Mathematical Proceedings of the Cambridge Philosophical Society

VOL. 120 NOVEMBER 1996 PART 4

Math. Proc. Camb. Phil. Soc. (1996), **120**, 579
Printed in Great Britain

Finite equilibrated groups

BY NORMAN BLACKBURN
Department of Mathematics, University of Manchester, Manchester, M13 9PL

MARIAN DEACONESCU
Faculty of Mathematics, University of Timisoara, Timisoara, Rumania

AND AVINOAM MANN
Einstein Institute of Mathematics, Hebrew University of Jerusalem, Jerusalem 91904, *Israel*

(*Received* 7 *August* 1995; *revised* 14 *November* 1995)

1. *Introduction*

If H, K are subgroups of a group G, then HK is a subgroup of G if and only if $HK = KH$. This condition certainly holds if $H \leqslant N_G(K)$ or $K \leqslant N_G(H)$. But the majority of groups can also be expressed as HK, where neither H nor K is normal. In this paper we consider groups G for which no subgroup G_1 can be expressed as the product of non-normal subgroups of G_1. Such a group is said to be equilibrated. Thus G is equilibrated if and only if either $H \leqslant N_G(K)$ or $K \leqslant N_G(H)$ whenever H, K and HK are subgroups of G.

The most obvious examples of equilibrated groups are the Dedekind groups, that is, the finite groups in which every subgroup is normal. Again, all groups of order p^3 or pq, for primes p and q, are equilibrated. But the 'Tarski monsters' are equilibrated: these are simple groups of prime exponent. We shall confine our attention to finite equilibrated groups, which we call E-groups for short. The symmetric group S_n is not an E-group for $n \geqslant 4$, since it is the product of the stabilizer of a symbol and the subgroup generated by a cycle of length n.

In Section 3 we determine the simple E-groups and give some properties of soluble ones. In Section 4 we look at E-groups of prime-power order and show that for $p > 3$ they are all except one of class at most 2. But the situation looks more complicated for $p = 2$.

Our notation is standard and conforms with that of Gorenstein [5] or Huppert [6].

https://doi.org/10.1017/S0305004100001560 Published online by Cambridge University Press

2. *Preliminary lemmas*

Throughout this section G denotes an E-group.

LEMMA 2·1. *If H, K are subgroups of G and $G = HK$, then either $H \trianglelefteq G$ or $K \trianglelefteq G$. In particular a simple E-group cannot be expressed as the product of two proper subgroups.*

LEMMA 2·2. *Every section of G is an E-group.*

LEMMA 2·3. *Let D be a Dedekind group. Then D is either Abelian or a direct product $D = A \times B \times Q$, where A is Abelian of odd order, B is of exponent at most 2 and Q is the quaternion group of order 8.*

Proof. See [**6**], III, 7·12 (p. 308).

LEMMA 2·4. *Suppose H, K are subgroups of G and $G = HK$.*

(i) *If K is not normal in G, then G/H is a Dedekind group. If, in particular, $|G/H|$ is odd, G/H is Abelian.*
(ii) *Either G/H or G/K is a Dedekind group.*

Proof. (i) If $H \leqslant H_1 \leqslant G$, then $G = H_1K$, so by Lemma 2·1, $H_1 \trianglelefteq G$. Thus $H \trianglelefteq G$ and G/H is a Dedekind group. If $|G/H|$ is odd, G/H is Abelian by 2·3.

(ii) By (i) we may suppose that H, K are both normal subgroups of G. If G/H is not a Dedekind group, there exists a subgroup H_1 such that $H \leqslant H_1 \leqslant G$ and H_1 is not normal in G. Then $G = H_1K$, so by (i) G/K is a Dedekind group.

For any group X let $L(X)$ denote the intersection of all non-normal maximal subgroups of X; if X is nilpotent, $L(X) = X$. The following result is proved in [**3**] (see [**6**], p. 276).

LEMMA 2·5. *For any group X, $L(X)$ is a characteristic nilpotent subgroup of X, $[L(X), X] \leqslant \Phi(X)$, and $F(X/L(X)) = F(X)/L(X)$, where $F(X)$ denotes the Fitting subgroup of X and $\Phi(X)$ the Frattini subgroup.*

LEMMA 2·6. *Suppose that the E-group G is not nilpotent. If $H \lhd G$ and $H \not\leqslant L(G)$, then G/H is a Dedekind group.*

Proof. Since $H \not\leqslant L(G)$, there exists a non-normal maximal subgroup M of G such that $H \not\leqslant M$. Thus $G = HM$, so G/H is a Dedekind group by Lemma 2·4(i).

The next lemma will be used to construct 2-groups which are not E-groups.

LEMMA 2·7. *Suppose that S is a special 2-group of exponent 4. If $x, y \in S$ and $T = \langle x, y \rangle$ is of order 32, then T is not an E-group. (Hence neither is S.)*

Proof. The group T/T' is the direct product of two cyclic groups of order at most 4; if one of them were of order less than 4, $|T'|$ would be at most 2 and $|T|$ would be less than 32. Thus $T/T' = \langle xT' \rangle \times \langle yT' \rangle$, and if $[x, y] = z$, every element of T is uniquely expressible as $x^\alpha y^\beta z^\gamma$, with $0 \leqslant \alpha < 4$, $0 \leqslant \beta < 4$, $0 \leqslant \gamma < 2$. Since $x^\alpha y^\beta z^\gamma = x^{\alpha - 2\gamma} y^\beta (x^2 z)^\gamma$,

$$T = \langle x \rangle \langle y, x^2 z \rangle.$$

But neither factor contains z, so they are both non-normal.

https://doi.org/10.1017/S0305004100001560 Published online by Cambridge University Press

In this note we shall not go further into the case of 2-groups, but we remark that the group P generated by x, y with defining relations

$$x^4 = y^4 = 1, \quad [x, y] = x^2y^2, \quad [x^2, y] = [x, y^2] = 1$$

is not an E-group, since $P = \langle x \rangle \langle y \rangle$ but $\langle x \rangle, \langle y \rangle$ are both non-normal. This group is of order 16 and arises in the theory of monotone groups.

3. *E-groups which are not p-groups*

First we determine all the simple E-groups.

THEOREM 3·1. *The simple non-Abelian E-groups are the $L_2(p)$, where p is a prime, $p \equiv 5(8)$, $p^2 \equiv -1(5)$, $(p+1)$ is twice a prime-power, and $(p-1)$ is four times a prime-power.*

Proof. Let G be a simple non-Abelian E-group. Since S_4 is not an E-group, no section of G is isomorphic to S_4. The non-Abelian simple groups with this property were determined by Goldschmidt and Glauberman ([**4**], theorem C, p. 47); they are

(i) $L_2(q)$ for $q = 2^n$ and $n \geqslant 3$, or for $q \geqslant 5$, $q \equiv \pm 3(8)$;
(ii) the groups of Ree type;
(iii) Janko's first simple group J_1;
(iv) the Suzuki groups $Sz(2^{2m+1})$, $m \geqslant 1$; and
(v) PSU $(3, 2^n)$ for $n \geqslant 2$.

We deal with each of these cases in turn.

(i) The group G is not factorizable, so if $G \cong L_2(q)$, $q \equiv 1(4)$ (see [**9**]). Thus $q \equiv 5(8)$. If $q = p^f$, $L_2(p)$ is a subgroup of G, so also $p \equiv 5(8)$. Thus f is odd. We use the Dickson list of subgroups of $L_2(q)$ ([**6**], II, 8·27). Thus G has a dihedral subgroup D of order $p^g + 1$ for any divisor g of f. Since g is odd, $\frac{1}{2}(p^g + 1) \equiv 3(4)$ so $\frac{1}{2}(p^g + 1)$ is odd. Since D is an E-group, $\frac{1}{2}(p^g + 1)$ is a prime-power.

We deduce that $f = 1$. If not, let g be a prime divisor of f, and suppose $\frac{1}{2}(p^g + 1)$ is a power of the prime r. Then $\frac{1}{2}(p+1)$ is a power of r:

$$p = 2r^k - 1, \quad k \geqslant 1.$$

Since $g > 1$, $p^g \equiv 2gr^k - 1(r^{k+1})$. Since $\frac{1}{2}(p^g + 1)$ is a power of r, it follows that $g = r$. Thus $\frac{1}{2}(p^r + 1)$ is a power of r:

$$\tfrac{1}{2}(p^r + 1) = r^s, \quad s > k.$$

Hence

$$2r^s = (2r^k - 1)^r + 1 \equiv 2r^{k+1}(r^{k+2}).$$

Thus $s = k + 1$, and

$$2r^{k+1} = (2r^k - 1)^r + 1 > r^{kr} \geqslant r^{3k},$$

which is impossible.

Thus $f = 1$. Since the dihedral groups of orders $p+1$ and $p-1$ are subgroups of G, these groups are E-groups, so $p+1$ is twice a prime-power and $p-1$ is four times one. And since A_5 is not an E-group, A_5 is not a subgroup of G. From the Dickson list, $p^2 \equiv -1(5)$.

Conversely, the $L_2(p)$ with the stated values of p are E-groups.

https://doi.org/10.1017/S0305004100001560 Published online by Cambridge University Press

(ii) Suppose G is a group of Ree type of order $q^3(q^3+1)(q-1)$, where $q = 3^{2k+1}(k \geqslant 1)$. Then G contains a subgroup isomorphic to $L_2(q)$ ([**8**], p. 292). Since $q \equiv 3(8)$, $L_2(q)$ is factorizable, so G is not an E-group.

(iii) The group J_1 contains a subgroup isomorphic to $A_5 \simeq L_2(5)$ (see [**10**]). Since A_5 is not an E-group, neither is J_1.

We shall rule out cases (iv) and (v) by considering the Sylow 2-subgroups. In both $Sz(2^{2m+1})$ and $\mathrm{PSU}(3, 2^n)$, these are special 2-groups of exponent 4.

(iv) Let F be the finite field with 2^{2m+1} elements $(m \geqslant 1)$ and let θ be the automorphism of F given by $x\theta = x^{2^{m+1}}$ for all $x \in F$. Thus $x\theta^2 = x^2$. The Sylow 2-subgroups of $Sz(2^{2m+1})$ are isomorphic to $A(2m+1, \theta)$, where

$$A(2m+1, \theta) = \{(a, b) \mid a, b \in F\}$$

and
$$(a, b)(a', b') = (a + a', b + b' + a'(a\theta)) \quad (a, b, a', b' \in F).$$

Thus $(a, b)^2 = (0, a(a\theta))$, $[(a, b), (a', b')] = (0, a(a'\theta) + a'(a\theta))$ for all $a, b, a', b' \in F$.

We show that $A(2m+1, \theta)$ is not an E-group by finding a subgroup $T = \langle x, y \rangle$ of order 2^5 which satisfies the condition of Lemma 2·7. Let

$$x = (1, 0), \quad y = (a, 0),$$

where a is a generator of the multiplicative group of non-zero elements of F. Let

$$z = [x, y] = (0, a + a\theta).$$

The condition $|T| = 2^5$ means that $z \notin \langle x^2, y^2 \rangle$, since $A(2m+1, \theta)$ is of exponent 4 and class 2; thus we must have

$$a + a\theta \notin \{0, 1, a(a\theta), 1 + a(a\theta)\}.$$

Hence

$$a\theta \notin \{a, 1 + a, a(1+a)^{-1}, 1\}.$$

It is certainly the case that $a\theta \neq a$ and $a\theta \neq 1$. If $a\theta = 1 + a$, then $a^2 = a\theta^2 = 1 + a\theta = a$, and if $a\theta = a(1+a)^{-1}$, then $1 + a\theta = (1+a)^{-1}$ and

$$1 + a^2 = 1 + a\theta^2 = (1 + a\theta)\theta = (1+a)^{-1}\theta = (1 + a\theta)^{-1} = 1 + a.$$

Thus T is indeed of order 2^5. By Lemma 2·7, T is not an E-group; thus neither are $A(2m+1, \theta)$ and $Sz(2^{2m+1})$.

(v) The case when $G = \mathrm{PSU}(3, 2^n)$ $(n \geqslant 2)$ is very similar. Let $q = 2^n$ and let F be the finite field with q^2 elements. By [**6**], II, 10·12b), the Sylow 2-subgroup Q of $\mathrm{PSU}(3, 2^n)$ consists of elements $Q(x, y)$, where x, y are in F and $y + y^q + xx^q = 0$. Multiplication is defined by

$$Q(x, y)\, Q(x', y') = Q(x + x', y + y' + xx'^q).$$

Given $x \in F$, there exists z in some extension of F such that $z + z^q + xx^q = 0$, and since $z^{q^2} = (z + xx^q)^q = z^q + x^q x = z$, $z \in F$. Then $Q(x, z) \in Q$ and $Q(x, y) \in Q$ if and only if $y + y^q = z + z^q$, that is, $z + y \in F_0$, where F_0 is the subfield of F having q elements. Thus $|Q| = q^3$.

We have

$$Q(x, y)^2 = Q(0, xx^q),$$

$$[Q(x, y), Q(x', y')] = Q(0, xx'^q + x'x^q).$$

https://doi.org/10.1017/S0305004100001560 Published online by Cambridge University Press

Thus Q is of exponent 4 and class 2. (In [7], VIII, 7·10, it is shown that Q is a Suzuki 2-group. In the paragraph following this (p. 315), elements $Q(a+b\eta, 0)$ are erroneously introduced; these should be replaced by $Q(a+b\eta, y)$ for an appropriate $y \in F$.)

As in (iv) we seek a subgroup T of Q of order 2^5 with two generators. Let a be an element of F of multiplicative order $q+1$ and put

$$T = \langle Q(1,z), Q(a,z') \rangle$$

with z, z' so chosen that $Q(1,z) \in Q$ and $Q(a,z') \in Q$. The condition for T to be of order 2^5 is

$$[Q(1,z), Q(a,z')] \notin \langle Q(1,z)^2,\ Q(a,z')^2 \rangle.$$

This is equivalent to

$$a + a^q \notin \{0, 1, aa^q, 1+aa^q\}.$$

Since $a^q = a^{-1}$, this amounts to

$$a + a^{-1} \notin \{0, 1\}.$$

But if $a+a^{-1} = 0$, $a^2 = 1$, and if $a+a^{-1} = 1$, $a^3 = 1$, contrary to $q \geqslant 4$. Thus $|T| = 2^5$, and by Lemma 2·7, T, Q and G are not E-groups.

The proof of Theorem 3·1 is thus complete.

THEOREM 3·2. *If G is a soluble E-group, then G is an extension of a p-group by a Dedekind group. In particular $|G'|$ is either a prime-power or twice a prime-power.*

Proof. If G has a non-normal Hall complement H, then $G = HS$ for a Sylow subgroup S, so by Lemma 2·4 (i) G/S is a Dedekind group, as required. If all the Hall complements of G are normal, G is nilpotent. If G/S is not a Dedekind group for every Sylow subgroup S, then by Lemma 2·4 (ii) G/H is a Dedekind group for every Hall complement H. Hence every Sylow subgroup of G is a Dedekind group and so is G.

COROLLARY 3·3. *Suppose G is a soluble E-group.*

(i) *G has a Sylow tower.*
(ii) *Every non-normal Sylow p-subgroup of G is a Dedekind group.*
(iii) *There is at most one prime p for which the Sylow p-subgroups of G are not Dedekind groups.*
(iv) *If G is nilpotent, G is the direct product of a group of prime-power order and a Dedekind group.*
(v) *If the Sylow 2-subgroup of G is normal, G' is nilpotent.*

Proof. These assertions all follow at once from Theorem 3·2.

THEOREM 3·4. *Suppose that G is an E-group which is soluble but not nilpotent. Then $G/L(G)$ is a Frobenius group; the Frobenius kernel, $F(G)/L(G)$, is a minimal normal subgroup of $G/L(G)$ and the complement is a Dedekind group.*

Proof. We use induction on $|G|$. By Lemma 2·5, $G/L(G)$ is not nilpotent, so if $L(G) \neq 1$, the assertions follow from the inductive hypothesis applied to $G/L(G)$. Thus we may suppose that $L(G) = 1$. Let M be a non-normal maximal subgroup of G, and let K be the core of M. If $K \neq 1$, then G/K is a Dedekind group by Lemma 2·6. But then G/K is nilpotent and $M \lhd G$, a contradiction. Hence $K = 1$. Thus $F(G) \nleqslant M$, so $G = F(G)M$. And, if $N = N_G(F(G) \cap M)$, then since $F(G)$ is nilpotent,

https://doi.org/10.1017/S0305004100001560 Published online by Cambridge University Press

$N \cap F(G) > M \cap F(G)$. But $M \leqslant N$, so $M < N$ and $N = G$. Hence $F(G) \cap M = 1$. Since M is maximal, $F(G)$ is a minimal normal subgroup of G and is elementary Abelian. By Lemma 2·4, $G/F(G)$ is a Dedekind group; hence so is M.

It remains to show that if $1 \neq x \in F(G)$, then $C_G(x) = F(G)$. Otherwise there exists $y \in M - [1]$ such that x, y commute. We show that x^g, y commute for every $g \in G$. For $g = ab$ with $a \in F(G)$, $b \in M$, and since M is a Dedekind group $[y, b^{-1}] = y^\alpha$ for some $\alpha \in \mathbb{Z}$. Then

$$[x^g, y] = [x^{ab}, y] = [x^a, y^{b^{-1}}]^b = [x, y^{1+\alpha}]^b = 1.$$

But the normal closure of x is $F(G)$, since $F(G)$ is a minimal normal subgroup. Thus $y \in C_G(F(G))$ and $\langle y, F(G)\rangle$ is a normal nilpotent subgroup of G, contrary to $y \notin F(G)$.

By Corollary 3·3 (iv), the nilpotent case reduces to that of groups of prime-power order.

4. *E-groups of prime-power order*

We have already encountered some 2-groups which are not E-groups. But the small primes are not typical, as we shall see by looking at the p-groups of maximal class (co-class 1). The properties of these that are needed are found in [**1**] or [**6**].

Example 1. The 2-groups of maximal class are E-groups. This is proved by induction on the order 2^n of such a group G. For suppose $n > 3$ and $G = HK$ with H, K non-normal. Then $|H| > 2$ and $|K| > 2$. But all subgroups of G of order greater than 2 intersect the cyclic maximal subgroup non-trivially and thus contain the centre Z of G. Thus H/Z, K/Z are non-normal subgroups of G/Z the product of which is G/Z, contrary to the inductive hypothesis. And all subgroups of a 2-group of maximal class are either cyclic or of maximal class.

We shall examine the p-groups of maximal class for p odd, and we use the following notation for such a group G. Let $G \geqslant G_2 \geqslant G_3 \geqslant \ldots$ be the lower central series of G and let G_1/G_4 be the centralizer of G_2/G_4 in G/G_4. Let $G = \langle s, G_1\rangle$, $G_1 = \langle s_1, G_2\rangle$, $s_i = [s_{i-1}, s]$ $(i > 1)$.

Example 2. For p odd, let G be a group of order p^4 and class 3. In this case, G_1/G_3 and G_2 are elementary Abelian, and G_1 is Abelian. G is an E-group if and only if G_1 is not elementary Abelian.

Proof. Since groups of order p^3 are E-groups, G is not an E-group if and only if $G = HK$ with H, K non-normal. If this is so, $|H| = |K| = p^2$ and $H \cap K = 1$, so G_3 cannot be contained in both H and K, say $G_3 \nleqslant H$. If $H \nleqslant G_1$, H contains an element of the form sx with $x \in G_1$, so $H \leqslant C_G(sx) = \langle s, G_3\rangle$; but $|\langle s, G_3\rangle| = p^2 = |H|$, so $G_3 \leqslant H$, as contradiction. Hence $H \leqslant G_1$. Since $H \not\geqslant G_3$, $H \cap G_3 = 1$ and H is elementary Abelian. Since $G_2 \lhd G$, $H \nleqslant G_2$, so $G_1 = HG_2$ is elementary Abelian.

Conversely, suppose that G_1 is elementary Abelian, so $\langle s_1, s_2\rangle$ does not contain $s_3 = [s_2, s]$ and is therefore non-normal. Also $s^p \in \langle s_3\rangle$, so $\langle s, s_3\rangle$ is non-normal as it does not contain $[s_1, s] = s_2$. But $G = \langle s, s_3\rangle\langle s_1, s_2\rangle$, so G is not an E-group.

Example 3. For $p > 3$, every p-group of maximal class G of order greater than p^4 is not an E-group. For the unique factor group of G of order p^4 is of the kind described in Example 2 with G_1 elementary Abelian: this follows from the relation

$$s_1^p s_2^{-\binom{p}{2}} \ldots s_p = s_{n-1}^\gamma \tag{1}$$

https://doi.org/10.1017/S0305004100001560 Published online by Cambridge University Press

(see [1], pp. 83–4). Thus G is in fact expressible as the product of two non-normal subgroups.

Example 4. In contrast, every 3-group of maximal class G of order $3^n (n > 4)$ is not expressible as the product of two non-normal subgroups.

In this case $G_i^3 = G_{i+2}$ for all $i \geqslant 1$, and $G_1' \leqslant G_{n-1}$. Let $Z = G_{n-1}$. We prove the assertion by induction on n. Suppose that $G = HK$ with H, K non-normal. Then $G/Z = (HZ/Z)(KZ/Z)$, so for $n > 5$ it follows from the inductive hypothesis that either HZ or KZ is normal. It follows from Example 2 that this is also the case for $n = 5$, as by (1) G_1/Z is not elementary Abelian. Suppose $HZ \lhd G$. Since the normal subgroups of G are the maximal subgroups and the terms of the lower central series, it follows that either $HZ \geqslant G_{n-3}$ or $HZ = G_{n-2}$. In the first case this implies that

$$Z = G_{n-1} = G_{n-3}^3 \leqslant (HZ)^3 = H^3 \leqslant H,$$

and this is also true in the second case since $|H| > p$ implies $H = G_{n-2}$. Thus $H = HZ \lhd G$.

The subgroups of G which are of maximal class are thus inexpressible as products of non-normal subgroups, as the G_1-terms of those of order p^4 are not elementary Abelian. So G is an E-group if and only if G_1 is not expressible as the product of two non-normal subgroups. Therefore G is an E-group if G_1 is Abelian. But, if G_1 is non-Abelian and n is odd, $G_1 = \langle s_1 \rangle \langle s_1 s_2 \rangle$, so G is not an E-group. If G_1 is non-Abelian and n is even, G is an E-group.

THEOREM 4·1. *Suppose p odd and let G be an E-group of order a power of p. If G has two generators, one of the following holds.*

(a) *G is metacyclic.*
(b) *G is of order p^3 and exponent p.*
(c) *G is of order p^4 and of class 3.*
(d) *G is a 3-group of maximal class.*

Proof. Let $N = \gamma_2(G)^p \gamma_3(G)$. If G/N is metacyclic, so is G [2, theorem 2·3] and (a) holds.

Suppose that G/N is not metacyclic. Then G/N is generated by elements x, y with defining relations

$$[y, x] = z, \quad [z, x] = [z, y] = 1, \quad z^p = 1, \quad x^{p^r} = y^{p^s} = 1,$$

where $|G/N| = p^{r+s+1}$. Thus $G/N = \langle x^p z, y \rangle \langle x \rangle$. Since G/N is an E-group, it follows that $\langle x^p z, y \rangle$ is normal in G/N, so $z = [y, x] \in \langle x^p z, y \rangle$ and $r = 1$. Similarly $s = 1$, so G/N is of order p^3 and exponent p. Hence $|G : \gamma_2(G)| = p^2$ and $|\gamma_2(G) : \gamma_3(G)| = p$. Also $N = \gamma_3(G)$.

If $N = 1$, (b) holds. If $|N| = p$, (c) holds. Suppose that $|N| > p$.

If $|\gamma_3(G) : \gamma_4(G)| = p$, choose $M \lhd G$ with $|\gamma_4(G) : M| = p$. Then G/M is of maximal class, so by Example 3, $p = 3$. By [1, theorem 3·9] (d) holds.

It remains to show that $|\gamma_3(G) : \gamma_4(G)| > p$ is impossible; to do this we may suppose that $|\gamma_3(G)| = p^2$ and $\gamma_4(G) = 1$. Thus $|G| = p^5$ and $\gamma_3(G)$ is central and elementary Abelian of order p^2. There exist elements a, b such that $G = \langle a, b \rangle$; let $c = [a, b]$, $x = [c, a]$, $y = [c, b]$. Thus $\gamma_2(G) = \langle c, \gamma_3(G) \rangle$, $\gamma_3(G) = \langle x, y \rangle$. Since $[c, a] \neq 1$, $a^p \in \langle x, y \rangle$. So

$$a^p = (a^p)^b = (a^b)^p = (ac)^p = a^p c^p x^{\binom{p}{2}},$$

https://doi.org/10.1017/S0305004100001560 Published online by Cambridge University Press

and $c^p = 1$. Now every element of G is expressible as $a^\alpha x^\beta b^\gamma c^\delta y^\epsilon$, so $G = \langle a, x\rangle \langle b, c\rangle$. But $\langle a, x\rangle$ is not normal, since $c = [a, b] \notin \langle a, x\rangle$. Thus $\langle b, c\rangle \lhd G$. Hence $x \in \langle b, c\rangle$ since $x = [c, a]$. If $x = b^\lambda c^\mu y^\rho$, it follows from the fact that $x \in \gamma_3(G)$ that $\lambda \equiv \mu \equiv 0(p)$. Put $\lambda = p\sigma$: then $x = b^{p\sigma} y^\rho$, and $(\sigma, p) = 1$. Choose $\tau \not\equiv -\rho(p)$. Then

$$\langle b\rangle \cap \langle c, xy^\tau\rangle \leqslant \langle b^{p\sigma}\rangle \cap \langle xy^\tau\rangle = 1,$$

so $\langle b, c\rangle = \langle b\rangle \langle c, xy^\tau\rangle$. But neither $\langle b\rangle$ nor $\langle c, xy^\tau\rangle$ contains $[c, b] = y$, so both these subgroups are non-normal in $\langle b, c\rangle$, and G is not an E-group.

THEOREM 4·2. *For p odd, an E-group G which is metacyclic of order a power of p is of class at most 2.*

Proof. Let M be a normal subgroup of G for which M and G/M are both cyclic: let $M = \langle a\rangle$, $G/M = \langle bM\rangle$. We prove that

$$G = \langle b\rangle \langle ba\rangle; \tag{2}$$

this implies the assertion. For since G is an E-group, either $\langle b\rangle \lhd G$ or $\langle ba\rangle \lhd G$; hence $[b, a]$ lies in either $\langle b\rangle$ or $\langle ba\rangle$. But also $[b, a] \in M = \langle a\rangle$, so $[b, a]$ commutes with both b and a. Hence G' is contained in the centre of G.

Suppose that $b^{-1}ab = a^k$, so $k \equiv 1(p)$. To prove (2) it must be shown that every element of G is expressible in the form

$$b^\alpha (ba)^\beta = b^{\alpha+\beta} a^{b^{\beta-1}} \dots a^b a = b^{\alpha+\beta} a^{1+k+\dots+k^{\beta-1}}.$$

Thus it must be shown that every integer can be expressed modulo p^n in the form $1 + k + \dots + k^{\beta-1}$, where p^n is the order of a. If this is not so, there exist integers β, γ, with $0 \leqslant \beta < \gamma < p^n$, such that

$$1 + k + \dots + k^{\beta-1} \equiv 1 + k + \dots + k^{\gamma-1} \quad \text{modulo} \quad p^n.$$

Hence

$$1 + k + \dots + k^{\gamma-\beta-1} \equiv 0 \quad \text{modulo} \quad p^n, \tag{3}$$

and $0 < \gamma - \beta < p^n$. Hence $k \not\equiv 1$ modulo p^n. But $k \equiv 1(p)$; thus if $k = 1 + p^m s$ with $(s, p) = 1$, $1 \leqslant m < n$. By (3), $k^{\gamma-\beta} \equiv 1$ modulo p^{n+m}. But since p is odd, the order of k modulo p^{n+m} is p^n; (this follows from [**6**], I, 13·18). Hence $\gamma - \beta \geqslant p^n$, a contradiction. Hence Theorem 4·2 is proved.

The metacyclic maximal subgroups of 3-groups of maximal class show that the converse of Theorem 4·2 is false.

LEMMA 4·3. *Suppose that G is an E-group of order a power of an odd prime p.*

(a) *If G is of exponent p, G is either Abelian or of order p^3.*
(b) *If G is of order p^5 and $|\gamma_2(G)| = p^2$, then $\gamma_3(G) = 1$.*
(c) *If G has a subgroup H of order at least p^4 and maximal class, then G is of maximal class.*

Proof. (*a*) Suppose that G is non-Abelian; let x, y be elements of G which do not commute. By Theorem 4·1 applied to $\langle x, y\rangle$, $\langle x, y\rangle$ is of order p^3: $\langle x, y\rangle$ is not metacyclic since it is non-Abelian, $\langle x, y\rangle$ is not of order p^4 and class 3 by Example 2, and 3-groups of maximal class of order greater than 3^4 are not of exponent 3. If $\langle x, y\rangle \neq G$, let L be a subgroup of G of order p^4 containing $\langle x, y\rangle$. Again, L is not of maximal class by Example 2, so the class of L is 2 and $|L'| = p$. Also the order of the

https://doi.org/10.1017/S0305004100001560 Published online by Cambridge University Press

centre Z of L is p^2. Suppose that $L = \langle Z, u, v\rangle$ and $[u, v] = a$. Then $L' = \langle a\rangle$ and $Z = \langle a, b\rangle$ for some b. Now every element of L is of the form

$$u^\alpha v^\beta b^\gamma a^\delta = u^\alpha (ba)^\delta v^\beta b^{\gamma-\delta},$$

so $L = \langle u, ba\rangle\langle v, b\rangle$. Since $[u, v] = a$ and a lies in neither of these factors, both of them are non-normal in L, contrary to G being an E-group. Thus $G = \langle x, y\rangle$.

(*b*) If $d(G) = 2$, then G is metacyclic by Theorem 4·1, and the class of G is 2 by Theorem 4·2.

If $d(G) = 3$, let $C = C_G(\gamma_2(G))$. If $C \neq G$, then $|G:C| = p$ and $G = \langle C, s\rangle$ for some $s \in G$. Given $x \in C$, then sx does not centralize $\gamma_2(G)$. Thus if $N \lhd G$, $N < \gamma_2(G)$ and $|N| = p$, we have $(sx)^p \in N$. Since p is odd, it follows that G/N has exponent p, contrary to (*a*). Thus $C = G$ and $\gamma_3(G) = 1$.

(*c*) We may suppose that H is a maximal element of the set of subgroups of G of maximal class. If $H \neq G$, there is a subgroup K of G such that $K \geqslant H$ and $|K:H| = p$. Then K is not of maximal class. By Theorems 4·1 and 4·2, $d(K) > 2$. Thus $\gamma_2(K) = \gamma_2(H)$, and $K/\gamma_4(H)$ satisfies (*b*), a contradiction. Thus $G = H$ is of maximal class.

Corollary. *If G is an E-group of order a power of an odd prime p, then either $d(G) = 2$ or G is powerful.*

Proof. If G is not powerful, $G' \not\leqslant U$, where $U = \langle x^p \mid x \in G\rangle$. Hence G/U is non-Abelian. By Lemma 4·3(*a*), G/U is non-Abelian of order p^3, so $|G:\Phi(G)| = p^2$.

A p-group G is *modular* if any two subgroups of G commute. For p odd, G is modular if and only if every subgroup having two generators is metacyclic.

Theorem 4·4. *If G is an E-group of order a power of an odd prime p, one of the following holds.*

(a) *G is a modular p-group in which $[x, y, y] = 1$ for any $x, y \in G$.*
(b) *$G = EN$, where $E = \Omega_1(G)$, $|E| = p^3$, $G' = E'$, N is cyclic and $E \cap N = G'$.*
(c) *G is a group of order p^4 and class 3.*
(d) *G is a 3-group of maximal class.*

Proof. First suppose that there are elements x, y in G for which $[x, y, y] \neq 1$. Then the class of $\langle x, y\rangle$ is greater than 2, so by Theorem 4·2, $\langle x, y\rangle$ is not metacyclic. By Theorem 4·1, $\langle x, y\rangle$ is of maximal class and of order at least p^4. By Lemma 4·3(*c*), G is of maximal class. By Example 3, either $p = 3$ or G is of order p^4. Thus either (*c*) or (*d*) holds.

We suppose now that (*a*), (*c*) and (*d*) are all false. We have just seen that this implies that $[x, y, y] = 1$ for all $x, y \in G$. This shows that the class of any subgroup of G having two generators is at most 2; hence G is regular. Since (*a*) is false, G is not modular, so there exist elements x, y of G such that $\langle x, y\rangle$ is not metacyclic. Again, Theorem 4·1 shows that $\langle x, y\rangle$ is of maximal class, and if $|\langle x, y\rangle| > p^3$, Lemma 4·3(*c*) shows that (*c*) or (*d*) holds. Thus $E = \langle x, y\rangle$ is non-Abelian of order p^3 and exponent p. So $\Omega_1(G)$ is non-Abelian, and by Lemma 4·3(*a*), $|\Omega_1(G)| = p^3$. Hence $E = \Omega_1(G)$. Also $|G:U| = p^3$, so $d(G) \leqslant 3$.

Suppose $d(G) = 2$. By Theorem 4·1, G is metacyclic or of order p^3 and exponent p, since (*c*), (*d*) are false. Since (*a*) is false, G cannot be metacyclic, by Theorem 4·2. Thus (*b*) holds with $N = E'$.

https://doi.org/10.1017/S0305004100001560 Published online by Cambridge University Press

Now suppose $d(G) = 3$. Then

$$\Phi(G) = U = \{t^p \mid t \in G\}.$$

Suppose $E \cap \Phi(G) > \Phi(E)$. Then there exists $u \in E \cap \Phi(G)$, $u \notin \Phi(E)$. Hence $E = \langle u, v \rangle$ for some $v \in E$, and since $u \in \Phi(G)$, $u = t^p$ for some $t \in G$. Thus $|\langle t, v \rangle| \geqslant p^4$. By Theorem 4·1, $|\langle t, v \rangle|$ is of maximal class, since E is not metacyclic. But Lemma 4·3 (*c*) then leads to a contradiction. So $E \cap \Phi(G) = \Phi(E)$.

Since $G/\Phi(G)$ is elementary Abelian, there exists a subgroup N of G such that $N \geqslant \Phi(G)$ and

$$G/\Phi(G) = (E\Phi(G)/\Phi(G)) \times (N/\Phi(G)).$$

Thus $G = E\Phi(G)N = EN$ and $E\Phi(G) \cap N = \Phi(G)$. Hence $E \cap N = \Phi(E)$ and $|G:N| = |E:E \cap N| = p^2$. Thus $|N:U| = p$. But it is easily seen that $U = \{x^p \mid x \in N\}$, so N is cyclic. Finally, $G' = E'N'[N, E] = E'$, so (*b*) holds.

COROLLARY. *Suppose that G is an E-group of order a power of an odd prime p and that G is not a 3-group of maximal class. Then the class of G is at most 3; indeed the class of G is at most 2 except when $p = 3$ or G is of order p^4.*

In case (*a*), this follows using the theorem of Levi and van der Waerden (see [**6**], III, 6·5).

There is no bound on the number of generators of an E-group of prime-power order. For let

$$G = D \times C_1 \times \ldots \times C_r,$$

where $p > 2$, D is the non-Abelian p-group of order p^3 and exponent p^2 and $C_1, \ldots, C_r$ are cyclic groups of order p. If H is a non-Abelian subgroup of G, H contains non-commuting elements x, y with x of order p^2, y of order p; further

$$x^p = [x, y]^\alpha$$

for some α with $(\alpha, p) = 1$. If A, B are subgroups of H for which $H = AB$, then $x = ab$ for some $a \in A$, $b \in B$. Since $p > 2$, $x^p = a^p b^p$. And

$$a^p = [x, y]^\beta, \quad b^p = [x, y]^{\alpha - \beta}$$

for some β. Since $(\alpha, p) = 1$, it follows that $[x, y]$ lies in A or B; hence either A or B is normal in H. Then G is an E-group with $r+2$ generators.

REFERENCES

[1] BLACKBURN, N. On a special class of p-groups. *Acta Math.* **100**, 45–92 (1958).

[2] BLACKBURN, N. On prime-power groups with two generators. *Proc. Cambridge Phil. Soc.* **54**, 327–337 (1958).

[3] GASCHÜTZ, W. Über die Φ-Untergruppe endlicher Gruppen. *Math. Z.* **58**, 160–170 (1953).

[4] GLAUBERMAN, G. Factorizations in local subgroups of finite groups. *Regional Conf. series in Math.* **33** (1977), A.M.S., Providence, R.I.

[5] GORENSTEIN, D. *Finite groups* (Harper and Row, 1968).

[6] HUPPERT, B. *Endliche Gruppen I* (Springer-Verlag, 1967).

[7] HUPPERT, B. and BLACKBURN, N. *Finite Groups II* (Springer-Verlag, 1982).

[8] HUPPERT, B. and BLACKBURN, N. *Finite Groups II* (Springer-Verlag, 1982).

[9] ITO, N. On the factorizations of the linear fractional groups $LF(2, p^n)$. *Acta Sci. Math. Szeged* **15**, 79–84 (1953).

[10] JANKO, Z. A new finite simple group with Abelian Sylow 2-subgroups and its characterization. *J. of Algebra*, **3**, 147–186 (1966).

https://doi.org/10.1017/S0305004100001560 Published online by Cambridge University Press