) $$[s_1 s_2, s_i s_{i+1}] \equiv [s_1 s_2, s_i] \pmod{\gamma_{m-p+i+1}(G)}.$$

But again by (1) $$[s_1 s_2, s_i] = [s_1, s_i]^{s_2}\,[s_2, s_i] = [s_1, s_i],$$

since $\gamma_2(G)$ is Abelian. Thus

$$[s_1, s_i]^s \equiv [s_1, s_i] \pmod{\gamma_{m-p+i+1}(G)},$$

or, $[s_1, s_i]$ belongs to the centraliser of s modulo $\gamma_{m-p+i+1}(G)$. But also $[s_1, s_i]$ lies in $\gamma_2(G)$, and so by applying Lemma 2.14 to $G/\gamma_{m-p+i+1}(G)$, we find that $[s_1, s_i]$ is an element of $\gamma_{m-p+i}(G)$. Clearly this implies the stated result.

Finally we generalize this to the groups of ECF(m, n, p).

THEOREM 3.10. *If* $G \in \mathrm{ECF}(m, n, p)$ $(m \geqslant p + 1)$ *and* $\gamma_2(G)$ *is Abelian, then*

$$[\gamma_1(G), \gamma_i(G)] \leqslant \gamma_{m-p+i}(G) \quad (i = 1, 2, \ldots, p).$$

The group generated by s and s_1 is a p-group of maximal class with the same lower central series as G, and so the result which we have proved above shows that for $i = 2, 3, \ldots, p$, s_1 lies in the centraliser of $\gamma_i(G)$ modulo $\gamma_{m-p+i}(G)$. Now s_1 denotes an arbitrary element of $\gamma_1(G)$ which does not belong to $\zeta_{m-2}(G)$. Thus if y is a given element of $\zeta_{m-2}(G)$, this is also true for $s_1 y$, and hence for y itself. Hence any element of $\gamma_1(G)$ lies in the centraliser of $\gamma_i(G)$, modulo $\gamma_{m-p+i}(G)$, and so

$$[\gamma_1(G), \gamma_i(G)] \leqslant \gamma_{m-p+i}(G) \quad (i = 2, 3, \ldots, p).$$

It remains to prove that the derived group $\gamma_1'(G)$ of $\gamma_1(G)$ is contained in $\gamma_{m-p+1}(G)$. This follows at once from the following lemma.

LEMMA 3.11. *If* $G \in \mathrm{ECF}(m, n, p)$ $(m > 3)$ *and* $[\gamma_1(G), \gamma_2(G)] \leqslant \gamma_r(G)$, *then* $\gamma_1'(G) \leqslant \gamma_{r-1}(G)$.

Let T be defined as in Theorem 2.15, so that $\gamma_1(G)$ is generated by s_1, T and $\gamma_2(G)$. Hence by Theorem 1.1 $\gamma_1'(G)$ is generated by $[\gamma_1(G), \gamma_2(G)]$, together with the elements $[s_1, t]$, $[t, u]$, as t, u run through T. It is therefore only necessary to prove that these elements lie in $\gamma_{r-1}(G)$. By Theorem 2.15 $[t, u] \in \gamma_{m-1}(G) \leqslant \gamma_{r-1}(G)$. To prove it for $[s, t]$ we observe that since $t \in S$,

$$[s_1, t]^s = [s_1^s, t^s] = [s_1 s_2, t] = [s_1, t]\, [s_1, t, s_2]\, [s_2, t],$$

by (1). Since $[\gamma_1(G), \gamma_2(G)] \leqslant \gamma_r(G)$, it follows that $[s_1, t]$ commutes with s, modulo $\gamma_r(G)$. We deduce that $[s_1, t] \in \gamma_{r-1}(G)$ by applying Lemma 2.14 to $G/\gamma_r(G)$.

We now consider a group G of $\mathrm{ECF}(m, n, p)$ in which $\gamma_3(G)$ is Abelian. Let K be defined as in Lemma 3.1, so that $\gamma_i(K) = \gamma_{i+1}(G)$ $(i = 1, 2, \ldots, m-2)$. Thus $\gamma_2(K)$ is Abelian, and by Theorem 3.10

$$[\gamma_1(K), \gamma_{i-1}(K)] \leqslant \gamma_{m-p+i-2}(K) \quad (i = 3, 4, \ldots, p+1),$$

or

$$[\gamma_2(G), \gamma_i(G)] \leqslant \gamma_{m\ p+i-1}(G) \quad (i = 3, 4, \ldots, p+1). \tag{22}$$

We shall prove that G has degree of commutativity $m - p - 2$. If $m = p + 3$, this follows from Theorem 3.8: thus we may use induction on m. By applying the inductive hypothesis to $G/\gamma_{m-1}(G)$, we see that this group has degree of commutativity $m - p - 3$. Also

$$[\gamma_i(G), \gamma_{p+4-i}(G)] = 1 \quad (i = 2, 3, \ldots, p+2),$$

on account of (22) and the fact that $\gamma_3(G)$ is Abelian. Thus by Lemma 3.7 G has degree of commutativity $m - p - 3$, and so

$$[\gamma_1(G), \gamma_i(G)] \leqslant \gamma_{m-p+i-2}(G) \quad (i = 1, 2, \ldots, p+2).$$

Hence we may write

$$[s_1, s_i] \equiv s^{\alpha_i}_{m-p+i-2} \pmod{\gamma_{m-p+i-1}(G)} \quad (i = 2, 3, \ldots, p+1).$$

Also, by (23) we may write

$$[s_2, s_i] \equiv s^{\beta_i}_{m-p+i-1} \pmod{\gamma_{m-p+i}(G)} \quad (i = 3, 4, \ldots, p).$$

We now apply Lemma 3.5 and obtain

$$\begin{aligned} &\alpha_2 \equiv \alpha_3 \pmod{p}, \\ &\alpha_{j+1} + \beta_j \equiv \alpha_j \pmod{p} \quad (j = 3, 4, \ldots, p), \\ &\beta_3 \equiv \beta_4 \equiv \ldots \equiv \beta_p \pmod{p}. \end{aligned}$$

Hence

$$\alpha_j \equiv \alpha_2 - (j-3)\beta_3 \pmod{p} \quad (j = 3, 4, \ldots, p).$$

But by Lemma 3.6 $[s_1, s_p]$ lies in $\gamma_{m-1}(G)$ and

$$[s_2, s_p] = s_{m-1}^{-\alpha_2};$$

that is,
$$\alpha_p \equiv \beta_p + \alpha_2 \equiv 0 \pmod{p}.$$

Hence
$$\alpha_2 - (p-3)\beta_3 \equiv \alpha_2 + \beta_3 \equiv 0 \pmod{p}.$$

Hence $\alpha_2 \equiv \beta_3 \equiv 0 \pmod{p}$, (we neglect the trivial case $p = 2$), and so $\alpha_i \equiv \beta_j \equiv 0 \pmod{p}$ $(i = 2, 3, \ldots, p+1;\ j = 3, 4, \ldots, p)$.

Since the β_j are zero, modulo p, it follows that $[s_2, s_i]$ lies in $\gamma_{m-p+i}(G)$ and so

$$[\gamma_2(G), \gamma_i(G)] \leqslant \gamma_{m-p+i}(G) \quad (i = 3, 4, \ldots, p).$$

Since the α_i are zero, modulo p, it follows that $[s_1, s_i]$ lies in $\gamma_{m-p+i-1}(G)$, and hence that s_1 lies in the centraliser of $\gamma_i(G)$ modulo $\gamma_{m-p+i-1}(G)$. By the usual argument it follows that this holds for any element of $\gamma_1(G)$, and thus

$$[\gamma_1(G), \gamma_i(G)] \leqslant \gamma_{m-p+i-1}(G) \quad (i = 2, 3, \ldots, p+1).$$

By Lemma 3.11 this is also true for $i = 1$. Since also $\gamma_3(G)$ is Abelian, it follows that G has degree of commutativity $m - p - 2$, as stated.

We generalize this result in the following theorem.

THEOREM 3.12. *Suppose that* $G \in \mathrm{ECF}(m, n, p)$, and that $\gamma_a(G)$ *is Abelian, where* a *is an integer such that* $m \geqslant p + 2a - 4$ *and* $a \geqslant 3$. *Then* G *has degree of commutativity* $m - p - 2a + 4$.

As is seen by considering the case $p = 2$, this is not always a very powerful result. It is the best one, however, that the methods of the present work yield, and is probably the best possible result if $a < p$. Note that it is incorrect for $a = 2$.

Theorem 3.12 is trivial for $m = p + 2a - 4$, and has already been proved for $a = 3$. It is proved in general by a double induction on a and m under which we assume that it is true (i) for smaller values of a and all values of m and (ii) for the given value of a and smaller values of m. Assuming that $m > p + 2a - 4$ we may apply the result to $G/\gamma_{m-1}(G)$ on account of (ii). Hence $G/\gamma_{m-1}(G)$ has degree of commutativity $m - p - 2a + 3$. Let K be defined as in Lemma 3.1, so that K is a p-group of maximal class of order p^{m-1} and $\gamma_i(K) = \gamma_{i+1}(G)$ $(i = 1, 2, \ldots, m-1)$. Thus $\gamma_{a-1}(K)$ is Abelian, and so, assuming that $a > 3$, we may apply the result to K, on account of (i). Thus K has degree of commutativity $m - p - 2a + 5$. Hence if $i \geqslant 2, j \geqslant 2$,

$$[\gamma_i(G), \gamma_j(G)] = [\gamma_{i-1}(K), \gamma_{j-1}(K)] \leqslant \gamma_{i+j+m-p-2a+3}(K) = \gamma_{i+j+m-p-2a+4}(G). \tag{23}$$

In particular, if $2 \leqslant i \leqslant p - 2a - 4$,

$$[\gamma_i(G), \gamma_{p+2a-i-2}(G)] = 1,$$

and so we can apply Lemma 3.7. Hence G has degree of commutativity $m-p-2a+3$, and in particular

$$[\gamma_1(G), \gamma_i(G)] \leqslant \gamma_{i+m-p-2a+4}(G) \quad (i=1, 2, \ldots, p+2a-4).$$

By (23) we have only to prove that

$$[\gamma_1(G), \gamma_i(G)] \leqslant \gamma_{i+m-p-2a+5}(G) \quad (i=1, 2, \ldots, p+2a-5).$$

Using (23) we deduce from Lemma 3.5 that if

$$[s_1, s_2] \equiv s^{\alpha}_{m-p-2a+6} \pmod{\gamma_{m-p-2a+7}(G)},$$

then $$[s_1, s_i] \equiv s^{\alpha}_{m-p-2a+i+4} \pmod{\gamma_{m-p-2a+i+5}(G)}, \quad (i=2, 3, \ldots, p+2a-5).$$

But by Lemma 3.6 $[s_1, s_p]$ lies in $\gamma_{m-2a+5}(G)$, and so $\alpha \equiv 0 \pmod{p}$. Thus s_1 commutes with each element of $\gamma_i(G)$, modulo $\gamma_{m-p-2a+i+5}(G)$, and by the usual argument we deduce that

$$[\gamma_1(G), \gamma_i(G)] \leqslant \gamma_{m-p-2a+i+5}(G) \quad (i=2, 3, \ldots, p+2a-5).$$

This is also true for $i=1$, by Lemma 3.11, and so Theorem 3.12 is proved.

It would be desirable to obtain a degree of commutativity for the groups of ECF (m, n, p) which depends only on m and p, but the author is unable to do so. In the case $p=2$ of course the problem is very simple, for as we have already seen, $[\gamma_1(G), \gamma_2(G)]=1$, and so by Lemma 3.11, $\gamma_1'(G) \leqslant \gamma_{m-1}(G)$; thus G has degree of commutativity $m-3$. For $p=3$, we have the following.

THEOREM 3.13. *A group of* ECF$(m, n, 3)$ $(m \geqslant 4)$ *has degree of commutativity* $m-4$.

This may be deduced at once from Theorem 2.16, Corollary 2 and Theorem 3.10. Alternatively we may prove it by induction on m. For $m=5$, the theorem is true by Theorem 2.11. For $m>5$, we find by applying the inductive hypothesis to $G/\gamma_{m-1}(G)$ that $G/\gamma_{m-1}(G)$ has degree of commutativity $m-5$. If we apply the inductive hypothesis to the group K defined in Lemma 3.1, we find that

$$[\gamma_2(G), \gamma_4(G)] = [\gamma_3(G), \gamma_3(G)] = 1;$$

hence by Lemma 3.7 G has degree of commutativity $m-5$. Hence

$$[\gamma_2(G), \gamma_3(G)] = 1,$$

and by Lemma 2.1 $\gamma_2(G)$ is Abelian. It follows from Theorem 3.10 that G has degree of commutativity $m-4$, as required.

These results for $p=2$ and $p=3$ suggest that the desired degree of commutativity for the groups of ECF(m, n, p) will be some such simple form as $m-p-1$. That this is not so is shown by the case $p=5$; for example there exists a group of order 5^{14} and class

13 with degree of commutativity 4 but not 5. The best result which our methods yield for $p = 5$, and probably the best possible result, is the following.

THEOREM 3.14. *If $G \in \mathrm{ECF}(m, n, 5)$ and $m > 5$, then G has degree of commutativity $[\frac{1}{2}(m-5)]$. In particular $\gamma_1(G)$ is of class at most 3.*

To deduce that $\gamma_1(G)$ is of class at most 3 from the first assertion, we observe that

$$\gamma_2(\gamma_1(G)) = [\gamma_1(G), \gamma_1(G)] \leqslant \gamma_{2+[\frac{1}{2}(m-5)]}(G),$$

$$\gamma_3(\gamma_1(G)) = [\gamma_1(G), \gamma_2(\gamma_1(G))] \leqslant [\gamma_1(G), \gamma_{2+[\frac{1}{2}(m-5)]}(G)] \leqslant \gamma_{3+2[\frac{1}{2}(m-5)]}(G),$$

and similarly

$$\gamma_4(\gamma_1(G)) \leqslant \gamma_{4+3[\frac{1}{2}(m-5)]}(G).$$

If m is odd it follows that $\gamma_4(\gamma_1(G)) = 1$ for $m \geqslant 7$, and if m is even, then $\gamma_4(\gamma_1(G)) = 1$ for $m \geqslant 10$. But for $m = 8$ $\gamma_3(\gamma_1(G)) \leqslant \gamma_5(G)$, and by Lemma 3.6 $[\gamma_1(G), \gamma_5(G)] \leqslant \gamma_8(G) = 1$, since G has degree of commutativity 1; hence $\gamma_4(\gamma_1(G)) = 1$. The only remaining cases are $m \leqslant 6$. For $m = 4$ it is trivial and for $m = 5, 6$ we see from Theorem 2.6 that $\gamma_2(\gamma_1(G)) \leqslant \gamma_3(G)$, and, since $G/\gamma_5(G)$ has degree of commutativity 1,

$$\gamma_3(\gamma_1(G)) \leqslant [\gamma_1(G), \gamma_3(G)] \leqslant \gamma_5(G).$$

Hence $\gamma_4(\gamma_1(G)) = 1$.

Theorem 3.14 is trivial for $m = 6$, and for $m > 6$ we use induction on m. By Theorem 3.8 G has degree of commutativity greater than 0. We may therefore assume that $m > 7$. Applying the inductive hypothesis to $G/\gamma_{m-1}(G)$ gives

$$[\gamma_i(G), \gamma_j(G)] \leqslant \gamma_{i+j+[\frac{1}{2}(m-6)]}(G) \quad (i+j \leqslant [\tfrac{1}{2}(m+5)]).$$

Applying the inductive hypothesis to the group K defined in Lemma 3.1 gives

$$[\gamma_i(K), \gamma_j(K)] \leqslant \gamma_{i+j+[\frac{1}{2}(m-6)]}(K),$$

and this yields, for $i = 2, 3, \ldots, [\frac{1}{2}(m+5)]$,

$$[\gamma_i(G), \gamma_{[\frac{1}{2}(m+9)]-i}(G)] = 1.$$

Hence by Lemma 3.7 G has degree of commutativity $[\frac{1}{2}(m-6)]$. If m is even this completes the proof.

If m is odd, put $m = 2r+1$, so that $r \geqslant 4$, and G has degree of commutativity $r-3$; that is,

$$[\gamma_i(G), \gamma_j(G)] \leqslant \gamma_{i+j+r-3}(G) \ \ (i+j \leqslant r+4). \tag{24}$$

Let $$[s_i, s_j] \equiv s_{i+j+r-3}^{\alpha_{ij}} \pmod{\gamma_{i+j+r-2}(G)} \quad (1 \leqslant i < j,\ i+j \leqslant r+3).$$

By Lemma 3.5

$$\alpha_{ii+2} \equiv \alpha_{ii+1} \pmod 5 \ \ (i = 1, 2, \ldots, [\tfrac{1}{2}(r+1)]), \tag{25}$$

$$\alpha_{ij+1} + \alpha_{i+1j} \equiv \alpha_{ij} \pmod 5 \ \ (1 \leqslant i \leqslant j-2,\ i+j \leqslant r+2). \tag{26}$$

By Lemma 3.6

$$\alpha_{15} \equiv 0 \pmod 5,$$

$$\alpha_{1i} + \alpha_{i5} \equiv 0 \pmod 5 \quad (i = 2, \ldots, \min(r-2, 4)), \tag{27}$$

$$\alpha_{1i} \equiv \alpha_{5i} \pmod 5 \quad (i = 6, 7, \ldots, r-2). \tag{28}$$

We deduce that

$$\alpha_{ij} \equiv \sum_{k=1}^{i} (-1)^{k-1} \binom{i-1}{k-1} \alpha_{1j+k-1} \pmod 5 \quad (1 \leqslant i < j.\ i+j \leqslant r+3). \tag{29}$$

This is correct for $i = 1$; for $i > 1$ we proceed by induction on i. If $i < j$ and $i + j \leqslant r + 3$, we have from (26)

$$\alpha_{ij} \equiv \alpha_{i-1j} - \alpha_{i-1\,j+1} \pmod 5,$$

so that by the inductive hypothesis

$$\alpha_{ij} \equiv \sum_{k=1}^{i-1} (-1)^{k-1} \binom{i-2}{k-1} \alpha_{1j+k-1} - \sum_{k=1}^{i-1} (-1)^{k-1} \binom{i-2}{k-1} \alpha_{1j+k} \pmod 5.$$

Hence $$\alpha_{ij} \equiv \alpha_{1j} + \sum_{k=1}^{i-1} (-1)^{k-1} \left\{ \binom{i-2}{k-1} + \binom{i-2}{k-2} \right\} \alpha_{1j+k-1} + (-1)^{i-1} \alpha_{1i+j-1} \pmod 5,$$

and (29) follows.

More precisely we may deduce that if $\alpha_{12} = \alpha$, then for $i = 2, 3, \ldots, r+2$,

$$\left.\begin{aligned} \alpha_{1i} &\equiv \alpha && \pmod 5 \quad (i \equiv 2 \pmod 4)), \\ \alpha_{1i} &\equiv \alpha && \pmod 5 \quad (i \equiv 3 \pmod 4)), \\ \alpha_{1i} &\equiv 3\alpha && \pmod 5 \quad (i \equiv 0 \pmod 4)), \\ \alpha_{1i} &\equiv 0 && \pmod 5 \quad (i \equiv 1 \pmod 4)). \end{aligned}\right\} \tag{30}$$

For $i = 2, 3, \ldots, 9$ this has to be proved rather carefully from (25), (26) and (27), paying particular attention to the cases which arise when r is small. The details are as follows:

$i = 3$, $\alpha_{13} \equiv \alpha_{12}$ (by (25));

$i = 4$, $\alpha_{23} \equiv \alpha_{24}$ (by (25)), $\alpha_{23} \equiv \alpha_{13} - \alpha_{14}$, $\alpha_{24} \equiv \alpha_{14} - \alpha_{15}$ (by (26)), $\alpha_{15} \equiv 0$;

$i = 6$, $\alpha_{16} \equiv \alpha_{15} - \alpha_{25}$ (by (26)), $\alpha_{25} \equiv -\alpha_{12}$ (by (27));

$i = 7$, $\alpha_{17} \equiv \alpha_{16} - \alpha_{26}$, $\alpha_{26} \equiv \alpha_{25} - \alpha_{35}$ (by (26)), $\alpha_{35} \equiv -\alpha_{13}$ (by (27));

$i = 8$, $\alpha_{18} \equiv \alpha_{17} - \alpha_{27}$, $\alpha_{27} \equiv \alpha_{26} - \alpha_{36}$, $\alpha_{36} \equiv \alpha_{35} - \alpha_{45}$ (by (26)), $\alpha_{45} \equiv -\alpha_{14}$ (by (27)).

$i = 9$, $\alpha_{19} \equiv \alpha_{18} - \alpha_{28}$, $\alpha_{28} \equiv \alpha_{27} - \alpha_{37}$, $\alpha_{37} \equiv \alpha_{36} - \alpha_{46}$ (by (26)), $\alpha_{46} \equiv \alpha_{45}$ (by (25)).

For $i \geqslant 10$ we use induction on i; by (28) and (29),

$$\alpha_{1i-4} \equiv \alpha_{5i-4} \equiv \sum_{k=1}^{5} (-1)^{k-1} \binom{4}{k-1} \alpha_{1i+k-5} \pmod 5,$$

or $$4\alpha_{1i-3} - 6\alpha_{1i-2} + 4\alpha_{1i-1} \equiv \alpha_{1i} \pmod 5.$$

From this (30) readily follows.

(30) comprises all the information which Lemmas 3.5 and 3.6 yield. To prove that $\alpha \equiv 0 \pmod 5$ it is therefore necessary to perform a further calculation with the group elements, and this we do as follows. We have

$$[s_1, s_2] = s_r^{\alpha} x,$$

where $x \in \gamma_{r+1}(G)$. Transforming by s_3 we obtain

$$[s_1^{s_3}, s_2^{s_3}] \equiv (s_r^{s_3})^{\alpha} x^{s_3}.$$

By (24) $$[\gamma_{r+1}(G), \gamma_3(G)] = 1,$$

and so $x^{s_3} = x = s_r^{-\alpha}[s_1, s_2]$. Hence, since $\gamma_r(G)$ is Abelian,

$$[s_1^{s_3}, s_2^{s_3}] = [s_r, s_3]^{\alpha} [s_1, s_2]. \tag{31}$$

Now $$[s_1, s_3] = s_{r+1}^{\alpha_{13}} y, \qquad [s_2, s_3] = s_{r+2}^{\alpha_{23}} z,$$

where $y \in \gamma_{r+2}(G)$, $z \in \gamma_{r+3}(G)$. Since

$$[\gamma_2(G), \gamma_{r+2}(G)] = [\gamma_1(G), \gamma_{r+3}(G)] = 1$$

and $[s_1, s_{r+2}]$, $[s_2, s_{r+1}]$ are elements of the centre of G, we see from (1) and Theorem 1.4 that

$$\begin{aligned}[s_1^{s_3}, s_2^{s_3}] &= [s_1 s_{r+1}^{\alpha_{13}}, s_2 s_{r+2}^{\alpha_{23}}] \\ &= [s_1, s_2][s_1, s_{r+2}]^{\alpha_{23}} [s_2, s_{r+1}]^{-\alpha_{13}}\end{aligned}$$

Hence by (31) $$[s_r, s_3]^{\alpha} = [s_1, s_{r+2}]^{\alpha_{23}} [s_2, s_{r+1}]^{-\alpha_{13}}.$$

This gives $$\alpha\alpha_{3r} + \alpha_{23}\alpha_{1r+2} \equiv \alpha_{13}\alpha_{2r+1} \pmod 5.$$

or, using (30), $$\alpha(\alpha_{3r} - \alpha_{2r+1} + 3\alpha_{1r+2}) \equiv 0 \pmod 5,$$

and so by (29)

$$\alpha(\alpha_{1r} - 2\alpha_{1r+1} + \alpha_{1r+2} - \alpha_{1r+1} + \alpha_{1r+2} + 3\alpha_{1r+2}) \equiv 0 \pmod 5;$$

that is, $$\alpha(\alpha_{1r} - 3\alpha_{1r+1}) \equiv 0 \pmod 5.$$

Thus by (30), $$(-1)^r.\ 3\alpha^2 \equiv 0 \pmod 5,$$

and so $\alpha \equiv 0 \pmod 5$. By (30) and (29) $\alpha_{ij} \equiv 0 \pmod 5$ for $1 \leqslant i < j$, $i + j \leqslant r + 3$. Hence

$$[\gamma_i(G), \gamma_j(G)] \leqslant \gamma_{i+j+r-2}(G) \quad (2 \leqslant i < j,\ i + j \leqslant r + 3)$$

and $$[s_1, s_i] \in \gamma_{i+r-1}(G).$$

Since s_1 is an arbitrarily chosen element of $\gamma_1(G)$ which does not lie in $\zeta_{m-2}(G)$, it follows that if $y \in \zeta_{m-2}(G)$, then $s_1 y$ belongs to the centraliser of $\gamma_i(G)$ modulo $\gamma_{i+r-1}(G)$, and so

$$[\gamma_1(G), \gamma_i(G)] \leqslant \gamma_{i+r-1}(G) \quad (i = 2, 3, \ldots, r+2).$$

By Lemma 3.11
$$\gamma_1'(G) \leqslant \gamma_r(G)$$

and so G has degree of commutativity $r - 2 = [\frac{1}{2}(m-5)]$. This completes the proof of Theorem 3.14.

4. We conclude by turning to the problem of determining the types of p-groups in certain classes. Our primary aims are to find all 3-groups of maximal class and all groups of order p^6 and class 5. To this end we proceed as follows.

Let G be a metabelian group of order p^n and class $n-1$ where $n \geqslant 4$, and suppose that

$$[\gamma_1(G), \gamma_2(G)] \leqslant \gamma_{n-2}(G).$$

We use the notation of the last paragraph, and so

$$s_i = [s_{i-1}, s] \quad (i = 2, 3, \ldots, n-1). \tag{32}$$

Suppose that
$$[s_1, s_2] = s_{n-2}^{\alpha} s_{n-1}^{\beta}. \tag{33}$$

By Theorem 3.13 we may take $\alpha = 0$ if $p = 3$; for $p = 2$ we take $\alpha = \beta = 0$. Also, by Theorem 2.11 we may take $\alpha = 0$ if $n = 5$; for $n = 4$ we take $\alpha = \beta = 0$. Then

$$[s_1, s_3] = s_3^{-s_1} s_3 = [s, s_2]^{s_1} s_3 = [s^{s_1}, s_2^{s_1}] s_3 = [s s_2^{-1}, s_2 s_{n-2}^{-\alpha}] s_3 = [s, s_2 s_{n-2}^{-\alpha}] s_3,$$

and so
$$[s_1, s_3] = s_{n-1}^{\alpha}, \tag{34}$$

using (1) and (2). And by exactly the same calculations, for $n > 4$

$$[s_1, s_i] = 1 \quad (i = 4, 5, \ldots, n-1). \tag{35}$$

We shall now work out $(s s_1^{\zeta})^p$. For $p > 3$ we may do this by applying Theorem 1.6 taking $x = s, y = s_1^{\zeta}$. The group there denoted by Y is $\gamma_1(G)$, and by Lemma 2.1 Y' becomes $[\gamma_1(G), \gamma_2(G)]$. Since this is contained in $\gamma_{n-2}(G)$ and by Theorem 3.4, Corollary 1 $\gamma_{n-2}(G)$ is elementary Abelian, $P_1(Y')$ becomes 1. It is clear from (35) and the fact that G is metabelian that $[Y, \gamma_{p-1}(G)]$ becomes 1 and that

$$\prod_{i=2}^{p-2} [\gamma_i(G), \gamma_{p-i}(G)] = 1.$$

Hence Theorem 1.6 gives

$$(s s_1^{\zeta})^p = s^p s_1^{p\zeta} \sigma_2^{\binom{p}{2}} \dots \sigma_i^{\binom{p}{i}} \dots \sigma_p,$$

where $\sigma_i = \sigma_i(s, s_1^{\zeta})$. Now

$$\sigma_2 = [s_1^{\zeta}, s] = s_1^{-\zeta}(s_1^{\zeta})^s = s_1^{-\zeta}(s_1^s)^{\zeta} = s_1^{-\zeta}(s_1\ s_2)^{\zeta}.$$

Since $[\gamma_1(G), \gamma_{n-2}(G)] = 1$, $\gamma_1(G)$ is of class 2, and so by Theorem 1.4

$$(s_1 s_2)^{\zeta} = s_1^{\zeta} s_2^{\zeta} [s_2, s_1]^{\binom{\zeta}{2}}.$$

Hence $$\sigma_2 = s_2^{\zeta} s_{n-2}^{-\alpha\binom{\zeta}{2}} s_{n-1}^{-\beta\binom{\zeta}{2}}.$$

Further $$\sigma_3 = [s_2^{\zeta} s_{n-2}^{-\alpha\binom{\zeta}{2}} s_{n-1}^{-\beta\binom{\zeta}{2}}, s] = s_3^{\zeta} s_{n-1}^{-\alpha\binom{\zeta}{2}},$$

and for $i = 4, 5, \dots, p$ $\sigma_i = s_i^{\zeta}$. Again since $\gamma_{n-2}(G)$ is elementary Abelian, we see that for $i = 2, 3, \dots, p$

$$\sigma_i^{\binom{p}{i}} = s_i^{\binom{p}{i}\zeta},$$

and so $$(s s_1^{\zeta})^p = s^p s_1^{p\zeta} s_2^{\binom{p}{2}\zeta} \dots s_i^{\binom{p}{i}\zeta} \dots s_p^{\zeta}.$$

For $p = 2$ $\gamma_1(G)$ is Abelian and we simply have

$$(s s_1^{\zeta})^2 = s^2 (s_1 s_2)^{\zeta} s_1^{\zeta} = s^2 s_1^{2\zeta} s_2^{\zeta}.$$

For $p = 3$ we have

$$(s s_1^{\zeta})^3 = s^3 (s_1^{\zeta})^{s^2} (s_1^{\zeta})^s s_1^{\zeta} = s^3 (s_1 s_2^2 s_3)^{\zeta} (s_1 s_2)^{\zeta} s_1^{\zeta}.$$

Since again $\gamma_1(G)$ is of class 2, we obtain, using Theorem 1.4,

$$(s s_1^{\zeta})^3 = s^3 s_1^{\zeta} s_2^{2\zeta} s_3^{\zeta} s_1^{\zeta} s_2^{\zeta} s_1^{\zeta} [s_2^2 s_3, s_1]^{\binom{\zeta}{2}} [s_2, s_1]^{\binom{\zeta}{2}}.$$

Collecting together the s_1^{ζ} and using the fact that

$$(s_2^{\lambda})^{s_1^{\mu}} = (s_2 [s_2, s_1^{\mu}]^{\lambda} = s_2^{\lambda} s_{n-1}^{-\beta\lambda\mu},$$

this gives $$(s s_1^{\zeta})^3 = s^3 s_1^{3\zeta} s_2^{3\zeta} s_3^{\zeta} s_{n-1}^{\beta\zeta^2}.$$

Hence for all p $$(s s_1^{\zeta})^p = s^p (s_1^p s_2^{\binom{p}{2}} \dots s_p)^{\zeta} s_{n-1}^{\beta\zeta^2\binom{p}{3}}, \qquad (39)$$

since the elements $s_1^p, s_2^{\binom{p}{2}}, \dots$ all lie in $\gamma_2(G)$ and therefore commute with one another.

By Lemma 2.14 s^p and $(s s_1)^p$ belong to $\gamma_{n-1}(G)$. It follows from (39) that $s_1^p s_2^{\binom{p}{2}} \dots s_p$ lies in $\gamma_{n-1}(G)$, and we write

$$s^p = s_{n-1}^{\delta} \tag{36}$$

$$s_1^p \, s_2^{\binom{p}{2}} \dots s_p = s_{n-1}^{\gamma}. \tag{37}$$

Finally by Theorem 2.15, Corollary 2 $s s_i$ is a conjugate of s for $2 \leqslant i \leqslant n \mathbin{\dot{-}} 1$, and so $(s s_i)^p$, s^p are conjugate. Thus $(s s_i)^p = s^p$. By Theorem 1.6 or by a simple direct calculation this reduces to

$$s_i^p \, s_{i+1}^{\binom{p}{2}} \dots s_{i+p-1} = 1 \quad (i = 2, 3, \dots, n-1). \tag{38}$$

Equations (32)–(38) are the defining relations of G, and it is easy to verify that such a group exists for arbitrary α, β, γ and δ (except in the cases mentioned when n or p is small) by using the theorem on cyclic extensions (see [13], Kap. III, § 7).

It follows from (36), (37) and (39) that

$$(s s_1^{\zeta})^p = s_{n-1}^{\delta + \gamma\zeta + \beta\zeta^2 \binom{p}{3}}.$$

We deduce from this that if ξ is not divisible by p, then

$$(s^{\xi} s_1^{\xi_1} \dots s_{n-1}^{\xi_{n-1}})^p = s_{n-1}^{\delta\xi + \gamma\xi_1 + \beta\xi\xi_1^2 \binom{p}{3}}. \tag{40}$$

For let ξ' be a number such that $\xi\xi' \equiv 1 \pmod{p}$; when $p = 3$, we take $\xi' = \xi$. Then $s^{\xi} s_1^{\xi_1} \dots s_{n-1}^{\xi_{n-1}}$ is congruent to the ξ-th power of $s s_1^{\xi'\xi_1}$ modulo $\gamma_2(G)$ and is therefore a conjugate of this element, by Theorem 2.15, Corollary 2. Hence

$$(s^{\xi} s_1^{\xi_1} \dots s_{n-1}^{\xi_{n-1}})^p = (s s_1^{\xi'\xi_1})^{p\xi},$$

and (40) is obtained by applying the above formula for $(s s_1^{\zeta})^p$.

Now each group of this kind is determined by the four parameters $(\alpha, \beta, \gamma, \delta)$. We wish to find what relations exist between the sets of parameters of two isomorphic groups of this kind. Thus suppose that $\bar{G}$ is another group and that θ is an isomorphic mapping of $\bar{G}$ onto G. In $\bar{G}$ we use the notation $\bar{s}, \bar{s}_i$ instead of s, s_i and we suppose that the four parameters are $(\bar{\alpha}, \bar{\beta}, \bar{\gamma}, \bar{\delta})$. From $\gamma_i(\bar{G})^{\theta} = \gamma_i(G)$ $(i = 2, 3, \dots, n-1)$ follows $\gamma_1(\bar{G})^{\theta} = \gamma_1(G)$. Hence we may write

$$\bar{s}^{\theta} = s^{\xi} s_1^{\xi_1} s_2^{\xi_2} \dots s_{n-1}^{\xi_{n-1}}, \qquad \bar{s}_1^{\theta} = s_1^{\eta_1} s_2^{\eta_2} \dots s_{n-1}^{\eta_{n-1}}, \tag{41}$$

where p does not divide $\xi\eta_1$. By (32)

$$\bar{s}_2^{\theta} = [\bar{s}_1, \bar{s}]^{\theta} = [\bar{s}_1^{\theta}, \bar{s}^{\theta}] = [s_1^{\eta_1} s_2^{\eta_2} \dots s_{n-1}^{\eta_{n-1}}, s^{\xi} s_1^{\xi_1} s_2^{\xi_2} \dots s_{n-1}^{\xi_{n-1}}].$$

By working out each $\bar{s}_i^{\theta}$ in this way and substituting in all equations corresponding to (33)–(38), such as

$$[\bar{s}_1^{\theta}, \bar{s}_2^{\theta}] = (\bar{s}_{n-2}^{\bar{\alpha}} \bar{s}_{n-1}^{\bar{\beta}})^{\theta},$$

we obtain the transformation laws between the parameters $(\alpha, \beta, \gamma, \delta)$ of G and the parameters $(\bar{\alpha}, \bar{\beta}, \bar{\gamma}, \bar{\delta})$ of $\bar{G}$. (Actually of course there is no need to substitute in such equations as those corresponding to (38), since these are automatically satisfied on account of the general theory). The necessary and sufficient condition for isomorphism between G and $\bar{G}$ is therefore that it is possible to find integers ξ, ξ_i, η_j with $\xi\eta_1 \not\equiv 0 \pmod{p}$ such that these transformation laws are satisfied.

For the calculation of $\bar{s}_2^\theta$, $\bar{s}_3^\theta$, ... we need only proceed to a small degree of accuracy, and we find the following, using (1) and (2):

$$\begin{array}{lll}
\bar{s}_2^\theta \equiv s_2^{\xi\eta_1} s_3^{\binom{\xi}{2}\eta_1 + \xi\eta_2} & (\text{mod } \gamma_4(G)) & (n \geqslant 4), \\
\bar{s}_3^\theta \equiv s_3^{\xi^2\eta_1} & (\text{mod } \gamma_4(G)) & (n = 4,\ 5), \\
\bar{s}_3^\theta \equiv s_3^{\xi^2\eta_1} s_4^{-\alpha\xi\xi_1\eta_1 + 2\xi\binom{\xi}{2}\eta_1 + \xi^2\eta_2} & (\text{mod } \gamma_5(G)) & (n = 6), \\
\bar{s}_4^\theta \equiv s_4^{\xi^3\eta_1} s_5^{-2\alpha\xi^2\xi_1\eta_1 + 3\xi^2\binom{\xi}{2}\eta_1 + \xi^3\eta_2} & & (n = 6), \\
\bar{s}_i^\theta \equiv s_i^{\xi^{i-1}\eta_1} s_{i+1}^{(i-1)\xi^{i-2}\binom{\xi}{2}\eta_1 + \xi^{i-1}\eta_2} & (\text{mod } \ \gamma_{i+2} G)) & (2 \leqslant i \leqslant n-2;\ n \geqslant 7), \\
\bar{s}_{n-1}^\theta \equiv s_{n-1}^{\xi^{n-2}\eta_1} & & (n \geqslant 4).
\end{array}$$

It will simplify matters if we replace β by another parameter ε which we define as follows. For $p = 2, 3$ we put $\varepsilon = \beta$, $\bar{\varepsilon} = \bar{\beta}$, and for $p > 3$ we put

$$\varepsilon = \beta + \tfrac{1}{2}(n-4)\alpha, \qquad \bar{\varepsilon} = \bar{\beta} + \tfrac{1}{2}(n-4)\bar{\alpha}.$$

If we now substitute in the equation

$$[\bar{s}_1^\theta, \bar{s}_2^\theta] = (\bar{s}_{n-2}^{\bar{\alpha}} \bar{s}_{n-1}^{\bar{\beta}})^\theta$$

and use the fact that $\gamma_{n-2}(G)$ is elementary Abelian when p is odd, we obtain the transformation laws

$$\alpha\eta_1 \equiv \bar{\alpha}\xi^{n-4} \pmod{p} \quad (n \geqslant 6), \tag{42}$$

$$\varepsilon\eta_1 \equiv \bar{\varepsilon}\xi^{n-3} \pmod{p} \quad (n \geqslant 5,\ n \neq 6), \tag{43}$$

$$\varepsilon\eta_1 \equiv \bar{\varepsilon}\xi^3 - 2\alpha\bar{\alpha}\xi\xi_1 \pmod{p} \quad (n = 6). \tag{43$'$}$$

To obtain the transformation laws involving γ and δ we use (40). This gives

$$(\bar{s}^p)^\theta \quad = s_{n-1}^{\delta\xi + \gamma\xi_1 + \beta\xi\xi_1^3\binom{p}{3}}.$$

But also
$$(\bar{s}^p)^\theta \quad = (\bar{s}_{n-1}^{\bar{\delta}})^\theta = s_{n-1}^{\xi^{n-2}\eta_1\bar{\delta}},$$

and so
$$\bar{\delta}\,\xi^{n-2}\,\eta_1 \equiv \delta\,\xi + \gamma\,\xi_1 + \varepsilon\,\xi\,\xi_1^2\binom{p}{3} \quad (\text{mod } p). \tag{44}$$

We also deduce from (40) that

$$(s\,s_1)^p = s_{n-1}^{\delta+\gamma+\beta\binom{p}{3}}.$$

It follows that the analogous formula in $\bar{G}$ holds, namely

$$(\bar{s}\,\bar{s}_1)^p = \bar{s}_{n-1}^{\bar{\delta}+\bar{\gamma}+\bar{\beta}\binom{p}{3}}.$$

We transform this equation by θ and substitute for each $\bar{s}_i^\theta$; the left-hand side becomes

$$(s^{\xi}\,s_1^{\xi_1}\,\dots\,s_{n-1}^{\xi_{n-1}}\,s_1^{\eta_1}\,s_2^{\eta_1}\,\dots\,s_{n-1}^{\eta_{n-1}})^p,$$

and by Theorem 2.15, Corollary 2 this is equal to $(s^{\xi}\,s_1^{\xi_1+\eta_1})^p$. Hence we obtain

$$\delta\,\xi + \gamma\,(\xi_1+\eta_1) + \beta\,\xi\,(\xi_1+\eta_1)^2\binom{p}{3} \equiv \xi^{n-2}\left(\bar{\delta} + \bar{\gamma} + \bar{\beta}\binom{p}{3}\right) \quad (\text{mod p}).$$

If we substitute with (44) for $\bar{\delta}$ and, for $p=3$, with (43) or (43′) for $\bar{\beta}=\bar{\varepsilon}$, remembering that for $p=3$ $\alpha=\bar{\alpha}=0$, we obtain

$$\bar{\gamma}\,\xi^{n-2} \equiv \gamma - 4\,\varepsilon\,\xi\,\xi_1\binom{p}{3} \quad (\text{mod } p). \tag{45}$$

(42)–(45) are the required transformation laws. The number of types of groups of the kind considered is therefore equal to the number of classes of parameters, where the parameters $(\alpha, \varepsilon, \gamma, \delta)$ and $(\bar{\alpha}, \bar{\varepsilon}, \bar{\gamma}, \bar{\delta})$ belong to the same class if and only if there exist numbers ξ, ξ_1 and η_1 with $\xi\eta_1 \not\equiv 0$ (mod p) such that (42)–(45) hold. We determine this number by finding a standard set of parameters in each class.

We consider first the case when

$$[\gamma_1(G), \gamma_2(G)] = \gamma_{n-2}(G),$$

that is, when $\alpha \not\equiv 0$ (mod p), and this case arises only when $p \geqslant 5$, $n \geqslant 6$. In (42) we may put $\xi = 1$ and choose η_1 such that $\alpha\eta_1 \equiv 1$ (mod p), from which it follows that in each class of parameters there exists at least one set in which $\alpha \equiv 1$ (mod p). Therefore in each such class we may consider the standard set to have $\alpha = 1$, and for further reductions we only consider those sets in which $\alpha = 1$. Thus by (42)

$$\eta_1 \equiv \xi^{n-4} \quad (\text{mod } p),$$

and (43)–(45) reduce to

$$\varepsilon \equiv \bar{\varepsilon}\,\xi \pmod p \ (n \geqslant 7); \quad \varepsilon\xi \equiv \bar{\varepsilon}\xi^2 - 2\xi_1 \pmod p \ (n = 6);$$

$$\delta\xi + \gamma\xi_1 \equiv \bar{\delta}\,\xi^{2n-6} \pmod p; \quad \gamma \equiv \bar{\gamma}\xi^{n-2} \pmod p.$$

For $n > 6$ we now argue in exactly the same way with ε; in all sets in a given class either p divides all the ε or it divides none of them. We consider first those classes in which $\varepsilon \not\equiv 0 \pmod p$, and by putting $\xi = \varepsilon, \xi_1 = 0$, we see that in each such class there exists at least one set in which $\varepsilon = 1$. Thus we may take $\varepsilon = 1$ in the standard set of each such class and need only consider those sets in which $\varepsilon = 1$. Thus $\xi \equiv 1 \pmod p$, and the transformation laws reduce to

$$\bar{\delta} \equiv \delta + \gamma\xi_1 \pmod p; \quad \bar{\gamma} \equiv \gamma \pmod p.$$

It follows that γ cannot be altered within a class. If in any class $\gamma \not\equiv 0 \pmod p$, we choose a number γ' such that $\gamma\gamma' \equiv 1 \pmod p$ and put $\xi_1 = -\gamma'\delta$; thus there exists a set in this class having $\delta \equiv 0 \pmod p$. If in any class $\gamma \equiv 0 \pmod p$, than δ cannot be altered. Thus we obtain the $2p - 1$ standard sets $(1, 1, \gamma, 0)$ where $\gamma = 1, 2, \ldots, p-1$, and $(1, 1, 0, \delta)$ where $\delta = 0, 1, \ldots, p - 1$.

If $\alpha = 1$ but $\varepsilon = 0$, we observe that throughout the sets of such a class either p divides γ or it does not. In the latter case there must exist in each class a set with $\delta \equiv 0 \pmod p$, for we may put $\xi = 1$, $\xi_1 = -\gamma'\delta$ as before. Within such a class γ can be multiplied by any number of the form ξ^{n-2} with $\xi \not\equiv 0 \pmod p$, and there are $(p-1)/(n-2, p-1)$ residue classes modulo p expressible in this form, since the number of solutions of the congruence $\xi^{n-2} \equiv 1 \pmod p$ is $(n-2, p-1)$. Hence γ may be reduced to one of $(n-2, p-1)$ standard forms, and we obtain this number of standard sets of parameters. When $\gamma \equiv 0 \pmod p$ a similar argument shows that δ may be reduced to one of $(2n-7, p-1)$ standard values which are not divisible by p or to zero. Altogether the number of standard sets in which p does not divide α is

$$2p + (n-2, p-1) + (2n-7, p-1).$$

In the remaining cases similar arguments are used and they need only be sketched. If $\alpha = 1$ and $n = 6$ we can make $\varepsilon = 0$ and must then have $\xi_1 \equiv 0 \pmod p$. If $\gamma \not\equiv 0 \pmod p$, γ can be assigned one of $(4, p-1)$ values, and so $\xi^4 \equiv 1 \pmod p$; δ may then be chosen to have one of $(p-1)/(4, p-1) + 1$ values, and so the total number of standard sets is $p - 1 + (4, p-1)$. If $\gamma \equiv 0 \pmod p$, δ can be assigned one of $1 + (5, p-1)$ values. We have therefore proved the following.

Theorem 4.1. *For $p > 3$ the number of types of metabelian groups G of order p^n and class $n - 1$ in which*

$$[\gamma_1(G), \gamma_2(G)] = \gamma_{n-2}(G)$$

is $p + (4, p-1) + (5, p-1)$ *if* $n = 6$ *and* $2p + (n-2, p-1) + (2n-7, p-1)$ *if* $n > 6$.

We now consider the case

$$[\gamma_1(G), \gamma_2(G)] = \gamma_{n-1}(G),$$

which arises when $n \geqslant 5$ and $p \geqslant 3$. This case is characterized by $\alpha \equiv 0$, $\varepsilon \not\equiv 0 \pmod{p}$. From (43) and (43′) we see that we may take $\varepsilon = 1$ and must then assume that $\eta_1 \equiv \xi^{n-3} \pmod{p}$. For $p > 3$ we see from (45) that, if p does not divide γ, then γ may be assigned one of $(n-2, p-1)$ standard values and from (44) that we may take $\delta = 0$, whilst if p divides γ, then δ may be assigned one of $1 + (2n-6, p-1)$ values. For $p = 3$ we may take $\gamma = 0$ and must then have $\xi_1 \equiv 0 \pmod{p}$; δ cannot then be altered since $\xi^2 \equiv 1 \pmod{3}$.

THEOREM 4.2. *For* $n \geqslant 5$ *and* $p > 2$ *the number of types of metabelian groups* G *of order* p^n *and class* $n-1$ *in which*

$$[\gamma_1(G), \gamma_2(G)] = \gamma_{n-1}(G)$$

is 3 *for* $p = 3$ *and* $1 + (2n-6, p-1) + (n-2, p-1)$ for $p > 3$.

Finally we consider the case when $\gamma_1(G)$ is Abelian, that is, when $\alpha \equiv \varepsilon \equiv 0 \pmod{p}$: this arises when $n \geqslant 4$ for all p. If γ is prime to p, then γ can be assigned one of $(n-2, p-1)$ values and δ can be chosen to be zero. If p divides γ, then δ can be chosen to be either 0 or 1.

THEOREM 4.3. *For* $n \geqslant 4$ *the number of types of p-groups of maximal class of order* p^n *which possess an Abelian maximal subgroup is* $2 + (n-2, p-1)$.

Theorem 4.3 was proved by Wiman [11]. The number of groups of order p^5 and class 4 is by Theorems 4.2 and 4.3 $3 + (4, p-1) + 2(3, p-1)$ for $p > 3$, and this coincides with the result of Schreier [9]. Theorem 4.1 is in conflict with a result of Wiman (see [12], page 344).

Theorem 4.3 contains the well-known result that the number of 2-groups of maximal class of order 2^n is 3 provided that $n \geqslant 4$. Similarly all 3-groups of maximal class may be determined from Theorems 4.2 and 4.3. For $n \geqslant 5$ there exist 3 groups which possess no Abelian maximal subgroups: their defining relations are (32)–(38) with $\alpha = \gamma = 0$, $\beta = 1$ and $\delta = 0, 1, 2$. If n is even and $n \geqslant 4$ there exist 4 groups with an Abelian maximal subgroup: their defining relations are (32)–(38) with $\alpha = \beta = \delta = 0, \gamma = 1, 2$ or $\alpha = \beta = \gamma = 0$, $\delta = 0, 1$. If n is odd and $n \geqslant 5$ there exist 3 groups with an Abelian maximal subgroup: their defining relations are (32)–(38) with $\alpha = \beta = \delta = 0, \gamma = 1$ or $\alpha = \beta = \gamma = 0, \delta = 0, 1$. The first of these results is different from that of Wiman [12].

These results do not enable us to determine all groups of order p^6 and class 5 because not all such groups are metabelian. Thus let G be a non-metabelian group of order p^6 and class 5. We then have

$$1 < \gamma_2'(G) = [\gamma_2(G), \gamma_3(G)] \leqslant \gamma_5(G)$$

by Lemma 2.1: hence $[\gamma_2(G), \gamma_3(G)] = \gamma_5(G)$. Thus G does not have degree of commutativity greater than 0, and so by Theorem 3.8 $p > 3$. Also the centraliser of $\gamma_4(G)$ is a maximal subgroup different from $\gamma_1(G)$, and so we may choose s to be an element which belongs to the centraliser of $\gamma_4(G)$ but not to $\gamma_2(G)$. s_1 denotes as usual an element of $\gamma_1(G)$ which does not belong to $\gamma_2(G)$, and we define

$$s_2 = [s_1, s], \quad s_3 = [s_2, s], \quad s_4 = [s_3, s], \quad s_5 = [s_4, s_1]. \tag{46}$$

Then s_i and $\gamma_{i+1}(G)$ generate $\gamma_i(G)$ for $i = 2, 3, 4, 5$. By the definition of s

$$[s_4, s] = 1, \tag{47}$$

and by Lemma 2.9
$$[s_2, s_3] = s_5. \tag{48}$$

We transform the first equation of (46) by s_2 and obtain

$$s_2 = [s_1^{s_2}, s^{s_2}] = [s_1[s_1, s_2], s[s, s_2]].$$

Since $[s_1, s_2]$ lies in $\gamma_4(G)$ and the elements of $\gamma_4(G)$ commute with s and the elements of $\gamma_3(G)$, this gives

$$s_2 = [s_1, s\,s_3^{-1}] = [s_1, s_3^{-1}]\,s_2^{s_3^{-1}} = [s_3, s_1]\,s_2 s_5^{-1}$$

by (1), (2) and (48). Hence
$$[s_1, s_3] = s_5^{-1}. \tag{49}$$

Let us now put $\bar{s} = s$, $\bar{s}_1 = s_1 s_3^{\zeta}$ and define $\bar{s}_2, \bar{s}_3, \bar{s}_4, \bar{s}_5$ by relations similar to (46).

Then
$$\bar{s}_2 = s_2 s_4^{\zeta} s_5^{\zeta}, \qquad \bar{s}_3 = s_3, \qquad \bar{s}_4 = s_4, \qquad \bar{s}_5 = s_5.$$

Hence
$$[\bar{s}_1, \bar{s}_2] = [s_1 s_3^{\zeta}, s_2 s_4^{\zeta}] = [s_1, s_2]\,s_5^{-2\zeta},$$

so that if
$$[s_1, s_2] = s_4^{\alpha} s_5^{\beta}, \text{ then } [\bar{s}_1, \bar{s}_2] = \bar{s}_4^{\alpha} \bar{s}_5^{\beta-2\zeta}.$$

Thus by suitably choosing ζ we may ensure that $[\bar{s}_1, \bar{s}_2] = \bar{s}_4^{\alpha}$. We drop the bars and write

$$[s_1, s_2] = s_4^{\alpha}. \tag{50}$$

Finally by Theorem 3.2 we may write

$$s_1^p = s_5^{\gamma}, \qquad s^p = s_5^{\delta}, \qquad s_2^p = s_3^p = s_4^p = s_5^p = 1. \tag{51}$$

(46)–(51) are therefore the defining relations of G.

To determine the types we shall adopt the same procedure as above. It will be seen that this amounts to making a substitution

$$s \to \bar{s}, \quad s_1 \to \bar{s}_1,$$

and finding what conditions on $\bar{s}$ and $\bar{s}_1$ are required to preserve each of the defining relations, apart from replacing the parameters; we must also find the relations between the old and the new parameters. $\bar{s}$ and $\bar{s}_1$ are to be chosen to stand in the same relation to the characteristic subgroups of G as s and s_1 respectively. Hence we must take

$$\bar{s} = s^{\xi} s_2^{\xi_2} \dots s_5^{\xi_5}, \qquad \bar{s}_1 = s_1^{\eta_1} s_2^{\eta_2} \dots s_5^{\eta_5},$$

where $\xi\eta_1$ is not divisible by p. $\bar{s}_2, \bar{s}_3, \bar{s}_4, \bar{s}_5$ are defined by relations similar to (46), and so

$$\bar{s}_2 \equiv s_2^{\xi\eta_1} \pmod{\gamma_3(G)}; \qquad \bar{s}_3 \equiv s_3^{\xi^2\eta_1} \pmod{\gamma_4(G)};$$
$$\bar{s}_4 \equiv s_4^{\xi^3\eta_1} \pmod{\gamma_5(G)}; \qquad \bar{s}_5 = s_5^{\xi^3\eta_1^2}.$$

Thus the relation
$$[\bar{s}_1, \bar{s}_2] \equiv \bar{s}_4^{\bar{\alpha}} \pmod{\gamma_5(G)}$$
yields
$$\alpha\eta_1 \equiv \bar{\alpha}\xi^2 \pmod{p}. \tag{52}$$

Similarly we must work out the relations

$$\bar{s}_1^p = \bar{s}_5^{\bar{\gamma}}, \qquad \bar{s}^p = \bar{s}_5^{\bar{\delta}}.$$

Now the group generated by $\bar{s}$ and $\gamma_2(G)$ is a regular p-group, since its order is p^5 and $p \geqslant 5$. Also $\gamma_2(G)$ is of exponent p, and so

$$\bar{s}^p = s^{p\xi} = s_5^{\delta\xi}.$$

Also
$$\bar{s}^p = \bar{s}_5^{\bar{\delta}} = s_5^{\bar{\delta}\xi^3\eta_1^2}.$$

Hence
$$\xi^2\eta_1^2\bar{\delta} \equiv \delta \pmod{p}, \tag{53}$$

and similarly
$$\xi^3\eta_1\bar{\gamma} \equiv \gamma \pmod{p}. \tag{54}$$

There is one more fact to be considered: the substitution must be so chosen that

$$[\bar{s}_1, \bar{s}_2] = \bar{s}_4^{\bar{\alpha}},$$

and not merely that this holds as a congruence modulo $\gamma_5(G)$. However we may ignore this because if this equation fails to be valid after the substitution made in reducing the parameters to a standard set, we may make it true by making a second substitution in which $\xi = \eta_1 = 1$ and all the ξ_i, η_j are zero except η_3. This will not affect the values of α, γ, δ on account of the transformation laws (52)–(54).

To find the standard sets of parameters we consider first the case

$$[\gamma_1(G), \gamma_2(G)] = \gamma_4(G);$$

this is characterized by $\alpha \not\equiv 0 \pmod{p}$. By (52) we may take $\alpha = 1$ and must then assume that $\eta_1 \equiv \xi^2 \pmod{p}$; (53) and (54) then become

$$\delta \equiv \bar{\delta}\xi^6, \qquad \gamma \equiv \bar{\gamma}\xi^5 \pmod{p}$$

If p does not divide γ, then γ may be reduced to one of $(5, p-1)$ standard values, and we must then assume that $\xi^5 \equiv 1 \pmod{p}$. δ may then be assigned one of $1 + (p-1)/(p-1, 5)$ standard values, and so altogether we obtain $p - 1 + (p-1, 5)$ standard sets of parameters. If $\gamma \equiv 0 \pmod{p}$, then δ may be assigned one of $1 + (p-1, 6)$ values.

THEOREM 4.4. *For $p > 3$ the number of types of non-metabelian groups G of order p^6 and class 5 in which*

$$[\gamma_1(G), \gamma_2(G)] = \gamma_4(G)$$

is $p + (p-1, 5) + (p-1, 6)$.

In the case

$$[\gamma_1(G), \gamma_2(G)] = \gamma_5(G),$$

that is, $\alpha \equiv 0 \pmod{p}$, we proceed as follows. If γ is not divisible by p, we may suppose that $\gamma = 1$ by (54) and must then assume that $\xi^3\eta_1 \equiv 1 \pmod{p}$. Hence $\xi^4\delta \equiv \bar{\delta} \pmod{p}$ and δ can take one of $1 + (p-1, 4)$ standard values. If $\gamma \equiv 0 \pmod{p}$, then δ can be assigned the value 0, 1 or a quadratic non-residue modulo p by (54).

THEOREM 4.5. *For $p > 3$ the number of types of non-metabelian groups G of order p^6 and class 5 in which*

$$[\gamma_1(G), \gamma_2(G)] = \gamma_5(G)$$

is $4 + (p-1, 4)$.

From these results all groups of order p^6 and class 5 can be determined and for $p > 3$ the total number of them is

$$2p + 7 + 4(p-1, 4) + 2(p-1, 5) + 2(p-1, 6).$$

The five classes into which these groups are divided in Theorems 4.1–4.5 are the five families into which they fall in the sense of Hall [5]. Using the ideas of Hall's classification theory Easterfield [2] has determined all groups of order p^6, and the above results coincide with those of this author. For $p = 2, 3$ the groups of order p^6 and class 5 are of course already determined by Theorems 4.2, 4.3.

References

[1]. N. Blackburn, On prime-power groups in which the derived group has two generators. *Proc. Camb. Phil. Soc.* 53 (1957), 19–27.

[2]. T. E. Easterfield, Ph.D. dissertation, University of Cambridge, 1940.

[3]. P. Hall, A contribution to the theory of groups of prime-power order. *Proc. London Math. Soc.* (2), 36 (1933), 29–95.

[4]. ——, On a theorem of Frobenius. *Proc. Lond. Math. Soc.* (2), 40 (1935), 468–501.

[5]. ——, The classification of prime-power groups. *J. reine angew. Math.* 182 (1940), 130–141.

[6]. L. Kaloujnine, La structure des p-groupes de Sylow des groupes symmétriques finis. *Ann. sci. Éc. norm. sup.*, Paris, (3), 65 (1948), 239–276.

[7]. ——, Sur quelques propriétés des groupes d'automorphismes d'un groupe abstrait. *C. R. Acad. Sci. Paris,* 230 (1950), 2067–2069.

[8]. ——, Sur quelques propriétés des groupes d'automorphismes d'un groupe abstrait, (Généralisation d'un théorème de M. Ph. Hall). *C. R. Acad. Sci. Paris,* 231 (1950), 400–402.

[9]. O. Schreier, Über die Erweiterung von Gruppen, II. *Hamburg. Abh.* 4 (1926), 321–346.

[10]. J. A. Séguier, *Éléments de la théorie des groupes abstraits.* Paris, 1904.

[11]. A. Wiman, Über mit Diedergruppen verwandte p-Gruppen. *Arkiv för Matematik, Astronomi och Fysik* 33A (1946).

[12]. ——, Über p-Gruppen von maximaler Klasse, *Acta Math.*, 88 (1952), 317–346.

[13]. H. Zassenhaus, *Lehrbuch der Gruppentheorie.* Leipzig–Berlin, 1937.