J. Austral. Math. Soc. 25 (Series A) (1978), 291-313.

A CONVERSE TO LAGRANGE'S THEOREM

T. R. BERGER

(Received 10 June 1976)

Abstract

An integer $n > 0$ is called a CLT-number if any group of order n has subgroups of order d for every divisor d of n. The set $\mathcal{S}$ of CLT-numbers n is characterized by properties of the prime factorization of n. In addition, if G has order dividing a CLT-number then the structure of $G/C_G(U)$ is given where U is a chief factor of G. As a consequence, it is shown that G is solvable of Fitting height at most 3.

One of the very first theorems taught in introductory group theory courses is the following.

LAGRANGE'S THEOREM. *If G is a group and H is a subgroup of G then the order of H divides the order of G.*

Most students then want to know: "Is the following statement true?"

CONVERSE TO LAGRANGE'S THEOREM. *If G is a group of order n, and d is a divisor of n, then G contains a subgroup of order d.*

Of course, the standard example A^4, the alternating group on 4 points, is of order 12 and has no subgroup of order 6. Therefore, CLT (the converse to Lagrange's Theorem) *is false*. The fundamental importance of Lagrange's Theorem has led to attempts to describe the groups G and the integers n for which CLT is valid. We shall say that a group G of order n is a *CLT-group* if CLT holds for G and any divisor d of n. We shall say that an integer $n > 0$ is a *CLT-number* if any group of order n is a CLT-group. The CLT-groups are a very complex class of groups. By a theorem of P. Hall (see Huppert (1967), VI, 1.10) we know that all such groups are solvable. On the other hand,

This research was partially supported by the Australian Research Grants Comission and by National Science Foundation.

https://doi.org/10.1017/S1446788700021042 Published online by Cambridge University Press

Gagen (to appear) shows that any solvable group may be embedded in an indecomposable CLT-group.

We shall be content here to look at CLT-numbers, giving a characterization of the set of CLT-numbers $n > 1$ by the divisors and prime factors of n. In other words, we shall give an effective procedure for determining a set $\mathscr{S}$ of integers $n > 1$ such that $\mathscr{S} \cup \{1\}$ is precisely the set of CLT-numbers. The basic idea is that most numbers are not CLT-numbers. In Sections 2 and 3 we describe a class of numbers which are not CLT-numbers. These numbers are given in Propositions (3.5)–(3.9). The obvious guess is then that these propositions completely describe non-CLT-numbers. Accordingly, we define a set $\mathscr{S}$ of integers $n > 1$ in Section 1 rigged so that $\mathscr{S}$ is precisely the set of integers for which Propositions (3.5)–(3.9) fail. We call the integers in $\mathscr{S}$ *good*, and those not in $\mathscr{S}$ *bad*. In particular, these propositions show that any CLT-number $n > 1$ is good.

To complete the circuit we must show that any good integer $n > 1$ is a CLT-number. At this point we must show that any group of order n is solvable. We do this in Section 4 using far too much heavy artillery. In Section 5, the heart of the paper, we examine the structure of chief factors of a group of order n where $n > 1$ is good. One upshot of this analysis (Theorem (7.1)) is that if G has order a good number n then G has fitting height at most 3 and that this bound is best possible, indicating that groups of order a CLT-number are rather limited in structure.

In Section 6 we prove a theorem which enables us (1) to ascertain that if G has a noncyclic chief factor then G has a noncyclic minimal normal subgroup, and (2) to split G over this minimal normal subgroup. In Section 7 we use the facts in Section 5 to prove that the theorem of Section 6 applies. The splitting so obtained allows us to use induction on the order of G and the splitting subgroup obtained in G to complete the proof that a good integer $n > 1$ is a CLT-number.

Included in the bibliography is a selection of papers related to CLT. Some of these are not cited in the text of this paper. For a general discussion of CLT see McCarthy (1971).

I would like to thank Rebecca Struik for suggesting this problem to me. She has characterized most of the CLT-numbers of the form $p^a q^b$ where p and q are primes Struik (preprint).

1. Definitions

Let $d > 1$ be an integer, and set $\mathscr{I}(d) = \{1, 2, \cdots, d-1, 2d-1\}$ and $\mathscr{I}'(d) = \{1, 2, \cdots, d-1\}$. Fix a prime q and a positive integer m. We define a set $\mathscr{S}(m, q)$ as follows:

https://doi.org/10.1017/S1446788700021042 Published online by Cambridge University Press

(1) if p is a prime, $p \neq q$, d is the exponent of $q \pmod p$, and $d > 1$, then $\mathcal{S}(p,q) = \mathcal{I}(d)$ if d is odd and $\mathcal{S}(p,q) = \mathcal{I}'(d)$ if d is even;

(2) if p is a prime, $p \mid q-1$, and $p^2 \nmid q-1$, then $\mathcal{S}(p^2,q) = \mathcal{I}(p)$ when $p > 2$ and $\mathcal{S}(4,q) = \mathcal{I}'(2)$;

(3) if p is a prime and $p \mid q-1$, then $\mathcal{S}(p^3,q) = \mathcal{I}(p)$ when $p > 2$ and $\mathcal{S}(8,q) = \mathcal{I}'(2)$; or

(4) if $\mathcal{S}(m,q)$ is not defined by (1), (2), or (3) then let $\mathcal{S}(m,q)$ be the set of positive integers.

Next we define a set of positive integers $\mathcal{S}(r,p^u,q)$ where r, p, q are primes and $u \geqq 1$ is an integer as follows:

(a) if $rp \mid q-1$, $r \neq p$, and p has odd exponent $u \pmod r$ then $\mathcal{S}(r,p^u,q) = \mathcal{I}(r)$ when $r > 2$ and $\mathcal{S}(2,p^u,q) = \mathcal{I}'(2)$; and

(b) if $\mathcal{S}(r,p^u,q)$ is not defined by (a) then let $\mathcal{S}(r,p^u,q)$ be the set of positive integers.

Suppose that $n > 1$ is an integer and q is a prime divisor of n. We define

$$\mathscr{E}(q) = \mathscr{E}_n(q) = (\cap \mathcal{S}(m,q)) \cap (\cap \mathcal{S}(r,p^u,q))$$

where m, r, p, u are positive integers, r and p are primes, and both m and rp^u range over all possible such divisors of n. We shall write

$$n = \prod q^{e(q)}$$

where q ranges over the distinct prime divisors of n (i.e. $e(q)$ is the highest exponent of q such that $q^{e(q)}$ divides n). We shall say that an integer $n > 1$ is *good* if $e(q) \in \mathscr{E}(q)$ for all prime divisors q of n, otherwise we say that n is *bad*.

The main object of this paper is to prove the following theorem.

THEOREM 1.1. *An integer $n > 1$ is a CLT-number if and only if n is a good integer.*

EXAMPLE 1.2. Suppose that $n > 1$ is an integer with prime factors 3, 13, 79. What are the possible values for good n? If p and q are primes, let d be the order of $q \pmod p$. Below we list those solutions where $d > 1$.

q	p	d
3	13	3
3	79	78
13	79	39

We obtain the following sets *different* from the set of all positive integers.

https://doi.org/10.1017/S1446788700021042 Published online by Cambridge University Press

$$\begin{aligned}
\mathscr{S}(13,3) &= \{1,2,5\}\\
\mathscr{S}(79,3) &= \{1,\cdots,77\}\\
\mathscr{S}(79,13) &= \{1,\cdots,38,77\}\\
\mathscr{S}(3^2,13) = \mathscr{S}(3^3,13) &= \{1,2,5\}\\
\mathscr{S}(3^2,79) = \mathscr{S}(3^3,79) &= \{1,2,5\}\\
\mathscr{S}(13^2,79) = \mathscr{S}(13^3,79) &= \{1,\cdots,12,25\}\\
\mathscr{S}(3,13,79) &= \{1,2,5\}\\
\mathscr{S}(13,3^3,79) &= \{1,\cdots,12,25\}
\end{aligned}$$

We now have

$$\begin{aligned}
\mathscr{E}(3) &= \{1,2,5\}\\
\mathscr{E}(13) &= \{1,\cdots,38,77\} \quad \text{if} \quad e(3)=1, \quad \text{or}\\
&= \{1,2,5\} \quad \text{if} \quad e(3)>1\\
\mathscr{E}(79) &= \{1,2,5\}
\end{aligned}$$

From these values, the possibilities for good n may be listed. For example $3^5 \cdot 13^2 \cdot 79^2$ is a good number, as are $3 \cdot 13^{77} \cdot 79^5$ or $3 \cdot 13 \cdot 79^5$.

The notation and terminology are standard and follow that given in Gorenstein (1968) and Huppert (1967). We quote here one more theorem which will be of use and is relevant to our discussion.

THEOREM 1.3. *A finite group G is supersolvable if and only if G and all its subgroups are CLT-groups.*

Proofs may be found in Bray (1968), Deskins (1968), Doerk (1968), McLain (1957), Ore (1939) or Zappa (1940).

2. The examples

HYPOTHESIS 2.1. *For this section, let q be a prime, H a q'-group of order h, and V a faithful irreducible $\mathbf{F}[H]$-module of dimension d where $\mathbf{F}$ is the field $GF(q)$ of q elements.*

The groups of main interest will be constructed from the following examples for the pair H, V.

EXAMPLES 2.2. (1) Let H be cyclic of prime order h $(\neq q)$, and V be a faithful irreducible $F[H]$-module. If e is the exponent of q $(\operatorname{mod} p)$ then $d = e$.

(2) Suppose that p is a prime such that $p \mid q-1$ and $p^2 \nmid q-1$. Let H

https://doi.org/10.1017/S1446788700021042 Published online by Cambridge University Press

be cyclic of order $h = p^2$, and V be a faithful irreducible $\boldsymbol{F}[H]$-module. In this case, $d = p$.

(3) Suppose that p is a prime such that $p \mid q - 1$. Let H be an extraspecial p-group of order $h = p^3$, and V be a faithful irreducible $\boldsymbol{F}[H]$-module. In this case, $d = p$. (If $p = 2$ assume that H is quaternion.)

(4) Suppose that r and p are two distinct primes such that $p \mid q - 1$ and $r \neq q$. Let H denote the nonabelian group with an elementary abelian normal Sylow p-subgroup which is a chief factor, and a Hall p'-subgroup of order r. The order of H is $h = rp^f$ where f is the exponent of $p \pmod r$. Let V be a faithful irreducible $\boldsymbol{F}[H]$-module so that $d = r$.

It is straightforward to verify that examples do exist with the given properties. There is some ambiguity in the statement of these examples:

(a) in example (3) there are two isomorphism classes of such groups H, and more generally, (b) once H is given, there may be several choices for V up to isomorphism. For our purposes it does not matter which of all possible choices is made in each case, except in Example (2.2) (3) when $p = 2$. If $p = 2$ in this example, we assume that H is quaternion.

LEMMA 2.3. *Suppose that a group G contains normal subgroups L and M such that $L \cap M = \{1\}$. If T is a subgroup of G then $|T| = [TL : L][(T \cap L)M : M]$.*

Note that $TL/L \cong T/T \cap L$ and that $T \cap L = (T \cap L)/(T \cap L \cap M) \cong (T \cap L)M/M$. From this, the lemma follows.

In the following constructions we shall let

$$k \times V = V \oplus \cdots \oplus V \qquad (k \text{ copies})$$

where k is a positive integer, and $0 \times V = (0)$.

(I) *The group $G_1(H, V, k)$.*

LEMMA 2.4. *There is a group $G_1(H, V, k)$, where $k \geqq 0$ is an integer, with the following properties:*

(1) *it has order hq^{kd};*

(2) *it has a normal abelian Sylow q-subgroup $Q_1(H, V, k)$; and*

(3) *if K is a subgroup of order hq^c then $c = k'd$ for $0 \leqq k' \leqq k$.*

Let $Q_1(H, V, k) = k \times V$, so that there is an obvious action for H upon $Q_1(H, V, k)$. Form the semidirect product

$$G_1(H, V, k) = H \cdot Q_1(H, V, k).$$

Since (1) and (2) are easily verified, we check only (3). Replacing K by a conjugate, we may assume that $K \geqq H$. Now $K \cap Q_1(H, V, k)$ is an $\boldsymbol{F}[H]$-

https://doi.org/10.1017/S1446788700021042 Published online by Cambridge University Press

submodule of $Q_1(H, V, k)$. Since $Q_1(H, V, k)$ is a homogeneous $\boldsymbol{F}[H]$-module with irreducible components of dimension d, $c = k'd$ where $0 \leqq k' \leqq k$.

(II) *The group* $G_2(H, V, k)$ $(k \geqq 2)$.

LEMMA 2.5. *There is a group* $G_2(H, V, k)$, *where* $k \geqq 2$ *is an integer, with the following properties*:

(1) *it has order* hq^{kd+1};

(2) *it has a normal Sylow* q-*subgroup* $Q_2(H, V, k)$; *and*,

(3) *if* K *is a subgroup of order* hq^c *then* $c = k'd$ *where* $0 \leqq k' \leqq k - 1$ *or* $c = k'd + 1$ *where* $0 \leqq k' \leqq k$.

Let $\hat{V} = \mathrm{Hom}_{\boldsymbol{F}}(V, \boldsymbol{F})$ be the dual space of V. If $f \in \hat{V}$ and $x \in H$ then define $fx \in \hat{V}$ by the equations

$$fx(v) = f(vx^{-1}). \tag{2.6}$$

This defines an action of H upon $\hat{V}$ contragradient to the action of H upon V so that $\hat{V}$ is a faithful irreducible $\boldsymbol{F}[H]$ – module. Form the Cartesian product

$$Q_2(H, V) = (V \oplus \hat{V}) \times \boldsymbol{F}. \tag{2.7}$$

If $(v \oplus f, z), (v' \oplus f', z') \in Q_2 = Q_2(H, V)$ then define multiplication in Q_2 via

$$(v \oplus f, z)(v' \oplus f', z') = ((v + v') \oplus (f + f'), z + z' + f(v')). \tag{2.8}$$

If $x \in H$ and $(v \oplus f, z) \in Q_2$ then define an action of H on Q_2 via

$$(v \oplus f, z)^x = ((vx) \oplus (fx), z). \tag{2.9}$$

Verification of the following facts is straightforward.

LEMMA 2.10. *Equations* (2.6)–(2.9) *define an extraspecial* q-*group* $Q_2 = Q_2(H, V)$ *of order* q^{2d+1}. *The group* H *acts upon* Q_2 *in such a way that* H *centralizes* $Z(Q_2)$ *and* $Q_2/Z(Q_2) \simeq V \oplus \hat{V}$ *as an* $\boldsymbol{F}[H]$-*module*.

The construction given here is standard and the proof of this lemma is straightforward.

We set

$$Q_2(H, V, k) = Q_2(H, V) \times Q_1(H, V, k - 2)$$

where k $(\geqq 2)$ is an integer. Since H has an obvious action upon $Q_2(H, V, k)$ we define

$$G_2(H, V, k) = H \cdot Q_2(H, V, k)$$

to be the semidirect product. Parts (1) and (2) of Lemma (2.5) are easily verified so that we prove only (3). By conjugating K, we may assume that $K \geqq H$. Set $G_1 = G_1(H, V, k - 2)$, $G_2 = G_2(H, V, k)$, $G_2^* = G_2(H, V, 2)$, $Q_1 = Q_1(H, V, k - 2)$, and $Q_2 = Q_2(H, V)$. We have the following isomorphisms:

https://doi.org/10.1017/S1446788700021042 Published online by Cambridge University Press

$$G_2/Q_2 \simeq G_1, \quad \text{and} \quad G_2/Q_1 \simeq G_2^*.$$

By these isomorphisms, we may view $\bar{K}_1 = KQ_2/Q_2$ as a subgroup of G_1 and $\bar{K}_2 = H(K \cap Q_2)Q_1/Q_1$ as a subgroup of G_2^*. In both cases, we are looking at subgroups of order $hq^{c'}$ for some c'. By Lemma (2.3) the order of the Sylow q-subgroup of K is the product of the orders of the Sylow q-subgroups of $\bar{K}_i$, $i = 1, 2$. If $\bar{K}_i$ has order q^{c_i}, $i = 1, 2$ then $c_1 + c_2 = c$. By Lemma (2.4), $c_1 = k'd$ for $0 \leqq k' \leqq k - 2$. Viewing $\bar{K}_2$ as a subgroup of G_2^*, Lemma (2.10), implies that $\tilde{K}_2 = \bar{K}_2 Z(Q_2)/Z(Q_2)$ is a subgroup of order $hq^{c''}$ in the semidirect product $H(V \oplus \hat{V})$. Such a subgroup must have order $hq^{k''d}$ where $0 \leqq k'' \leqq 2$ as may be proved by a method analogous to that used to prove Lemma (2.4). Thus $c_2 = k''d + k_0$ where $k_0 = 0, 1$ and $0 \leqq k'' \leqq 2$. Suppose that $k'' = 2$ so that

$$Q_2 = \langle \bar{K}_2 \cap Q_2, Z(Q_2) \rangle = \bar{K}_2 \cap Q_2$$

since $Z(Q_2)$ is the Frattini subgroup of Q_2. In particular, if $k'' = 2$ then $k_0 = 1$. Since $c_1 + c_2 = c$, Lemma (2.5) follows.

(III) *The group* $G_3(H, V)$.

LEMMA 2.11. *Assume that H, V are as in* (a) *Example* (2.2) (1) *with d even,* (b) *Examples* (2.2) (2) *or* (3) *with $p = 2$, or* (c) *Example* (2.2) (4) *with $r = 2$ and $f = 1$.*

There is a group $G_3(H, V)$ with the following properties:

(1) *it has order hq^{d+1}*;

(2) *it has a normal Sylow q-subgroup $Q_3(H, V)$*; *and*

(3) *if K is a subgroup of order hq^c then $c = 0, 1, d + 1$.*

The group $G_3(H, V)$ exists under very general conditions on H and V, but we shall only need the cases cited here.

The group $G_3 = G_3(H, V) = H \cdot Q_3(H, V)$ is a semidirect product where $Q_3 = Q_3(H, V)$ is extraspecial of order q^{d+1} and $Q_3/Z(Q_3) \simeq V$ as an $\boldsymbol{F}[H]$-module. If H is cyclic of prime order and d is even, the existence of G_3 is well known. (Berger (1973a), Gorenstein (1968) (Exercise 18 p. 215), Winter (1972)). We shall give a construction which works for G_3 whenever $q > 2$. Since $p \mid q - 1$ in Example (2.2) (4) this is certainly the case there. Therefore, the only case omitted by this construction is the one where we are considering Example (2.2) (1), $q = 2$, and h is an odd prime.

Now assume that $q > 2$, T is a group, and W is an $\boldsymbol{F}[T]$-module which is endowed with a nonsingular alternating bilinear form $g: W \times W \to \boldsymbol{F}$. Suppose that T has a normal subgroup T_0 of odd order and of index 1 or 2. If $\alpha \in T \backslash T_0$ then assume that $\alpha^2 = 1$ and α inverts the elements of T_0 by conjugation. Suppose that for $x \in T$ and $u, v \in W$

$$g(ux, vx) = \varepsilon g(u, v)$$

https://doi.org/10.1017/S1446788700021042 Published online by Cambridge University Press

where $\varepsilon = 1$ if $x \in T_0$ and $\varepsilon = -1$ if $x \notin T_0$.

Form the Cartesian product

$$Q^* = W \times F, \tag{2.12}$$

and for (v, z), $(v', z') \in Q^*$ define multiplication via

$$(v, z)(v', z') = (v + v', z + z' + g(v, v')). \tag{2.13}$$

If $x \in T$ and $(v, z) \in Q^*$ then define an action of T on Q^* via

$$(v, z)^x = (vx, \varepsilon z) \tag{2.14}$$

where $\varepsilon = 1$ if $x \in T_0$ and $\varepsilon = -1$ if $x \notin T_0$.

LEMMA 2.15. *Equations* (2.11)–(2.14) *define an extraspecial q-group Q^* of order q^{d+1} where* dim $W = d$. *The group T acts upon Q^* in such a way that $C_T(Z(Q^*)) = T_0$ and $Q^*/Z(Q^*) \simeq W$ as an $\boldsymbol{F}[T]$-module.*

The proof is a straightforward verification. Incidentally, the construction may be completed when $q = 2$, but in that case, Q^* is abelian.

Let H, V be as in the hypothesis of Lemma (2.11). With $H = T$ and $V = W$ we wish to prove the existence of a form g. Running through the Examples (2.2), the form g is given for (1) by [Berger (1975), (2.1)], for (2) also by [Berger (1975), (2.1)] for (3) by [Berger (1975), (2.2), (2.3)].

Consider finally Example (2.2) (4) with $r = 2$ and $f = 1$. Then q is necessarily odd. Let H_0 be the normal subgroup of index 2 in H. Now $V|_{H_0} = V_1 \oplus V_2$ where V_1 and V_2 are 1-dimensional. Fix $y \in H \backslash H_0$, $v_1 \in V_1$, $v_1 \neq 0$, and set $v_2 = yv_1$ so that v_2 is a basis vector for V_2. If $\alpha v_1 + \beta v_2$, $\alpha' v_1 + \beta' v_2 \in V$ where $\alpha, \beta, \alpha', \beta' \in \boldsymbol{F}$ then set

$$g_2(\alpha v_1 + \beta v_2, \alpha' v_1 + \beta' v_2) = \alpha\beta' - \alpha'\beta.$$

With $H = T$, $H_0 = T_0$, $V = W$, and $g_2 = g$, the conditions of Lemma (2.15) are satisfied for an example of type Example (2.2) (4).

To prove Lemma (2.11) we set

$$Q_3(H, V) = Q^*, \quad \text{and} \quad G_3(H, V) = H \cdot Q_3(H, V),$$

a semidirect product. Since $Q_3/Z(Q_3) \simeq V$, the verification of (1), (2), (3) of Lemma (2.11) is routine.

3. Bad numbers

In this section we produce a large store of non-*CLT* groups.

HYPOTHESIS 3.1. *In Lemmas* (3.2)–(3.4) *we assume that q is a prime, $\boldsymbol{F} = GF(q)$, $h > 1$ and $m \geqq 1$ are integers such that $(hm, q) = 1$, and $n = hmq^b$*

https://doi.org/10.1017/S1446788700021042 Published online by Cambridge University Press

where $b \geqq 0$ is an integer. In addition, we assume that H is a group of order h, and that V is a faithful irreducible $F[H]$-module of dimension $d > 1$.

Lemma 3.2. *If $b = kd + j$ where $k \geqq 1$ and $0 \leqq j \leqq d-2$ then there is a non-CLT group of order n which has no subgroup of order hmq^{kd-1}.*

Let M be an abelian group of order mq^j so that

$$G = M \times G_1(H, V, k)$$

has order hmq^b by Lemma (2.4). Suppose that K is a subgroup of G of order hmq^{kd-1}. If $L = G_1 = G_1(H, V, k)$ then Lemma (2.3) implies that $kd - 1 = c_1 + c_2$ where $H(K \cap M)G_1/G_1$ and KM/M have Sylow q-subgroups respectively of orders q^{c_1} and q^{c_2}. Since $G/M \simeq G_1$ and KM/M is a subgroup of order hq^{c_2}, by Lemma (2.4) $c_2 = k'd$ where $0 \leqq k' \leqq k$. Clearly $0 \leqq c_1 \leqq j$ so that $kd - 1 = k'd + c_1$ or $-1 \equiv c_1 \pmod{d}$ where $0 \leqq c_1 \leqq d-2$. Since this is impossible, the lemma follows.

Lemma 3.3. *If $b = kd + (d-1)$ where $k \geqq 2$ then there is a non-CLT group of order n which has no subgroup of order hmq^{kd}.*

Let M be an abelian group of order mq^{d-2} so that

$$G = M \times G_2(H, V, k)$$

has order hmq^b by Lemma (2.5). Suppose that K is a subgroup of G of order hmq^{kd}. If $L = G_2 = G_2(H, V, k)$ then Lemma (2.3) implies that $kd = c_1 + c_2$ where $H(K \cap M)G_2/G_2$ and KM/M have Sylow q-subgroups respectively of orders q^{c_1} and q^{c_2}. Since $G/M \simeq G_1$ and KM/M is a subgroup of order hq^{c_2}, Lemma (2.5) implies that $c_2 = k'd$ where $0 \leqq k' \leqq k-1$ or $c_2 = k'd + 1$ where $0 \leqq k' \leqq k$. Clearly $0 \leqq c_1 \leqq d-2$ so that $kd = c_1 + c_2 = k'd + e$ where $0 \leqq k' \leqq k$, $0 \leqq e \leqq d-1$, and if $e = 0$ then $k' \leqq k-1$. Since $e \equiv 0 \pmod{d}$, $e = 0$ and $k' < k$ contradicting the fact that $kd = k'd$. The proof of the lemma is complete.

Lemma 3.4. *Assume that $G_3(H, V)$ exists and satisfies the conclusion of Lemma (2.11). If $b = 2d - 1$ then there is a non-CLT group of order n which contains no subgroup of order hmq^d.*

Let M be an abelian group of order mq^{d-2} (recall that d is even) so that

$$G = M \times G_3(H, V)$$

has order hmq^b by Lemma (2.11). Suppose that K is a subgroup of G of order hmq^d. Since $G/M \simeq G_3 = G_3(H, V)$, as previously, we see that $d = c_1 + c_2$ where c_1 is the exponent of q in $|K \cap M|$ and c_2 is the exponent of q in $|KM/M|$. By (3) of Lemma (2.11) we have $c_2 = 0, 1, d+1$. Obviously, $0 \leqq c_2 \leqq d-2$ so that $d = c_1 + c_2$ is impossible, completing the proof of the lemma.

PROPOSITION 3.5. *If $n = lp^aq^b$ where* (a) *p and q are distinct primes,* (b) $(l, pq) = 1$, (c) $a \geqq 1$ *and* (d) $d > 1$ *where d is the exponent of q* (mod p), *then there is a non-CLT group of order n unless*

(1) *d is odd and $b = 0, 1, \cdots, d - 1, 2d - 1$,*

or

(2) *d is even and $b = 0, 1, \cdots, d - 1$.*

With $p = h$, let H, V be as in Example (2.2) (1). Assume first that $b = kd + j$ where $k \geqq 1$ and $0 \leqq j \leqq d - 2$. With $m = lp^{a-1}$ and $h = p$, Lemma (3.2) guarantees the existence of a non-CLT group of order n. If $b = kd + (d - 1)$ where $k \geqq 2$ then again with $m = lp^{a-1}$ and $h = p$, Lemma (3.3) assures the existence of a non-CLT group of order n. If d is odd, conclusion (1) follows. We therefore assume that $b = 2d - 1$ and that d is even. Now Lemmas (2.11) and (3.4) imply that there is a non-CLT group of order n. From this, conclusion (2) and the proposition follow.

PROPOSITION 3.6. *If $n = l2^aq^b$ where* (a) *q is an odd prime,* (b) $(l, 2q) = 1$, *and* (c) $a \geqq 2$ *then there is a non-CLT group of order n unless*

(1) $b = 0, 1$, *or*

(2) $a = 2$ *and* $q \equiv 1$ (mod 4).

If $a = 2$ and $q \equiv 3$ (mod 4) we let H, V be as in Example (2.2) (2) with $p = 2$. If $a \geqq 3$ we let H, V be as in Example (2.2) (3) with $p = 2$. In either case, dim $V = 2$. As in the previous proposition, Lemmas (3.2) and (3.3) imply that there is a non-CLT group of order n unless $b = 0, 1, 3$. But now Lemma (3.4) applies to show that there is a non-CLT group of order n if $b = 3$. The proof is complete.

PROPOSITION 3.7. *If $n = 2lp^aq^b$ where* (a) *p and q are distinct odd primes,* (b) $(l, pq) = 1$, (c) $a \geqq 1$, *and* (d) $p \mid q - 1$, *then there is a non-CLT group of order n unless $b = 0, 1$.*

Let H, V be as in Example (2.2) (4) where $r = 2$ (so that $f = 1$ and $2p \mid q - 1$). By Lemmas (3.2) and (3.3) we may argue that there is a non-CLT group of order n unless $b = 0, 1, 3$. If $b = 3$ then by Lemma (3.4) there is a non-CLT group of order n, completing the proof of the proposition.

PROPOSITION 3.8. *If $n = lp^aq^b$ where* (a) *p and q are distinct odd primes,* (b) $(l, pq) = 1$, (c) $a \geqq 2$, *and* (d) $p \mid q - 1$, *then there is a non-CLT group of order n unless*

(a) $b = 0, 1, \cdots, p - 1, 2p - 1$ *or*

(b) $a = 2$ *and* $q \equiv 1$ (mod p^2).

https://doi.org/10.1017/S1446788700021042 Published online by Cambridge University Press

If $a \geqq 3$ we use H, V as in Example (2.2) (3). If $a = 2$ and $g \not\equiv 1 \pmod{p^2}$ then we use H, V as in Example (2.2) (2). Lemmas (3.2) and (3.3) imply that there is a non-*CLT* group of order n unless (a) holds. Since we have excluded (b), the proposition is valid.

PROPOSITION 3.9. *If* $n = rlp^aq^b$ *where* (a) r, p *and* q *are distinct odd primes,* (b) $(l, pq) = 1$, (c) $a \geqq u$ *where* u *is the exponent of* $p \pmod{r}$, *and* (d) $rp \mid q - 1$, *then there is a non-CLT group of order* n *unless* $b = 0, 1, \cdots, r - 1, 2r - 1$.

Let H, V be as in Example (2.2) (4). The proposition follows from Lemmas (3.2) and (3.3).

Using these propositions, we have the following immediate corollary.

THEOREM 3.10. *If* n *is a CLT-number then* $e(q) \in \mathscr{E}(q)$ *for every prime divisor* q *of* n.

The various sets $\mathscr{S}(m, q)$ are defined in terms of Propositions (3.5)–(3.9). Therefore, (3.10) follows from these.

4. Good numbers: solvability

In this section we indulge in pounding thumbtacks with sledgehammers. This section could be avoided entirely if we considered only the class of solvable groups. We prove:

THEOREM 4.1. *Suppose that* $n > 1$ *is an integer and for each prime* q *dividing* n, $e(q) \in \mathscr{E}(q)$. *If* G *is a group of order dividing* n *then* G *is solvable.*

If n is odd, the result follows from the paper of Feit and Thompson (1963) on the solvability of groups of odd order. So we assume that n is even. Assume that $n = 3^a 2^b m$ where $a \geqq 1$, $b \geqq 1$, *and* $(6, m) = \{1\}$. The exponent v of $2 \pmod 3$ is 2 so that $\mathscr{S}(3, 2) = \{1\}$. In particular, $\mathscr{E}(2) = \{1\}$ so that $b = 1$. Since n is 2 times an odd number, any group of order dividing n is solvable. We may now assume that n is a 3′-number. Suppose that G is a nonsolvable 3′-group. Thompson's classification of 3′-groups (Thompson (1964)) implies that G has a section isomorphic to a simple Suzuki group. But all Suzuki groups have order divisible by $2^6 \cdot 5$. The exponent of $2 \pmod 5$ is $v = 4$ so that $\mathscr{S}(5, 2) = \{1, 2, 3\}$. If we assume $|G| \mid n$ then $\mathscr{E}(2) \subseteq \mathscr{S}(5, 2) = \{1, 2, 3\}$. Thus $e(2) = 6 \not\in \mathscr{E}(2)$ and n is not a good number. From this, we conclude that any group of order dividing n, where n is good, must be solvable. This completes the proof of the theorem.

It may be possible to avoid the use of such powerful results in the proof of this theorem, but the result does not seem to warrant the effort.

https://doi.org/10.1017/S1446788700021042 Published online by Cambridge University Press

5. Good numbers: group sections

In this section we analyze what can happen on a section of a group whose order divides a good number.

Hypothesis 5.1.

(1) *$n > 1$ is a good integer.*

(2) *G is a group whose order divides n.*

(3) *V and W are q-chief factors of G for a prime q.*

(4) *$T = G/C_G(V)$.*

(5) *$\boldsymbol{F} = GF(q)$.*

Lemma 5.2. *If p is a prime, $p \mid |F(T)|$, $p \nmid q-1$, and P is a minimal normal p-subgroup of T then:*

(1) dim $V = d$, *d is odd, and $e(q) = 2d - 1$ where d is the exponent of q* $(\operatorname{mod} p)$;

(2) *P has order p and $V|_P$ is irreducible;*

(3) *$F(T)$ is cyclic, $F(T) = C_T(P)$, $T/F(T)$ is cyclic of order dividing $(d, p-1)$, and every prime dividing $[T: F(T)]$ divides $q(q-1)$;*

(4) *P acts fixed-point-freely on $V \otimes_{\boldsymbol{F}} V$; and*

(5) *if $P \not\leqq C_G(W)C_G(V)/C_G(V)$ then* dim $W \geqq d$.

Observe that $V|_P \simeq V_1 \oplus \cdots \oplus V_t$ where each V_i is a nontrivial irreducible $\boldsymbol{F}[P]$-module. Since $P/C_P(V_i)$ has order p, dim $V_i = d$ and dim $V = td$. Since $pq \mid n$, and since $e(q) \in \mathscr{E}(q) \subseteq \mathscr{S}(p, q)$, we must have dim $V \leqq e(q) \leqq d - 1$ if d is even or $\leqq 2d - 1$ if d is odd. We conclude that $t = 1$, dim $V = d$, d is odd, and $e(q) = 2d - 1$ proving (1). Since $V|_P \simeq V_1$, it is a faithful irreducible $F[P]$-module proving (2).

Note that $C_T(P) \geqq F(T)$. Now $V|_P$ is irreducible and $\boldsymbol{F}$ is a finite field so that Schur's Lemma and Wedderburn's theorem on finite division algebras imply that

$$\hat{\boldsymbol{F}} = \operatorname{Hom}_{F[P]}(V, V)$$

is a finite extension field of $\boldsymbol{F}$. Since P generates $\hat{\boldsymbol{F}}$ over $\boldsymbol{F}$, $\boldsymbol{F} = GF(q^d)$. Clearly $C_T(P)$ is in the multiplicative group $\hat{\boldsymbol{F}}^\times$ of $\boldsymbol{F}$ so that $C_T(P)$, being a finite group in the multiplicative group of a field, is cyclic. Since $C_T(P)$ is normal in T and contains $F(T)$, we conclude that $F(T) = C_T(P)$ and that $F(T)$ is self-centralizing in T. By [Passman (1968), Proposition 19.8] $T/F(T)$ acts upon $F(T)$ as a subgroup of $\operatorname{Aut}(\hat{\boldsymbol{F}})$ (which has order d and is cyclic). Since P generates $\hat{\boldsymbol{F}}$ over $\boldsymbol{F}$, we conclude that $\operatorname{Aut}(\hat{\boldsymbol{F}})$ acts faithfully on P proving that d divides $p - 1$. Suppose that r is a prime dividing $[T: F(T)]$ but not $q(q-1)$. Let R be a Sylow r-subgroup of T and $\bar{V}$ be a nontrivial irreducible $F[R]$-composition factor of V. With $V_0 = \bar{V}$, $T_0 = R/C_R(V_0)$, and

https://doi.org/10.1017/S1446788700021042 Published online by Cambridge University Press

$p_0 = r$ we may apply (1) of the lemma concluding that $e(q) = 2u - 1$ whence u is odd and u is the exponent of $q \pmod r$. Since $e(q) = 2d - 1$, $u = d$. This cannot be since r divides d and u divides $r - 1$. Therefore, r divides $q(q-1)$ completing the proof of (3).

The following lemma will be useful in proving (4).

LEMMA 5.3. *Assume hypothesis* (5.1). *Let P be a minimal normal p-subgroup of T and $\tilde{F}$ a finite splitting field for $V|_P$ over F. Set $\tilde{V} = V \otimes_F \tilde{F}$ and suppose that $\tilde{V}|_P \simeq \tilde{V}_1 \oplus \cdots \oplus \tilde{V}_t$ where $\tilde{V}_i$ are homogeneous components. If* $\dim V$ *is odd and $p > 2$ then P acts fixed-point-freely on $V \otimes_F V$.*

There are homomorphisms λ_i of P into the pth roots of unity of $\tilde{F}^x$, the multiplicative group of $\tilde{F}$, such that if $v \in \tilde{V}_i$ and $x \in P$ then $xv = \lambda_i(x)v$. Suppose that $\lambda_i\lambda_j = 1$ for some $i, j = 1, \cdots, t$. Since $p > 2$, $i \neq j$. Note that $\lambda_i = \lambda_j^{-1}$. Let $V|_P \simeq W_1 \oplus \cdots \oplus W_l$ where the W_i are homogeneous components. Since $\tilde{V} = V \otimes_F \tilde{F}$, we may assume that $W_1 \otimes \tilde{F} \simeq \tilde{V}_1 \oplus \cdots \oplus \tilde{V}_m$ so that $t = lm$. We may even choose our numbering so that $i = 1$. Fix an index $1 \leqq k \leqq t$. For some $x \in T$, $x\tilde{V}_k$ lies in $W_1 \otimes \tilde{F}$ since T is transitive on the W's. But then there is a $\sigma \in \operatorname{Aut}(\tilde{F})$ such that $\sigma(x\tilde{V}_k) = \tilde{V}_1$ since $\operatorname{Aut}(\tilde{F})$ is transitive on $\tilde{V}_1, \cdots, \tilde{V}_m$. In other words, $\lambda_k^{x^{-1}\sigma^{-1}} = \lambda_1$ so that $\lambda_k^{-1} = \lambda_j^{\sigma x} = \lambda_{j'}$ for some j'. Since each λ_k has an inverse $\lambda_{j'}$, and since $\lambda_k \neq \lambda_k^{-1}$, there must be an even number of λ_k's. Since $\dim V = t \dim \tilde{V}_1$ is odd, t is odd. We conclude that $\lambda_i\lambda_j \neq 1$ for any $i, j = 1, \cdots, t$.

If i, j are fixed then there is an $x \in P$ such that $\lambda_i(x)\lambda_j(x) \neq 1$. But x acts upon $\tilde{V}_i \otimes_{\tilde{F}} \tilde{V}_j$ as $\lambda_i(x)\lambda_j(x)$ so that P acts fixed-point-freely on $\tilde{V}_i \otimes_F \tilde{V}_j$. Consequently, P acts fixed-point-freely on $\tilde{V} \otimes_{\tilde{F}} \tilde{V}$ since it is a sum of $\tilde{V}_i \otimes_{\tilde{F}} \tilde{V}_j$'s. If w is a fixed vector of P on $V \otimes_F V$ then since $(V \otimes_F V) \otimes_F \tilde{F} \simeq \tilde{V} \otimes_{\tilde{F}} \tilde{V}$ as $\tilde{F}[P]$-modules, $w \otimes 1$ gives rise to a fixed vector of P on $\tilde{V} \otimes_{\tilde{F}} \tilde{V}$ so that $w = 0$ proving Lemma (5.3).

Since d is odd and $p > 2$, part (4) of Lemma (5.2) follows immediately from the preceding lemma.

If U is any nontrivial irreducible $F[P_0]$-module where P_0 is of order p then $\dim U = d$. Since $P \not\leqq C_G(W)C_G(V)/C_G(V)$, $G/C_G(W)$ contains a subgroup P_0 of order p. Thus W contains a nontrivial irreducible module U as above. Therefore, $\dim W \geqq \dim U = d$ proving (5) and Lemma (5.2).

LEMMA 5.4. *Assume that if p is a prime and $p \mid |F(T)|$ then $p \mid q - 1$. If $2r \mid (q - 1, n)$ for an odd prime r then* $\dim V = 1$. *In particular, if* $\dim V > 1$ *then n is odd.*

If $2r \mid (q-1, n)$ then $e(q) \in \mathscr{E}(q) \subseteq \mathscr{S}(2, r, q) = \{1\}$ so that $e(q) = 1 \geqq \dim V$. Assume that n is even and $\dim V > 1$. Since any prime p dividing $|F(T)|$, of necessity, divides $q - 1$, q must be an odd prime. Since n is even,

https://doi.org/10.1017/S1446788700021042 Published online by Cambridge University Press

$2|(q-1,n)$ so that $\dim V>1$ implies that no odd prime $r|(q-1,n)$. We conclude that $F(T)$ is a 2-group because all prime factors of $|F(T)|$ divide $q-1$. If $8|n$ or $4|n$ (where $q\equiv 3 \pmod 4$) then $\mathcal{S}(8,q)=\mathcal{S}(4,q)=\{1\}$ implies that $e(q)=1\geqq \dim V$. If $F(T)$ is a cyclic 2-group then $\operatorname{Aut}(F(T))$ is a 2-group so that $T=F(T)$. Since T can only have order 2 or 4 (where $q\equiv 1 \pmod 4$), if T is cyclic, then $\dim V=1$. We now know that $F(T)$ must be a Klein 4-group and $e(2)=2$. Now $T/F(T)$ has odd order (since $8\nmid n$) and acts faithfully on $F(T)$ so that $[T\colon F(T)]=3$. From this it follows that $\dim V=3$. If $3|q-1$ then $e(q)\in\mathcal{S}(2,3,q)=\{1\}$. We conclude that the exponent of $q \pmod 3$ is 2. Therefore, $\dim V\leqq e(q)\in\mathscr{E}(q)\subseteq\mathcal{S}(3,q)=\{1\}$. This final contradiction proves that if $\dim V>1$ then n is odd. The proof of the lemma is finished.

LEMMA 5.5. *Assume that n is odd, every minimal normal subgroup of T is central, and if $p\,||F(T)|$ for a prime p then $p|q-1$. If* $\dim V>1$ *then there is a minimal normal p-subgroup P of T for a prime p such that*:

(1) $\dim V=p$ *and* $e(q)=2p-1$;

(2) *T is nilpotent and $T=Z(T)O_p(T)$*;

(3) *P acts fixed point freely on $V\otimes_F V$; and*

(4) *if $P\not\leqq C_G(W)C_G(V)/C_G(V)$ then* $\dim W\geqq p$.

If $F(T)$ acts via scalar multiplication on V then $F(T)\leqq Z(T)$ so that $T=F(T)$ and $\dim V=1$. Therefore, for some $p\,||F(T)|$, $P_0=O_p(T)$ does not act via scalar multiplication on V. If P_0 is nonabelian, choose P_1 minimal such that P_1 is normal in T and P_1 is nonabelian. If P_0 is abelian then choose P_1 minimal such that P_1 is normal in T and P_1 does not act via scalar multiplication on V. Restricting V to P_1 we obtain

$$V|_{P_1}\simeq V_1\oplus\cdots\oplus V_t$$

where the V_i are homogeneous components. Now V_1 is isomorphic to a multiple of a single irreducible $\boldsymbol{F}[P_1]$-module U.

Assume that $\dim U>1$. Since $p|q-1$, p divides $\dim U$ and therefore, also, $\dim V$. In any case, $|P_1|\geqq p^3$ or $[P_1\colon C_{P_1}(U)]=p^2$ and $p^2\nmid q-1$. Therefore, $\mathscr{E}(q)\subseteq\{1,\cdots,p-1,2p-1\}$. Since $p\,|\dim V$ and $\dim V\leqq e(q)$ we have $t=1$, $U=V$, $\dim V=p$, and $e(q)=2p-1$.

Assume that $\dim U=1$ so that $\boldsymbol{F}$ is a splitting field for P_1 and P_0 is abelian. Since P_1 does not act via scalar multiplication on V, P_1 is not in $Z(T)$, and thus, $C_1=C_T(P_1)\neq T$. Since P_0 is abelian, $C_1\geqq F(T)$. This observation will allow us to eventually show that the case $\dim U=1$ does not occur at all. Let $C_2=C_T(P_1/P_2)$ where $P_2=P_1\cap Z(T)$. The minimal choice of P_1 assures us that P_1/P_2 is a chief factor of T and that P_2 acts via scalar multiplication on V. Assume that $C_1=C_2$ so that $C_2\neq T$. Choose $\bar{M}$, a minimal normal subgroup of T/C_2. Now $\bar{M}$ operates fixed-point-freely on P_1/P_2; $\bar{M}$ central-

https://doi.org/10.1017/S1446788700021042 Published online by Cambridge University Press

izes P_2; and P_1 is abelian so that $P_1 = P_2 \times [P_1, \bar{M}]$ is a T-decomposition of P_1. Therefore, $[P_1, \bar{M}] \simeq P_1/P_2$ is a minimal normal noncentral subgroup of T. We must have $C_1 < C_2$. Now C_2/C_1 acts upon P_1 and stabilizes the chain $1 < P_2 < P_1$ so that C_2/C_1 is a nontrivial p-group (Gorenstein (1968) (5.3.1)). Note now that $[C_2: C_1] \geqq p$, $|P_2| \geqq p$, and $[P_1: P_2] \geqq p$ so that $p^3 | n$.

The group P_1 acts via scalar multiplication on V_1 so that $C_T(P_1)$ stabilizes V_1. Since $C_{P_1}(C_2)$ is normal in T and contains P_2, the minimality of P_1 implies that $C_{P_1}(C_2) = P_2$. We show now that the stabilizer in C_2 of V_1 is C_1. There is a homomorphism λ_1 of P_1 into $\boldsymbol{F}$ such that if $x \in P_1$ and $v \in V_1$ then $xv = \lambda_1(x)v$. Suppose that $y \in C_2 \backslash C_1$. Choose $x \in P_1$ so that $[x, y] = z \neq 1$. Note that since $z \in P_2 \leqq Z(T)$, $\lambda_1(z) \neq 1$. If $v \in V_1$ then $xyv = yx[x, y]v = \lambda_1(x)\lambda_1(z)yv \neq \lambda_1(x)yv$ so that yV_1 is not isomorphic to V_1 as an $\boldsymbol{F}[P_1]$-module. We conclude that the stabilizer in C_2 of V_1 is C_1. From this it follows that $[C_2: C_1]$ divides t, and hence p divides $\dim V$. Recall that $p^3 | n$ so that $p \leqq \dim V \leqq e(q) \in \mathscr{S}(p^3, q) = \{1, \cdots, p-1, 2p-1\}$ proving that $U = V_1$, $t = p$, $\dim V = p$, and $e(q) = 2p - 1$. We now may conclude that (1) holds.

Our argument shows that if $r \,|\, |F(T)|$ where $r \neq p$ is a prime then $O_r(T)$ acts via scalar multiplication on V since $\dim V \neq r$. In particular, $O_r(T) \leqq Z(T)$ so that $F(T) = Z(T)O_p(T)$.

Assume again that $\dim U = 1$ so that $\dim V_1 = 1$. The group C_1 stabilizes each V_i and acts via scalar multiplication on each V_i; therefore, C_1 is abelian, and $C_1 \leqq F(T)$. From the fact that $F(T) = Z(T)P_0$ and P_0 is abelian we have $C_1 = F(T)$. From our previous observations, C_2/C_1 is a p-group, and $F(T)/Z(T)$ is a p-group so that $C_2/Z(T)$ is a p-group. This implies that C_2 is nilpotent so that $C_1 = C_2 = F(T)$. Previously we showed that $C_2 > C_1$. This contradiction shows that the case $\dim U = 1$ does not occur. We now have (since $V|_{P_1}$ is irreducible) $V|_{P_0}$ irreducible of dimension p. In particular, P_0 contains a unique normal subgroup P of order p. If P_0 is abelian then it is cyclic. Now $Z(T)P_0 = F(T)$ and $Z(T) \cap P_0 \geqq P$. Therefore, if P_0 is abelian, $T/F(T)$ acts as automorphisms faithfully on P_0 and trivially on P. But then $T/F(T)$ is a p-group so that $T/Z(T)$ is a p-group. Consequently, $T = F(T)$ is nilpotent. In proving (2), we may assume that P_0 is nonabelian.

Note that $T \leqq GL(V) = GL(p, \boldsymbol{F})$ so that P_0 is a nonabelian subgroup of $\boldsymbol{Z}_{p^d} \sim \boldsymbol{Z}_p$ where p^d is the highest power of p dividing $q - 1$ (Weir (1955)). Therefore, $P_0/\Phi(P_0)$ is a 2-dimensional space over $\boldsymbol{K} = GF(p)$. Since $Z(T)P_0 = F(T)$, $T/F(T)$ acts faithfully on P_0 and, therefore, on $P_0/\Phi(P_0)$. We have now shown that $T/F(T)$ acts faithfully as an odd order solvable subgroup of $GL(2, p)$ with no normal p-subgroup. All such subgroups are cyclic of order dividing $p + 1$ or are isomorphic to subgroups of $\boldsymbol{Z}_{p-1} \times \boldsymbol{Z}_{p-1}$. Suppose first that $r \,|\, [T: F(T)]$ and $r \,|\, p + 1$. Then $e(p) \in \mathscr{S}(r, p) = \{1\}$ since p

https://doi.org/10.1017/S1446788700021042 Published online by Cambridge University Press

has order 2 (mod r). But P_0 is nonabelian so that $e(p) \geqq |P_0| \geqq p^3$. Such an r as this cannot exist. Suppose second that $r \mid p-1$. Since $p \mid q-1$, $r < p < q$. If q has order $d > 1$ (mod r) then $e(q) \in \mathcal{S}(r,q) \subseteq \{1, \cdots, d-1, 2d-1\}$. Now $d \mid r-1$ and $r \mid p-1$ so that $r \leqq (p-1)/2$ and $d \leqq (p-1)/2 - 1$. Thus $e(q) \leqq 2d - 1 \leqq p - 4 < 2p - 1 = e(q)$. This contradiction shows that $r \nmid p-1$. We now have shown that $T = F(T) = Z(T)O_p(T)$ proving (2).

Since $p > 2$ and $\dim V = p$ is odd, Lemma (5.3) implies (3).

Let W be as in (4). Then $P \cap (C_G(W)C/C) \neq \{1\}$ where $C = C_G(V)$. Choose P^* a minimal p-subgroup of G such that $P^*C/C = P_0$. Let $D = C_G(W)$ so that $P^* \cap D \leqq P^*C \cap DC = C$ since $(P^*C \cap DC)/C$ does not contain the unique minimal normal subgroup P of P_0. Therefore, P_0 is a homomorphic image of $\bar{P}^* = P^*D/D$. If P_0 is nonabelian then $\bar{P}^*$ is nonabelian. In this case, since W is a faithful $\bar{P}^*$-module, $\dim W \geqq p$. If P_0 is abelian, it is cyclic of some order p^a. Further, any faithful irreducible $\boldsymbol{F}[P_0]$-module has dimension p. Since P_0 is a homomorphic image of $\bar{P}^*$, $\bar{P}^*$ contains a cyclic subgroup $\bar{P}_0$ of order p^a. Now W contains a faithful irreducible $\boldsymbol{F}[\bar{P}_0]$-module of dimension p so that $\dim W \geqq p$. This completes the proof of (4) and the lemma.

Lemma 5.6. *Assume that n is odd, P is a noncentral minimal normal p-subgroup of T for a prime p, and if a prime s divides $|F(T)|$ then $s \mid q-1$. Then*:

(1) $\dim V > 1$;

(2) *there is a prime $r \mid [T: F(T)]$ such that* $\dim V = r$ *and* $e(q) = 2r - 1$;

(3) *$T/F(T)$ is an r-group and $r \mid q-1$*

(4) *P acts fixed-point-freely on $V \otimes_F V$; and*

(5) *if $P \not\leqq C_G(W)C_G(V)/C_G(V)$ then* $\dim W \geqq r$.

Since $p \mid q-1$, $\boldsymbol{F}$ contains a primitive pth root of unity so that $V|_P \simeq V_1 \oplus \cdots \oplus V_t$ where each V_i is a homogeneous component and $t > 1$. Further, each V_i is a sum of 1-dimensional irreducible $\boldsymbol{F}[P]$-modules. In particular, $\dim V \geqq t \neq 1$ proving (1).

Let $T_0 = T/C_T(P)$ and $\boldsymbol{F}_0 = GF(p)$ so that P is an irreducible $\boldsymbol{F}_0[T_0]$-module. Since P is not central in T, $T_0 \neq \{1\}$. Let R_0 be a minimal normal r-subgroup of T_0 for some prime r. Let R be an r-subgroup of T chosen minimal such that $RC_T(P)/C_T(P) = R_0$. Notice that $U \to x \otimes_{\boldsymbol{F}[P]} U$ determines an action of T on the 1-dimensional $\boldsymbol{F}[P]$-modules contragredient to the action (given by conjugation) of T upon P. Since R acts fixed-point-freely on P, every nontrivial R-orbit on P has length divisible by r. Since the modules V_i, $i = 1, \cdots, t$ form a union of nontrivial R-orbits, contragredience implies that r divides t. That is, since all V_i have the same dimension, $r \mid \dim V$.

https://doi.org/10.1017/S1446788700021042 Published online by Cambridge University Press

Suppose that $r \neq q$ and that d is the exponent of q (mod r). If $d > 1$ then $e(q) \in \mathcal{S}(r, q) \subseteq \{1, \cdots, d-1, 2d-1\}$. Some element of T will act nontrivially upon V with order r so that $d \leqq \dim V \leqq e(q)$. These inequalities require that $e(q) = 2d - 1$ and d be odd. Since d is odd and divides $r - 1$, $\dim V \leqq e(q) = 2d - 1 \leqq 2(r-1)/2 - 1 < r$. This contradicts the fact that $r \mid \dim V$. We have shown that if $r \neq q$ then $r \mid q - 1$.

Change d now to the exponent of p (mod r). Every irreducible $F_0[R_0]$-module in P represents R_0 as a group of order r and, therefore, has dimension d. In particular, $|P| \geqq p^d$ so that $rp^d \mid n$. We next establish that $r \neq q$ so that $rp \mid q - 1$ since $r \neq p$. If $d = 1$ then $r \mid p - 1$ so that $r < p < q$. Assume that $r = q$ so that $d > 1$. Applying Lemma (5.2) with T_0, R_0, P in place of T, P, V we conclude that $|P| = p^d$, d is odd, and $e(p) = 2d - 1$. Since $d > 1$ is odd, $p^3 \mid n$. Thus $e(q) \in \mathcal{S}(p^3, q) = \{1, \cdots, p-1, 2p-1\}$. We now have $q = r \leqq \dim V \leqq e(q) \leqq 2p - 1$. Since p and q are odd, and since $p \mid q - 1$ we have $p \leqq (q-1)/2$ so that $q = r \leqq 2p - 1 \leqq q - 2$. We have established that $r \neq q$.

Since $rp^d \mid n$, d is odd, and $rp \mid q - 1$, $e(q) \in \mathcal{S}(r, p^d, q) = \{1, \cdots, r-1, 2r-1\}$. But now $r \leqq \dim V \leqq e(q)$ so that $r = \dim V$ and $e(q) = 2r - 1$. We have completed the proof of (2).

From the facts that $r \mid t$ and $\dim V = r$ we conclude that $\dim V_i = 1$. In particular, $C_T(P)$ acts via scalar multiplication on each V_i and is, therefore, an abelian group. Since $C_T(P) \geqq F(T)$, $F(T) = C_T(P)$. We show next that T has Fitting length 2, or equivalently, T_0 is nilpotent.

Suppose that $T_0/F(T_0)$ contains a nontrivial minimal normal s-subgroup for a prime s. Each orbit of T_0 upon the nonidentity elements of P is faithful. Clearly $F(T)$ stabilizes each V_i so that T acts as a permutation group on the V_i with kernel $F(T)$. In other words, T_0 has a faithful permutation representation of degree $r = \dim V$. Thus $s \mid r!$ and $s \leqq r$. Let R_1 be a Sylow r-subgroup of S', the symmetric group on r-letters. Viewing T_0 as a subgroup of S', we may consider R_1 to be R_0. Since $T_0 \leqq N_{S'}(R_1)$, and since $[N_{S'}(R_1): R_1] = r - 1$, $s \mid r - 1$. Now $s < r < q$, and $s \mid r - 1$ so that if $sr \mid q - 1$ then $e(q) \in \mathcal{S}(s, r, q) = \{1, \cdots, s-1, 2s-1\}$. But $2r - 1 = e(q) \leqq 2s - 1 < 2r - 1$ proving that $s \nmid q - 1$. Let u be the exponent of q (mod s). Then $u \mid s - 1$ so that $u < r$. At this point we know that $e(q) \in \mathcal{S}(s, q) \subseteq \{1, \cdots, u-1, 2u-1\}$ so that $2r - 1 = e(q) \leqq 2u - 1 < 2r - 1$. Therefore, T_0 is nilpotent. Now r could have been any prime divisor of T_0 so that $\dim V = r$ implies that T_0 is an r-group. Since $r \mid q - 1$, (3) holds.

Since $r = \dim V$ and p are odd, lemma (5.3) implies (4).

Note that P is a noncentral chief factor of G and that $T/C_T(P)$ is an r-group where $r \mid q - 1$. Since $P \nleqq C_G(W)C_G(V)/C_G(V)$, P is isomorphic to a chief factor of $T_1 = G/C_G(W)$. In particular, the nilpotent length of T_1 is bounded below by 2. We now view T_1, W in place of T, V. Suppose that Lemma (5.2) applies to W for a prime s. Let d be the order of $q \pmod{s}$ so that $\dim W = d$. By (5.2) (3) T_1 has nilpotent length 2 and $r \mid [T_1 \colon F(T_1)]$. Thus $r \mid d$. We now have $\dim W = d \geqq r = \dim V$. Since T_1 is not nilpotent, Lemma (5.5) does not apply to W. Assume that Lemma (5.2) does not apply to W. By Lemma (5.4) n is odd, and by our remarks above, Lemma (5.6), the present one, describes the situation on W. By (3) and our preceding discussion, $T_1/F(T_1)$ is an r-group for the prime r we have always been considering, and by (2), $\dim W = r = \dim V$. We conclude that (5) and the lemma hold.

6. Minimal normal subgroups

HYPOTHESIS 6.1.

(1) *G is a solvable group.*

(2) *P is a p-subgroup of G for a prime p.*

(3) *H is a normal q-subgroup of G for a prime $q \neq p$.*

(4) *If K is a proper subgroup of H normal in G then $[K, P] = 1$.*

(5) *There is a G-chief factor $V = H/H_0$ such that if $\boldsymbol{F} = GF(q)$ then P acts fixed point freely on $V \otimes_{\boldsymbol{F}} V$.*

(6) *$PC_G(H/H_0)$ is normal in G.*

(7) *P centralizes every G-chief factor of $C_G(H/H_0)/H$ whose order is a power of q.*

(8) *P normalizes a Sylow q-subgroup of $C_G(H)$.*

THEOREM 6.2. *If* Hypothesis (6.1) *holds then*

(1) *H is a minimal normal subgroup of G;*

(2) *there is a subgroup G_0 of G such that $G_0H = G$ and $G_0 \cap H = \{1\}$.*

We prove this theorem via a sequence of lemmas.

LEMMA 6.3. *H_0 is the unique maximal G-invariant subgroup of H.*

Suppose that H_1 and H_2 are distinct maximal G-invariant subgroups of H. Then $H_1H_2 = H$. But $\{1\} \neq [H, P] = [H_1H_2, P] \leqq [H_1, P][H_2, P] = \{1\}$.

LEMMA 6.4. *$H_0 \leqq Z(H)$.*

Now $[H_0, P] = \{1\}$ so that $P \times H_0$ acts upon H. By the $p \times q$ lemma [Gorenstein (1968), (5.3.4)] P acts nontrivially upon $C_H(H_0)$ so that $H = C_H(H_0)$, proving the lemma.

LEMMA 6.5. *H is elementary abelian.*

Let $H' = W$ and suppose that $H' \neq \{1\}$. The commutator mapping of H induces a bracket on $L = V \oplus W$ such that L is a Lie ring [Gorenstein (1968), Section 5.6]. The bracket is an $\boldsymbol{F}[G]$-bilinear mapping of $V \times V$ onto W and, as such, induces an $\boldsymbol{F}[G]$-homomorphism of $V \otimes_{\boldsymbol{F}} V$ onto W. Since $W \neq (0)$,

https://doi.org/10.1017/S1446788700021042 Published online by Cambridge University Press

P is nontrivial on W. But H' is a normal subgroup of G proper in H and centralized by P. We conclude that H is abelian.

The mapping $\varphi(x) = x^q$ is a G-homomorphism of H onto $H^q = \langle x^q \mid x \in H \rangle$. Since $H^q \neq H$ we have $H^q \leqq H_0$. Therefore, $[H, P] \leqq \ker \varphi$. But $\ker \varphi$ is G-invariant so that $H = \ker \varphi$ proving that H has exponent q.

Lemma 6.6. *H is a minimal normal subgroup of G.*

Write H additively and view it as an $\boldsymbol{F}[G]$-module. Then H is indecomposable, and H_0 is the unique maximal $\boldsymbol{F}[G]$-submodule. Let $C_1 = C_G(H)$, $\bar{G} = G/C_1$, $\bar{P} = PC_1/C_1$, and $\bar{C} = C_G(H/H_0)/C_1$. We prove that $\bar{C} = \{1\}$.

Suppose that $\bar{Q} = O_q(\bar{C}) \neq \{1\}$ and $\bar{Q} = \bar{Q}_1 > \bar{Q}_2 > \cdots > \bar{Q}_{t+1} = \{1\}$ is a G-chief series for $\bar{Q}$. By (7), $[\bar{Q}_i, \bar{P}] \leqq \bar{Q}_{i+1}$ for $i = 1, 2, \cdots, t$. Thus [Gorenstein (1968), (5.3.1)] $\bar{P}$ centralizes $\bar{Q}$. Now $H = [H, \bar{P}] \oplus C_H(\bar{P})$ is a $\bar{Q}$ decomposition of H. Since, by (5), $\bar{P}$ is fixed point free on H/H_0 and centralizes H_0, $H_0 = C_H(\bar{P})$. But $H/H_0 \simeq [H, \bar{P}]$ as a $\bar{Q}$-module and H/H_0 is a G-chief factor so that $[H, \bar{P}] \leqq C_H(\bar{Q})$. Since $C_H(\bar{Q})$ is a G-submodule on which P is nontrivial, $C_H(\bar{Q}) = H$ proving that $\bar{Q} = \{1\}$.

Suppose that $\bar{M} = O_{q'}(\bar{C}) \neq \{1\}$. Then $H = [H, \bar{M}] \oplus C_H(\bar{M})$ is an $\boldsymbol{F}[G]$-decomposition of H. Now $C_H(\bar{M})H_0 = H$ since $\bar{M}$ is a q'-group. Since H is indecomposable, $H = C_H(\bar{M})$ proving that $\bar{M} = \{1\}$. Since $\bar{C}$ is solvable and $O_q(\bar{C}) = O_{q'}(\bar{C}) = \{1\}$ we conclude that $\bar{C} = \{1\}$.

Now $\bar{P}$ is normal in $\bar{G}$ so that $H = [H, \bar{P}] \oplus C_H(\bar{P})$ is a $\bar{G}$-decomposition. Since $[H, \bar{P}] \neq (0)$ and since H is indecomposable, we conclude that $H_0 = C_H(\bar{P}) = \{1\}$. Since H is a chief factor of G, H is minimal normal in G.

Lemma 6.7. *There is a subgroup G_0 of G such that $G_0H = G$ and $G_0 \cap H = \{1\}$.*

A theorem of Gaschütz [see Huppert (1967), (I, 17.4)] tells us that if $D \geqq H$ is a subgroup of G and every Sylow r-subgroup of D splits over H then D splits over H. Since H is a q-group, any Sylow r-subgroup of D obviously splits over H if $r \neq q$.

We argue that $C_G(H) = A \times H$ for some subgroup A of $C_G(H)$. Let Q_1 be a Sylow q-subgroup of $C_G(H)$ normalized by P. Let $C_G(H) = C_1 > \cdots > C_t = H > C_{t+1} = \{1\}$ be a G-chief series of $C_G(H)$. Suppose that i is maximal such that $Q_1 \cap C_i \geqq [Q_1, P]$ so that $Q_1 \cap C_{i+1} \ngeqq [H, P]$. Notice that $Q_1 \cap C_i \neq Q_1 \cap C_{i+1}$ so that C_i/C_{i+1} is a q-chief factor. Suppose that $i < t$. Then $[Q_1, P] = [Q_1, P, P] \leqq [Q_1 \cap C_i, P] \leqq Q_1 \cap [C_i, P] \leqq Q_1 \cap C_{i+1}$ since P centralizes C_i/C_{i+1}. We must therefore have $i = t$ and $[Q_1, P] = H$. Now $Q_1 = C_{Q_1}(P) \cdot H$ where $C_{Q_1}(P) \cap H = \{1\}$. Set $Q_2 = C_{Q_1}(P)$. By the Theorem of Gaschütz, there is a complement $A \geqq Q_2$:

$$C_G(H) = AH$$

where $A \cap H = \{1\}$. But H is central so that $C_G(H) = A \times H$.

Let $M/C_G(H)' = O_{q'}(C_G(H)/C_G(H)')$ so that M is a normal subgroup of G. Since $C_G(H)' \leqq A$, $M \leqq A$ and $C_G(H)/M = A/M \times HM/M$ is a abelian q-group. Now $Q_2M = A$ $(Q_2 = C_{Q_1}(P))$ so that $A/M = C_{C/M}(\bar{P})$ where $C = C_G(H)$ and $\bar{P} = PC/C$. Since $\bar{P}$ is normal in $\bar{G} = G/C$, A/M is $\bar{G}$-invariant. Now set $\tilde{G} = G/A$, $\tilde{H} = HA/A$, and $\tilde{P} = PA/A$. It is straightforward to verify that $\tilde{H} = O_q(\tilde{G})$ is the unique minimal normal subgroup of $\tilde{G}$. In other words, $\tilde{G} = \tilde{B}\tilde{H}$ where $\tilde{B} \cap \tilde{H} = \{1\}$. Let B be the inverse image in G of $\tilde{B}$ so that $B \geqq A$, $BH = G$, and $B \cap H \leqq H \cap A = \{1\}$. Therefore, G splits over H completing the proof of the theorem.

7. Good numbers: *CLT* groups

In this section we prove the following theorems.

THEOREM 7.1. *If $n > 1$ is a good number and G is a group of order dividing n then G is solvable and has Fitting height at most* 3.

THEOREM 7.2. *If $n > 1$ is a good number and G is a group of order n then G is a CLT group.*

First we prove the following.

LEMMA 7.3. *Suppose that G is a solvable group and that every G-chief factor of $F(G)$ is cyclic. Then G is supersolvable.*

Let $\mathcal{T}$ be the set of G-chief factors of $F(G)$. Let T be the direct product of the groups $G/C_G(V)$ as V ranges over $\mathcal{T}$. If $x \in G$ then the mapping that sends x to the components $xC_G(V)$, $V \in \mathcal{T}$, in T is a homomorphism of G into T with kernel $N = \cap\, C_G(V)$, $V \in \mathcal{T}$. Since $V \in \mathcal{T}$ is cyclic, $G/C_G(V)$ is abelian. We conclude that G/N is abelian, that is, G-chief factors of G/N are cyclic. The G-chief factors of N are all central so that N is nilpotent. Since $N \leqq F(G)$, the G-chief factors of N are cyclic. We conclude that the chief factors of G are cyclic and G is supersolvable.

To prove Theorem (7.1) we apply Theorem (4.1) and note that $F(G)$ has a G-chief factor V such that $T = G/C_G(V)$ has Fitting height one less than the Fitting height of G (Berger (1973b), (1.1) (Use S_1/S_1^*)). Since T, V satisfy the hypotheses (5.1), either V is cyclic, in which case T is abelian, or T has Fitting height at most 2 by Lemmas (5.2), (5.5) and (5.6). We conclude that G has Fitting height at most 3. The proof of Theorem (7.1) is complete.

EXAMPLE 7.4. In (1.2) we showed that $n = 3 \cdot 13 \cdot 79^5$ is a good number. Let $\boldsymbol{K} = GF(79)$ and H be the group with minimal normal elementary abelian noncentral Sylow 13-subgroup and Hall 13′-subgroup of order 3. Thus H is nonabelian of order $3 \cdot 13$. Let V be a faithful irreducible $\boldsymbol{K}[H]$-module so that V has order 79^3. Form the semidirect product $K = H \cdot V$. Let L be of order 79^2 and set

$$G = K \times L.$$

Now G has Fitting height 3 and order n. The bound of Theorem (7.1) is best possible. The Lemmas of Section 5 give ideas on constructing other examples of Fitting height 3. This example fits into the scheme described by Lemma (5.6).

Next we prove Theorem (7.2). By Theorem (4.1), any group of order n is solvable. Assume (7.2) is false and choose n minimal such that a counter-example exists. Let G be a counter-example of order n. Certainly G is solvable. If every G-chief factor of $F(G)$ is cyclic then by Lemma (7.3), G is supersolvable. By (1.3) G is a CLT-group. We conclude that $O_q(G)$ has a noncyclic G-chief factor for some prime q. Choose $H \leqq O_q(G)$ minimal such that H is normal in G and H has a noncyclic G-chief factor. Evidently, there is a subgroup H_0 of H which is normal in G for which H/H_0 is a noncyclic G-chief factor. Further, all G-chief factors of H_0 are cyclic. Set $V = H/H_0$ and $T = G/C_G(V)$. Hypothesis (5.1) now holds for G, T, V. In particular, there is a p-subgroup $\bar{P}$ of T for a prime p such that:

(a) $\bar{P}$ is a G-chief factor,

(b) $\bar{P}$ acts fixed-point-freely on $V \otimes_F V$ where $\boldsymbol{F} = GF(q)$;

(c) if W is a q-chief factor of G such that $\bar{P} \not\leqq C_G(W)C_G(V)/C_G(V)$ then $\dim W \geqq \dim V$; and

(d) $\dim V = d$ where $e(q) = 2d - 1$ and d is odd.

These conclusions follow from Lemmas (5.2), (5.4), (5.5), and (5.6). Recalling the definition of $\mathscr{E}(q)$, either $\mathscr{E}(q) = \{m \mid 1 \leqq m \leqq 2d - 1\}$ or $\mathscr{E}(q) = \{1, \cdots, d-1, 2d-1\}$. (Actually it is the latter case, but we ignored the necessary inclusion in Section 5 to prove this.)

Let M be the inverse image in G of $\bar{P}$. Set $C = C_G(V) = C_G(H/H_0)$ and let Q be a Sylow q-subgroup of C. By the Frattini argument $M = N_M(Q)C$. Since $[M: C]$ is a power of p, $M = P_0C$ for a Sylow p-subgroup P_0 of $N_M(Q)$. Choose $P \leqq P_0$ minimal such that $PC = M$. We now verify Hypothesis (6.1). Notice that (1), (2), (3) and (6) of (6.1) are more or less obvious. Since $Q \cap C_G(H)$ is a Sylow q-subgroup of $C_G(H)$ (which is in C and normal in G), it is normalized by P proving (8). Let W be a G-chief factor of either H_0 or C/H whose order is a power of q. By our choice of W, we know that $|W||V|$ divides n, that is, $e(q) \geqq \dim W + \dim V$. If P acts nontrivially on W, then by the minimal choice of P, $\bar{P} \not\leqq C_G(W)C/C$ so that $\dim W \geqq \dim V$ by (c)

https://doi.org/10.1017/S1446788700021042 Published online by Cambridge University Press

above. By (d) we obtain $e(q) = 2d - 1 \geqq \dim W + \dim V \geqq 2d$. This contradiction proves that P centralizes W verifying (7). If $H_0 > H_1 > \cdots > H_m = \{1\}$ is a G-chief series of H_0 then we also have shown that P stabilizes the chain of H_i's. We conclude that $[H_0, P] = 1$ (Gorenstein (1968) (5.3.1)). By the minimality of H, H_0 is the unique maximal G-invariant subgroup of H so that (4) holds. Finally (5) holds by (b) above.

Since Hypothesis (6.1) holds, by Theorem (6.2), H is a minimal normal subgroup of G and there is a subgroup G_0 of G such that $G_0H = G$ and $G_0 \cap H = \{1\}$.

Let $n' = n/q^d$, $\mathscr{E}'(q) = \mathscr{E}_{n'}(q)$, and $e'(q)$ be the e's for n'. then $e'(q) = d - 1$. By the definition of $\mathscr{E}(r)$ for a prime r, $\mathscr{E}(r) \subseteq \mathscr{E}'(r)$ for all primes r dividing either n or n'. Since $e(r) = e'(r)$ for $r \neq q$ and $e(q) = 2d - 1$, $e'(q) = d - 1$ we conclude that n' is a good number. The group G_0 has order n' so that Theorem (7.2) is valid for G_0.

Suppose that m is a divisor of n. We may write $m = m'q^s$ where $0 \leqq s \leqq 2d - 1$ and $(m', q) = 1$. If $s \leqq d - 1$ then m divides n'. Since G_0 is a CLT-group, G_0 (hence G) contains a subgroup of order m. If $s > d - 1$ then $s = d + d'$ where $0 \leqq d' \leqq d - 1$. Since $m'' = m'q^{d'}$ divides n', and since G_0 is a CLT-group, it contains a subgroup L of order m''. Since LH has order m, G contains a subgroup of order m. We conclude that G is a CLT-group. This contradiction completes the proof of Theorem (7.2).

Theorems (3.10) and (7.2) prove the main Theorem (1.1) of this paper. Using the results of Section 5, one should be able to give a fairly complete description of the structure of groups whose order is a CLT-number.

REFERENCES

T. R. Berger (1973a), 'Hall-Higman type theorems. IV', *Proc. Amer. Math. Soc.* **37**, 317–325.

Thomas R. Berger (1973b), 'Nilpotent fixed point free automorphism groups of solvable groups', *Math. Z.* **131**, 305–312.

T. R. Berger (1975), 'Hall-Higman type theorems. II', *Trans. Amer. Math. Soc.* **205**, 47–69.

Henry G. Bray (1968), 'A note on *CLT* groups', *Pacific J. Math.* **27**, 229–231.

W. E. Deskins (1968), 'A characterization of finite supersolvable groups', *Amer. Math. Monthly* **75**, 180–182.

Klaus Doerk (1966), 'Minimal nicht überauflösbare, endliche Gruppen', *Math. Z.* **91**, 198–205.

Walter Feit and John G. Thompson (1963), 'Solvability of groups of odd order', *Pacific J. Math.* **13**, 775–1029.

T. M. Gagen (to appear), 'A note on groups with the inverse Lagrange property', *Proc. Miniconf. Group Theory*, Canberra 1975 (Lecture Notes in Mathematics).

Daniel Gorenstein (1968), *Finite Groups* (Harper's Series in Modern Mathematics. Harper and Row, New York, Evanston, London, 1968).

B. Huppert (1967), *Endliche Gruppen I* (Die Grundlehren der mathematischen Wissenschaften, **134**. Springer-Verlag, Berlin, Heidelberg, New York, 1967).

Donald J. McCarthy (1971), 'A survey of partial converses to Lagrange's theorem on finite groups', *Trans. New York Acad. Sci.* (2) **33**, 586–594.

https://doi.org/10.1017/S1446788700021042 Published online by Cambridge University Press

D. H. McLain (1957), 'The existence of subgroups of given order in finite groups', *Proc. Cambridge Philos. Soc.* **53**, 278–285.

Oystein Ore (1939), 'Contributions to the theory of groups of finite order', *Duke Math. J.* **5**, 431–460.

Donald Passman (1968), *Permutation Groups* (Mathematics Lecture Note Series. Benjamin, New York, Amsterdam, 1968).

R. R. Struik (preprint), 'Partial converses to Lagrange's theorem'.

J. G. Thompson (1974), 'Simple 3'-groups', *Symposia Mathematica*, **8**, 517–530 (Convegno di Gruppi e loro Rappresentazioni, INDAM, Roma, 1972. Academic Press, London, 1974).

A. J. Weir (1955), 'Sylow p-subgroups of the classical groups over finite fields with characteristic prime to p', *Proc. Amer. Math. Soc.* **6**, 529–533.

David L. Winter (1972), 'The automorphism group of an extraspecial p-group', *Rocky Mountain J. Math.* **2**, 159–168.

Guido Zappa (1940), 'Remark on a recent paper of O. Ore', *Duke Math. J.* **6**, 511–512.

Department of Mathematics,
University of Minnesota,
Minneapolis, Minn.,
U.S.A.

https://doi.org/10.1017/S1446788700021042 Published online by Cambridge University Press