FINITE GROUPS WITH A GIVEN NUMBER OF CONJUGATE CLASSES

JOHN POLAND

1. Introduction. This paper presents a list of all finite groups having exactly six and seven conjugate classes and an outline of the background necessary for the proof, and gives, in particular, two results which may be of independent interest. In 1903 E. Landau **(8)** proved, by induction, that for each k the equation

$$(*) \qquad 1 = \frac{1}{m_1} + \frac{1}{m_2} + \ldots + \frac{1}{m_k} \qquad (m_1 \geqslant m_2 \geqslant \ldots \geqslant m_k)$$

has only finitely many solutions over the positive integers. This equation holds in any finite group G if k is interpreted as the number of conjugate classes K_i of G and m_i as $|G|/|K_i|$; therefore it follows that there are only finitely many non-isomorphic finite groups having exactly k conjugate classes. About 1910 G. A. Miller **(9)** and W. Burnside **(4**, Note A**)** derived those finite groups having at most five classes, together with the corresponding solutions of $(*)$. D. T. Sigley **(15)** in 1935 examined those with $k = 6$, and for $k = 7$ he derived those with non-trivial centre; his list for $k = 6$ was in fact incomplete (cf. §2). No other notice was taken of Landau's result until it reappeared recently in *The Collected Works of Otto Schmidt** **(13)**; lately W. R. Scott **(14)** and R. Brauer **(1; 2)** have referred to it.

The basic outstanding problem concerning Landau's result, as formulated by R. Brauer **(1)**, is:

Problem. "Give upper bounds for the order n of a group with a given class number k, which lie substantially below the bounds obtainable by Landau's method."

For by Landau's method, when $k = 6$ the upper bound is 3,263,442 and when $k = 7$ it is 10,650,056,950,806; see Miller **(10)**; the upper bound can be approximated by $3^{2^{k-2}}$). In contrast, the largest finite group with six classes is LF(2, 7) of order 168 and that with seven classes is Alt(6) of order 360. However, until radically new methods are developed, obtaining even good estimates of the true upper bounds involves determining all groups with the

Original version received August 24, 1966, and revised version January 18, 1967.
This material formed part of the author's dissertation, McGill University, May, 1966.

*I thank my director H. Schwerdtfeger for calling my attention to Landau's theorem, from this reference.

given class number, so that actually the Problem is solved at present only for $k \leqslant 7$. Note that for $k = 5$, 6, and 7, the largest finite group with k classes is simple; and, roughly speaking, the closer a group approaches the structure of a simple group the higher its order becomes (for a fixed class number $k \leqslant 7$). This suggests that it might be useful to answer the Problem when the group satisfies certain conditions. For p-groups, Ph. Hall (unpublished) has established a formula for k which almost completely resolves the Problem in this case; see also **(12)**.

Throughout this paper we discuss only finite groups, and we let $k = k(G)$ denote the number of (conjugate) classes of G, $Z(G)$ the centre of G, G' the derived group, and $p^a \,\|\, n = |G|$ that p^a divides the order n of G but p^{a+1} does not (p prime). Often, we shall implicitly take $(*)$ as a relation satisfied by the indices of the classes of some group G.

2. The case $k \leqslant 7$.

THEOREM 2.1. *If G is a finite non-abelian group with exactly six conjugate classes, then one of the following holds:*

(i) *equation* $(*)$ *reads*

$$1 = \frac{1}{18} + \frac{1}{9} + \frac{1}{9} + \frac{1}{9} + \frac{1}{9} + \frac{1}{2}$$

and $\quad G = \langle x, y, z \mid x^3 = y^3 = z^2 = 1, x^y = x, x^z = x^2, y^z = y^2 \rangle,$

or $\quad G = \langle x, y \mid x^9 = y^2 = 1, x^y = x^8 \rangle;$

(ii) *equation* $(*)$ *reads*

$$1 = \frac{1}{168} + \frac{1}{8} + \frac{1}{7} + \frac{1}{7} + \frac{1}{4} + \frac{1}{3}$$

and $\quad G = \mathrm{LF}(2, 7);$

(iii) *equation* $(*)$ *reads*

$$1 = \frac{1}{36} + \frac{1}{9} + \frac{1}{9} + \frac{1}{4} + \frac{1}{4} + \frac{1}{4}$$

and $\quad G = \langle x, y, z \mid x^4 = y^3 = z^3 = 1, x^y = z, y^z = y, z^x = y^2 \rangle;$

(iv) *equation* $(*)$ *reads*

$$1 = \frac{1}{72} + \frac{1}{9} + \frac{1}{8} + \frac{1}{4} + \frac{1}{4} + \frac{1}{4}$$

and $\quad G = \langle w, x, y, z \mid w^4 = x^4 = y^3 = z^3 = 1, w^2 = x^2, x^w = x^3, y^z = y, y^w = z, z^w = y^2, y^x = yz, z^x = yz^2 \rangle;$

(v) *equation* (*) *reads*

$$1 = \frac{1}{12} + \frac{1}{12} + \frac{1}{6} + \frac{1}{6} + \frac{1}{4} + \frac{1}{4}$$

and $G = \langle x, y, z \mid x^3 = y^2 = z^2 = 1, x^z = x^2, x^y = x, y^z = y \rangle$,

or $G = \langle x, y \mid x^3 = y^4 = 1, x^y = x^2 \rangle$.

THEOREM 2.2. *If G is a finite non-abelian group with exactly seven conjugate classes, then one of the following holds*:

(i) *equation* (*) *reads*

$$1 = \frac{1}{22} + \frac{1}{11} + \frac{1}{11} + \frac{1}{11} + \frac{1}{11} + \frac{1}{11} + \frac{1}{2}$$

and $G = \langle x, y \mid x^{11} = y^2 = 1, x^y = x^{10} \rangle$;

(ii) *equation* (*) *reads*

$$1 = \frac{1}{39} + \frac{1}{13} + \frac{1}{13} + \frac{1}{13} + \frac{1}{13} + \frac{1}{3} + \frac{1}{3}$$

and $G = \langle x, y \mid x^{13} = y^3 = 1, x^y = x^3 \rangle$;

(iii) *equation* (*) *reads*

$$1 = \frac{1}{52} + \frac{1}{13} + \frac{1}{13} + \frac{1}{13} + \frac{1}{4} + \frac{1}{4} + \frac{1}{4}$$

and $G = \langle x, y \mid x^{13} = y^4 = 1, x^y = x^5 \rangle$;

(iv) *equation* (*) *reads*

$$1 = \frac{1}{16} + \frac{1}{16} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{4} + \frac{1}{4}$$

and G is quaternion, dihedral, or semi-dihedral;

(v) *equation* (*) *reads*

$$1 = \frac{1}{120} + \frac{1}{12} + \frac{1}{8} + \frac{1}{6} + \frac{1}{6} + \frac{1}{5} + \frac{1}{4}$$

and $G = \mathrm{Sym}(5)$;

(vi) *equation* (*) *reads*

$$1 = \frac{1}{360} + \frac{1}{9} + \frac{1}{9} + \frac{1}{8} + \frac{1}{5} + \frac{1}{5} + \frac{1}{4}$$

and $G = \mathrm{Alt}(6)$;

(vii) *equation* (*) *reads*

$$1 = \frac{1}{24} + \frac{1}{24} + \frac{1}{6} + \frac{1}{6} + \frac{1}{6} + \frac{1}{6} + \frac{1}{4}$$

and $G = \langle x, y, z \mid x^2 = y^2, x^4 = z^3 = 1, x^y = x^3, x^z = y, y^z = xy \rangle$;

https://doi.org/10.4153/CJM-1968-042-9 Published online by Cambridge University Press

(viii) *equation* $(*)$ *reads*

$$1 = \frac{1}{55} + \frac{1}{11} + \frac{1}{11} + \frac{1}{5} + \frac{1}{5} + \frac{1}{5} + \frac{1}{5}$$

and $$G = \langle x, y \mid x^{11} = y^5 = 1, x^y = x^4 \rangle;$$

(ix) *equation* $(*)$ *reads*

$$1 = \frac{1}{42} + \frac{1}{7} + \frac{1}{6} + \frac{1}{6} + \frac{1}{6} + \frac{1}{6} + \frac{1}{6}$$

and $$G = \langle x, y \mid x^7 = y^6 = 1, x^y = x^3 \rangle.$$

The proof follows Landau's method (in contrast to the methods employed by G. A. Miller (**9**)). If G is not to be abelian, then obviously $2 \leqslant m_k \leqslant k - 1$. Fixing k (here as 6 or 7) we take some value in this range for m_k. Then m_{k-1} is bounded (roughly between $m_k/(m_k - 1)$ and $(k-1)m_k/(m_k - 1)$) and we choose some intermediate value for m_{k-1}. Continuing in this way we fill in the denominators in $(*)$ and then check whether any group exists with these values as its class indices. This latter condition enables us to apply a number of restrictions to the possible value of m_i when $m_k, m_{k-1}, \ldots, m_{i+1}$ are already chosen; for, if $x \in K_i$ and $m_i = |G|/|K_i|$, then $m_i = |C_G(x)|$. The most basic restrictions stem from

PROPOSITION 2.3 (Burnside, **4**, Note A). *If for some $i > 1$, $m_i = p$, p prime, then $p^2 \nmid |G|$, and if, for some $j > 1$, $p \mid m_j$, then $m_j = p$.*

PROPOSITION 2.4 (Miller, **9**). *G is a Frobenius group with kernel of index p, p prime, if and only if $m_i = p$ for $p - 1$ distinct values of i.*

PROPOSITION 2.5 (Miller, **11**). *If for exactly b values of $i > 1$, $m_i = p$, p prime, then $b \mid (p-1)$ and $(p-1)/b$ is the order of some element of G.*

PROPOSITION 2.6. *If for some $i > 1$, $m_i = pq$, p and q distinct primes, then for at least three distinct values of $j > 1$, pq divides m_j.*

Actually we require more general forms of these propositions (for example, see Proposition 4.1) but usually the statement of the generalized proposition is too lengthy and awkward to warrant presentation here. We should note, however, the general principle underlying Proposition 2.6 since it is quite useful: m_i is the order of a subgroup of G with non-trivial centre so that if m_i is not a prime power, then for every prime $p \mid m_i$ there exists a prime $q \mid m_i$ $(q \neq p)$ and elements of order p and q which commute.

In order to give a better idea of the actual proof, let us just indicate it briefly for $k = 6$. First, $2 \leqslant m_6 \leqslant 5$. If $m_6 = 5$, no group exists because of Theorem 3.2 of the next section. If $m_6 = 2$, the groups of 2.1 (i) follow from Proposition 3.1. Because $m_6 = 3$ leads to a lengthy discussion, we examine the case $m_6 = 4$ instead; this should illustrate the methods sufficiently. If

$m_6 = 4$ and $m_5 \geqslant 7$, then m_2, m_3, and m_4 are at least 7, and $m_1 \geqslant 28$, so $(*)$ can never be satisfied. Therefore $m_5 = 4, 5$, or 6. If $m_5 = 6$, then $m_2 = 6$ and $m_1 = 12$ by the same reasoning, and no such group of order 12 exists. If $m_5 = 5$, then m_4 cannot be 6 or greater, so $m_4 = 5$, and then $m_3 < 7$; if $m_3 = 6$ we contradict Proposition 2.6 and if $m_3 = 5$, then $m_2 = 5$ by Proposition 2.5, contradicting $(*)$. Finally if $m_5 = 4$, then either $m_4 = 8$, in which case $m_1 = 8$ and no such group exists, or $m_4 < 7$. If $m_4 = 6$, then using Proposition 2.6 and the bounds, $m_3 = 6$, and so $m_2 = m_1 = 12$ and we have 2.1 (v). If next $m_4 = 5$, then either $m_3 = 5$ and so $m_2 = 12$, or $m_3 = 6$, both of which contradict Proposition 2.6. Last, when $m_4 = 4$, Proposition 4.2 of the last section gives two possible types of Frobenius group, and the remark that a cyclic group of order 9 has automorphism group of order 6 suffices to yield 2.1 (iii) and (iv). We should remark that occasionally quite large values for m_1 occur in $(*)$ even when Propositions 2.3 to 2.6 are not contradicted; because of their size we cannot refer to lists of such groups, and rather sophisticated arguments are required to show that no corresponding groups exist.*

3. The case $m_k = k - 1$. As we remarked above, m_k is bounded by 2 below and by $k - 1$ above, if G is non-abelian. Now when $k \leqslant 7$, the values near the middle of the interval $[2, k - 1]$, when assumed by m_k, give quite a variety of groups; from the smallest to the largest. Therefore it might be expected that, for a general k, as m_k nears the extreme values, the corresponding groups are of a rather particular character. In fact, when $m_k = 2$, we have, as a corollary of Proposition 2.4:

PROPOSITION 3.1 (Burnside **4**, Note A). *If $m_k = 2 \neq |G|$, then $m_j = 2k - 3$ for $1 < j < k$, and $G = \langle x, M \mid x^2 = 1, y^x = y^{-1}$ for all $y \in M\rangle$ where M can be any abelian group of order $2k - 3$.*

In addition, Burnside (**4**, Note A) gave one possible solution for G when $m_k = k - 1$. Here we describe all solutions in this case.

THEOREM 3.2. *If $m_k = k - 1$, then either*
(i) $k = p^a$ *(p prime); equation $(*)$ reads*

$$1 = \frac{1}{k(k-1)} + \frac{1}{k} + \frac{1}{k-1} + \ldots + \frac{1}{k-1};$$

and G is a Frobenius group of order $p^a(p^a - 1)$ in which the kernel is elementary abelian and has cyclic complement of order $p^a - 1$; or
(ii) $k = 2^{2^b} + 1$; *equation $(*)$ reads*

$$1 = \frac{1}{2(k-1)} + \frac{1}{2(k-1)} + \frac{1}{k-1} + \ldots + \frac{1}{k-1};$$

*Cf. my Ph.D. thesis "On the group class equation," McGill University (1966).

https://doi.org/10.4153/CJM-1968-042-9 Published online by Cambridge University Press

and G is an extra-special 2-group of order 2^{b+1}.

For each such value of k, corresponding such groups exist.

Proof. To begin, let us show that only two forms of equation $(*)$ expressed above can occur. To simplify the proof, let λ denote $k - 1$.

If $i > 1$, $m_i \leqslant 2\lambda = 2(k-1)$, since

$$\frac{i}{m_i} \geqslant 1 - \left(\frac{1}{m_k} + \ldots + \frac{1}{m_{i+1}}\right) \geqslant 1 - \frac{k-i}{k-1},$$

using $(*)$. Thus we can write $m_i = \lambda + \rho_i$ where $\rho_i \leqslant \lambda$ $(i > 1)$. Note that $(\lambda, m_i) = (\lambda, \rho_i) \leqslant \rho_i$. Let ρ be the minimum non-zero value of the ρ_i, so that for some j,

$$m_j = \lambda + \rho, \qquad m_{j+1} = m_{j+2} = \ldots = m_k = \lambda.$$

Put $(\lambda, \rho) = \rho' \leqslant \rho$. Since $m_1 = |G| = \text{l.c.m.}\{m_i \neq m_1\} \geqslant \lambda(\lambda + \rho)/\rho'$,

$$1 = \frac{1}{m_1} + \ldots + \frac{1}{m_k} \leqslant \frac{\rho'}{\lambda(\lambda+\rho)} + \frac{j}{\lambda+\rho} + \frac{\lambda - j}{\lambda}.$$

Therefore $\lambda(\lambda + \rho) \leqslant \rho' + j\lambda + (\lambda - j)(\lambda + \rho)$; that is, $j \leqslant \rho'/\rho \leqslant 1$. It follows that $\rho' = \rho$ and $j = 1$, so we have $m_3 = m_4 = \ldots = m_k = \lambda = k - 1$, $k \leqslant m_2 \leqslant 2\lambda$, and if $m_2 = \lambda + \rho$, then $1 \leqslant \rho \leqslant \lambda$ and $\rho = (m_2, \lambda)$.

Now the values of the $m_i \neq m_1$ are the orders of the centralizers of the elements of G not in $Z(G)$ (these centralizers are called the fundamental subgroups of G; cf. Ito **(7)**). Thus if $m_2 < 2\lambda$, then no fundamental subgroup is a proper subgroup of any other fundamental subgroup of G. By a theorem of Ito **(7**, 4.2**)** the fundamental subgroups of G must be abelian, and hence must be Hall subgroups of G **(**Brauer and Fowler **3**, Section 14**)**. In particular, $(m_2, \lambda) = 1$, and since $m_2 = \lambda + \rho$ with $\rho = (m_2, \lambda)$, we conclude that $m_2 = \lambda + 1 = k$.

Thus if $m_k = k - 1$, then $m_3 = m_4 = \ldots = m_k$ and $m_2 = k$ or $m_2 = 2(k-1)$. If $m_2 = k$, then we have seen that the fundamental subgroups of G are abelian Hall subgroups; by a generalization of Proposition 2.6 $m_2 = k$ must be a prime power, say $k = p^a$. The solutions of $x^{p^a} = 1$ lie in K_1 and K_2; conversely, because $m_2 = p^a$, every element of K_1 and K_2 must be a solution of $x^{p^a} = 1$. Therefore there are exactly $1 + |K_2| = p^a$ such solutions. Since $m_2 = p^a$, it follows that G possesses a normal subgroup of order p^a. Using the fact that the order of any non-trivial element of G divides p^a or $p^a - 1$, a theorem of Feit **(5**, 2.1**)** now shows that G is a Frobenius group. The kernel, of order p^a, must be elementary abelian **(**Burnside **4**, p. 182**)**, and its complement, being abelian, must be cyclic **(18)**. Burnside **(4**, Section 140**)** has shown that for all prime powers $p^a \geqslant 3$, such a group exists.

If $m_2 = 2(k-1)$, then $|Z(G)| = 2$. Ito **(7)** has shown that a group whose centre and non-central classes have order 2 is a 2-group. Then, applying Section 99 of Burnside **(4)**, we have $G' = Z(G)$ and G/G' elementary abelian with an even number of generators, say $2b$. Such (extra-special) 2-groups exist, for each positive integral value of b, as the central product of b quaternion and dihedral groups of order 8.

4. The case $m_k = m_{k-1} = m_{k-2} = 4$. A majority of the groups having $k \leqslant 7$ are Frobenius groups. Often they arise through Proposition 2.3 and a generalization of this result proves useful.

PROPOSITION 4.1. *Let S be a subset of the integers from 2 to k and p a prime such that in* $(*)$, *if $s \in S$, m_s is a power of p, and*

$$\sum_{s \in S} \left(\frac{1}{m_s}\right) = \frac{p^a - 1}{p^a},$$

with $p^a \| n = |G| \neq p^a$. Then G is a Frobenius group with kernel of index p^a.

Proof. Denote the number of solutions in G of $x^{p^a} = 1$ by t. Let P be a p-Sylow subgroup of G and let λ be the number of p-Sylow subgroups of G. Note that $\lambda | N_G(P)| = n$ so $\lambda \leqslant n/p^a$. Now if $x = 1$ or $x \in K_s$ for some $s \in S$, then $x^{p^a} = 1$ and so

$$t \geqslant \left(\frac{p^a - 1}{p^a}\right) n + 1 \geqslant (p^a - 1)\lambda + 1.$$

On the other hand, $x^{p^a} = 1$ means that $x \in yPy^{-1}$ for some y and as $P \cap yPy^{-1} \geqslant 1$, then $t \leqslant 1 + (p^a - 1)\lambda$. It follows that $P \cap yPy^{-1} = 1$ if $y \notin N_G(P)$ and that $N_G(P) = P$. Hence G is a Frobenius group and P is a complement of the kernel.

It is natural to ask if we can eliminate the condition "$p^a \| n$" in the above proposition. The simplest related case to examine is that of $p = 2$, $a = 2$, and the answer here is:*

THEOREM 4.2. *Let G satisfy* (α) $m_k = m_{k-1} = m_{k-2} = 4$. *Then G is one of*:

(i) *a Frobenius group whose kernel is abelian of order* $4k - 15$ *and index* 4 (so $m_j = 4k - 15$ for $2 \leqslant j \leqslant k - 3$);

(ii) *a Frobenius group whose kernel is abelian of order* $8k - 39$ *and any complement is quaternion of order* 8 (so $m_{k-3} = 8$, $m_j = 8k - 39$ *for* $2 \leqslant j \leqslant k - 4$);

(iii) *abelian of order* 4; *or*

(iv) *quaternion or dihedral of order* 8.

Proof. First we need a formula for the class number of a Frobenius group, and this follows directly from the properties of Frobenius groups:

LEMMA 4.3. *If G is a Frobenius group with kernel M and a complement H of order h, then*

$$k(G) = k(H) + \frac{k(M) - 1}{h}.$$

*I thank T. Gagen for his help in completing the proof of this theorem.

Now let G be a minimal counterexample, $n = |G|$. By (iii), $n \neq 4$. If $4 \parallel n$, then by Proposition 4.1 G is a Frobenius group whose kernel has index 4. By a theorem of Burnside (**4**, p. 172) the kernel is abelian and so by Lemma 4.3 it has order $4k - 15$, contradicting (i). Therefore $8 \mid n$ and Suzuki (**16**; **17**) has shown the 2-Sylow subgroups of G to be dihedral or quaternion, or possibly semi-dihedral of order at least 16. Of these, only the quaternion and dihedral groups of order 8 satisfy (α), as is easily checked. By (iv), $n \neq 8$. Let P be a 2-Sylow subgroup of G and $1 \neq t \in Z(P)$; t is an involution of G. Since $P \leqslant C_G(t)$, then $C_G(t)$ satisfies (α). If $C_G(t) = P$, then for some i, $m_i = 8$, and since $8 \parallel n$, $8 \neq n, G$ is a Frobenius group with kernel of index 8 by Proposition 4.1. Again the kernel is abelian, and $k(P) = 5$, so by Lemma 4.2 the kernel has order $8k - 39$. Finally, Zassenhaus (**18**) has shown that P cannot be dihedral, so (ii) forces us to conclude that $C_G(t) \neq P$. If P were quaternion, then by Proposition 4 of Suzuki (**17**), $C_G(t)$ is SL(2, 3) or SL(2, 5), neither of which satisfy (α). Hence P is dihedral,

$$P = \langle x, y \mid x^4 = y^2 = 1, x^y = x^{-1} \rangle, \qquad t = x^2.$$

By Lemma 8 of Gorenstein and Walter (**6**), $C_G(t)$ has a (non-trivial) normal 2-complement N. Then xy and y act as fixed-point-free automorphisms of N of order 2 by (*), sending every element of N into its inverse. But then $(xy)(y) = x$ leaves N elementwise fixed, contradicting (*). Therefore G does not exist.

It is an open question what happens if $p \neq 2$ or if $a > 2$.

References

1. R. Brauer, *Representations of finite groups*, Lectures on Modern Mathematics, ed. T. L. Saaty. Vol. I (New York, 1963).
2. ——— *Some applications of the theory of blocks of characters of finite groups*. I, J. Alg., *1* (1964), 152–167.
3. R. Brauer and K. A. Fowler, *On groups of even order*, Ann. of Math., *62* (1955), 565–583.
4. W. Burnside, *Theory of groups of finite order* (2nd ed.; New York, 1911).
5. W. Feit, *On the structure of Frobenius groups*, Can. J. Math., *9* (1957), 587–596.
6. D. Gorenstein and J. H. Walter, *On finite groups with dihedral Sylow 2-subgroups*, Illinois J. Math., *6* (1962), 553–593.
7. N. Ito, *On finite groups with given conjugate types I*, Nagoya Math. J., *6* (1953), 17–28.
8. E. Landau, *Über die Klassenzahl der binaren quadratischen Formen von negativer Discriminante*, Math. Ann., *56* (1903), 671–676.
9. G. A. Miller, *Groups involving only a small number of sets of conjugate operators*, Arch. Math. and Phys., *17* (1910), 199–204.
10. ——— *Groups possessing a small number of sets of conjugate operators*, Trans. Amer. Math. Soc., *20* (1919), 260–270.
11. ——— *Groups involving a small number of sets of conjugate operators*, Proc. Nat. Acad. Sci., *30* (1944), 359–362.
12. J. Poland, *Two problems on finite groups with k conjugate classes*, J. Austral. Math. Soc. (to appear).
13. O. J. Schmidt, *Selected works of Otto Schmidt* (Moscow, 1959).
14. W. R. Scott, *Group Theory* (Englewood Cliffs, 1964).

15. D. T. Sigley, *Groups involving five complete sets of non-invariant conjugate operators*, Duke Math. J., *1* (1935), 477–479.

16. M. Suzuki, *A characterization of simple groups* LF(2.p), J. Fac. Sci. Univ. Tokyo Sect. I, *6* (1951), 259–293.

17. ——— *On finite groups containing an element of order four which commutes only with its powers*, Illinois J. Math., *3* (1959), 255–271.

18. H. Zassenhaus, *Über endliche Fastkorper*, Hamb. Abh., *11* (1936), 187–220.

Department of Mathematics,
Institute of Advanced Studies,
Australian National University,
Canberra, and
Carleton University,
Ottawa

https://doi.org/10.4153/CJM-1968-042-9 Published online by Cambridge University Press