ON A SPECIAL CLASS OF REGULAR p-GROUPS

BY
J. L. ALPERIN(1)

CHAPTER 1. INTRODUCTION

The concept of a finite p-group being regular was first defined and studied by P. Hall in two papers [3; 4]. Besides proving structure theorems for such groups and showing they had several properties in common with abelian groups, Hall gave a few sufficient conditions for a p-group to be regular. These criteria, in a vague sense, showed that if the "commutator structure" or "power structure" of a p-group was suitably restrictive then the group was regular. For example, if the class of a finite p-group, as a nilpotent group, is less than p, then the group is regular. This result evokes the converse question, namely, if a p-group is regular, is its class necessarily bounded by some function of p. This is, however, false for odd primes p, since there are metacyclic p-groups which are regular and of arbitrarily high class. Nevertheless, we can weaken the query and ask whether, for any regular p-group G, is there necessarily any bound on the derived length of G as a solvable group? This is true if $p = 2$, since every regular 2-group is abelian. However, for $p \geqq 5$, P. Hall, in yet unpublished work, has constructed regular p-groups of arbitrary derived length. This leaves only the prime $p = 3$ to be considered. We shall answer the question raised above by the following result:

THEOREM 1. *Any regular 3-group is metabelian.*

The proof of this assertion is by induction on the group order and involves obtaining a contradiction in the structure of a minimal counterexample. In fact, if G is such a counterexample, then we are able, at long length, to construct a subgroup H of G such that H can be generated by two elements but H', the derived group of H, is not cyclic. This contradicts the fact that all regular 3-groups that are generated by two elements have cyclic derived groups.

In view of this last statement the following theorem contains the above one as a special case.

THEOREM 2. *If G is a finite nilpotent group of odd order in which every two-generator subgroup of G has a cyclic derived group, then G is metabelian.*

It is this assertion that we shall prove, and this proof will constitute the major

Presented to the Society, December 11, 1961; received by the editors December 20, 1961.
(1) Supported by an N. S. F. predoctoral fellowship.

part of this work. The title of this paper derives from the fact that any finite p-group satisfying the hypothesis of this theorem is necessarily regular.

Whether the restriction to groups of odd order is necessary is not known to us. That is, if a group G is of order a power of two and satisfies the hypotheses of Theorem 2, then we are not able to prove that G is metabelian. In fact the proof of Theorem 2 breaks down in three different places if the prime two is considered. However, no counterexample is known to us to the possibility that Theorem 2 remains true for all finite nilpotent groups.

Nevertheless, we are able to prove the following infinite analogue of Theorem 2, namely:

THEOREM 3. *If G is a torsion-free nilpotent group in which every two-generator subgroup has a cyclic derived group, then G is metabelian.*

In the course of proving Theorem 2 it is necessary to investigate groups in which every subgroup, which can be generated by at most three elements, is metabelian. B. H. Neumann [7] has studied such groups with relation to questions on varieties of groups. He showed that such a group is not necessarily metabelian. However, the example he constructed to show this was a finite group of order a power of two. The next result shows that this was not mere chance.

THEOREM 4. *If G is a finite, nilpotent group of odd order in which every three-generator subgroup is metabelian, then G is metabelian.*

Although subgroups and factor groups of regular p-groups are regular, direct products of regular p-groups need not be regular. For this reason the following assertion becomes interesting.

THEOREM 5. *If G is a regular 3-group then $G \times H$ is regular for all regular 3-groups H if and only if G' is of exponent at most three.*

Theorem 2 arouses the question of whether the restriction to nilpotent groups was necessary. The concluding theorem, due to G. Higman, for which we have found an elementary proof, gives a partial answer to that question:

THEOREM 6. *Let G be a finite group in which every subgroup which can be generated by two elements has a cyclic derived group. Then G is solvable and moreover, if p is the largest prime dividing the order of G, then a Sylow p-subgroup of G is normal in G.*

The proofs of these theorems are organized in the following fashion. In the remainder of Chapter 1 the pertinent definitions and notations are described and a summary of the basic results on finite p-groups, which we shall require, is given. Chapter 2 contains the proof of Theorem 2 with the proof of Theorem 4 inserted in §2.2. Chapter 3 is devoted to the proof of two consequences of Theorem

2, namely, Theorem 1 and Theorem 3. The proofs of Theorem 5 and Theorem 6 are to be found in Chapters 4 and 5, respectively.

Before proceeding further, the author would like to acknowledge, with deep appreciation, the advice and encouragement given him by Professor G. Higman.

1.1. **Notation and definitions.** Let G be any group and $x, y, x_1, y_1, x_2, y_2, \ldots$ be some of its elements. Then $|G|$ is the order of G and $|x|$ is the order of the element x. We denote the subgroup of G generated by $x_1, x_2, \ldots$, by $\{x_1, x_2, \ldots\}$. Furthermore, we define a commutator

$$(x, y) = x^{-1}y^{-1}xy$$

and inductively

$$(x_1, \ldots, x_n, x_{n+1}) = ((x_1, \ldots, x_n), x_{n+1}).$$

We also let $x^y = y^{-1}xy = x(x,y)$ and

$$(x_1, \ldots, x_m;\ y_1, \ldots, y_n) = ((x_1, \ldots, x_m),\ (y_1, \ldots, y_n)).$$

If $K, H, H_1, H_2, \ldots$ are subgroups of G then we denote by (H, K) the subgroup of G generated by all elements (h, k) for $h \in H$, $k \in K$. And recursively,

$$(H_1, \ldots, H_n, H_{n+1}) = ((H_1, \ldots, H_n),\ H_{n+1}).$$

The derived series of G is defined as follows:

$$G' = (G, G),$$

$$G^{(n+1)} = (G^{(n)}, G^{(n)})$$

and $G^{(n)}$ is called the nth derived group of G. G' is also called the commutator subgroup of G. The lower central series of G is obtained by letting

$$G_1 = G,$$

$$G_{n+1} = (G_n, G).$$

Note that $G_2 = G'$. If $G'' = 1$ then we say that G is metabelian and if $G_{c+1} = 1$ but $G_c \neq 1$ then we say that G is nilpotent of class c. The center of the group G is denoted by $Z(G)$.

A finite group of prime-power order, say p^m, is called a p-group. If G is a p-group then $\mho^\alpha G$ denotes the subgroup of G generated by all elements x^{p^α}, where $x \in G$. The subgroup of G generated by all elements of order at most p^α is denoted by $\Omega_\alpha G$. The Frattini subgroup of G is written $\Phi(G)$, and is the intersection of the maximal subgroups of G.

A p-group G is said to be regular provided for any two elements x and y of G we can express, for each positive integer α,

$$(xy)^{p^\alpha} = x^{p^\alpha} y^{p^\alpha} c_1^{p^\alpha} c_2^{p^\alpha} \ldots c_s^{p^\alpha}$$

for suitable elements $c_1, c_2, \ldots, c_s$ of the derived group of the subgroup generated by x and y. Of course, $c_1, \ldots, c_s$ depend on α as well as x and y. From this definition it is clear that subgroups and factor groups of regular groups are regular and that a p-group G is regular if and only if every two-generator subgroup of G is regular.

1.2. **Basic results on p-groups.** In this section we summarize the fundamental facts on p-groups that we shall require in later arguments. For the proofs of these assertions the reader should consult [2] (especially Chapters 10 and 12) and [3]. Throughout this section G will denote a finite p-group.

A very fundamental result is the *Burnside Basis Theorem.* The factor group $G/\Phi(G)$ is an elementary abelian group. If this factor group has order p^r then any set of elements which generate G contains a subset of r elements which generate G and which map onto a basis of $G/\Phi(G)$ under the natural homomorphism. Conversely, any set of r elements of G, which map onto a basis of $G/\Phi(G)$, will generate G.

Because of this theorem the phrase "G is an r-generator group" is unambiguous and if we say that G is generated by r elements then we mean the number r defined by the theorem. If however, we should say G can be generated by s elements then we mean only $r \leqq s$.

Since $G/\Phi(G)$ is elementary abelian we have that $\Phi(G) \geqq G'\mathfrak{V}^1(G)$. However, equality holds, that is, $\Phi(G) = G'\mathfrak{V}^1(G)$. Also, the above theorem then implies that if G is generated by $x_1, \ldots, x_s$ and G' then G can be generated by $x_1, \ldots, x_s$.

Let $G = G_1 \supseteq G_2 \supseteq G_3 \supseteq \ldots$ be the lower central series of G. There exists some integer k such that $G_k = 1$ so that G is nilpotent. If G is generated by $x_1, \ldots, x_r$ then G_n can be generated by all elements $(x_{i_1}, \ldots, x_{i_n})$, for $x_{i_1}, \ldots, x_{i_n}$ among the x_j, and G_{n+1}. If N is a normal subgroup of G then the nth member of the lower central series of G/N is $(G/N)_n = G_nN/N$.

If H is a nonidentity normal subgroup of G then $H \cap Z(G) \neq 1$. In particular, if H has order p then $H \subseteq Z(G)$. Finally, there exists a normal subgroup K of G such that $K \subseteq H$ and the index $[H:K]$ of K in H is equal to p.

The following commutator identities will be frequently used in later arguments. If x, y and z are elements of G then

$$(xy, z) = (x, z)(x, z, y)(y, z),$$

$$(x, yz) = (x, z)(x, y)(x, y, z).$$

As with all the material in this section, no reference will be given to these equations when they are used. If the derived group of G is central and of exponent at most p and if n is a positive integer then

$$(xy)^{p^n} = x^{p^n}y^{p^n}$$

provided p is an *odd* prime.

We can now prove the well-known assertion we made above that any regular 2-group is abelian. For let G be a regular and nonabelian 2-group. Then $G/\mathfrak{V}'(G')$ is nonabelian. But the definition of regularity, for $\alpha = 1$, insures that if x and y are elements of $G/\mathfrak{V}^1(G')$ then

$$(xy)^2 = x^2y^2.$$

If we cancel an x on the left and a y on the right of this equation then we have $xy = yx$ which is a contradiction because this holds for all x and y in $G/\mathfrak{V}^1(G')$.

Chapter 2. Proof of Theorem 2

We first note that it is sufficient to prove this theorem for finite p-groups, where p is an odd prime. If the theorem is not true then we can choose a finite p-group G which is a minimal counterexample to the theorem. That is, Theorem 2 holds for every p-group having its order smaller than the order of G. This group G shall remain fixed throughout Chapter 2, and we shall study G and finally obtain a contradiction to its supposed structure.

The proof proceeds in four stages. In §2.1 we prove some lemmas which give a general description of G. In §2.2 we insert the proof of Theorem 4 and make an application of that theorem to G. §2.3 contains many technical lemmas which give detailed information on G. The last section contains the final contradiction.

2.1. **A general description of** G. The first lemma of this section is a technical lemma which we shall use in various calculations with commutators. The last two lemmas give us a general description of the structure of the group G. For example, we determine the order of G'', the class of G' and the structure of the center of G.

Lemma 2.1.1. *Let H be any group.*

(i) *If $(H_2, H_3) = 1$ and $x \in H'$, $y \in H$ then*

$$(x, y)^{-1} = (x^{-1}, y).$$

(ii) *If $H'' = 1$ and $x, y, z \in H$ then*

$$(x, y, z)(y, z, x)(z, x, y) = 1.$$

(iii) *If $H'' = 1$ and $x \in H', y, z \in H$ then*

$$(x, y, z) = (x, z, y).$$

(iv) *If $x, y \in H$ such that $(x, y, x) = 1$ then for any positive integer n,*

$$(x^n, y) = (x, y)^n.$$

(v) *If $H'' = 1$ and $x, y \in H$ then for any positive integer n,*

$$(x, y^n) = (x, y)^{\binom{n}{1}}(x, y, y)^{\binom{n}{2}} \cdots (x, \overbrace{y, \ldots, y}^{n})^{\binom{n}{n}}.$$

Proof. (i) First note that $(x, y, x^{-1}) \in (H_2, H, H_2) = (H_3, H_2) = 1$ so $(x, y, x^{-1}) = 1$. Hence $1 = (xx^{-1}, y) = (x, y)(x, y, x^{-1})(x^{-1}, y) = (x, y)(x^{-1}, y)$.

(ii) This statement follows from the equation $(x, y)^z = (x^z, y^z)$ (see Zassenhaus [8, p. 83]).

(iii) First $(y, z, x) = 1$ because $(y, z) \in H'$. Thus, from part (ii) of this lemma, we have

$$1 = (x, y, z)(z, x, y)$$

so $(x, y, z) = (z, x, y)^{-1} = ((z, x)^{-1}, y) = (x, z, y)$, by part (i).

(iv) We shall prove this assertion by induction on n. For $n=1$ the equation is trivial. If it is true for n then

$$\begin{aligned}(x^{n+1}, y) &= (x^n x, y) = (x^n, y)(x^n, y, x)(x, y)\\ &= (x, y)^n((x, y)^n, x)(x, y)\end{aligned}$$

by the inductive hypothesis, so

$$\begin{aligned}&= (x, y)^n(x, y, x)^n(x, y)\\ &= (x, y)^{n+1}\end{aligned}$$

follows from the inductive hypothesis applied to the elements (x, y) and x since $(x, y, x; x, y) = (1; x, y) = 1$.

(v) This part will also be proved by induction on n. If it is true for n then

$$\begin{aligned}(x, y^{n+1}) &= (x, y^n y) = (x, y)(x, y^n)(x, y^n, y)\\ &= (x, y) \cdot (x, y)^{\binom{n}{1}}(x, y, y)^{\binom{n}{2}} \cdots (x, \overbrace{y, \ldots, y}^{n})^{\binom{n}{n}}\\ &\quad \cdot (x, y)^{\binom{n}{1}}(x, y, y)^{\binom{n}{2}} \cdots (x, \overbrace{y, \ldots, y}^{n})^{\binom{n}{n}}, y\end{aligned}$$

which is, because $H'' = 1$ and by part (iv),

$$\begin{aligned}&= (x, y) \cdot (x, y)^{\binom{n}{1}}(x, y, y)^{\binom{n}{1}+\binom{n}{2}} \cdots\\ &\quad \cdot (x, \overbrace{y, \ldots, y}^{k})^{\binom{n}{k-1}+\binom{n}{k}} \cdots (x, \overbrace{y, \ldots, y}^{n+1})^{\binom{n}{n}}\\ &= (x, y)^{\binom{n+1}{1}}(x, y, y)^{\binom{n+1}{2}} \cdots (x, \overbrace{y, \ldots, y}^{n+1})^{\binom{n+1}{n+1}}.\end{aligned}$$

LEMMA 2.1.2. (i) *Every proper subgroup and proper factor group of G satisfies the hypothesis of the theorem and so is metabelian.*

(ii) *G has either three or four generators in a minimal generating set.*

(iii) *The center $Z(G)$ of G is cyclic.*

(iv) *G'' has order p.*

(v) *G' is of class two.*

(vi) *$\mathfrak{V}^1(G')$ is a central subgroup of G'.*

(vii) *G is a regular p-group.*

Proof. (i) Since G is assumed to be a minimal counterexample to the theorem, the last part of the assertion is implied by the first part. However, every subgroup of G clearly satisfies the hypothesis of the theorem. Finally, if N is a normal subgroup of G and xN and yN are elements of G/N, for elements x and y of G, then $(x, y)N$ generates the derived group of the group generated by xN and yN.

(ii) Since G is not metabelian G' cannot be generated by a commutative set. Hence, there exist elements a, b, c, and d of G such that $(a, b; c, d) \neq 1$. The subgroup of G generated by a, b, c and d is not metabelian, so by part (i), this subgroup is G itself. Hence, G has at most four generators. But, if G could be generated by two elements then G' would be cyclic so that $G'' = 1$ and this would be a contradiction. Therefore, G has either three or four generators.

(iii) If the center of G is not cyclic then we may choose central subgroups Z_1 and Z_2 of G, each of order p, such that $Z_1 \cap Z_2 = 1$. The mapping of G into $G/Z_1 \times G/Z_2$ defined by sending $g \in G$ to $\langle gZ_1, gZ_2 \rangle$ is consequently a monomorphism. But G/Z_1 and G/Z_2 are metabelian, by the first part of this lemma, so we have G embedded in a metabelian group (which does not necessarily satisfy the hypothesis of the theorem) so G is metabelian, and this is a contradiction.

(iv) If G'' has order greater than p then we may choose a normal subgroup H of G contained in G'' and of index p in G''. Then $(G/H)' = G'/H$ so G/H is not metabelian and this contradicts part (i) of this lemma.

(v) Since G'' is normal in G' and of order p it is contained in the center of G' so $(G')_3 = (G'', G') = 1$ and G' has class two.

(vi) The subgroup $\mathfrak{V}^1(G')$ is generated by all elements x^p for $x \in G'$. Therefore, it is enough to show that $(x^p, y) = 1$ whenever $x, y \in G'$. But $(x^p, y) = (x, y)^p$ by Lemma 2.1.1.(iv) and part (v) and $(x, y)^p = 1$ because G'' has order p.

(vii) For any elements x and y of G we need only show the existence of the equation defining regularity for $\alpha = 1$ (see M. Hall [2, p. 184]). That is, it is enough to show there exists an integer k such that $(xy)^p = x^p y^p (x, y)^{kp}$. If H is the subgroup of G generated by x and y then H' is cyclic and hence generated by (x, y). The derived group of $H/\mathfrak{V}^1(H')$ is $H'/\mathfrak{V}^1(H')$ and therefore of order p. Thus $H/\mathfrak{V}^1(H')$ is of class two and

$$(xy)^p \equiv x^p y^p (y, x)^{\binom{p}{2}} (\text{modulo } \mathfrak{V}^1(H')),$$

or

$$(xy)^p \equiv x^p y^p (\text{modulo } \mathfrak{V}^1(H')),$$

because p is odd. Since $(x, y)^p$ generates $\mathfrak{V}^1(H')$ we are done.

LEMMA 2.1.3. (i) *$G/\mathfrak{V}^1(G')$ is of class at most three if $p = 3$ and is of class at most two if $p > 3$.*

(ii) *$G'(\mathfrak{V}^1(G')$ is abelian so $\Phi(G') = \mathfrak{V}^1(G')$.*

(iii) *If $x_1, \ldots, x_n$ generate G then the elements (x_i, x_j), for $i < j$, and (x_l, x_j, x_k),*

for $i<j<k$, generate G'. However, *if $p>3$ then G' is generated by the elements (x_i, x_j), for $i<j$.*

(iv) *If x and y are elements of G then (x,y,y), $(y,x,y)\in\mathfrak{V}^1(G')$. If $p>3$ and $z\in G$ then $(x,y,z)\in\mathfrak{V}^1(G')$.*

(v) *If x_1, x_2 and x_3 are elements of G and σ is a permutation of $\{1,2,3\}$ then*

$$(x_{\sigma_1}, x_{\sigma_2}, x_{\sigma_3}) \equiv (-1)^{\sigma}(x_1, x_2, x_3) \text{ (modulo } \mathfrak{V}^1(G'))$$

where $(-1)^{\sigma}=-1$ if σ is an odd permutation and $(-1)^{\sigma}=1$ otherwise.

Proof. If x and y are elements of G then let H be the subgroup generated by them. H' will be generated by (x,y). If $H'=1$ then $(x,y,y)=1$ and if $H'\neq 1$ then H_3 is a proper subgroup of H' so (x,y,y) is an element of the cyclic subgroup generated by $(x,y)^p$. In either case, in $G/\mathfrak{V}^1(G')$ every two elements a and b satisfy the identical relation $(a,b,b)=1$. From this identity the structure of $G/\mathfrak{V}^1(G')$ follows, Levi, [5], and we have (i), the first part of (ii), (iv) and (v). Also $\Phi(G')=\mathfrak{V}^1(G')G''$ but since $G'/\mathfrak{V}^1(G')$ is abelian implies $\mathfrak{V}^1(G')\geqq G''$ we have $\Phi(G')=\mathfrak{V}^1(G')$. Finally, (iii) follows from (i) and (ii).

This last lemma surprisingly shows that the case $p=3$ is the most difficult with which to deal. In fact, several lemmas that we shall prove later are trivial if $p>3$.

2.2. **Proof of Theorem 4.** We wish now to improve the statement of Lemma 2.1.2.(ii). To do this it will be necessary to prove Theorem 4. Indeed, Theorem 4 has the following consequence:

COROLLARY 2.2.1. *The group G has exactly three generators in a minimal generating set.*

Proof. By Lemma 2.1.2.(ii) we know that G has either three or four generators. Suppose that the latter possibility occurs. Then every three-generator subgroup of G is a proper subgroup and hence is metabelian, by Lemma 2.1.2.(i). By Theorem 4, G is metabelian and this is a contradiction.

We now turn to a proof of Theorem 4. Let H be a group which satisfies the hypotheses of the theorem and assume that every group which also satisfies these hypotheses, but has smaller order than H, is metabelian. It is enough to show that H is metabelian. To do this we require the following sequence of three lemmas.

LEMMA 2.2.2. (i) *Every proper subgroup of H is metabelian.*

(ii) *H has four generators in a minimal generating set or $H''=1$.*

Proof. (i) The hypotheses of the theorem are clearly inherited by subgroups so by assumption every proper subgroup of H is metabelian.

(ii) If H can be generated by less than four elements then it is clearly metabelian. Suppose, however, that H cannot be generated by four elements so every four-generator subgroup of H is a proper subgroup. Then, if $x,y,u,v\in H$, the subgroup $\{x,y,u,v\}=K$ is proper so $K''=1$ and therefore $(x,y:u,v)=1$

Hence, H is metabelian, because we have just shown every two commutators commute.

LEMMA 2.2.3. *If H is generated by four elements then $(H_2, H_3) = 1$.*

Proof. It is sufficient to demonstrate that if $x_1, \ldots, x_m, y_1, \ldots, y_n \in H$ and $m \geqq 2$, $n \geqq 3$ then $(x_1, \ldots, x_m; y_1, \ldots, y_n) = 1$. Consider the subgroup K generated by $(x_1, \ldots, x_{m-1}), x_m, (y_1, \ldots, y_{n-1})$ and y_n, where $(x_1, \ldots, x_{m-1}) = x_{m-1}$ if $m = 2$. Since $(y_1, \ldots, y_{n-1}) \in H'$ and the subgroup $\{(x_1, \ldots, x_{m-1}), x_m, y_n\}$ is proper, having less than four generators, it follows that K is proper and therefore metabelian. Thus, the elements $(x_1, \ldots, x_m)$ and $(y_1, \ldots, y_n)$ of K' commute.

LEMMA 2.2.4. *If H has four generators then $H'' = 1$.*

Proof. Let a, b, c and d be generators of H. The subgroup H_2 is generated by the elements (a, b), (a, c), (a, d), (b, c), (b, d), (c, d) and H_3. By the previous lemma it is enough to show these six elements commute with each other. But any two of these which involve together only three of the generators, for example (a, b) and (a, c), must commute by the hypothesis of the theorem. Therefore, it is enough to prove that each of the elements

$$\xi = (a, b; c, d), \quad \eta = (a, c; b, d), \quad \zeta = (a, d; b, c)$$

is equal to 1. Since H has odd order it is sufficient to show that $\xi^2 = \eta^2 = \zeta^2 = 1$. However, by the hypotheses of the theorem we have

$$1 = (a, bc; bc, d),$$

so expanding this commutator and using Lemma 2.2.3 we have

$$\begin{aligned} 1 &= ((a, c)(a, b)(a, b, c), (b, d)(b, d, c)(c, d)) \\ &= (a, c; c, d)(a, c; b, d)(a, b; c, d)(a, b; b, d) \\ &= (a, c; b, d)(a, b; c, d) = \eta\xi. \end{aligned}$$

Similarly, from $1 = (ad, b; c, ad)$ we obtain

$$\begin{aligned} 1 &= (a, b; c, d)(d, b; c, a) \\ &= (a, b; c, d)(a, c; b, d)^{-1} = \xi\eta^{-1} \end{aligned}$$

by Lemma 2.1.1.(i). Hence $\eta = \xi = \eta^{-1}$ so $\eta^2 = 1$. Similarly, one can show $\xi^2 = \zeta^2 = 1$.

2.3. **Detailed lemmas.** In this section we shall prove a series of six lemmas each of which gives us detailed information about some aspect of the structure of G. These results are all to be applied to the final lemmas in the next section, at which time their roles will be clear. The first of these lemmas is analogous to Lemma 2.2.3.

LEMMA 2.3.1. $(G_2, G_3) = 1$.

Proof. By Corollary 2.2.1 we may choose three elements a, b and c which generate G. By Lemma 2.1.3.(iii) G' is generated by (a,b), (a,c), (b,c), (a,b,c) and $\Phi(G')$. Also that lemma implies that G_3 is generated by (a,b,c) and $G_3 \cap \Phi(G')$. Since $\Phi(G')$ is a central subgroup of G', to prove this lemma it is enough to show that (a,b,c) commutes with each of (a,b), (a,c) and (b,c). But if (a,b,c) and (a,b) did not commute then (a,b) and (a,c,b) would not commute because

$$(a,b,c) \equiv (a,c,b)^{-1} (\text{modulo } \Phi(G'))$$

by Lemma 2.1.3.(v). However, if $(a,b;a,c,b) \neq 1$ then the proper subgroup of G generated by a, b and (a,c) would not be metabelian, contradicting Lemma 2.1.2.(i). Also if $(a,c;a,b,c) \neq 1$ or $(b,c;a,b,c) \neq 1$ then either the proper subgroup of G generated by a,c and (a,b) or the proper subgroup of G generated by b,c and (a,b) would not be metabelian.

LEMMA 2.3.2. *If a,b and c generate G then $(a,b,c)^p = 1$ or (a,b,c) generates a cyclic normal subgroup containing G''.*

Proof. Let H be the subgroup of G generated by G'' and (a,b,c). We shall, as a first step, prove that H is a normal subgroup of G. Since G'' is a central subgroup of G it suffices to show that every conjugate of (a,b,c) is contained in H. To do this it is enough to prove that $(a,b,c)^a$, $(a,b,c)^b$ and $(a,b,c)^c$ lie in H. But this is true if and only if (a,b,c,a), (a,b,c,b) and (a,b,c,c) are elements of H. By Lemma 2.1.1.(iii),

$$(a,b,c,a) \equiv (a,b,a,c) \text{ modulo } G''.$$

Also (a,b,a) is some power of (a,b), say $(a,b,a) = (a,b)^k$. By Lemma 2.1.1.(iv) it follows that $(a,b,a,c) = (a,b,c)^k$ since $(G_2, G_3) = 1$. Hence $(a,b,c,a) \in H$. Similarly $(a,b,c,b) \in H$. Finally, (a,b,c,c) is an element of the derived group of the group generated by (a,b) and c, so (a,b,c,c) is a power of (a,b,c) and thus lies in H.

Since G'' is central in G every element of H can be written as a product of an element of G'' and a power of (a,b,c). Such elements clearly commute so H is abelian. Then either H is cyclic and we are done or H is of type (p^n, p) and is the direct product of the cyclic group generated by (a,b,c) of order p^n and G''. In this case either $n = 1$ so $(a,b,c)^p = 1$ or $\mho^1(H)$ is a characteristic subgroup of H. In the latter case $\mho^1(H)$ will be a normal subgroup of G such that $\mho^1(H) \cap G'' = (1)$. However, $\mho^1(H)$ must contain nonidentity central elements and, because $Z(G)$ is cyclic, must contain G''. Hence, we have a contradiction unless $n = 1$.

LEMMA 2.2.3. *Let a, b and c generate G. Then $\{(a,b)\} \cap Z(G) \neq 1$ if and only if $|(a,b,c)| < |(a,b)|$.*

Proof. If (a,b) has order p^n then $\{(a,b)\} \cap Z(G) \neq 1$ if and only if $(a,b)^{p^{n-1}} \in Z(G)$. However, this holds if and only if $(a,b)^{p^{n-1}}$ commutes with a, b and c.

There exist integers s and t such that

$$(a,b,a) = (a,b)^{sp}, (a,b,b) = (a,b)^{tp}$$

so

$$((a,b)^{p^{n-1}},a) = (a,b,a)^{p^{n-1}} = 1,$$
$$((a,b)^{p^{n-1}},b) = (a,b,b)^{p^{n-1}} = 1$$

by Lemma 2.1.1.(iv). Since $(G_2,G_3)=1$, $((a,b)^{p^{n-1}},c) = (a,b,c)^{p^{n-1}}$ so $\{(a,b)\} \cap Z(G) \neq 1$ if and only of $(a,b,c)^{p^{n-1}} = 1$, that is $|(a,b,c)| < |(a,b)|$.

LEMMA 2.3.4. *There exist generators a, b and c of G such that no two of the elements (a,b), (a,c) and (b,c) commute.*

Proof. Let a',b' and c' be any set of generators for G. Then G' is generated by (a',b'), (a',c'), (b',c') and (a',b',c'). Since $(a',b',c') \in G_3$ it is central in G'. Since G' is not abelian at least two of the elements (a',b'), (a',c') and (b',c') must not commute.

First suppose that $(a',b';\ a',c')=1$ but that $(a',b';\ b',c') \neq 1$ and $(a',c';\ b',c') \neq 1$. Then let $a=a'c'$, $b=b'$, $c=c'$ so that a, b and c generate G and

$$\begin{aligned}(a,b;\,a,c) &= ((a',b')(a',b',c')(c',b'),(a',c')(a',c',c')) \\ &= (a',b';\,a',c')(c',b';\,a',c') \\ &= (a',c';\,b',c') \neq 1,\end{aligned}$$
$$\begin{aligned}(a,b;\,b,c) &= ((a',b')(a',b',c')(c',b'),(b',c')) \\ &= (a',b';\,b',c')(c',b';\,b',c') \\ &= (a',b';\,b',c') \neq 1,\end{aligned}$$
$$\begin{aligned}(a,c;\,b,c) &= ((a',c')(a',c',c');\,b',c') \\ &= (a',c';\,b',c') \neq 1.\end{aligned}$$

However suppose that we have instead that $(a',b';\,b\,,c') = (a',b';\,a',c')=1$ but that $(a',c';\,b',c') \neq 1$. Then, let $a=a'c'$, $b=b'c', c=c'$, so that

$$\begin{aligned}(a,b;\,a,c) &= (a'c',b'c';\,a'c',c') \\ &= ((a',c')(a',b')(c',b')g;\,(a',c')(a',c',c'))\end{aligned}$$

where g is some element of $\mathfrak{V}^1(G')$, so

$$\begin{aligned}(a,b;\,a,c) &= ((a',c')(a',b')(c',b'),(a',c')) \\ &= (a',b';\,a',c')(c',b';\,a',c') \\ &= (a',c';\,b',c') \neq 1.\end{aligned}$$

Similarly

$$\begin{aligned}(a,b;\,b,c) &= (a'c',b'c';\,b'c',c')\\ &= ((a',b')(a',c')(c',b'),(b',c'))\\ &= (a',c';\,b',c') \neq 1\end{aligned}$$

and

$$\begin{aligned}(a,c;\,b,c) &= (a'c',c';\,b'c',c')\\ &= (a',c';\,b',c') \neq 1.\end{aligned}$$

All other possibilities may be handled in an entirely similar manner.

LEMMA 2.3.5. *Let a, b and c be any set of generators of G. Then, among the elements (a,b,c), (a,c,b) and (b,c,a), the highest order appears twice.*

Proof. Since $(a,c,b) = ((a,c)^{-1},b)^{-1} = (c,a,b)^{-1}$ by Lemma 2.1.1.(i) and Lemma 2.3.1, we have, by Lemma 2.1.1.(ii) that

$$(a,b,c)(a,c,b)^{-1}(b,c,a) \in G''.$$

But suppose this lemma is not true. Then without any loss of generality we may assume (a,b,c) has order p^n and $(a,c,b)^{p^{n-1}} = (b,c,a)^{p^{n-1}} = 1$. We then have, because G'' has order p,

$$(a,b,c)^{p^{n-1}}(a,c,b)^{-p^{n-1}}(b,c,a)^{p^{n-1}} = 1$$

unless $n = 1$. This gives a contradiction unless $n = 1$. To conclude the poof of this lemma we need only show this case cannot arise. If it did then,

$$(a,b,c)^p = 1, (a,c,b) = (b,c,a) = 1.$$

If we can now show that $(a,b;\,a,c) = (a,b;\,b,c) = (a,c;\,b,c) = 1$ this would imply $G'' = 1$, by the argument in the first paragraph of the proof of the previous lemma. However,

$$\begin{aligned}1 &= (a,c,b,c) = ((a,c),b,c)\\ &= (b,c,(a,c))^{-1}(c,(a,c),b)^{-1}\end{aligned}$$

by Lemma 2.1.1.(iii) and Lemma 2.1.2.(i). Hence, by Lemma 2.1.1.(i),

$$1 = (a,c;\,b,c)\,(a,c,c,b).$$

But $(a,c,c) = (a,c)^{sp}$ for some integer p so that

$$(a,c,c,b) = ((a,c)^{sp},b) = (a,c,b)^p = 1.$$

Thus $(a,c;\,b,c) = 1$. Similarly, we have

$$\begin{aligned}1 &= (a,c,b,a) = ((a,c),b,a)\\ &= (b,a,(a,c))^{-1}(a,(a,c),b)^{-1}\\ &= (a,b;\,a,c)(a,c,a,b) = (a,b;\,a,c),\end{aligned}$$

and finally

$$\begin{aligned} 1 &= (b,c,a,b) = ((b,c),a,b) \\ &= (a,b,(b,c))^{-1}(b,(b,c),a)^{-1} \\ &= (a,b;\,b,c)^{-1}(b,c,b,a) = (a,b;\,b,c)^{-1}. \end{aligned}$$

LEMMA 2.3.6. *Suppose G is generated by a, b and c such that $(a,b;a,c) \neq 1$ and $\{(a,b)\} \cap \{(a,c)\} = \{1\}$. If G' has exponent p^n then $\mho^{n-1}(G')$ is generated by $(a,b)^{p^{n-1}}$, $(a,c)^{p^{n-1}}$ and $(b,c)^{p^{n-1}}$.*

Proof. Since G' is generated by (a,b), (a,c), (b,c) and (a,b,c), $\mho^{-1}(G')$ is generated by the p^{n-1}th powers of these four elements. Since $n > 1$, or else $\mho^1(G') = \Phi(G') = 1$ so G' is abelian, we will have proved this lemma if we can show that $(a,b,c)^p = 1$ or $\{(a,b,c)\} \cap \{(a,b)\}\{(a,c)\} \neq 1$. For in the latter case $(a,b,c)^{p^{n-1}}$ can be expressed as a product of a power of (a,b) and a power of (a,c). But $|(a,b,c)| \leqq |(a,b)|$, since $(a,b,c)^{p^i} = ((a,b)^{p^i},c)$ for any integer i, so this expression shows that either $(a,b,c)^{p^{n-1}} = 1$ or $(a,b,c)^{p^{n-1}}$ can be expressed as a product of a power of $(a,b)^{p^{n-1}}$ and a power of $(a,c)^{p^{n-1}}$.

However, suppose that $(a,b,c)^p \neq 1$ and that $\{(a,b,c)\} \cap \{(a,b)\}\{a,c)\} = 1$. Then, by Lemma 2.3.2, $\{(a,b,c)\}$ contains G'', so the product $H = \{(a,b)\}\{(a,c)\}\cdot\{(a,b,c)\}$ is a subgroup. Our assumption that $\{(a,b,c)\} \cap \{(a,b)\}\{(a,c)\} = 1$ implies that every element of H can be expressed uniquely as a product

$$(a,b)^{s_1}(a,c)^{s_2}(a,b,c)^{s_3}. \quad \begin{aligned} 0 &\leqq s_1 < |(a,b)|, \\ 0 &\leqq s_2 < |(a,c)|, \\ 0 &\leqq s_3 < |(a,b,c)|. \end{aligned}$$

For suppose that

$$(a,b)^{s_1}(a,c)^{s_2}(a,b,c)^{s_3} = (a,b)^{t_1}(a,c)^{t_2}(a,b,c)^{t_3}$$

so

$$(a,b)^{s_1}(a,b,c)^{s_3-t_3}(a,c)^{s_2} = (a,b)^{t_1}(a,c)^{t_2}$$

because $(G_2, G_3) = 1$. Hence

$$(a,b,c)^{s_3-t_3} = (a,b)^{t_1-s_1}(a,c)^{t_2-s_2}$$

so $s_1 = t_1$, $s_2 = t_2$, $s_3 = t_3$.

Now consider the subgroup of G generated by the two elements a and bc. Therefore, (a,bc,a) must be a power of $(a,bc)^p$. But

$$\begin{aligned} (a,bc) &= (a,c)(a,b)(a,b,c), \\ (a,bc,a) &= (a,c,a)(a,b,a)(a,b,c,a) \\ &= (a,b,a)(a,c,a)(a,b,c,a). \end{aligned}$$

Also $(a,bc)^p = ((a,b)(a,c)(a,b,c))^p$ because $(a,b;\,a,c)^p = 1$. Furthermore,

$$\begin{aligned} (a,b,c,a) &= ((a,b),c,a) = (c,a,(a,b))^{-1}(a,(a,b),c)^{-1} \\ &= (a,c;\,a,b)(a,b,a,c). \end{aligned}$$

Let A_1 and A_2 be integers such that

$$(a, b, a) = (a, b)^{p^{A_1}},\ (a, c, a) = (a, c)^{p^{A_2}}.$$

Then $(a, b, c, a) = (a, c; a, b)(a, b, c)^{p^{A_1}}$ and the condition that (a, bc, a) is a power of (a, bc) is that

$$(a, b)^{p^{A_1}}(a, c)^{p^{A_2}}(a, c;\ a, b)(a, b, c)^{p^{A_1}}$$

is a power of $(a, b)^p(a, c)^p(a, b, c)^p$. Hence $(a, c)^{p^{(A_2-A_1)}}(a, c;\ a, b)$ is a power of $(a, b)^p(a, c)^p(a, b, c)^p$. But by Lemma 2.3.2 $(a, c;\ a, b)$ is an element of $\{(a, b, c)\}$. Therefore, we must have $|(a, b, c)| > |(a, b)|$. This however contradicts the fact that if i is a positive integer then $(a, b, c)^{p^i} = ((a, b)^{p^i}, c)$ and $|(a, b, c)| \leqq |(a, b)|$.

2.4 **Conclusion of the proof.** If the elements a, b and c generate G then (a, b), (a, c), (b, c) and (a, b, c) generate G'. In fact one can easily see that every element of G' can be expressed as a product $(a, b)^i(a, c)^j(b, c)^k(a, b, c)^l$ for suitable integers i, j, k and l. We should like such expressions to be as unique as possible. The next lemma shows that a given set of generators of G may sometimes be replaced by a more "suitable" set of generators. This lemma will be applied to obtain a set of generators of G which satisfy many special conditions. Once we obtain these generators we shall be able to pick out a two-generator subgroup of G which does not have a cyclic derived group and the theorem will be proved.

LEMMA 2.4.1. *Suppose G is generated by a, b and c such that $|(a, c)| \leqq |(a, b)|$ and $\{(a, c)\}$ is not a subgroup of $\{(a, b)\}$. Then we may define, for suitable non-negative integers t and γ,*

$$a'' = a,\ b'' = b,\ c'' = cb^{tp^\gamma}$$

so that

(i) $\{(a'', b'')\} \cap \{(a'', c'')\} = 1$,
(ii) $(a'', b'') = (a, b)$,
(iii) $\{(b'', c'')\} = \{(b, c)\}$,
(iv) $(a'', b''; b'', c'') = (a, b; b, c)$, $(a'', b''; a'', c'') = (a, b; a, c)$,
(v) *a'', b'' and c'' generate G.*

Proof. First let us show that parts (ii)–(v) hold for any elements a'', b'' and c'' so defined. Part (ii) is immediate and part (iii) follows from

$$(b'', c'') = (b, cb^{tp^\gamma}) = (b, c)(b, c, b^{tp^\gamma})$$

because (b, c, b^{tp^γ}) must be a power of $(b, c)^p$. Similarly, since $(G_2, G_3) = 1$, we may prove (iv):

$$\begin{aligned}(a'', b''; b'', c'') &= (a, b; (b, c)(b, c, b^{tp^\gamma})) \\ &= (a, b; b, c), \\ (a'', b''; a'', c'') &= (a, b; (a, b^{tp^\gamma})(a, c)(a, c, b^{tp^\gamma})) \\ &= (a, b; a, c),\end{aligned}$$

for (a, b^{tp^γ}) is a power of (a, b) because $\{a, b\}$ has a cyclic derived group. Part (v) is clear because $a = a''$, $b = b''$ and $c = (b'')^{-tp^\gamma} c''$.

There remains only to choose t and γ so that (i) holds. We show that such t and γ exist by induction on the order $|(a,c)|$ of (a,c). If $|(a,c)| = p$ then $t = \gamma = 0$ suffice because $\{(a,b)\} \cap \{(a,c)\} = 1$. If $|(a,c)| > p$ then either $\{(a,b)\} \cap \{(a,c)\} = 1$ and $t = \gamma = 0$ again suffice or this does not hold. In that case one of the subgroups $\mathfrak{V}^1\{(a,c)\}$, $\mathfrak{V}^2\{(a,c)\}, \ldots$ of $\{(a,c)\}$ must be contained in $\{(a,b)\}$ because these are all the subgroups of $\{(a,c)\}$. Let $\mathfrak{V}^\beta\{(a,c)\}$ be the first of these subgroups contained in $\{(a,b)\}$ so that $\beta > 0$ and we must have a relation

$$(a,c)^{p^\beta} = (a,b)^{up^\alpha}$$

where $\alpha \geqq \beta$, because $|(a,c)| \leqq |(a,b)|$, and u is an integer with $u \not\equiv 0$ (modulo p). We can write this equation, denoting $\alpha = \beta + \gamma$ and $s = -u$, in the form

$$(a,c)^{p^\beta}(a,b)^{sp^{\beta+\gamma}} = 1.$$

Before defining an intermediate set of generators a', b' and c' we pause to record a consequence of this equation. We have, in fact,

$$((a,c)^{p^\beta}(a,b)^{sp^{\beta+\gamma}}, b^{sp^\gamma}) = 1,$$

$$((a,c)^{p^\beta}, b^{sp^\gamma})((a,b)^{sp^{\beta+\gamma}}, b^{sp^\gamma}) = 1,$$

$$(a,c,b^{sp^\gamma})^{p^\beta}(a,b,b^{sp^\gamma})^{sp^{\beta+\gamma}} = 1$$

by using Lemma 2.3.1 and Lemma 2.1.1.(iv). But, since (a, b, b^{sp^γ}) is equal to a power of $(a,b)^p$, we have that

$$(a,c,b^{sp^\gamma})^{p^\beta} \in \{(a,b)^{p^{\beta+\gamma+1}}\}.$$

Now let $a' = a$, $b' = b$ and $c' = cb^{sp^\gamma}$. We need now only prove that $(a',c')^{p^\beta} \in \{(a,b)^{p^{\alpha+1}}\}$. For then $|(a',c')| < |(a,c)|$ and $\{(a',c')\}$ is not a subgroup of $\{(a',b')\}$. Indeed,

$$(a',c') = (a,b^{sp^\gamma})(a,c)(a,c,b^{sp^\gamma})$$

is a power of $(a',b') = (a,b)$ if and only if

$$(a,c)(a,c,b^{sp^\gamma}) \in \{(a,b)\}$$

or

$$(a,c)^{b^{sp^\gamma}} \in \{(a,b)\}$$

or

$$(a,c) \in \left\{ (a,b)^{b^{-sp^\gamma}} \right\} \subseteq \{(a,b)\}$$

which is against our original assumption. Hence, by the inductive hypothesis we can now choose integers γ_1 and t_1 such that if

$$a'' = a',\ b'' = b',\ c'' = c'(b')^{t_1 p^{\gamma_1}},$$

then

$$\{(a'', b'')\} \cap \{(a'', c'')\} = 1.$$

But then

$$a'' = a,\ b'' = b,\ c'' = cb^{sp^\gamma} b^{t_1 p^{\gamma_1}}$$

and we are done.

Thus we need only do the following calculation

$$\begin{aligned}(a', c')^{p^\beta} &= (a, cb^{sp^\gamma})^{p^\beta} \\ &= [(a, b^{sp^\gamma})(a, c)(a, c, b^{sp^\gamma})]^{p^\beta} \\ &= (a, b^{sp^\gamma})^{p^\beta}(a, c)^{p^\beta}(a, c, b^{sp^\gamma})^{p^\beta}.\end{aligned}$$

But since $\beta > 0$ this is

$$(a', c')^{p^\beta} = (a, c)^{p^\beta}(a, b^{sp^\gamma})^{p^\beta}(a, c, b^{sp^\gamma})^{p^\beta}.$$

From above we know that $(a, c, b^{sp^\gamma})^{p^\beta}$ is an element of $\{(a, b)^{p^{\beta+\gamma+1}}\} = \{(a, b)^{p^{\alpha+1}}\}$. Thus to show that $(a', c')^{p^\beta} \in \{(a, b)^{p^{\alpha+1}}\}$ we need only prove that

$$(a, c)^{p^\beta}(a, b^{sp^\gamma})^{p^\beta} \in \{(a, b)^{p^{\alpha+1}}\}.$$

However, by Lemma 2.1.1.(v), we have

$$\begin{aligned}(a, c)^{p^\beta}(a, b^{sp^\gamma})^{p^\beta} &= (a, c)^{p^\beta}\left[(a, b)^{\binom{sp^\gamma}{1}} \ldots (a, \overbrace{b, \ldots, b}^{sp^\gamma})^{\binom{sp^\gamma}{sp^\gamma}}\right]^{p^\beta} \\ &= \left[(a, c)^{p^\beta}(a, b)^{sp^{\beta+\gamma}}\right]\left[(a, b, b)^{\binom{sp^\gamma}{2}} \ldots (a, \overbrace{b, \ldots, b}^{sp^\gamma})^{\binom{sp^\gamma}{sp^\gamma}}\right]^{p^\beta}.\end{aligned}$$

But the original relation with which we began was that the first factor of this expression was equal to 1. Therefore, to conclude the proof of this lemma, it is enough to prove that

$$(a, \overbrace{b, \ldots, b}^{i})^{\binom{sp^\gamma}{i}} \in \{(a, b)^{p^{\gamma+1}}\}$$

for $i = 2, 3, \ldots, sp^\gamma$. We shall do so by induction. Since $(a, b, b) \in \{(a, b)^p\}$ and

$$p^\gamma \mid \binom{sp^\gamma}{2} \qquad \text{for } p > 2,$$

we have

$$(a, b, b)^{\binom{sp^\gamma}{2}} \in \{(a, b)^{p^{\gamma+1}}\}.$$

Suppose that the assertion is true for i. Say that

$$(a, \overbrace{b, \ldots, b}^{i}) \in \{(a, b)^{p^j}\}$$

and p^k divides

$$\binom{sp^\gamma}{i} \text{ so } j + k \geqq \gamma + 1.$$

If p^k is the highest power of p dividing

$$\binom{sp^\gamma}{i}$$

then $p^{\gamma-k}$ is the highest power of $p \geqq i$ so the highest power of $p \geqq i+1$ is at most $p^{\gamma-k+1}$ and so

$$p^{k-1} \mid \binom{sp^\gamma}{i+1}.$$

Also

$$(a, \overbrace{b, \ldots, b}^{i+1}) \in \{(a,b)^{p^{j+1}}\}$$

and so, since $(j+1)+(k-1) = j+k \geqq \gamma+1$, we are done.

LEMMA 2.4.2. *There exist generators a, b and c of G such that*
(i) $|(a,b)| \geqq |(a,c)| \geqq |(a,b,c)|$,
(ii) $|(a,b)| > |(a,b,c)|$,
(iii) $\{(a,b)\} \cap \{(a,c)\} = 1$,
(iv) $(a,b;a,c) \neq 1$.

Proof. By Lemma 2.3.4 we may choose generators a_1, b_1 and c_1 for G such that no two of the elements (a_1,b_1), (a_1,c_1), (b_1,c_1) commute. Without any loss of generality we may assume that

$$|(a_1,b_1)| \geqq |(a_1,c_1)| \geqq |(b_1,c_1)|.$$

For if this is not the case then we may rename the generators suitably.

We also wish to show that we may assume that $\{(a_1,b_1)\} \cap Z(G) \neq 1$. There are two possibilities to consider. First, suppose that $\{(a_1,b_1)\} \cap \{(a_1,c_1)\} \neq 1$. Then there is an integer s such that

$$(a_1,b_1)^{p^{n-1}} = (a_1,c_1)^s$$

where $p^n = |(a_1,b_1)|$. Let r be an integer such that

$$(a_1,c_1,c_1) = (a_1,c_1)^{pr}.$$

Then

$$\begin{aligned}(a_1,b_1,c_1)^{p^{n-1}} &= ((a_1,b_1)^{p^{n-1}}, c_1)\\ &= ((a_1,c_1)^s, c_1)\\ &= (a_1,c_1,c_1)^s\\ &= (a_1,c_1)^{prs}\\ &= (a_1,b_1)^{prp^{n-1}} = 1\end{aligned}$$

so $\{(a_1,b_1)\} \cap Z(G) \neq 1$ by Lemma 2.3.3.

On the other hand suppose that $\{(a_1,b_1)\} \cap \{(a_1,c_1)\} = 1$. We may assume that $|(a_1,b_1,c_1)| = p^n$ or we can again apply Lemma 2.3.3. Similarly, if

$|(a_1, c_1)| = p^n$ then we may assume $|(a_1, c_1, b_1)| = p^n$ and if $|(b_1, c_1)| = p^n$ we may then assume $|(b_1, c_1, a_1)| = p^n$ or we can have our assumption by renaming the generators. However, let us show that all these possibilities cannot occur.

By Lemma 2.3.6, $\mho^{n-1}(G')$ is generated by $(a_1, b_1)^{p^{n-1}}$, $(a_1, c_1)^{p^{n-1}}$ and $(b_1, c_1)^{p^{n-1}}$. Also $\Omega^{n-1}(G')$, being a characteristic subgroup of G', is certainly a normal subgroup of G and so contains central nonidentity elements of G. But $n > 1$, or else $\Phi(G') = 1$ and $G'' = 1$, so these three given generators of $\mho^{n-1}(G')$ commute with one another, by Lemma 2.1.2. Therefore, any element $g \neq 1$, $g \in \mho^{n-1}(G')$ may be expressed as

$$g = (a_1, b_1)^{ip^{n-1}}(a_1, c_1)^{jp^{n-1}}(b_1, c_1)^{kp^{n-1}}$$

for suitable integers i, j and k. Suppose $(a_1, b_1)^{ip^{n-1}} \neq 1$. Then

$$(g, c_1) = ((a_1, b_1)^{ip^{n-1}}, c_1) = (a_1, b_1, c_1)^{ip^{n-1}} \neq 1$$

since

$$((a_1, c_1)^{jp^{n-1}}, c_1) = (a_1, c_1, c_1)^{jp^{n-1}} = 1$$

and

$$((b_1, c_1)^{kp^{n-1}}, c_1) = (b_1, c_1, c_1)^{kp^{n-1}} = 1.$$

Similarly, g will not commute with b_1 or a_1 if $(a_1, c_1)^{jp^{n-1}} \neq 1$ or $(b_1, c_1)^{kp^{n-1}} \neq 1$ respectively. Thus g is not central in G for any $g \neq 1$, $g \in \mho^{n-1}(G')$, a contradiction.

Thus we have just shown that there are generators a_1, b_1 and c_1 of G such that

(i) No two of (a_1, b_1), (a_1, c_1) and (b_1, c_1) commute,

(ii) $|(a_1, b_1)| \geqq |(a_1, c_1)| \geqq |(b_1, c_1)|$,

(iii) $\{(a_1, b_1)\} \cap Z(G) \neq 1$.

Because of (i) neither $\{(a_1, c_1)\}$ or $\{(b_1, c_1)\}$ are subgroups of $\{(a_1, b_1)\}$. Thus we are in a position to apply Lemma 2.4.1. In fact we may apply it to (a_1, b_1) and (a_1, c_1) and so obtain another set of generators a_2, b_2 and c_2 such that

(i) $\{(a_2, b_2)\} \cap \{(a_2, c_2)\} = 1$,

(ii) $(a_2, b_2; a_2, c_2) \neq 1$, $(a_2, b_2; b_2, c_2) \neq 1$,

(iii) $|(a_2, b_2)| \geqq |(a_2, c_2)|$, $|(a_2, b_2)| \geqq |(b_2, c_2)|$,

(iv) $\{(a_2, b_2)\} \cap Z(G) \neq 1$.

The third statement is clear because $(a_2, b_2) = (a_1, b_1)$ has order equal to the exponent of G'.

We may now apply Lemma 2.4.1 again, this time to the elements (a_2, b_2) and (b_2, c_2) and obtain a new set of generators a_3, b_3 and c_3 such that

(i) $\{(a_3, b_3)\} \cap \{(a_3, c_3)\} = 1$, $\{(a_3, b_3)\} \cap \{(b_3, c_3)\} = 1$,

(ii) $(a_3, b_3; a_3, c_3) \neq 1$, $(a_3, c_3; b_3, c_3) \neq 1$,

(iii) $|(a_3, b_3)| \geqq |(a_3, c_3)|$, $|(a_3, b_3)| \geqq |(b_3, c_3)|$,

(iv) $\{(a_3, b_3)\} \cap Z(G) \neq 1$.

On account of (iv) we have $|(a_3, b_3)| > |(a_3, b_3, c_3)|$. If $|(a_3, c_3)| \geqq |(a_3, b_3, c_3)|$ then the elements $a = a_3$, $b = b_3$ and $c = c_3$ will satisfy the conclusions of this lemma. Similarly, if $|(b_3, c_3)| \geqq |(a_3, b_3, c_3)|$ then by defining $a = b_3$, $b = a_3$,

$c = c_3$ we would be done because $(a_3, b_3, c_3) = (b_3, a_3, c_3)^{-1}$ by Lemma 2.1.1.(i). Thus we need only show that we cannot have $|(a_3, b_3, c_3)| > |(a_3, c_3)|$ and $|(a_3, b_3, c_3)| > |(b_3, c_3)|$. But if this did occur then we would have, since $|(a_3, c_3)| \geqq |(a_3, c_3, b_3)|$ and $|(b_3, c_3)| \geqq |(b_3, c_3, a_3)|$, that $|(a_3, b_3, c_3)| > |(a_3, c_3, b_3)|$ and $|(a_3, b_3, c_3)| > |(b_3, c_3, a_3)|$, contradicting Lemma 2.3.5. Thus, the lemma is proved.

We now conclude the proof of the theorem.

LEMMA 2.4.3. *Let a, b and c be generators of G as in the previous lemma. Let H be the subgroup of G generated by a^b and c. Then H' is not cyclic.*

Proof. Denote $x = (a, b)$, $y = (a, c)$ and $w = (a, b, c)$. Let A_1 and A_2 be integers such that $(x, a) = x^{pA_1}$, $(y, a) = y^{pA_2}$. Then using Lemma 2.1.1,

$$\begin{aligned}(w, a) &= (x, c, a) = (c, a, x)^{-1}(a, x, c)^{-1} \\ &= (y, x)(x, a, c) = (y, x)(x^{pA_1}, c) \\ &= (y, x)(x, c)^{pA_1} = (y, x)w^{pA_1}.\end{aligned}$$

Since $|w| < |x|$, we have by Lemma 2.3.3 that $\{x\} \cap Z(G) \neq 1$ so $G'' = \Omega_1(Z(G))$ is a subgroup of $\{x\}$. If $|x| = p^n$ then there is an integer t, $t \not\equiv 0$ (modulo p) such that $(y, x) = x^{tp^{n-1}}$.

Before proving the assertion of this lemma we first shall determine a relation between the constants A_1 and A_2. This is done by considering the subgroup of G generated by a and bc,

$$\begin{aligned}(a, bc) &= yxw, \\ (a, bc, a) &= y^{pA_2}x^{pA_1}x^{tp^{n-1}}w^{pA_1}.\end{aligned}$$

However, (a, bc, a) is a power of (a, bc) and this implies $y^{p(A_2-A_1)}x^{tp^{n-1}}$ is a power of yxw. Therefore, there exist integers m and s, $0 < m \leqq n-1$ and $s \not\equiv 0$ (modulo p) such that

$$(yxw)^{sp^m} = y^{pA_2-pA_1}x^{tp^{n-1}}$$

so

$$w^{sp^m} = y^{pA_2-pA_1-sp^m}x^{tp^{n-1}-sp^m}.$$

If $m < n-1$ this implies $|w| = |x$ since $\{x\} \cap \{y\} = 1$. Hence $m = n-1$ and $w^{p^{n-1}} = 1$, because $|w| < |x|$, and thus

$$y^{pA_2-pA_1-sp^{n-1}}x^{tp^{n-1}-sp^{n-1}} = 1.$$

Therefore we may assume that

$$\begin{aligned}s &= t, \\ pA_2 &= pA_1 + tp^{n-1}.\end{aligned}$$

Now we are in a position to deal with the subgroup H.

$$
\begin{aligned}
(a^b, c) &= (a(a,b),c) = (ax,c) = y(y,x)w \\
&= yx^{tp^{n-1}}w, \\
(a^b, c, a^b) &= (yx^{tp^{n-1}}w, ax) = (yw, ax) \\
&= (yw,x)(yw,a)(yw,a,x) \\
&= (y,x)(y,a)(w,a) \\
&= x^{tp^{n-1}}y^{pA_1+tp^{n-1}}x^{tp^{n-1}}w^{pA_1} \\
&= x^{2tp^{n-1}}y_p^{A_1+tp^{n-1}}w^{pA_1}.
\end{aligned}
$$

If (a^b, c, a^b) is a power of $(a^b, c)^p = (yw)^p$ then we must have that $x^{2tp^{n-1}}y^{tp^{n-1}}$ is a power of $(y\,w)^p$. If $w^p = 1$ this is impossible because $\{x\} \cap \{y\} = 1$. Hence $w^p \neq 1$ and by Lemma 2.3.2 $\{w\}$ contains G'' as a subgroup. But $G'' = \{x^{p^{n-1}}\}$ so we must now have that $\{y\} \cap \{w\} = 1$. But then there must exist integers q and r with $r \not\equiv 0$ (modulo p) so that

$$(yw)^{rp^q} = y^{tp^{n-1}}x^{2tp^{n-1}}.$$

Then $q < n-1$ because $|w| < |x|$. Hence

$$y^{rp^q} = y^{tp^{n-1}}.$$

But this implies $y^{rp^q} = y^{tp^{n-1}} = 1$. Then $w^{rp^q} = 1$ since $|w| \leqq |y|$ so we finally have that $x^{2tp^{n-1}} = 1$, which contradicts one assumption that x has order precisely p.

Chapter 3. Consequences of Theorem 2

3.1. **Proof of Theorem 1.** The following lemma gives Theorem 1 as a corollary of Theorem 2.

Lemma 3.1.1. *If H is any regular 3-group which can be generated by two elements then H' is cyclic.*

Proof. Since H is a regular 3-group, given any element u and v of H we can express

$$(uv)^3 = u^3v^3w$$

when w is a product of cubes of commutators in u and v. Hence the group $H/\mathfrak{V}^1(H')$ satisfies the identical relation

$$(xy)^3 = x^3y^3.$$

By results of Levi [6] any group which satisfies that identical relation satisfies the identical relation

$$(x,y,y) = 1.$$

But since $H/\mathfrak{V}^1(H')$ can be generated by two elements this implies $H'/\mathfrak{V}^1(H')$ is cyclic so H' is cyclic.

However, instead of using Levi's results, we can apply the "collection process" and prove the next lemma, which completes the above proof without a reference to Levi.

LEMMA 3.1.2. *Let H be a 3-group such that*
(i) *H can be generated by two elements,*
(ii) *H satisfies the identical relation $(xy)^3 = x^3y^3$,*
(iii) *Every element of H' has order at most three. Then H is of class at most two.*

Proof. If H is not of class two then neither is H/H_4 and this factor group also satisfies conditions (i), (ii), and (iii). Therefore we may assume that H has class at most three. Therefore, if $x, y \in H$,

$$\begin{aligned} x^3y^3 = (xy)^3 &= xyxyxy \\ &= x^2y(y,x)yxy \\ &= x^3y(y,x)^2(y,x,x)y(y,x)y \\ &= x^3y^2(y,x)^2(y,x,y)^2(y,x,x)(y,x)\,y \\ &= x^3y^2(y,x)^2(y,x,y)^4(y,x,x)(y,x)(y,x,y)\,. \end{aligned}$$

Hence

$$(y,x,y)^2(y,x,x) = 1.$$

But this must also hold if we replace y by y^2, so

$$(y,x,y)^2(y,x,x)^2 = 1$$

and

$$(y,x,x) = (y,x,y) = 1.$$

Therefore, H has class at most two.

3.2. **Proof of Theorem 3.** Let G be any torsion-free nilpotent group in which every two-generator subgroup has a cyclic derived group. Suppose $G'' \neq 1$ so that there exist elements a, b, c and d of G such that $(a,b;\,c,d) \neq 1$. Consequently, the subgroup K generated by a, b, c and d is not metabelian. However, since K is a finitely generated, torsion-free, nilpotent group, it is residually a finite p-group for any prime p (Gruenberg, [1]). This means, given any element u of K, that there exists a normal subgroup N of K such that u does not lie in N and K/N is a finite p-group. In particular, if $u = (a,b;\,c,d)$ and p is an odd prime, then K/N satisfies the hypotheses of Theorem 2 but is not metabelian, and this is a contradiction. Hence $G'' = 1$.

CHAPTER 4. DIRECT PRODUCTS OF REGULAR 3-GROUPS

In this section we shall prove Theorem 5. First, however, we shall prove a lemma, which incidentally justifies the title of this work.

LEMMA 4.1. *Let G be a finite p-group, for an odd prime p, such that every two-generator subgroup of G has a cyclic derived group. Then G is regular.*

Proof. The proof of part (vii) of Lemma 2.1.2 may be used.

As a consequence of this lemma and Lemma 3.1.1, we now have

LEMMA 4.2. *If G is a finite 3-group then G is regular if and only if every two-generator subgroup of G has a cyclic derived group.*

We may now use this lemma to prove Theorem 5. Indeed, let G be any regular 3-group in which $\mathfrak{V}^1(G') = 1$. Furthermore, let H be any other regular 3-group. Denote elements of $G \times H$ by $\langle g, h\rangle$ for $g \in G$, $h \in H$. Suppose that $\langle g_1, h_1\rangle$, $\langle g_2, h_2\rangle$ are elements of $G \times H$, $g_i \in G$, $h_i \in H_1$, $i = 1, 2$. Then

$$(\langle g_1, h_1\rangle, \langle g_2, h_2\rangle) = \langle (g_1, g_2), (h_1, h_2)\rangle$$

and

$$(\langle g_1, h_1\rangle, \langle g_2, h_2\rangle, \langle g_2, h_2\rangle) = \langle (g_1, g_2, g_2), (h_1, h_2, h_2)\rangle.$$

To show that $G \times H$ is regular we need only prove that the second of these elements is a power of the first one. But $(g_1, g_2, g_2) = 1$ since it must be a power of $(g_1, g_2)^3 = 1$. Therefore, the second element, $\langle 1, (h_1, h_2, h_2)\rangle$ is the same power of $\langle (g_1, g_2), (h_1, h_2)\rangle$ as (h_1, h_2, h_2) is of (h_1, h_2).

Conversely, suppose G is a regular 3-group and $\mathfrak{V}^1(G') \neq 1$. Let g_1 and g_2 be elements of G such that $(g_1, g_2)^3 \neq 1$. Then we may choose positive integers α and m, with $m \not\equiv 0$ (modulo 3), such that

$$(g_1, g_2, g_1) = (g_1, g_2)^{m3^\alpha}.$$

Let H be the group generated by h_1 and h_2 with relations

$$h_1^{3^{\alpha+1}} = h_2^{3^{\alpha+1}} = (h_1, h_2)^{3^{\alpha+1}} = 1,$$

$$(h_1, h_2, h_2) = 1,$$

$$(h_1, h_2, h_1) = (h_1, h_2)^{-m3^\alpha}$$

so H is a regular 3-group, by Lemma 4.2. Now consider the subgroup K of $G \times H$ generated by $\langle g_1, h_1\rangle$ and $\langle g_2, h_2\rangle$. Then

$$(\langle g_1, h_1\rangle, \langle g_2, h_2\rangle) = \langle (g_1, g_2), (h_1, h_2)\rangle$$

and

$$(\langle g_1, h_1\rangle, \langle g_2, h_2\rangle, \langle g_1, h_1\rangle) = \langle (g_1, g_2)^{m3^\alpha}, (h_1, h_2)^{-m3^\alpha}\rangle$$

so K' is not cyclic. Therefore $G \times H$ is not regular.

CHAPTER 5. THE SOLVABILITY OF A CERTAIN CLASS OF GROUPS

In this final section we shall prove Theorem 6. It is sufficient however to prove instead the following assertion: If G is a finite group in which every two-generator subgroup has a cyclic derived group and p is the largest prime dividing the order of G then a Sylow p-subgroup S of G is normal in G. Since the conditions of the hypothesis of this statement are inherited by subgroups and factor groups, this assertion implies that G is solvable. We now shall prove this statement by induction on the order of G. We may assume S is not normal in G and that D is a maximal intersection of Sylow p-subgroups of G. If N is the normalizer of D in G then N contains more than one Sylow p-subgroup (Zassenhaus [8, p. 138]), so by induction we must have $N=G$. Therefore D is a normal subgroup of G. If $D \neq 1$ we may conclude by applying the inductive hypothesis to G/D. Therefore, we may assume that any two Sylow p-subgroups of G have a trivial intersection.

Thus, to finish the proof it will be enough to prove the following: If x is an element of G of order a power of p, say p^m, and y is any element of G then x and x^y generate a subgroup of G of order a power of p. But suppose x and y are two such elements. The derived group K' of the group K generated by x and y is cyclic. The element (x, y) generates a characteristic subgroup of K', since every subgroup of a cyclic group is characteristic. Therefore $\{(x, y)\}$ is a normal subgroup of K. But K' is generated by (x, y) and its conjugates in K so $K' = \{(x, y)\}$. Let $(x, y) = uv$ where u is of order a power of p and v has order prime to p and $uv = vu$. Now $x^y = x(x, y)$ has order p^m, being a conjugate of x. Hence $1 = (xuv)^{p^m} = (xu)^{p^m} v^{p^m}$ because x must commute with v, since p is the largest prime dividing the order of G. But x normalizes $\{u\}$ so xu has order a power of p so $v^{p^m} = 1$. Hence $v = 1$ and $(x, y) = u$, $K = \{x, x^y\} = \{x, u\}$ is a p-group.

REFERENCES

1. K. W. Gruenberg, *Residual properties of infinite soluble groups*, Proc. London Math. Soc. **7** (1957), 29–62.

2. M. Hall, *The theory of groups*, Macmillan, New York, 1959.

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

4. ———, *On a theorem of Frobenius*, Proc. London Math. Soc. **40** (1937), 468–501.

5. F. W. Levi, *Groups in which the commutator operation satisfies certain algebraic conditions*, J. Indian Math. Soc. **6** (1942), 87–97.

6. ———, *Notes on group theory*. I, II, J. Indian Math. Soc. **8** (1944), 1–9.

7. B. H. Neumann, *On a conjecture of Hanna Neumann*, Proc. Glasgow Math. Assoc. **3** (1956), 13–17.

8. H. J. Zassenhaus, *The theory of groups*, 2nd ed., Chelsea, New York, 1958.

OXFORD UNIVERSITY,
OXFORD, ENGLAND