Permutation groups containing a regular abelian subgroup: the tangled history of two mistakes of Burnside

By Mark Wildon

(*Received*)

Abstract

A group K is said to be a B-group if every permutation group containing K as a regular subgroup is either imprimitive or 2-transitive. In the second edition of his influential textbook on finite groups, Burnside published a proof that cyclic groups of composite prime-power degree are B-groups. Ten years later in 1921 he published a proof that every abelian group of composite degree is a B-group. Both proofs are character-theoretic and both have serious flaws. Indeed, the second result is false. In this note we explain these flaws and prove that every cyclic group of composite order is a B-group, using only Burnside's character-theoretic methods. We also survey the related literature, prove some new results on B-groups of prime-power order, state two related open problems and present some new computational data.

1. *Introduction*

In 1911, writing in §252 of the second edition of his influential textbook [**6**], Burnside claimed a proof of the following theorem.

Theorem 1·1. *Let G be a transitive permutation group of composite prime-power degree containing a regular cyclic subgroup. Either G is imprimitive or G is 2-transitive.*

An error in the penultimate sentence of Burnside's proof was noted in [**7**, page 24], where Neumann remarks 'Nevertheless, the theorem is certainly true and can be proved by similar character-theoretic methods to those that Burnside employed'. In §3 we present the correct part of Burnside's proof in today's language. In §4 we prove Theorem 1·1 by the method proposed by Burnside, using the lemma on cyclotomic integers in §2 below to fix Burnside's error. In §5 we build on the correct part of Burnside's proof in a different way, obtaining an entirely character-theoretic proof of the following variation on Theorem 1·1.

Theorem 1·2. *Let G be a transitive permutation group of composite non-prime-power degree containing a regular cyclic subgroup. Either G is imprimitive or G is 2-transitive.*

In honour of Burnside, Wielandt [**37**, §25] defined a *B-group* to be a group K such that every permutation group containing K as a regular subgroup is either imprimitive or 2-transitive. Thus Theorems 1·1 and 1·2 imply that cyclic groups of composite order are B-groups.

The early attempts to prove this result by character-theoretic methods are rich with interest, but also ripe with errors. Our second aim, which occupies §6, is to untangle

this mess. We end in §7 with some new results on abelian B-groups which require the Classification Theorem of Finite Simple Groups. We state an open problem on when C_2^n is a B-group, present a partial solution, consider B-groups of prime-power order and make some further (much more minor) corrections to the literature.

At a late stage in this work, the author learned of [**25**], in which Knapp gives another way to fix Burnside's proof of Theorem 1·1, using essentially the same lemma as in §2. The key step in Knapp's proof is his Proposition 3.1. It uses two compatible actions of the Galois group of $\mathbf{Q}(\zeta) : \mathbf{Q}$, where ζ is a root of unity of order the degree of G: firstly on the set permuted by G, and secondly on the corresponding permutation module. The proof of Theorem 1·1 given here uses only the second action (in a simple way that is isolated in the second step), and is more elementary in several other respects. The inductive approach in our third step is also new. Given the historical importance of Theorem 1·1, the author believes it is worth putting this shorter proof on record. Theorem 1·2 is not proved in [**25**].

2. *Lemma on cyclotomic integers*

The following lemma is essentially the same as Lemma 4.1 in [**25**]. A proof is included for completeness. Recall that the degree of the extension of $\mathbf{Q}$ generated by a primitive d-th root of unity is $\phi(d)$, where ϕ is Euler's totient function.

LEMMA 2·1. *Let p be a prime and let $n \in \mathbf{N}$. For each r such that $1 \leq r < p^{n-1}$, let*

$$R(r) = \{r, r + p^{n-1}, \ldots, r + (p-1)p^{n-1}\}.$$

Let ζ be a primitive p^n-th root of unity and let $\omega = \zeta^{p^{n-1}}$. If $\sum_{i=0}^{p^n-1} a_i \zeta^i \in \mathbf{Q}[\omega]$ where $a_i \in \mathbf{Q}$ for each i, then the coefficients a_i are constant for i in each set $R(r)$.

Proof. By the Tower Law $[\mathbf{Q}(\zeta) : \mathbf{Q}(\omega)] = [\mathbf{Q}(\zeta) : \mathbf{Q}]/[\mathbf{Q}(\omega) : \mathbf{Q}] = \phi(p^n)/\phi(p) = (p-1)p^{n-1}/(p-1) = p^{n-1}$. Therefore $\Psi(X) = X^{p^{n-1}} - \omega$ is the minimal polynomial of ζ over $\mathbf{Q}(\omega)$. By hypothesis there exists $\gamma \in \mathbf{Q}[\omega]$ such that

$$f(X) = -\gamma + \sum_{0 \leq i < p^n} a_i X^i$$

has ζ as a root. Hence $f(X)$ is divisible in $\mathbf{Q}(\omega)[X]$ by $\Psi(X)$. There is a unique expression $f(X) = f_0(X) + \sum_{0<r<p^{n-1}} f_r(X)$ where

$$f_r(X) = \sum_{\substack{0 \leq i < p^n \\ i \equiv r \bmod p^{n-1}}} a_i X^i$$

for $0 < r < p^{n-1}$. The remainder when X^d is divided by $\Psi(X)$ has non-zero coefficients only for those X^c such that c is congruent to d modulo p^{n-1}. Therefore each $f_r(X)$ is divisible by $\Psi(X)$ and so $f_r(\zeta) = 0$ for each r. Since the coefficients of f_r for $0 < r < p^{n-1}$ are rational, it follows that each such f_r is divisible, *now in* $\mathbf{Q}[X]$, by the minimal polynomial of ζ over $\mathbf{Q}$, namely $\Phi_{p^n}(X) = 1 + X^{p^{n-1}} + \cdots + X^{(p-1)p^{n-1}}$. Since f_r has degree at most $p^n - 1$, this implies that $f_r(X) = b_r X^r \Phi_{p^n}(X)$ for some $b_r \in \mathbf{Q}$. The lemma follows. □

3. *Burnside's method: preliminary results*

We may suppose that G acts on $\{0, 1, \ldots, d-1\}$, where $d \in \mathbf{N}$ is composite, and that $g = (0, 1, \ldots, d-1)$ is a d-cycle in G. Let H be the point stabiliser of 0. Let

$M = \langle e_0, e_1 \ldots, e_{d-1}\rangle_{\mathbf{C}}$ be the natural permutation module for G. Let ζ be a primitive d-th root of unity and for $0 \le j < d$ let

$$v_j = \sum_{0\le i<d} \zeta^{-ij} e_i. \tag{3·1}$$

We use this notation throughout §§3–5.

Since $e_i g = e_{i+1}$, where subscripts are taken modulo d, we have $v_j g = \zeta^j v_j$ for each j. Note that $v_0 = \sum_{0\le i<d} e_i$ spans the (unique) trivial $\mathbf{C}G$-module of M. Let

$$M = \langle v_0\rangle \oplus V_1 \oplus \cdots \oplus V_t \tag{3·2}$$

be a direct sum decomposition of M into irreducible $\mathbf{C}G$-submodules. The v_j are eigenvectors of g with distinct eigenvalues. Therefore they form a basis of M. Moreover, since the eigenvalues are distinct, each of the summands $V_1, \ldots, V_t$ has a basis consisting of some of the v_j. Thus the decomposition in (3·2) is unique. For each summand V_k, let $B_k = \{j : 0 < j < p^n, v_j \in V_k\}$. Let ϕ_k be the character of V_k.

The following two lemmas are the key observations in Burnside's method.

LEMMA 3·1. *For each k such that $1 \le k \le t$, the vector $\sum_{j\in B_k} v_j$ spans the unique H-invariant submodule of V_k.*

Proof. The permutation character π of G is $1_G + \sum_{k=1}^{t} \phi_k$, where the summands are distinct and irreducible. By Frobenius reciprocity we have

$$1 = \langle \pi, \phi_k\rangle_G = \langle 1_H \big\uparrow^G, \phi_k\rangle_G = \langle 1_H, \phi_k\big\downarrow_H\rangle_H$$

for each k. Therefore each V_k has a unique 1-dimensional $\mathbf{C}H$-invariant submodule. Since $e_0 = \frac{1}{p^d}\sum_{0\le j<d} v_j$ is H-invariant, and the projection of e_0 into V_k is $\frac{1}{p^d}\sum_{j\in B_k} v_j$, this submodule is spanned by $\sum_{j\in B_k} v_j$. □

LEMMA 3·2. *If $\mathcal{O}$ is an orbit of H on $\{0, 1, \ldots, d-1\}$ and $1 \le k \le t$ then the sum $\sum_{i\in\mathcal{O}} \zeta^{ij}$ is constant for $j \in B_k$.*

Proof. Observe that $\sum_{i\in\mathcal{O}} e_i$ is H-invariant. An easy calculation (which may be replaced by the observation that the character table of C_d is an orthogonal matrix) shows that $e_i = \frac{1}{p^d}\sum_{0\le j<d} \zeta^{ij} v_j$ for each i. Therefore

$$\sum_{i\in\mathcal{O}} e_i = \sum_{0\le j<d} \Big(\sum_{i\in\mathcal{O}} \zeta^{ij}\Big) v_j.$$

The projection of the left-hand side into V_k is $\sum_{j\in B_k}\sum_{i\in\mathcal{O}} \zeta^{ij} v_j$. By Lemma 3·1 the coefficients are constant for $j \in B_k$. □

The following proposition is used in the final step of the proof of both main theorems.

PROPOSITION 3·3. *If there is a prime p dividing d and a summand V_k whose basis $\{v_j : j \in B_k\}$ contains only basis vectors v_j with j divisible by p then there exists a normal subgroup of G containing $g^{d/p}$ whose orbits form a non-trivial block system.*

Proof. Let N be the kernel of G acting on V_k. Since $v_j g = \zeta^j v_j$, N contains $g^{d/p}$. By Lemma 3·1, V_k has $\langle \sum_{j\in B_k} v_j\rangle$ as an HN-invariant subspace. Since V_k is not the trivial module, we have $HN < G$. Hence N is non-trivial but intransitive. The orbits of the normal subgroup N are blocks of imprimitivity for G. □

4. *Proof of Theorem* 1·1

We use the notation from §3.

First step

By hypothesis G has degree p^n where p is prime and $n \geq 2$. The Galois group $\mathrm{Gal}(\mathbf{Q}(\zeta) : \mathbf{Q})$ of the field extension $\mathbf{Q}(\zeta) : \mathbf{Q}$ permutes the basis vectors v_j while preserving the unique direct sum decomposition (3·2). Hence $\mathrm{Gal}(\mathbf{Q}(\zeta) : \mathbf{Q})$ permutes the sets $B_1, \dots, B_t$. By Proposition 3·3, we may assume that every B_k contains some j not divisible by p. Hence, given any m such that $0 < m < n$, there exists j not divisible by p such that the set B_k containing p^m also contains j. Let B_ℓ be the set containing 1. Since the Galois group is transitive on $\{\zeta^j : 0 < j < p^n, p \nmid j\}$, by conjugating ζ^j to ζ, we see that $p^m c \in B_\ell$ for some c not divisible by p.

Recall that H is the point stabiliser of 0. Let $\mathcal{P}$ be the partition of $\{1, \dots, p^n - 1\}$ into the orbits of H other than $\{0\}$. The previous paragraph and Lemma 3·2 imply that for all m such that $0 < m < n$ there exists $c_m \in \mathbf{N}$, not divisible by p, such that

$$\sum_{i \in \mathcal{O}} \zeta^i = \sum_{i \in \mathcal{O}} \zeta^{p^m c_m i} \tag{4·1}$$

for each $\mathcal{O} \in \mathcal{P}$.

Second step

We shall show by induction on n that (4·1) implies that $\mathcal{P}$ is the one-part partition. It then follows that H is transitive on $\{1, \dots, p^n - 1\}$ and so G is 2-transitive, as required.

Fix $\mathcal{O} \in \mathcal{P}$. Taking $m = n-1$ in (4·1) and applying Lemma 2·1 with $\omega = \zeta^{p^{n-1}c_{n-1}}$, we find that the coefficients in $\sum_{i \in \mathcal{O}} \zeta^i$ are constant on the sets $R(r) = \{r, r + p^{n-1}, \dots, r + (p-1)p^{n-1}\}$ for $0 < r < p^{n-1}$. Hence $\mathcal{O}$ is a union of some of these sets, together with some of $\{p^{n-1}\}$, …, $\{(p-1)p^{n-1}\}$. The contributions from $R(r)$ to (4·1) are

$$\sum_{i \in R(r)} \zeta^i = 0, \tag{4·2}$$

$$\sum_{i \in R(r)} \zeta^{p^m c_m i} = p\zeta^{p^m c_m r}. \tag{4·3}$$

Case $n = 2$.

Let $\omega = \zeta^{pc_1}$. Taking $m = 1$ in (4·1) and substituting the relations in (4·2) and (4·3) we get

$$\sum_{\substack{r \in \mathcal{O} \\ 0 < r < p}} 0 + \sum_{pi \in \mathcal{O}} \omega^i = \sum_{\substack{r \in \mathcal{O} \\ 0 < r < p}} p\omega^r + \sum_{\substack{pi \in \mathcal{O} \\ 0 < i < p}} 1.$$

This rearranges to

$$\big|\{\mathcal{O} \cap \{p, 2p, \dots, (p-1)p\}\big| + \sum_{0 < i < p} (p[i \in \mathcal{O}] - [pi \in \mathcal{O}])\omega^i = 0,$$

where the Iverson bracket $[P]$ is 1 if the statement P is true, and 0 if false. Since the minimal polynomial of ω, namely $1 + X + \cdots + X^{p-1}$, has degree $p - 1$ and constant coefficients, it follows that $\big|\{\mathcal{O} \cap \{p, \dots, (p-1)p\}\big| = p - 1$ and $i \in \mathcal{O}$ for each i such that $0 < i < p$. Thus $\mathcal{O} = \{1, \dots, p^2 - 1\}$ as required.

Inductive step

Let $n \geq 3$. Let $T = \{p^{n-1}, \ldots, (p-1)p^{n-1}\}$. Substituting (4·3) in the right-hand-side of (4·1) for first $m = 1$ and then a general m such that $0 < m < n$, we have

$$\sum_{\substack{r \in \mathcal{O} \\ 0<r<p^{n-1}}} p\zeta^{pc_1 r} + |\mathcal{O} \cap T| = \sum_{\substack{r \in \mathcal{O} \\ 0<r<p^{n-1}}} p\zeta^{p^m c_m r} + |\mathcal{O} \cap T|.$$

For each $\mathcal{O} \in \mathcal{P}$, define $\mathcal{O}_\star = \mathcal{O} \cap \{1, \ldots, p^{n-1} - 1\}$. Clearly $\{\mathcal{O}_\star : \mathcal{O} \in \mathcal{P}\}$ is a set partition of $\{1, \ldots, p^{n-1} - 1\}$. Let $\zeta_\star = \zeta^{pc_1}$ and, for each m such that $0 < m < n$, choose $d_m \in \mathbf{N}$ such that $c_1 d_m \equiv c_m \bmod p$. We may suppose that $d_1 = 1$. Replacing r with $i_\star$, the previous displayed equation implies

$$\sum_{i_\star \in \mathcal{O}_\star} \zeta_\star^i = \sum_{i_\star \in \mathcal{O}_\star} \zeta_\star^{p^{m-1} d_m i_\star}.$$

Comparing with (4·1), we see that all the conditions are met to apply the inductive hypothesis. Hence $\mathcal{O}_\star = \{1, \ldots, p^{n-1} - 1\}$ and so $\mathcal{O}$ contains $\{1, \ldots, p^n - 1\} \backslash T$. By (4·2) and (4·3) we have $\sum_{i \in \{1,\ldots,p^n-1\}\backslash T} \zeta^i = 0$ and

$$\sum_{\substack{0<i<p^{n-1} \\ i \notin T}} \zeta^{pc_1 i} = p \sum_{0<i<p^{n-1}} \zeta_\star^i = -p.$$

Substituting these two results in the case $m = 1$ of (4·1) we get

$$\sum_{p^{n-1} i \in \mathcal{O} \cap T} \zeta^{p^{n-1} i} = -p + |\mathcal{O} \cap T|.$$

It follows, as in the final step of the case $n = 2$, that $|\mathcal{O} \cap T| = p - 1$ and so $\mathcal{O} \supseteq T$ and $\mathcal{O} = \{1, \ldots, p^n - 1\}$, as required.

5. *Proof of Theorem* 1·2

We continue from the end of §3. Thus G acts on $\{0, 1, \ldots, d-1\}$ and has $\langle g \rangle \cong C_d$ as a regular cyclic subgroup. Let $\vartheta : \langle g \rangle \to \mathbf{C}$ be the faithful linear character of $\langle g \rangle$ defined by $\vartheta(g) = \zeta$, where as before ζ is a primitive d-th root of unity. For $1 \leq k \leq t$, let π_k be the character of V_k restricted to $\langle g \rangle$. Since $\langle v_j \rangle$ affords ϑ^j, we have $\pi_k = \sum_{j \in B_k} \vartheta^j$. Since the sets $B_1, \ldots, B_t$ are disjoint, the characters π_k are linearly independent. Moreover G acts on $\{\vartheta^j : 0 \leq j < d\}$ by $(\vartheta^j)^x = \vartheta^{jx}$ for $x \in G$, and by Lemma 3·1, the π_k span the H-invariant subspace of $\langle \vartheta^j : 0 \leq j < d \rangle_{\mathbf{C}}$. It follows from Exercise 3.5.5 in [**13**] that this subspace is closed under multiplication.

Let p be a prime dividing d. The character of $V_k^{\otimes p}$ is π_k^p. Since $(a+b)^p \equiv a^p + b^p \bmod p$ for all $a, b \in \mathbf{Z}$, we have

$$\pi_k^p = \sum_{0 \leq r < d/p} \big|\{j \in B_k : jp \equiv rp \bmod d\}\big| \vartheta_{rp} + p\pi \tag{5·1}$$

for some character π of $\langle g \rangle$. By the end of the previous paragraph, we may write $\pi_k^p - p\pi = a1_H + \sum_{\ell=1}^t a_\ell \pi_\ell$ where $a, a_1, \ldots, a_t \in \mathbf{Z}$. By the linear independence of the π_ℓ, it follows from (5·1) that if $a_\ell \neq 0$ then π_ℓ contains only characters of the form ϑ_{rp} with $1 \leq r < d/p$. Thus for any such ℓ, B_ℓ contains only basis vectors v_j with j divisible by p and, by Proposition 3·3, G is imprimitive. We may therefore assume that $\big|\{j \in B_k : jp \equiv rp \bmod d\}\big|$ is a multiple of p for each r such that $1 \leq r < d/p$. Identifying $\{0, 1, \ldots, d-1\}$

with $\mathbf{Z}/d\mathbf{Z}$, note that $jp \equiv rp \bmod d$ if and only if $j \in r + \langle d/p \rangle$. Therefore *for each prime p dividing d, each B_k is the union of a subset of $\langle d/p \rangle$ and some proper cosets $r + \langle d/p \rangle$.*

Let q be a prime dividing d other than p. Since the subgroups $\langle d/p \rangle$ and $\langle d/q \rangle$ of $\mathbf{Z}/d\mathbf{Z}$ meet in 0, each member of $\langle d/p \rangle \backslash \{0\}$ is in a proper coset of $\langle d/q \rangle$, and similarly with p and q swapped. By the conclusion of the previous paragraph, if B_k meets $\langle d/pq \rangle$ then B_k contains $\langle d/pq \rangle \backslash \{0\}$. At most one B_k has this property. If $t = 1$ then G is 2-transitive, so we may assume that $d > pq$ and there exists B_k not meeting $\langle d/pq \rangle$. For this B_k there exist $r_1, \ldots, r_s$ such that $0 < r_1 < \ldots < r_s < d/pq$ and

$$B_k = \bigcup_{e=1}^{s} (r_e + \langle d/pq \rangle).$$

Thus $|B_k| = spq$ and

$$\overline{\pi_k}\pi_k = s(\vartheta_0 + \vartheta_{d/pq} + \cdots + \vartheta_{(pq-1)d/pq}) + \psi \tag{5·2}$$

where the coefficient of ϑ_j in ψ is equal to the number of pairs (e, e') such that $j \in -r_e + r_{e'} + \langle d/pq \rangle$. There are exactly s such pairs if and only if for all e there exists a unique e' such that $r_e + j + \langle d/pq \rangle = r_{e'} + \langle d/pq \rangle$, or, equivalently, if and only if $B_k + j = B_k$, where the addition is performed in $\mathbf{Z}/d\mathbf{Z}$. Let

$$J = \{j \in \mathbf{Z}/d\mathbf{Z} : B_k + j = B_k\}.$$

Since J is a subgroup of $\mathbf{Z}/d\mathbf{Z}$ containing d/pq we have $J = \langle m \rangle$ for some m dividing d/pq. Since $0 \notin B_k$, and so $-r_1, \ldots, -r_s \notin J$, we have $m > 1$. Thus (5·2) may be rewritten as

$$\overline{\pi}_k\pi_k = s\big(\vartheta_0 + \vartheta_m + \cdots + \vartheta_{n-m}\big) + \phi$$

where $\langle \phi, \vartheta_j \rangle < s$ for all j not divisible by m. By the linear independence of $\pi_1, \ldots, \pi_t$, there exists π_k such that if $\langle \pi_k, \vartheta_j \rangle > 0$ then j is a multiple of m. The result now follows from Proposition 3·3.

6. *A historical survey of Burnside's method and B-groups*

6·1. *Burnside's work for prime-power degree*

We begin in 1901 with [**3**, §7], in which Burnside used character-theoretic arguments to prove the following important dichotomy. (All of the papers of Burnside discussed below appear in Volume II of his collected works [**8**].)

THEOREM 6·1 (Burnside 1901 [**3**, §7]). *A permutation group of prime degree p is either 2-transitive or contains a normal subgroup of order p.*

In the following §8 Burnside proves Theorem 1·1 for permutation groups of odd degree p^2 using character theory. He comments 'It appears highly probable that this result may be extended to any group of odd order which contains a regular substitution of order equal to the degree of the group; but I have not yet succeeded in proving this.'

In the revised second edition of his textbook [**6**], Burnside added five entirely new chapters on linear groups and characters. Most notably these include the well-known character-theoretic proof of the $p^a q^b$-Theorem. In §251 he used the method of cyclotomic sums and basis sets, introduced in his 1906 paper [**4**, §7] but presented in his textbook

with some simplifications, to prove Theorem 6·1. The following §252, whose correct part was presented in §3, attempts to prove Theorem 1·1. Burnside's argument appears to have been generally accepted, both at the time and later, until Neumann pointed out the error in his essay in [**38**]. For example, it is cited without critical comment by Wielandt in [**37**]. Its mistake is to assert that the only solutions to (4·1) when $m = n-1$ have $|\mathcal{O}| = p^n - 1$. This gives one solution, but there are others.

Recall that if $1 \le r < p^{n-1}$ then $R(r) = \{r, r+p^{n-1}, \dots, r+(p-1)p^{n-1}\}$. Define $Z \subseteq \{1, \dots, p^n-1\}$ to be *null* if there exists $s \in \mathbf{N}_0$ and distinct $r_{ij} \in \{1, \dots, p^{n-1}-1\}$ for $0 \le i \le p-1$ and $1 \le j \le s$ such that $r_{ij} \equiv i \bmod p$ for each i and j and $Z = \bigcup_{i=0}^{p-1} \bigcup_{j=1}^{s} R(r_{ij})$.

PROPOSITION 6·2. *Let $n \ge 2$ and let ω be a primitive p-th root of unity. Let $\mathcal{O} \subseteq \{1, \dots, p^n-1\}$. Then*

$$\sum_{i \in \mathcal{O}} \zeta^i = \sum_{i \in \mathcal{O}} \omega^i$$

if and only if either

(i) *$\mathcal{O}$ is null;* or

(ii) *$\mathcal{O} = \{p^{n-1}, \dots, (p-1)p^{n-1}\} \cup \bigcup_{i=1}^{p-1} R(r_i) \cup Z$ where Z is null, the r_i are distinct elements of $\{1, \dots, p^{n-1}-1\} \backslash Z$ and $r_i \equiv i \bmod p$ for each i.*

The proof is similar to the inductive step in §4; we use (4·2) and (4·3) to show that if Z is null then $\sum_{i \in Z} \xi^i = \sum_{i \in Z} \omega^i = 0$, and Lemma 2·1 to show that $\mathcal{O} \backslash \{p^{n-1}, \dots, (p-1)p^{n-1}\}$ is a union of the sets $R(r)$. Note that since $r_{01} \equiv 0 \bmod p$, and $1 \le r_{01} < p^{n-1}$, Case (i) is relevant only when $n \ge 3$. The smallest possible $\mathcal{O}$ has size $p^2 - 1$, coming from Case (ii); this shows Burnside's claim is false whenever $p \ge 3$ or $n \ge 3$. The lack of structure in the solutions, beyond that captured by the sets $R(r)$, suggests that any fix to Burnside's proof must involve significant further ideas.

6·2. *Burnside's 1921 paper*

In [**5**], Burnside claimed a 'remarkably simple' proof that every abelian group that is not elementary abelian is a B-group, as conjectured at the end of §252 of [**6**]. (Of course Burnside did not use the term 'B-group'.) The groups $S_d \wr S_2$ in their primitive action for d composite, seen in Example 1 below, show that this result is false. In [**31**, §15], D. Manning raised this family of counterexamples and observed 'the first and most important part of the proof must contain a serious mistake'.

In today's language, Burnside considers a permutation group G of degree dd' acting on $\{0, \dots, d-1\} \times \{0, \dots, d'-1\}$, containing a regular subgroup $K = \langle g_d \rangle \times \langle g'_{d'} \rangle$ where $g_d = (0, 1, \dots, d-1)$ and $g'_{d'} = (0, 1, \dots, d'-1)$. The natural $\mathbf{C}G$-permutation module M factorizes on restriction to K as $\langle e_0, \dots, e_{d-1} \rangle \otimes \langle e'_0, \dots, e'_{d'-1} \rangle$. Let ζ_d, $\zeta_{d'} \in \mathbf{C}$ be primitive roots of unity of orders d and d', respectively. The analogue of the v_j basis element defined earlier in (3·1) is

$$v_{(j,j')} = \sum_{0 \le i < d} \zeta_d^{-ij} e_i \otimes \sum_{0 \le i' < d'} \zeta_{d'}^{-i'j'} e'_{i'}$$

where $0 \le j < d$ and $0 \le j' < d'$. As before, M has a unique decomposition $\langle v_{(0,0)} \rangle \oplus V_1 \oplus \cdots \oplus V_t$ where each irreducible summand V_k has a basis $\{v_{(j,j')} : (j,j') \in B_k\}$ for some subset B_k of $\{0, \dots, d-1\} \times \{0, \dots, d'-1\}$. Let ϕ_k be the character of V_k. The

analogue of Lemma 3·2 is that if $\mathcal{O}$ is an orbit of the point stabiliser H of $(0,0)$, and $1 \leq k \leq t$ then

$$\sum_{(i,i')\in\mathcal{O}} \zeta_d^{ij}\zeta_{d'}^{i'j'} \tag{6·1}$$

is constant for $(j,j') \in B_k$. Burnside proves this, and also proves (in a similar way) the dual relation that the character value $\phi_k(g_d^i g_{d'}'^{i'}) = \sum_{(j,j')\in B_k} \zeta_d^{ij}\zeta_{d'}^{i'j'}$ is constant for $(i,i') \in \mathcal{O}$. Hence

$$\sum_{(i,i')\in\mathcal{O}} \sum_{(j,j')\in B_k} \zeta_d^{ij}\zeta_{d'}^{i'j'} = |B_k| \sum_{(i,i')\in\mathcal{O}} \zeta_d^{ij}\zeta_{d'}^{i'j'} \tag{6·2}$$

$$= |\mathcal{O}| \sum_{(j,j')\in B_k} \zeta_d^{ij}\zeta_{d'}^{i'j'} \tag{6·3}$$

provided $(j,j') \in B_k$ in the right-hand side of (6·2) and $(i,i') \in \mathcal{O}$ in the right-hand side of (6·3). Burnside chooses B_k to contain $(d/q, 0)$ where q is a prime factor of d and $\mathcal{O}$ to contain $(1,0)$. By taking $(j,j') = (d/q,0)$ in (6·2) and $(i,i') = (1,0)$ in (6·3) he obtains $|B_k| \sum_{(i,i')\in\mathcal{O}} \zeta_d^{id/q} = |\mathcal{O}| \sum_{(j,j')\in B_k} \zeta_d^j = |\mathcal{O}|\phi_k(g_d)$, and so

$$\phi_k(g_d) = \frac{|B_k|}{|\mathcal{O}|} \sum_{(i,i')\in\mathcal{O}} \omega^i \tag{6·4}$$

where $\omega = \zeta_d^{d/q}$ is a primitive root of unity of order q.

The fourth displayed equation on page 484 of [**5**] claims that $\phi_k(g_d^q) = |\mathcal{B}_k|$, and so g_d^q is in the kernel of ϕ_k. It appears that Burnside substitutes g_d^q for g_d in (6·4), and replaces ω with ω^q. If (6·4) expressed $\phi_k(g_d)$ as a sum of eigenvalues, as in (6·3), this would be legitimate. However this is not the case, and the following example shows that Burnside's claim is in general false.

Example 1. Let $d \in \mathbf{N}$. Let S be the symmetric group on the set $\{0,1,\ldots,d-1\}$. Let $N = S \times S$ and let $G \cong S \wr C_2$ be the wreath product $N \rtimes \langle\tau\rangle$ where τ has order 2 and acts on N by $(g,g')^\tau = (g',g)$. In the action of G on $\{0,1,\ldots,d-1\}^2$, the point stabiliser H of $(0,0)$, namely $(T \times T) \rtimes \tau$ where T is the symmetric group on $\{1,\ldots,d-1\}$, has two non-singleton orbits: $\big\{(j,0),(0,j) : 1 \leq j < d\big\}$ and $\big\{(j,j') : 1 \leq j,j' < d\big\}$. Therefore G is not 2-transitive. Provided $d \geq 3$, H is a maximal subgroup of G, so G is primitive. Let $g_d = g_d' = (0,1,\ldots,d-1)$. Since $\langle g_d\rangle \times \langle g_d'\rangle \leq N$ acts regularly, $C_d \times C_d$ is not a B-group whenever $d \geq 3$.

Let $d \geq 3$. The natural permutation character of S is $1_S + \chi$ where χ is irreducible. By the branching rule (see [**21**, Ch. 9] or [**20**, Lemma 2.3.10]), χ is the unique non-trivial character of S whose restriction to T contains the trivial character. By the classification of irreducible characters of wreath products [**20**, Theorem 4.3.34], it follows that the irreducible characters of G that contain the trivial character on restriction to H are 1_G, ϕ and $\widetilde{\chi^{\times 2}}$, where $\phi = (\chi \times 1_S)\uparrow_N^G$ and $\widetilde{\chi^{\times 2}}$ is the unique character of G whose restriction to N is $\chi \times \chi$. By Frobenius reciprocity, the permutation character of M is $1_G + \phi + \widetilde{\chi^{\times 2}}$. Considering restrictions to $\langle g_d\rangle \times \langle g_d'\rangle$, we get $M = \langle v_{(0,0)}\rangle \oplus \langle v_{(j,0)}, v_{(0,j')} : 1 \leq j < d, 1 \leq j' < d\rangle \oplus \langle v_{(j,j')} : 1 \leq j,j' < d\rangle$. The second summand has character ϕ and contains $v_{(1,0)}$ and $v_{(0,1)}$, so is a faithful $\mathbf{C}G$-module. Thus, contrary to Burnside's claim, no non-identity power of g_d is in the kernel of ϕ. Burnside's conclusion, that G has a proper normal subgroup containing g_d^q holds, since we may take the base group N, but clearly

Burnside intends the normal subgroup to be the kernel of ϕ, so that Proposition 3·3 can be applied, and the kernel of ϕ is trivial.

The penultimate paragraph of Burnside's paper considers the case where d and d' are distinct primes. This is the hardest part of the paper to interpret: the claims are correct, but the argument has a significant gap. Burnside has already assumed that G is not 2-transitive. If a basis set B_k is contained in $\{(1,0),\dots,(d-1,0)\}$ then, identifying (j,j') with $d'j+dj'$ mod dd', Proposition 3·3 implies that G has a normal intransitive subgroup N containing $\langle g_d\rangle$. This gives the first of Burnside's claims. While not stated explicitly, it seems that Burnside then assumes, as he may, that no B_k is contained in $\{(1,0),\dots,(d-1,0)\}$. He makes two further claims, equivalent to the following:

(i) If B_k meets $\{(1,0),\dots,(d-1,0)\}$ then B_k is a union of sets each of the form $\{(j,0),(j,1),\dots,(j,d'-1)\}$ where $1\le j<d$.
(ii) there is a set B_ℓ contained in $\{(0,1),\dots,(0,d'-1)\}$.

Clearly (i) implies (ii), and by Proposition 3·3, (ii) implies that G has a normal intransitive subgroup N containing $\langle g'_{d'}\rangle$. To prove (i), we use the italicised conclusion of the second paragraph in the proof of Theorem 1·2 in §5: taking $p=d'$, this implies that B_k is the union of a subset of $\{(0,1),\dots,(0,d'-1)\}$ and some sets of the required form. Since $[\mathbf{Q}(\zeta_{dd'}):\mathbf{Q}(\zeta_d)]=\phi(dd')/\phi(d)=\phi(d')=[\mathbf{Q}(\zeta_{d'}):\mathbf{Q}]$, the stabiliser of ζ_d in the Galois group $\mathrm{Gal}(\mathbf{Q}(\zeta_{dd'}):\mathbf{Q})$ acts transitively on the roots $\zeta_{d'},\dots,\zeta_{d'}^{d'-1}$. By the hypothesis in (i) there exists $(j,0)\in B_k$. For each r' such that $1\le r'<d'$ there exists $\sigma'\in\mathrm{Gal}(\mathbf{Q}(\zeta_{dd'}):\mathbf{Q})$ such that $\zeta_d^{\sigma'}=\zeta_d$ and $\zeta_{d'}^{\sigma'}=\zeta_{d'}^{r'}$. Since $v_{(j,0)}^{\sigma'}=v_{(j,0)}$ and $v_{(0,1)}^{\sigma'}=v_{(0,r')}$, we see that if B_k meets $\{(0,1),\dots,(0,d'-1)\}$ then it contains this set; a similar argument, taking $\sigma\in\mathrm{Gal}(\mathbf{Q}(\zeta_{dd'}):\mathbf{Q})$ such that $\zeta_d^{\sigma}=\zeta_d^{r}$ and $\zeta_{d'}^{\sigma}=\zeta_{d'}$ now shows that $B_k=\{0,\dots,d-1\}\times\{0,\dots,d'-1\}\setminus\{(0,0)\}$, and so G is 2-transitive, contrary to assumption. Therefore (i) holds.

Having proved (i), we instead follow Burnside's argument for (i) and (ii). Burnside chooses $\mathcal{O}$ to contain $(1,1)$ and takes $(m,0)\in B_k$. By (6·2) and (6·3), $|\mathcal{O}|\sum_{j'=0}^{d'-1}c_{j'}\zeta_{d'}^{j'}=|B_k|\sum_{(i,i')\in\mathcal{O}}\zeta_d^{im}$, where $c_{j'}=\sum_{j:(j,j')\in B_k}\zeta_d^{j}$ for $j'\in\{0,1,\dots,d'-1\}$. According to Burnside, this implies that the coefficients $c_{j'}$ are constant for all j'. It appears that Burnside assumes that every rational relation between the powers of $\zeta_{d'}$ is a multiple of $1+\zeta_{d'}+\cdots+\zeta_{d'}^{d'-1}$. But a more general relation is $a+\zeta_{d'}+\cdots+\zeta_{d'}^{d'-1}=a-1$, so we can only conclude that the $c_{j'}$ are constant for $j'\in\{1,\dots,d'-1\}$. However, it *is* true that if $\sum_{j\in J}\zeta_d^j=\sum_{j\in K}\zeta_d^j$ for non-empty sets J, $K\subseteq\{0,1,\dots,d-1\}$ then $J=K$, so this weaker conclusion implies that, for each $j'\in\{1,\dots,d'-1\}$, either $\{j:(j,j')\in B_k\}\supseteq\{1,\dots,d-1\}$ or $\{j:(j,j')\in B_k\}\subseteq\{0\}$. Hence

(i)′ If B_k meets $\{(1,0),\dots,(d-1,0)\}$ then B_k is a union of sets of the form $\{(j,0)\}$ and $\{(j,1),\dots,(j,d'-1)\}$ where $1\le j<d$.

The Galois action of the automorphisms σ in our proof of (i) shows that (i)′ implies (ii). Therefore Burnside's argument can be corrected.

The final sentence of the paragraph we have been reading is 'It is clear that the same method of proof will apply, when the transitive Abelian subgroup has three or more independent generators'. Taking $d=4$ in Example 1, we see that the subgroup $\langle(0,1,2,3)\rangle\times\langle(0,1)(2,3),(0,2)(1,3)\rangle\le G$ acts regularly in the primitive action of G on $\{0,1,2,3\}^2$. Therefore $C_4\times C_2\times C_2$ is not a B-group and Burnside's claim is false. The use of the Galois action in the previous paragraph required that both d and d' are prime.

In §6·5 below we extend the correct part of Burnside's proof to show that if p is an odd prime and $n \in \mathbf{N}$ then C_{2^n}, $C_{2^n p}$ and C_{2p^n} are B-groups. A proof of Conjecture 6·3 will rehabilitate Burnside's method for cyclic groups.

6·3. *Manning's 1936 paper*

In [**31**], D. Manning claimed a proof, using Burnside's method, that if p is prime and $a > b$ then $C_{p^a} \times C_{p^b}$ is a B-group. It is reported in [**37**, page 67] that she later acknowledged that the critical Lemma II in [**31**] is false. We extend Example 1 to show this.

Example 2. Recall from Example 1 that S is the symmetric group on $\{0, 1, \ldots, d-1\}$ and $G \cong S \wr C_2$ acting primitively on $\{0, 1, \ldots, d-1\}^2$. We took $g_d = g'_d = (0, 1, \ldots, d-1)$. By Example 1, the natural $\mathbf{C}G$-permutation module has a summand with basis set $B = \{(j, 0), (0, j') : 1 \leq j < d, 1 \leq j' < d\}$, with respect to the chosen generators $(g_d, 1)$ and $(1, g'_d)$ of the regular subgroup $K = \langle g_d \rangle \times \langle g'_d \rangle$.

We have

$$v_{(j,0)}(g_d, 1) = \zeta^j v_{(j,0)}, \quad v_{(0,j')}(g_d, 1) = v_{(0,j')},$$
$$v_{(j,0)}(g_d, g'_d) = \zeta^j v_{(j,0)}, \quad v_{(0,j')}(g_d, g'_d) = \zeta^{j'} v_{(0,j')}.$$

Therefore, with respect to the alternative generators $(g_d, 1)$ and (g_d, g'_d) of K, the basis set becomes $C = \{(j, j) : 1 \leq j < d\} \cup \{(0, j') : 1 \leq j' < d\}$. Observe that, as it must be, C is invariant under the action induced by $\mathrm{Gal}(\mathbf{Q}(\zeta_d) : \mathbf{Q})$. Manning's Lemma II asserts the stronger property that, given any $(i, i') \in \{0, 1, \ldots, d-1\}^2$ with i and i' coprime to d, C is invariant under the permutation $(j, j') \mapsto (ij, i'j')$, where the entries are taken modulo d. Taking $i = 1$ and $i' = -1$ we see that this is false whenever $d > 2$.

6·4. *Later proofs of Burnside's and Manning's claims*

In 1908, Schur introduced his method of S-rings and gave the first correct proof of Theorem 1 [**34**]. In 1933 Schur extended his method to prove, more generally, that any cyclic group of composite order is a B-group. As remarked in [**31**], it appears that Schur was unaware of Burnside's 1921 paper. In 1935, Wielandt wrote 'Der von Herrn Schur angegebene Beweis ist recht schwerig', and gave a short proof of the still more general result that any abelian group of composite order having a cyclic Sylow p-subgroup for some prime p is a B-group [**36**]. Wielandt's proof depends on several results on S-rings, in particular property (6) in [**36**], that the stabiliser of an element of an S-ring is itself in the ring. Wielandt's result and proof appear, in translation but essentially unchanged, in his 1964 textbook [**37**, Theorem 25.4]. The use of complex conjugation at the end of the proof of Theorem 1·2 in §5 involves some similar ideas to the proof of property (6) in Theorem 23.5 of [**37**], but the proof here is substantially shorter and more elementary.

The first essentially correct proof of the result claimed by D. Manning was given by Kochendörffer in 1937 using S-rings [**26**]; Wielandt comments in [**37**] that it is 'very complicated' (Bercov's translation). In his essay in [**38**], Neumann reports that in an unpublished note D. Manning found some slips in [**26**], but was able to correct them. Neumann's essay includes a proof of Theorem 1·1 that a reader, familiar with the prerequisites from modular representation theory and permutation groups, will find spectacularly short and beautiful.

Apart from [**25**], outlined in the introduction, the three papers [**3**, **5**, **31**] surveyed

in this section appear to exhaust the research literature on Burnside's method. It is intriguing that all err in ultimately the same way, by overlooking algebraic relations satisfied by roots of unity.

6·5. *Burnside's method in even degree*

Again we continue from the end of §3. There is an action of the Galois group $\mathrm{Gal}(\mathbf{Q}(\zeta_d) : \mathbf{Q})$ on the set $\{1, \ldots, d-1\}$ under which $\sigma \in \mathrm{Gal}(\mathbf{Q}(\zeta_d) : \mathbf{Q})$ sends i to i' if and only if σ sends ζ^i to $\zeta^{i'}$. In [**25**, Theorem 2.3(2)], Knapp extends Burnside's arguments to show that this action induces an action of the Galois group on the orbits of the point stabiliser H. (This result may also be proved using S-rings: see [**37**, Theorem 23.9].) Let D be the set of divisors of d. Set $\mathcal{O}(1) = \{0\}$ and for $r \in D$ with $r > 1$, set

$$\mathcal{O}(r) = \{md/r : 0 < m < r, \mathrm{hcf}(m, r) = 1\}.$$

Thus for each $r \in D$ the set $\{\zeta_d^i : i \in \mathcal{O}(r)\}$, consisting of all primitive r-th roots of unity, is an orbit of the Galois group on the powers of ζ_d. If d is even then, since $\mathcal{O}(2) = \{d/2\}$ corresponds to $\zeta_d^{d/2} = -1 \in \mathbf{Q}$, the H-orbit $\mathcal{O}$ containing $d/2$ is invariant under the Galois action. Hence $\mathcal{O} = \bigcup_{r \in E} \mathcal{O}(r)$ for some subset E of D. Observe that G is 2-transitive if and only if $E = D \backslash \{1\}$.

For $r \in D$ and $j \in \mathbf{N}$ we have $\sum_{i \in \mathcal{O}(r)} \zeta_d^{ij} = \sum_\alpha \alpha^j$ where α ranges over all primitive r-th roots of unity. If $\mathrm{hcf}(r, j) = j^\star$ then the map $\alpha \mapsto \alpha^j$ is $j^\star$ to 1, and each α^j is a primitive $r/j^\star$-th root of unity. It is well known that the sum of the $\phi(s)$ roots of unity of order s is $\mu(s)$, where μ is the Möbius function (see for instance [**35**, Exercise 2.8]). Therefore, if R is the matrix with rows and columns indexed by D, defined by

$$R_{rc} = \mu\Big(\frac{r}{\mathrm{hcf}(r,c)}\Big) \frac{\phi(r)}{\phi(\frac{r}{\mathrm{hcf}(r,c)})} \tag{6·5}$$

then, for any $r \in D$ and $j \in \mathbf{N}$,

$$\sum_{i \in \mathcal{O}(r)} \zeta_d^{ij} = R_{rc} \quad \text{where } c = \mathrm{hcf}(d, j). \tag{6·6}$$

(Here R stands for Ramanujan, who considered these cyclotomic sums in [**33**]; this was published in the interval between Burnside's 1901 and 1921 papers, but there is no evidence that Burnside was aware of its relevance.) As an *aide-memoire*, we note that R_{rc} is defined by taking c-th powers of r-th roots of unity. An example of these matrices is given after Lemma 6·4.

Let $\sim_E$ be the relation on $D \backslash \{d\}$ defined by

$$b \sim_E c \iff \sum_{r \in E} R_{rb} = \sum_{r \in E} R_{rc}. \tag{6·7}$$

Let $\mathcal{P}_E$ be the set of equivalence classes of $\sim_E$. Given $B \subseteq \{0, 1, \ldots, d-1\}$, let $Y(B) = \{c \in D \backslash \{d\} : B \cap \mathcal{O}(d/c) \neq \varnothing\}$. For example, $1 \in Y(B)$ if and only if B contains a number coprime to d, and $Y(\{0\}) = \varnothing$. If B_k and B_ℓ are distinct basis sets then necessarily $B_k \cap B_\ell = \varnothing$, but if neither B_k nor B_ℓ is invariant under the Galois action, we may still have $Y(B_k) \cap Y(B_\ell) \neq \varnothing$. However the asymmetry between orbits and basis sets in the conclusion of Lemma 3·2 works in our favour, to show that $\sum_{r \in E} R_{rc}$ is constant for $c \in Y(B_k)$. It follows that $Y(B_k)$ is contained in a single part of the partition $\mathcal{P}_E$ of $D \backslash \{d\}$. Hence, by Proposition 3·3, we may assume that the highest common factor

of the entries in each part of the partition $\mathcal{P}_E$ of $D\backslash\{d\}$ is 1. We say that such partitions are *coprime*.

For $c \in D$, an easy calculation from (6·6) shows that

$$\sum_{r\in D} R_{rc} = \sum_{i=0}^{d-1} \zeta_d^{ic} = c \sum_{i=0}^{d/c-1} \zeta_{d/c}^{i} = \begin{cases} 0 & \text{if } c < d, \\ d & \text{if } c = d. \end{cases}$$

Since $R_{1c} = 1$ for all $c \in D$, it follows that if $E = D\backslash\{1\}$ then $\mathcal{P}_E = \big\{D\backslash\{d\}\big\}$. This proves the 'if' direction of the following conjecture.

CONJECTURE 6·3. *Let $E \subseteq D$ contain 2. The partition $\mathcal{P}_E$ of $D\backslash\{d\}$ defined by the relation $\sim_E$ in (6·7) is coprime if and only if $E = D\backslash\{1\}$ or $E = D$.*

We have shown that if d is even then, defining E as above by the orbit $\mathcal{O}$ containing $d/2$, the 'only if' direction of Conjecture 6·3 implies that $E = D\backslash\{1\}$ and $\mathcal{O} = \{1, \dots, d-1\}$, and so C_d is a B-group.

The following lemma can be used to prove Conjecture 6·3 in several cases of interest. Let $R(d)$ denote the Ramanujan matrix defined for degree d.

LEMMA 6·4.

(i) *Let p be prime and let $n \in \mathbf{N}$. We have*

$$R(p^n)_{p^e p^f} = \begin{cases} 0 & \text{if } f < e-1, \\ -p^{e-1} & \text{if } f = e-1, \\ (p-1)p^{e-1} & \text{if } f \geq e. \end{cases}$$

(ii) *Let $p_1, \dots, p_s$ be distinct primes and let $n_1, \dots, n_s \in \mathbf{N}$. We have $R(d) = R(p_1^{n_1}) \otimes \cdots \otimes R(p_s^{n_s})$.*

Proof. Part (i) is immediate from (6·5). For (ii), it suffices to show that if d and d' are coprime and $r \mid d$, $r' \mid d'$ and $c \mid d$, $c' \mid d'$ then the entry in row rr' and column cc' of $R(dd')$ is $R_{rc}(d)R_{r'c'}(d')$. This follows from (6·5) using the multiplicativity of μ and ϕ, noting that $\operatorname{hcf}(r, r') = \operatorname{hcf}(c, c') = 1$. □

For example, if p is an odd prime then $R(2p^3)$ is as shown below, with D ordered $1, 3, 9, 27, 2, 6, 18, 54$ and row $2 \in E$ highlighted. The division indicates the tensor factorization $R(p^3) \otimes R(2)$.

$$\left(\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & p-1 & p-1 & p-1 & -1 & p-1 & p-1 & p-1 \\ 0 & -p & p(p-1) & p(p-1) & 0 & -p & p(p-1) & p(p-1) \\ 0 & 0 & -p^2 & p^2(p-1) & 0 & 0 & -p^2 & p^2(p-1) \\ \hline \mathbf{-1} & \mathbf{-1} & \mathbf{-1} & \mathbf{-1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} \\ 1 & -(p-1) & -(p-1) & -(p-1) & -1 & p-1 & p-1 & p-1 \\ 0 & p & -p(p-1) & -p(p-1) & 0 & -p & p(p-1) & p(p-1) \\ 0 & 0 & p^2 & -p^2(p-1) & 0 & 0 & -p^2 & p^2(p-1) \end{array}\right)$$

In particular $R(p^3)$ appears as the top-left block.

PROPOSITION 6·5. *Let $n \in \mathbf{N}$ and let p be an odd prime. Conjecture 6·3 holds when* (i) $d = 2^n$, (ii) $d = 2^n p$ *and* (iii) $d = 2p^n$.

Proof. The 'only if' direction remains to be proved. Recall that the rows and columns

of R are labelled by the divisors of d. Since row 1 of $R(d)$ is constant, we may assume that $1 \in E$.

Suppose, as in (i), that $d = 2^n$. If $n = 1$ then $E = \{1, 2\}$ and the conclusion is immediate. Suppose that $n \geq 2$. Let $R^\star$ be the matrix obtained from $R(2^n)$ by deleting row 1 and replacing row 2 with the sum of rows 1 and 2. Observe that column 1 of $R^\star$ has all zero entries, and the submatrix of $R^\star$ formed by columns 2^f for $1 \leq f \leq n$ is $2R(2^{n-1})$. Therefore $\sum_{r\in E} R(2^n)_{rc} = \frac{1}{2}\sum_{r\in E^\star} R(2^{n-1})_{rc}$ where $E^\star = \{1\} \cup \{r/2 : r \in E\backslash\{1, 2\}\}$. By induction $E^\star = \{1, 2, \ldots, 2^{n-1}\}$, and so $E = D$.

Part (ii) follows by a small extension of this argument. Let $R^\star$ be as defined in (i). By Lemma 6·4, the entry of $R^\star$ in row r and column c is odd if and only if $r \in \{p, 2p\}$ and $c = 2^m$ where $0 \leq m \leq n$. Any coprime partition has a part containing both 2^m and p for some such m. Therefore, by parity, either both p and $2p$ are contained in E, or neither are. Deleting row p and replacing row $2p$ with the sum of rows p and $2p$ of $R^\star$, we obtain $2R(2^{n-1}p)$, augmented by two zero columns. The inductive argument for (i) now shows that $E = D$.

Finally suppose that $d = 2p^n$. Let $\overline{R}(2p^n)$ denote $R(2p^n)$ with entries regarded as elements of $\mathbf{Z}/p^n\mathbf{Z}$. Let $\approx$ be the relation on $D\backslash\{2p^n\}$ defined as in (6·7), but working modulo p^n. Let $\overline{\mathcal{P}}_E$ denote the set of equivalence classes for $\approx$. We need this preliminary result: *if $\overline{\mathcal{P}}_E$ is coprime then 2, 2p, ..., $2p^n \in E$ and $\overline{\mathcal{P}}_E$ has a single part.* Again the proof is inductive. If $n = 1$ then, by Lemma 6·4,

$$\overline{R(2p)} = \left(\begin{array}{cc|cc} 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 \\ \hline -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & -1 \end{array}\right)$$

where the entries are in $\mathbf{Z}/p\mathbf{Z}$ and D is ordered $1, p, 2, 2p$. If $2p \notin E$ then, since 1, $2 \in E$, we have $\overline{\mathcal{P}}_E = \big\{\{1, p\}, \{2, 2p\}\big\}$, which is not coprime. Therefore $2p \in E$ and $\overline{\mathcal{P}}_E = \big\{\{1, p, 2, 2p\}\big\}$, as required. Suppose that $n \geq 2$. Let $\overline{R}^\star$ denote $R(2p^n)$ with the entries taken in $\mathbf{Z}/p^{n-1}\mathbf{Z}$. Observe that columns p^{n-1} and p^n of $\overline{R}^\star$ are equal, as are columns $2p^{n-1}$ and $2p^n$. Moreover, rows p^n and $2p^n$ have all zero entries. By a very similar inductive argument to (i), it follows that E contains 2, $2p$,..., $2p^{n-1}$. Let $R^\star$ be the matrix obtained from $R(p^n)$ by removing these rows, replacing row 2 with their sum, and adding p^{e-1} to each entry in row p^e, for $1 \leq e \leq n$. For example, if $n = 3$ then

$$R^\star = \left(\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & p & p & p & 0 & p & p & p \\ p & 0 & p^2 & p^2 & p & 0 & p^2 & p^2 \\ p^2 & p^2 & 0 & p^3 & p^2 & p^2 & 0 & p^3 \\ \hline \mathbf{0} & \mathbf{0} & \mathbf{-p^2} & \mathbf{-p^2} & \mathbf{0} & \mathbf{0} & \mathbf{p^2} & \mathbf{p^2} \\ 0 & 0 & p^2 & -p^2(p-1) & 0 & 0 & -p^2 & p^2(p-1) \end{array}\right)$$

where the row obtained by summation is highlighted. Since columns 1 and 2 of $R^\star$ are equal, and any part of a coprime partition of $D\backslash\{2p^n\}$ contains either 1 or 2, we see that $\overline{\mathcal{P}}_E$ has a single part. The column of $R^\star$ labelled $2p^{n-1}$ is greater, entry-by-entry, than every other column, except in rows p^n and $2p^n$. Since columns p^{n-1} and $2p^{n-1}$ of $R^\star$ are congruent except in the summed row and row $2p^n$, and the sum of entries in these columns is less than p^n, we have $2p^n \in E$. This proves the preliminary result.

We now prove (ii). Each part of $\overline{\mathcal{P}}_E$ is a union of parts of $\mathcal{P}_E$, so $\overline{\mathcal{P}}_E$ is coprime only if $\overline{\mathcal{P}}_E$ is coprime. By the preliminary result, 2, $2p$, ..., $2p^n \in E$. Let $R^{\star\star}$ be the matrix

defined as $R^\star$, but now adding all the rows 2, $2p$, …, $2p^{n-1}$, $2p^n$. The non-zero entries in the summed row for $R^{\star\star}$ are $-p^n$ in column p^n and p^n in column $2p^n$. Since p^n is in a non-singleton part of $\mathcal{P}_E$, we see from column p^n that E contains $1, p, \ldots, p^n$, as required. □

Despite its elementary statement, the author has been unable to prove Conjecture 6·3 in any significantly greater generality. We offer this as an open problem.

The HASKELL [**32**] program `RamanujanMatrix` on the author's website[1] has been used to verify Conjecture 6·3 for all degrees $d \leq 600$. We mention that

$$R(p^n) = \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 \\ 1 & 1 & 0 & \ldots & 0 \\ 1 & 1 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & \ldots & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ 0 & p & p & \ldots & p \\ 0 & 0 & p^2 & \ldots & p^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & p^n \end{pmatrix}.$$

It follows that each $R(d)$ is invertible; the determinant of $R(p^n)$ is $p^{n(n+1)/2}$ and its inverse is $R(p^n)^\circ/p^n$ where $R(p^n)^\circ$ is obtained from $R(p^n)$ by rotation by a half-turn. This leads to an alternative proof of Proposition 6·5(i) and may be useful more widely.

7. *Abelian B-groups*

7·1. *After CFSG*

We now skip over many later developments, referring the reader to Neumann's essays in the collected works [**7**, **38**] for some of the missing history, and consider the situation after the Classification Theorem of Finite Simple Groups. In an early application, it was used in [**12**] to determine all 2-transitive permutation groups. The resulting classification of all primitive permutation groups containing a regular cyclic subgroup is given in [**14**, Theorem 4.1] and [**24**, page 164], and independently refined in [**23**] and [**28**]. We state the version of this result relevant to Theorem 1·1 below. (Here S_d and A_d denote the symmetric and alternating groups of degree d, respectively; the other notation is also standard.)

THEOREM 7·1. *Let G be a permutation group containing a regular cyclic subgroup $\langle g \rangle$ of composite prime-power order p^n. Then either G is imprimitive, or G is 2-transitive and one of the following holds:*

(i) *$G = A_{p^n}$ or $G = S_{p^n}$ and g is a p^n-cycle;*
(ii) *$\mathrm{PGL}_d(\mathbf{F}_q) \leq G \leq \mathrm{P\Gamma L}_d(\mathbf{F}_q)$ where $p^n = (q^d - 1)/(q - 1)$;*
(iii) *$p = 3$, $n = 2$, $G = \mathrm{P\Gamma L}_2(\mathbf{F}_8)$ and $g = s\sigma$ where $s \in \mathrm{PGL}_2(\mathbf{F}_8)$ is semisimple of order 3 and σ is the automorphism of $\mathrm{PGL}_2(\mathbf{F}_8)$ induced by the Frobenius twist.*

Corollary 3 of [**29**] gives a rough classification of primitive permutation groups containing a regular subgroup. This was sharpened by Li in [**27**, Theorem 1.1] for regular abelian subgroups. Note that Case (2)(iv) of this theorem, on groups with socle $S_m \times \cdots \times S_m$ or $A_m \times \cdots \times A_m$, is missing the assumption $m \geq 5$. It is clear from Remark (b) following the theorem and the structure of the proof in §5 that this assumption was intended; it is required to exclude groups such as $S_2 \wr S_r$ and $A_3 \wr S_r$ with regular socle whose product action is imprimitive. (Primitive groups such as S_4 in its natural action or $S_3 \wr S_2$ in its product action are of affine type, and so already considered in Case (1) of the theorem.)

[1] See `www.ma.rhul.ac.uk/~uvah099/`

It will be useful to say that a group K is *m-factorizable* if there exists $r \geq 2$ and groups $K_1, \ldots, K_r$ such that $|K_1| = \ldots = |K_r| = m$ and $K \cong K_1 \times \cdots \times K_r$, and *factorizable* if it is m-factorizable for some $m \geq 3$.

PROPOSITION 7·2. *If K is a regular abelian subgroup of a primitive but not 2-transitive permutation group G then* either

(i) *$G = V \rtimes H$ where $V \cong \mathbf{F}_p^n$ is elementary abelian, the point stabiliser $H \leq \mathrm{GL}(V)$ acts irreducibly on V but intransitively on $V\backslash\{0\}$ and $|K| = p^n$;* or
(ii) *K is m-factorizable for some $m \geq 5$.*

Proof. If Case (1) of Li's theorem applies then $G \leq \mathrm{AGL}_d(\mathbf{F}_p)$ where p is prime and G acts on its socle $V \cong \mathbf{F}_p^d$. It is easy to show (see for example [**13**, Theorem 4.8]) that $G = V \rtimes H$ where $H \leq \mathrm{GL}(V)$ is irreducible. Since G is not 2-transitive, H is not transitive. In the remaining case of Li's theorem, G is of the form $(\widetilde{T}_1 \times \cdots \times \widetilde{T}_r).O.P$ where $O \leq \mathrm{Out}(\widetilde{T}_1) \times \cdots \times \mathrm{Out}(\widetilde{T}_r)$, P is transitive of degree r and each $\widetilde{T}_r$ is an almost simple permutation group of degree $m \geq 5$. Moreover $K = K_1 \times \cdots \times K_r$ where $K_i < \widetilde{T}_i$ and each K_i has order m. Therefore, if $r \geq 2$, then K is factorizable into m-subgroups with $m \geq 5$. If $r = 1$ then, as Li remarks following his theorem, G is 2-transitive, so need not be considered any further. □

Note that, as we discuss in §7·3, it is not necessarily the case that the subgroup K in case (i) is elementary abelian.

Theorem 25.7 in [**37**] generalizes Example 1 to show that if $m \geq 3$ and K is m-factorizable with r factors then K is a regular subgroup of $S_m \wr S_r$ in its primitive action on $\{1, \ldots, k\}^r$. This action is not 2-transitive, so K is not a B-group. We therefore have the following corollary, first observed in [**27**, Corollary 1.3].

COROLLARY 7·3. *No factorizable group is a B-group. Moreover, an abelian group not of prime-power order is a B-group if and only if it is not factorizable.*

It is an open problem to determine the non-factorizable abelian B-groups of prime-power order. We end with some partial results and reductions.

7·2. *Elementary abelian B-groups*

Exercise 3.5.6 in [**13**] asks for a proof that C_p^n is never a B-group. This is true when $p > 2$ by Corollary 7·3 (clearly C_p in its regular action is primitive but not 2-transitive), but false, in general, when $p = 2$.[2] For example, the primitive permutation groups of degree 8 containing a regular subgroup isomorphic to C_2^3 are A_8, S_8 and the affine groups $\mathbf{F}_2^3 \rtimes C_7$, $\mathbf{F}_2^3 \rtimes (C_7 \rtimes C_3)$ and $\mathbf{F}_2^3 \rtimes \mathrm{GL}_3(\mathbf{F}_2)$. All of these groups contain a 7-cycle, and so are 2-transitive. Therefore C_2^3 is a B-group.

These examples motivate the following lemma, whose proof requires Burnside's dichotomy on permutation groups of prime degree. The significance of Mersenne primes will be seen shortly.

LEMMA 7·4. *Let $V = \mathbf{F}_2^n$ where $2^n - 1$ is prime. A subgroup $H \leq \mathrm{GL}(V)$ is transitive on $V\backslash\{0\}$ if and only if $H \cong C_{2^n-1}$, $H \cong C_{2^n-1} \rtimes C_n$ or $H = \mathrm{GL}(V)$.*

[2] This mistake is corrected in the errata available at `people.math.carleton.ca/~jdixon/Errata.pdf`.

Proof. The 'if' direction is clear. By Theorem 6·1, if H is transitive on $V\backslash\{0\}$ then either $H \cong C_{2^n-1} \rtimes C_r$, for some r, or H is 2-transitive. Identifying $V\backslash\{0\}$ with $\mathbf{F}_{2^n}^\times$, we see that there exists $h \in H$ of order $2^n - 1$. (Such elements are called Singer cycles.) Let α be a primitive (2^n-1)-th root of unity. Note that h is conjugate to h^s in $\mathrm{GL}(V)$ if and only if the map $\beta \mapsto \beta^s$ permutes the eigenvalues $\alpha, \alpha^2, \ldots, \alpha^{2^{n-1}}$ of h. Thus $N_{\mathrm{GL}(V)}(\langle h\rangle) \cong C_n$ is generated by an element of prime order n conjugating h to h^2, and either $r = 1$ or $r = n$. If H is 2-transitive then $V \rtimes H$ is 3-transitive. Such groups were classified by Cameron and Kantor in [**9**]. By their Theorem 1 in the case of vector spaces over $\mathbf{F}_2$, the only such groups are $V \rtimes \mathrm{GL}(V)$ and, when $n = 4$, $V \rtimes A_7$. Since $2^4 - 1$ is composite, only the former case arises. □

It is worth noting that [**9**] predates the classification theorem; the methods used are mainly from discrete geometry rather than group theory. More generally, Hering [**16**, **17**] has classified the linear groups H transitive on non-zero vectors, under various assumptions on the composition factors of H.

PROPOSITION 7·5. *Let $V = \mathbf{F}_2^n$. The elementary abelian group C_2^n is a B-group if and only if $2^n - 1$ is a Mersenne prime and the only simple irreducible subgroups of $\mathrm{GL}(V)$ are C_{2^n-1} and $\mathrm{GL}(V)$.*

Proof. Suppose that $2^n - 1$ is composite. Let $h \in \mathrm{GL}(V)$ be a Singer cycle. If $n \neq 6$ then, by Zsigmondy's Theorem [**39**], there exist a prime r such that r divides $2^n - 1$ and r does not divide $2^m - 1$ for any $m < n$. Thus $h^{n/r}$ does not permute the vectors of a non-zero proper subspace of V, and so $\langle h^{n/r}\rangle$ acts irreducibly on V and intransitively on $V\backslash\{0\}$. Therefore $V \rtimes \langle h^{n/r}\rangle$ is primitive but not 2-transitive, and so C_2^n is not a B-group. In the exceptional case of Zsigmondy's Theorem when $n = 6$, we simply take h^3, of order 21.

Suppose that $2^n - 1$ is prime and that there is a simple irreducible group $T \leq \mathrm{GL}(V)$ other than C_{2^n-1} and $\mathrm{GL}(V)$. By Lemma 7·4, T is intransitive on $V\backslash\{0\}$, and so $V \rtimes T$ is not 2-transitive. Hence C_2^n is not a B-group. Conversely, assume that no such simple group exists, and, for a contradiction, that C_2^n is not a B-group. By Proposition 7·2, there exists a proper irreducible subgroup H of $\mathrm{GL}(V)$ such that H is intransitive on $V\backslash\{0\}$. Let M be a maximal subgroup of $\mathrm{GL}(V)$ containing H. The maximal subgroups of classical groups were classified by Aschbacher in [**1**]. Of the 11 Aschbacher classes, the first consists of reducible groups, and the remaining 10 of groups preserving a structure on V that can exist only when V has composite dimension. Therefore M is an almost simple group. Since M is a proper subgroup of $\mathrm{GL}(V)$, Lemma 7·4 implies that M is intransitive on $V\backslash\{0\}$. Let T be the simple normal subgroup of M. By Clifford's Theorem ([**11**, Theorem I]), the restriction of V to T decomposes as a direct sum of irreducible representations of T of the same dimension. Since n is prime, T acts irreducibly on V. Its orbits are contained in the orbits of M, so it acts intransitively on $V\backslash\{0\}$, contrary to our assumption. □

By Proposition 7·5, a solution to the following problem will imply that C_2^n is a B-group if and only if $2^n - 1$ is a Mersenne prime.

PROBLEM 7·6. *Show that if $2^n - 1$ is a Mersenne prime and $n \geq 3$ then no non-abelian finite simple group other than $\mathrm{GL}_n(\mathbf{F}_2)$ has an irreducible representation of dimension n over $\mathbf{F}_2$.*

The two remarks below give some partial progress on Problem 7·6.

(1) The Atlas [**22**] data available in GAP [**15**] shows that, with the possible exceptions of J_4, Ly, Th, Fi_{24}, B and M, no sporadic simple group has an irreducible representation over $\mathbf{F}_2$ of dimension n where $2^n - 1$ is a Mersenne prime. Indeed, it appears to be rare for a sporadic group or a finite group of Lie type to have a non-trivial irreducible representation over $\mathbf{F}_2$ of odd dimension. The author knows of no examples of such representations of alternating groups. Since a self-dual representation has an invariant alternating form, whereas an odd-dimensional orthogonal group over $\mathbf{F}_2$ has a 1-dimensional invariant subspace, such a representation is necessarily not self-dual.

(2) Inspection of tables of small dimensional representations of quasisimple groups [**18**, **19**] and (for the groups deliberately excluded therein), Chevalley groups in defining characteristic [**30**] show that no finite simple group except for $\mathrm{GL}_n(\mathbf{F}_2)$ has an irreducible representation over $\mathbf{F}_2$ of dimension $n \leq 250$ such that $2^n - 1$ is a Mersenne prime. Thus if $n \leq 250$ then C_2^n is a B-group if and only if

$$n \in \{1, 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127\}.$$

7·3. *Non-elementary abelian B-groups*

An interesting feature of the affine groups in Proposition 7·2(i) is that they may contain regular abelian subgroups other than C_p^n. In Remark 1.1 in [**27**], Li gives the example $V \rtimes S_n$ where V is the subrepresentation $\langle e_2 - e_1, \ldots, e_n - e_1 \rangle$ of the natural permutation representation $\langle e_1, \ldots, e_n \rangle$ of S_n over $\mathbf{F}_p$. To avoid a potential ambiguity, let $t_v \in V \rtimes H$ denote translation by $v \in V$. If $2s < n$ then the subgroup of $V \rtimes H$ generated by

$$(2,3)t_{e_1+e_2},\ \ldots,\ (2s, 2s+1)t_{e_1+e_{2s}},\ t_{e_{2s+2}},\ \ldots, t_{e_n}$$

is regular and isomorphic to $C_4^s \times C_2^{n-2s-1}$. Li claims that $V \rtimes H$ is primitive. However H acts irreducibly only when n is odd (and so $\dim V$ is even, as expected by Remark (1) above). Thus if $r \in \mathbf{N}_0$ and $s \in \mathbf{N}$ then $C_4^s \times C_2^{2r}$ is not a B-group, but Li's example sheds no light on when $C_4^s \times C_2^{2r+1}$, which may be non-factorizable, is a B-group. This is a special case of the following problem.

Problem 7·7. *Classify non-elementary abelian B-groups of prime-power order.*

By Proposition 7·2, this problem reduces to classifying regular abelian subgroups of affine groups $V \rtimes \mathrm{GL}(V)$. The main result of [**10**] is a beautiful bijective correspondence between such subgroups and nilpotent algebras with underlying vector space V. To explain part of this correspondence, observe that if K is an regular abelian subgroup of $V \rtimes H$ where $H \leq \mathrm{GL}(V)$ then, for each $v \in V$, there exists a unique $h_v \in H$ such that $h_v t_v \in K$. From $h_u h_v t_{uh_v+v} = h_u t_u h_v t_v = h_v t_v h_u t_u = h_v h_u t_{vh_u+u}$ for $u, v \in V$, we see that $\{h_v : v \in V\}$ is an abelian subgroup of H and $uh_v + v = vh_u + u$ for all u, $v \in V$. Replacing v with $v + w$, we obtain

$$uh_{v+w} + (v+w) = (v+w)h_u + u = vh_u + wh_u + u = uh_v + v + uh_w + w - u$$

and so, cancelling $v + w$ and subtracting u, we have

$$h_{v+w} - 1 = (h_v - 1) + (h_w - 1) \tag{7·1}$$

for all v, $w \in K$. This additivity property is highly restrictive.

Example 3. Let $K = \{h_v t_v : v \in V\}$ be a regular abelian subgroup of $V \rtimes S_n$, where V is as in Li's example. The matrix X representing h_v in the basis $e_2 - e_1, \ldots, e_n - e_1$ of V is a permutation matrix if and only if $1h_v = 1$. If $1h_v = a$ and $bh_v = 1$ then, since $(e_i - e_1)h_v = (e_{ih_v} - 1) - (e_a - 1)$, each entry of X in column $e_a - e_1$ is -1, row $e_i - e_1$ has a 1 in column $e_{ih_v} - e_1$ for each $i \neq b$, and X has no other non-zero entries. By (7·1), $h_{2v} = 2h_v - 1$, so h_{2v} is represented by $2X - I$, where I is the identity matrix. But $2X - I$ is not of either of these forms unless $p = 2$ or $X = I$. Therefore V is the unique regular abelian subgroup of $V \rtimes S_n$ if $p > 2$. Suppose that $p = 2$. If h_v has order 4 or more, the matrix representing $h_v + h_v^{-1} + 1$ has multiple non-zero entries in the columns for both $e_a - e_1$ and $e_b - e_1$, again contradicting (7·1). Therefore each h_v has order at most 2. It follows that K has exponent 2 or 4. Thus the examples given by Li are exhaustive.

When p divides n the representation V has an irreducible quotient $U = V/\langle e_1 + \cdots + e_n \rangle$. Similar arguments show that $U \rtimes S_n$ has a non-elementary abelian regular subgroup if and only if $p = 2$. Any such subgroup has exponent 4, with the exception that when $n = 6$, $U \rtimes S_6$ has an regular abelian subgroup isomorphic to $C_8 \times C_2$. This does not contradict the result first claimed by Manning (see §6·3) since in this case S_6 acts transitively on $U \backslash \{0\}$; the related 2-transitive action of A_7 on $\mathbf{F}_2^4$, coming from the isomorphism $A_8 \cong \mathrm{GL}_4(\mathbf{F}_2)$, was seen in the proof of Lemma 7·4.

We end with some consequences of the following observation: if J is the $m \times m$ unipotent Jordan block matrix over $\mathbf{F}_p$ then $J^{p^r} = I$ if and only if $p^r \geq m$ and $I + J + \cdots + J^{p^r - 1} = 0$ if and only if $p^r > m$. (The latter can be proved most simply using the identity $I + J + \cdots + J^{p^r - 1} = (J - I)^{p^r - 1}$.)

PROPOSITION 7·8. *Let $V = \mathbf{F}_p^n$ and let K be a regular abelian subgroup of $V \rtimes \mathrm{GL}(V)$.*
(i) *If $n < p$ then $K \cong C_p^n$.*
(ii) *If $K \cong C_{p^n}$ then either $n = 1$ or $p = 2$ and $n = 2$.*

Proof. For $h_v t_v \in K$ we have $(h_v t_v)^{p^r} = h_v^{p^r} t_w$ where $w = v + vh_v + \cdots + vh_v^{p^r - 1}$. Hence, using the observation just made, if $n < p$ then $(h_v - 1)^p = 0$ and so $h_v^p = 1$ and $(h_v t_v)^p = 1$, giving (i). Now suppose that $h_v t_v$ generates K. Since $(h_v t_v)^{p^{n-1}} \neq 1$, we have $v + vh_v + \cdots + vh_v^{p^{n-1} - 1} \neq 0$. Hence there is a $m \times m$ unipotent Jordan block in h_v with $m \geq p^{n-1}$. Therefore $n \geq p^{n-1}$ which implies (ii). □

The subgroups K in Proposition 7·8(i) may be classified up to conjugacy in the affine group using the theory in [**10**]. Using Proposition 7·8(i) to rule out degrees, it follows from an exhaustive search through the library of primitive permutation groups in MAGMA [**2**] that the abelian B-groups of composite prime-power degree d where $d \leq 255$ are precisely those listed in Table 1 overleaf. Finally we remark that Proposition 7·2 and Proposition 7·8(ii) together imply that C_{p^n} is a B-group for all primes p and all $n \in \mathbf{N}$ with $n \geq 2$, giving one final proof of Theorem 1·1.

Acknowledgements

I thank Nick Gill for his answer to a MathOverflow question outlining an alternative proof of Proposition 7·2 and Derek Holt for several helpful comments on this question (see `mathoverflow.net/questions/258434/`). I thank John Britnell and Peter M. Neumann for helpful comments.

d	p^n	$f(d)$	abelian B-groups of order d
4	2^2	0	C_2^2, C_4
8	2^3	0	$C_2^3, C_4 \times C_2, C_8$
9	3^2	2	C_9
16	2^4	9	$C_8 \times C_2$, C_{16}
25	5^2	17	C_{25}
27	3^3	9	$C_9 \times C_3$, C_{27}
32	2^5	0	$C_2^5, C_4 \times C_2^3, C_4^2 \times C_2, C_8 \times C_2^2, C_8 \times C_4, C_{16} \times C_2, C_{32}$
49	7^2	29	C_{49}
64	2^6	55	$C_{16} \times C_2^2$, $C_{16} \times C_4$, $C_{32} \times C_2$, C_{64}
81	3^4	125	$C_{27} \times C_3, C_{81}$
121	11^2	43	C_{121}
125	5^3	38	$C_{25} \times C_5, C_{125}$
128	2^7	0	$C_2^7, C_4 \times C_2^5, C_4^2 \times C_2^3, C_4 \times C_2^5, C_8 \times C_2^4, C_8 \times C_4 \times C_2^2, C_8 \times C_4^2,$ $C_8^2 \times C_2, C_{16} \times C_2^3, C_{16} \times C_4 \times C_2, C_{16} \times C_8, C_{32} \times C_2^2, C_{32} \times C_4,$ $C_{64} \times C_2, C_{128}$
169	13^2	64	C_{169}
243	3^5	30	$C_9 \times C_3^3$, $C_9 \times C_9 \times C_3$, $C_{27} \times C_3^2, C_{27} \times C_9, C_{81} \times C_3, C_{243}$

Table 1. *All abelian B-groups of composite prime-power degree d where $d \leq 255$; $f(d)$ is the number of primitive permutation groups of degree d that are not 2-transitive.*

REFERENCES

[**1**] M. Aschbacher, *On the maximal subgroups of the finite classical groups*, Invent. Math. **76** (1984), 469–514.

[**2**] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), 235–265, Computational algebra and number theory (London, 1993).

[**3**] W. Burnside, *On some properties of groups of odd order*, Proc. London Math. Soc. **33** (1901), 162–185.

[**4**] ———— *On simply transitive groups of prime degree*, Q. J. Math. **37** (1906), 215–221.

[**5**] ———— *On certain simply-transitive permutation-groups*, Proc. Cambridge Phil. Soc. **20** (1921), 482–484.

[**6**] ———— *Theory of groups of finite order*, Dover Publications Inc., New York, 1955, reprint of 2nd edition, Cambridge University Press, 1911.

[**7**] ———— *The collected papers of William Burnside. Vol. I*, Oxford University Press, Oxford, 2004, Commentary on Burnside's life and work; papers 1883–1899, edited by Peter M. Neumann, A. J. S. Mann and Julia C. Tompson and with a preface by Neumann and Mann.

[**8**] ———— *The collected papers of William Burnside. Vol. II*, Oxford University Press, Oxford, 2004, papers 1900–1926, edited by Peter M. Neumann, A. J. S. Mann and Julia C. Tompson and with a preface by Neumann and Mann.

[**9**] P. J. Cameron and W. M. Kantor, 2-*transitive and antiflag transitive collineation groups of finite projective spaces*, J. Algebra **60** (1979), 384–422.

[**10**] A. Caranti, Francesca Dalla Volta, and Massimiliano Sala, *Abelian regular subgroups of the affine group and radical rings*, Publ. Math. Debrecen **69** (2006), 297–308.

[**11**] A. H. Clifford, *Representations induced in an invariant subgroup*, Ann. of Math. (2) **38** (1937), 533–550.

[**12**] Charles W. Curtis, William M. Kantor, and Gary M. Seitz, *The* 2-*transitive permutation representations of the finite Chevalley groups*, Trans. Amer. Math. Soc. **218** (1976), 1–59.

[**13**] John D. Dixon and Brian Mortimer, *Permutation groups*, Graduate Texts in Mathematics, vol. 163, Springer-Verlag, New York, 1996.

[**14**] Walter Feit, *Some consequences of the classification of finite simple groups*, The Santa Cruz Conference on Finite Groups (Univ. California, Santa Cruz, Calif., 1979), Proc. Sympos. Pure Math., vol. 37, Amer. Math. Soc., Providence, R.I., 1980, pp. 175–181.

[**15**] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.7.4*, 2014.

[**16**] C. Hering, *Transitive linear groups and linear groups which contain irreducible subgroups*

of prime order, Geometriae Dedicata **2** (1974), 425–460.
[**17**] ———— *Transitive linear groups and linear groups which contain irreducible subgroups of prime order. II*, J. Algebra **93** (1985), 151–164.
[**18**] Gerhard Hiss and Gunter Malle, Low-dimensional representations of quasi-simple groups, LMS J. Comput. Math. **4** (2001), 22–63.
[**19**] ———— *Corrigenda: "Low-dimensional representations of quasi-simple groups"*, LMS J. Comput. Math. **5** (2002), 95–126.
[**20**] Gordon James and Adalbert Kerber, *The representation theory of the symmetric group*, Encyclopedia of Mathematics and its Applications, vol. 16, Addison-Wesley Publishing Co., Reading, Mass., 1981.
[**21**] G. D. James, *The representation theory of the symmetric groups*, Lecture Notes in Mathematics, vol. 682, Springer, Berlin, 1978.
[**22**] Christoph Jansen, Klaus Lux, Richard Parker, and Robert Wilson, *An atlas of Brauer characters*, London Mathematical Society Monographs. New Series, vol. 11, The Clarendon Press, Oxford University Press, New York, 1995, Appendix 2 by T. Breuer and S. Norton, Oxford Science Publications.
[**23**] Gareth A. Jones, *Cyclic regular subgroups of primitive permutation groups*, J. Group Theory **5** (2002), 403–407.
[**24**] William M. Kantor, *Some consequences of the classification of finite simple groups*, Finite groups—coming of age (Montreal, Que., 1982), Contemp. Math., vol. 45, Amer. Math. Soc., Providence, RI, 1985, pp. 159–173.
[**25**] Wolfgang Knapp, *On Burnside's method*, J. Algebra **175** (1995), 644–660.
[**26**] Rudolf Kochendörffer, *Untersuchungen über eine Vermutung von W. Burnside*, Schriften des mathematischen Seminars und des Instituts für angewandtemathematik der Universität Berlin. **3** (1937), 155–180.
[**27**] Cai Heng Li, *The finite primitive permutation groups containing an abelian regular subgroup*, Proc. London Math. Soc. (3) **87** (2003), 725–747.
[**28**] ———— *Permutation groups with a cyclic regular subgroup and arc transitive circulants*, J. Algebraic Combin. **21** (2005), 131–136.
[**29**] Martin W. Liebeck, Cheryl E. Praeger, and Jan Saxl, *Transitive subgroups of primitive permutation groups*, J. Algebra **234** (2000), 291–361.
[**30**] Frank Lübeck, *Small degree representations of finite Chevalley groups in defining characteristic*, LMS J. Comput. Math. **4** (2001), 135–169.
[**31**] Dorothy Manning, *On simply transitive groups with transitive abelian subgroups of the same degree*, Trans. Amer. Math. Soc. **40** (1936), 324–342.
[**32**] Simon Peyton Jones et al., *The Haskell 98 language and libraries: The revised report*, Journal of Functional Programming **13** (2003), 0–255, `http://www.haskell.org/definition/`.
[**33**] S. Ramanujan, *On certain trigonometrical sums and their applications in the theory of numbers*, Trans. Cambridge Philos. Soc. **22** (1918), 259–276.
[**34**] I. Schur, *Neuer Beweis eines Satzes von W. Burnside*, Jahresbericht der Deutschen Mathematik-Vereinigung **17** (1908).
[**35**] Lawrence C. Washington, *Introduction to cyclotomic fields*, second ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997.
[**36**] Helmut Wielandt, *Zur Theorie der einfach transitiven Permutationsgruppen*, Math. Z. **40** (1936), 582–587.
[**37**] ———— *Finite permutation groups*, Translated from the German by R. Bercov, Academic Press, New York-London, 1964.
[**38**] ———— *Mathematische Werke/Mathematical works. Vol. 1*, Walter de Gruyter & Co., Berlin, 1994, Group theory, With essays on some of Wielandt's works by G. Betsch, B. Hartley, I. M. Isaacs, O. H. Kegel and P. M. Neumann, edited with a preface by Bertram Huppert and Hans Schneider.
[**39**] K. Zsigmondy, *Zur Theorie der Potenzreste*, Monatsh. Math. Phys. **3** (1892), 265–284.