Can. J. Math.Vol. 43 (3), 1991 pp. 559–579

STRUCTURE OF p-SOLVABLE GROUPS WITH THREE p-REGULAR CLASSES

Dedicated to Professor Takasi Nagahara on his 60th birthday

YASUSHI NINOMIYA

1. **Introduction.** One of the important invariants of a p-block B of a group algebra is $\ell(B)$, the number of non-isomorphic simple B-modules. A number of authors calculated $\ell(B)$ for various types of defect groups of B. In particular, by Olsson [6], it has been proved that if $p = 2$ and the defect groups of the block B are dihedral or semi-dihedral or generalized quaternion, then $\ell(B)$ is at most 3. In this paper, we restrict our attention to the principal p-block B_0 of a finite p-solvable group with $\ell(B_0) \leq 3$. Let Γ be a finite p-solvable group and k a splitting field for Γ with characteristic p. As is well known, B_0 is isomorphic to the group algebra $k\Gamma/O_{p'}(\Gamma)$, and hence $\ell(B_0)$ is equal to the number of p-regular classes, namely, the number of conjugacy classes consisting of p'-elements, of $\Gamma/O_{p'p}(\Gamma)$. Therefore, if $\ell(B_0) = 1$ then B_0 is isomorphic to a group algebra of a p-group, that is, $\Gamma/O_{p'}(\Gamma)$ is a p-group. Next, let a p-group P act faithfully on a vector space V of dimension n over GF(q), where q is a prime distinct from p, and suppose that P acts transitively on $V^{\#} = V - \{0\}$. Then the values of p and q^n and the structure of P are completely determined in [7]. By making use of this result, we can immediately obtain the structure of p-solvable groups which have exactly two p-regular classes. This has been given in our previous paper [5]. We shall frequently refer to this result, but, for convenience, we here restate it.

THEOREM A. *Let G be a p-solvable group with $O_p(G) = \langle 1 \rangle$. Suppose that G has exactly two p-regular classes. Then G is either a p'-group or a p-nilpotent group; and*

(1) if G is a p'-group then p is odd and $G \simeq \mathbb{Z}_2$, and

(2) if G is a p-nilpotent group then one of the following holds:

(a) $p = 2$ and $G \simeq E_{3^2} \rtimes \mathbb{Z}_8$.

(b) $p = 2$ and $G \simeq E_{3^2} \rtimes Q_8$.

(c) $p = 2$ and $G \simeq E_{3^2} \rtimes S_{16}$.

(d) $p = 2$ and $G \simeq \mathbb{Z}_q \rtimes \mathbb{Z}_{2^n}$, where $q = 2^n + 1$ is a Fermat prime.

(e) $p = 2^n - 1$ (a Mersenne prime) and $G \simeq E_{2^n} \rtimes \mathbb{Z}_p$.

We therefore see that if $\ell(B_0) = 2$ then $\Gamma/O_{p'p}(\Gamma)$ is isomorphic to one of the groups mentioned in the theorem and $B_0 \simeq k\Gamma/O_{p'}(\Gamma)$. The purpose of this paper is to give the

Received by the editors January 9, 1990.
AMS subject classification: 20C20, 20D99.

structure of p-solvable groups which have exactly three p-regular classes. Our result is the following theorem.

THEOREM B. *Let G be a p-solvable group with $O_p(G) = \langle 1 \rangle$. Suppose that G has exactly three p-regular classes. Then the p'-length of G is at most 2, and one of the following holds:*

(1) $p \neq 3$ *and* $G \simeq \mathbb{Z}_3$.
(2) $p \neq 2, 3$ *and* $G \simeq \Sigma_3$.
(3) $p = 2$ *and* $G \simeq M(3) \rtimes P$, *where* P *is* $\mathbb{Z}_8$ *or* S_{16}.
(4) $p = 3$ *and* $G \simeq Q_8 \rtimes \mathbb{Z}_3$ $\left(\simeq SL(2,3)\right)$.
(5) $p = 2$ *and* $G \simeq E_{3^2} \rtimes P$, *where* P *is* $\mathbb{Z}_4$ *or* D_8.
(6) $p = 2$ *and* $G \simeq \mathbb{Z}_q \rtimes \mathbb{Z}_{2^n}$, *where* $q = 2^{n+1} + 1$ *is a Fermat prime.*
(7) $p \neq 2$ *and* $G \simeq \mathbb{Z}_q \rtimes \mathbb{Z}_{p^n}$, *where* $q = 2p^n + 1$ *is a prime.*
(8) $p \neq 2, 3$ *and* $G \simeq E_{3^\ell} \rtimes \mathbb{Z}_{p^n}$, *where* $3^\ell = 2p^n + 1$.
(9) $p = 2$ *and* $G \simeq E_{3^4} \rtimes P$, *where* P *is a 2-group which contains a normal subgroup* R *of index 2 satisfying one of the following conditions:*
  (a) $|R| = 2^5$ *and* $R = \mathbb{Z}_8 \times_s \mathbb{Z}_8$, $Q_8 \times_s Q_8$ *or* $S_{16} \times_s S_{16}$.
  (b) $|R| = 2^6$ *and* $R = \mathbb{Z}_8 \times \mathbb{Z}_8$, $Q_8 \times Q_8$ *or* $S_{16} \times_s S_{16}$.
  (c) $|R| = 2^7$ *and* $R = S_{16} \times_s S_{16}$.
  (d) $|R| = 2^8$ *and* $R = S_{16} \times S_{16}$.
(10) $p = 2$ *and* $G \simeq \mathbb{Z}_{q^2} \rtimes P$, *where* q *is a Fermat prime greater than 3 and* P *is either*
  (a) a Sylow 2-subgroup of $\mathrm{GL}(2, q)$, *or*
  (b) a 2-group defined by

$$\langle x, y \mid x^{2^e} = 1,\ x^{2^{e-1}} = y^{2^e},\ x^y = x^{-1} \rangle,$$

  where $2^e = q - 1$.
(11) $p = 2$ *and* $G \simeq E_{7^2} \rtimes T$, *where* T *is a group generated by a normal subgroup* R *isomorphic to* Q_8 *and two elements* w, x *with the following properties:*

$$w^3 = 1, \quad x^2 \in R, \quad x^4 = 1, \quad w^x = w^{-1}.$$

(12) $p = 2$ *and* $G \simeq E_{5^2} \rtimes T$, *where* T *is a group generated by a normal subgroup* R *isomorphic to* $\mathcal{T}_0(5)$ *and two elements* w, x *with the following properties:*

$$w^3 = 1, \quad x^2 \in R, \quad x^8 = 1, \quad w^x = w^{-1}.$$

We then see that if $\ell(B_0) = 3$ then $\Gamma / O_{p'p}(\Gamma)$ is isomorphic to one of the groups mentioned in the theorem and $B_0 \simeq k\Gamma / O_{p'}(\Gamma)$. The notation used in the above theorems is as follows:

$\mathbb{Z}_n$ the cyclic group of order n,
E_{p^n} the elementary abelian group of order p^n,

https://doi.org/10.4153/CJM-1991-034-2 Published online by Cambridge University Press

Σ_3	the symmetric group of degree 3,
Q_8	the quaternion group of order 8,
D_8	the dihedral group of order 8,
S_{16}	the semi-dihedral group of order 16,
$M(3)$	the nonabelian 3-group which is of order 3^3 and has exponent 3, that is, $M(3)$ is a group given by

$$\langle a, b, c \mid a^3 = b^3 = c^3 = 1,\ b^a = bc,\ c^a = c,\ c^b = c \rangle .$$

Let q be a prime. Following [7, p. 229], we denote by $\mathcal{T}_0(q^n)$ the subgroup of $\mathrm{GL}(2, q^n)$ consisting of the matrices

$$\begin{pmatrix} a & 0 \\ 0 & \pm a^{-1} \end{pmatrix}, \quad \begin{pmatrix} 0 & a \\ \pm a^{-1} & 0 \end{pmatrix}, \quad a \in \mathrm{GF}(q^n), \quad a \neq 0.$$

Given two groups H and K, $H \rtimes K$ denotes a semidirect product of H by K, namely, H is normal in $H \rtimes K$ and $(H \rtimes K)/H \simeq K$; and $H \times_s K$ denotes a subdirect product of H and K, namely, $H \times_s K$ is a subgroup of the direct product $H \times K$ which satisfies

$$\varphi_H(H \times_s K) = H, \quad \varphi_K(H \times_s K) = K,$$

where φ_H and φ_K are cononical homomorphisms of $H \times K$ onto H and K respectively.

Here we introduce some additional notation. The number of p-regular classes in G will be denoted by $r_{p'}(G)$, and the set of primes dividing the order of G will be denoted by $\pi(G)$. Given $g \in G$, we write C_g for the conjugacy class containing g. If X is a subset of G, $\langle X \rangle$ will denote the subgroup of G generated by X. The cardinality of X will be denoted by $|X|$. If X, Y are subsets of G with $X \subseteq Y$ then $Y - X$ will denote the set of elements of Y not contained in X. The set of nonidentity elements of G will be denoted by $G^{\#}$. Given two integers m, n, $m|n$ means m divides n and for a prime q, $q^a \| n$ means $q^a | n$ but q^{a+1} does not divide n. The other notation is standard and refer to the book of Gorenstein [1].

The following is trivial but important for our subsequent study.

LEMMA 1.1. *If G is a p-solvable group with $r_{p'}(G) = 3$, then*
(1) the p'-length of G is at most 2, and
(2) the number of primes distinct from p which divide $|G|$ is at most 2.

In what follows, we let G be a p-solvable group with $O_p(G) = \langle 1 \rangle$, and assume that $r_{p'}(G) = 3$. In Section 2, we prove that part (1) or (2) holds if G is a p'-group. If $G = O_{p'p}(G)$ we can see that $O_{p'}(G)$ is a q-group for some prime q. In Section 3, we deal with the case where $O_{p'}(G)$ is nonabelian, and prove that part (3) or (4) holds for this case. On the other hand, the case where $O_{p'}(G)$ is abelian is treated in Sections 4 and 5. If a Sylow p-subgroup of G acts $\frac{1}{2}$-transitively on $O_{p'}(G)^{\#}$, then part (5), (6), (7) or (8) holds. This will be proved in Section 4. On the other hand, if a Sylow p-subgroup of G does not act $\frac{1}{2}$-transitively on $O_{p'}(G)^{\#}$, then part (9) or (10) holds. This will be proved in Section 5. To complete the proof of Theorem B, it will suffice to prove that the case $G = O_{p'pp'}(G)$ does not occur and part (11) or (12) holds for the case $G = O_{p'pp'p}(G)$ because by Lemma 1.1 the p'-length of G is at most 2. In Section 6, we complete the proof of Theorem B by showing that this is in fact true.

2. **Proof of parts (1) and (2) of Theorem B.**

In this section, we prove the following:

PROPOSITION 2.1. *If G is a p'-group, then part (1) or (2) of Theorem B holds.*

PROOF. If G is abelian then clearly $G \simeq \mathbb{Z}_3$. Thus (1) holds. Suppose next that G is a nonabelian p'-group. By Lemma 1.1, $|\pi(G)| \leq 2$. We now show $|\pi(G)| = 2$. Suppose otherwise and let $\Phi(G)$ denote the Frattini subgroup of G. As $r_{p'}\big(G/\Phi(G)\big) = 2$, we have $G/\Phi(G) \simeq \mathbb{Z}_2$ and so G is cyclic, contrary to our assumption. Hence $|\pi(G)| = 2$. Set $\pi(G) = \{q, r\}$. Then G has a nontrivial normal q- or r-subgroup. Without loss we may assume that G has a nontrivial normal r-subgroup R. Noting that the conjugacy classes of G are given by C_1, C_x, C_y, where $x \in R^{\#}$, $y \in G - R$, we see that R is a Sylow r-subgroup of G. From the assumption $r_{p'}(G) = 3$, it follows at once that $r_{p'}(G/R) = 2$, and so $G/R \simeq \mathbb{Z}_2$. Then we have $R \simeq \mathbb{Z}_3$ because a Sylow 2-subgroup of G, which is isomorphic to $\mathbb{Z}_2$, acts transitively by conjugation on $R^{\#}$. Hence $G \simeq \Sigma_3$. Thus (2) follows.

3. **Proof of parts (3) and (4) of Theorem B.**

In this section we consider the case where G is p-nilpotent, that is, $G = O_{p'p}(G)$. We set $V = O_{p'}(G)$. First of all we prove the following:

LEMMA 3.1. $|\pi(V)| = 1$.

PROOF. Suppose the lemma is false. Then $|\pi(V)| = 2$ by Lemma 1.1. Set $\pi(V) = \{q, r\}$. From the assumption $r_{p'}(G) = 3$,it follows that every element of V is either a q-element or an r-element. We therefore immediately see that V is a Frobenius group. Let Q and R be Sylow q- and r-subgroups of V respectively. Without loss we may assume that R is the Frobenius kernel. Then we claim that $Q \simeq \mathbb{Z}_q$; for the set of nonidentity q-elements of V forms a single conjugacy class in G, and so Q is elementary abelian. But Q is a Frobenius complement. Hence $Q \simeq \mathbb{Z}_q$. Because $r_{p'}(G/R) = 2$, Theorem A applies to G/R, and we have $p = 2$ and $G/R \simeq \mathbb{Z}_q \rtimes \mathbb{Z}_{2^n}$, where $q = 2^n + 1$ is a Fermat prime. This forces r to be odd. Further, since G acts transitively on $R^{\#}$, setting $|R| = r^\ell$, we have

$$r^\ell - 1 = |R^{\#}| = 2^m q, \quad m \leq n.$$

We now claim that $m \geq 1$ and $\ell \geq 2$. Indeed, as r is odd, $r^\ell - 1$ is even, and so $m \geq 1$. On the other hand, if $\ell = 1$ then R is a cyclic group, and so G/R is abelian because G/R is contained isomorphically in $\operatorname{Aut} R$, an abelian group, which is not the case. Hence $m \geq 1$ and $\ell \geq 2$. If we can prove the following lemma we reach a desired contradiction and Lemma 3.1 will follow.

LEMMA 3.2. *Let $q = 2^n + 1$ be a Fermat prime. If m is an integer such that $1 \leq m \leq n$, then, for $\ell \geq 2$, there exist no positive integers r which satisfy the equality $r^\ell - 1 = 2^m q$.*

PROOF. Suppose the lemma is false and let r be a positive integer which satisfies the equality in the lemma. Then r is odd and

$$2^m q = (r-1)(r^{\ell-1} + r^{\ell-2} + \cdots + r + 1).$$

We first show that q does not divide $r-1$. In fact, if $q|(r-1)$ then $r > q$ and

$$(r^{\ell-1} + r^{\ell-2} + \cdots + r + 1) \mid 2^m;$$

but

$$r < r^{\ell-1} + r^{\ell-2} + \cdots + r + 1,$$

and so $r \leq 2^n = q - 1 < q$, a contradiction. Hence we may write

$$r - 1 = 2^a, \quad r^{\ell-1} + r^{\ell-2} + \cdots + r + 1 = 2^b q,$$

where $a + b = n$. We note that $a \neq 0$ because r is odd. We now show that $b \neq 0$. Suppose otherwise. Then

$$r^{\ell-1} + r^{\ell-2} + \cdots + r + 1 = q,$$

and so

$$r|(q-1).$$

This is impossible because r is odd and $q - 1 = 2^n$. Therefore $r^{\ell-1} + r^{\ell-2} + \cdots + r + 1$ is an even integer, which forces ℓ to be even, so that

$$(r^2 - 1) \mid (r^\ell - 1),$$

and

$$(r+1)|(r^{\ell-1} + r^{\ell-2} + \cdots + r + 1).$$

Therefore $r + 1$ is a divisor of $2^b q$. From this we have $a = 1$. For, if $a > 1$ then $2^{a-1} + 1$ would be odd, and so noting that

$$r + 1 = 2^a + 2 = 2(2^{a-1} + 1)|2^b q,$$

we have

$$2^{a-1} + 1 = q.$$

But

$$2^{a-1} + 1 < 2^n + 1 = q,$$

a contradiction. This proves that $a = 1$. Hence $r = 3$. If $\ell = 2$ then $r^\ell - 1 = 3^2 - 1 = 2^3$. This is not the case. Therefore $\ell > 2$. We distinguish two cases:

https://doi.org/10.4153/CJM-1991-034-2 Published online by Cambridge University Press

CASE 1. $\ell \not\equiv 0 \pmod 4$. Since ℓ is even, we have

$$3^{\ell} - 1 = (3^2 - 1)(3^{\ell-2} + 3^{\ell-4} + \cdots + 3^2 + 1).$$

But $3^{\ell-2} + 3^{\ell-4} + \cdots + 3^2 + 1$ is odd because it is the sum of $\ell/2$ odd numbers and $\ell/2$ is odd. Hence we have

$$3^{\ell-2} + 3^{\ell-4} + \cdots + 3^2 + 1 = q,$$

and so

$$3^{\ell-2} + 3^{\ell-4} + \cdots + 3^2 = q - 1 = 2^n.$$

This is impossible.

CASE 2. $\ell \equiv 0 \pmod 4$. Because $3^{\ell} - 1$ is divisible by $3^4 - 1 = 2^4 \cdot 5$, we have $m \geq 4$ and $q = 5$. But then $n = 2$. This contradicts our assumption that $m \leq n$. Thus we complete the proof of Lemma 3.2, and so Lemma 3.1 is proved.

PROPOSITION 3.3. *If G is p-nilpotent and $O_{p'}(G)$ is nonabelian then part (3) or (4) of Theorem B holds.*

PROOF. Set $V = O_{p'}(G)$. By Lemma 3.1 and our assumption, V is a nonabelian q-group for some prime q distinct from p. Hence V possesses a proper subgroup V_0 which is normal in G. Since $r_{p'}(G) = 3$, G must act transitively on $V_0^{\#}$, and hence we see that V_0 is a unique such subgroup. We therefore have

$$V_0 = \Phi(V) = Z(V),$$

where $\Phi(V)$ and $Z(V)$ are the Frattini subgroup and the center of V respectively. Further, since $r_{p'}(G/V_0) = 2$ Theorem A applies to G/V_0.

STEP 1. (b) of Theorem A is not applicable and if G/V_0 is type (a) or (c) then part (3) of Theorem B holds.

PROOF. Suppose that G/V_0 is type (a), (b) or (c). Then $p = 2$ and G/V_0 is isomorphic to one of the following groups:

$$E_{3^2} \rtimes \mathbb{Z}_8, \quad E_{3^2} \rtimes Q_8, \quad E_{3^2} \rtimes S_{16}.$$

Hence $q = 3$ and $V/V_0 \simeq E_{3^2}$. Since G acts transitively on $V_0^{\#}$, and $V_0 = Z(V)$, $|V_0^{\#}|$ is a divisor of the order of a Sylow 2-subgroup of G. Hence noting that V_0 is a 3-group, we have $|V_0^{\#}| = 2$ or 8. This implies that V_0 is isomorphic to $\mathbb{Z}_3$ or E_{3^2}. We argue that $V_0 \simeq \mathbb{Z}_3$. So assume that $V_0 \simeq E_{3^2}$ and let u be an element of $V - V_0$. Then $|C_V(u)| = 3^3$ because $V_0 = Z(V)$, and hence $|C_u| \leq 3 \cdot 16 = 48$. Therefore noting that the 2-regular classes of G are C_1, $V_0^{\#}$ and $C_u = V - V_0$, we have

$$3^4 = |V| = |V_0| + |C_u| \leq 9 + 48 < 3^4,$$

a contradiction. Thus we have $V_0 \simeq \mathbb{Z}_3$, which implies that V is a nonabelian 3-group of order 3^3. It is well known that such a group is isomorphic to $M(3)$ or $M_3(3)$ ([1, Theorem 5.5.1]). We now show that $V \simeq M(3)$. Suppose otherwise. Then there are elements

u, v in $V - V_0$ with $|u| = 3$, $|v| = 9$. Therefore G does not act transitively on $V - V_0$, and so G has at least four 2-regular classes, contrary to our assumption. Thus we have $V \simeq M(3)$. Since $\mathrm{Aut}\, M(3) \simeq E_{3^2} \rtimes \mathrm{GL}(2,3)$ ([4, Lemma 1.2]), we may regard a Sylow 2-subgroup P of G as a subgroup of $\mathrm{GL}(2,3)$. Because V is given by

$$V = \langle a, b, c \mid a^3 = b^3 = c^3 = 1,\ b^a = bc,\ c^a = c,\ c^b = c \rangle,$$

it is generated by a and b. Let $x = \begin{pmatrix} m & n \\ u & v \end{pmatrix}$ be an element of P. Then the action of x on V is given by

$$a^x = a^m b^n, \quad b^x = a^u b^v.$$

From this we have $c^x = c^{mv-nu}$. But $Z(V) = \langle c \rangle$, and so P acts transitively on $\langle c \rangle^\#$. Hence there exists an element x of P such that $c^x = c^{-1}$, which implies that P is not contained in $SL(2,3)$. Thus we have $P \simeq \mathbb{Z}_8$ or S_{16}, proving Step 1.

STEP 2. (d) of Theorem A is not applicable.

PROOF. Assume by way of contradiction that G/V_0 is type (d). Then $p = 2$ and $G/V_0 \simeq \mathbb{Z}_q \rtimes \mathbb{Z}_{2^n}$, where $q = 2^n + 1$ is a Fermat prime, and so V/V_0 is a cyclic group of order q. As $V_0 = \Phi(V)$, this implies that V is a cyclic group, which contradicts our assumption.

STEP 3. If G/V_0 is type (e) then part (4) of Theorem B holds.

PROOF. In this case, $p = 2^n - 1$ is a Mersenne prime and $G/V_0 \simeq E_{2^n} \rtimes \mathbb{Z}_p$. Hence $V/V_0 \simeq E_{2^n}$ and $V_0 = \Phi(V) = Z(V)$ is an elementary abelian 2-group. At first we show that $V_0 \subseteq Z(G)$. Suppose otherwise and choose v in V_0 so that $v \notin Z(G)$. Then $|V_0^\#| = |C_v| = p$, and so $|V_0| = p + 1 = 2^n$. Therefore

$$|V - V_0| = 2^{2n} - 2^n = 2^n(2^n - 1). \tag{3.4}$$

Now choose u in V to be of order 4. Then $C_G(u) \supseteq \langle V_0, u \rangle$, and so $|C_G(u)| = 2^k$ for some k, $k > n$. Therefore we have $|V - V_0| = |C_u| = 2^{2n-k}p$ because G acts transitively on $V - V_0$, which implies that

$$|V - V_0| = 2^{2n-k}p = 2^{2n-k}(2^n - 1) < 2^n(2^n - 1).$$

This contradicts (3.4). Hence $V_0 \subseteq Z(G)$. But G acts transitively on $V_0^\#$. Hence we have $|V_0| = 2$. This implies that V is an extra special 2-group of order 2^{n+1}. Therefore n must be even. But, as $2^n - 1$ is a Mersenne prime, n is a prime number. Hence we have $n = 2$. Thus it follows that $p = 3$ and V is a nonabelian 2-group of order 8. Therefore $V \simeq Q_8$ or D_8. Further $G/V(\simeq \mathbb{Z}_3)$ is contained isomorphically in $\mathrm{Aut}\, V$. But, as is well known, $\mathrm{Aut}\, D_8$ is a 2-group. We therefore have $V \simeq Q_8$, proving Step 3. Thus we complete the proof of Proposition 3.3.

4. **Proof of parts (5) through (8) of Theorem B.** In this section, we consider the case where G is p-nilpotent and $V = O_{p'}(G)$ is abelian. We saw in Lemma 3.1 that V is a q-group for some prime $q \neq p$. At first we prove the following:

LEMMA 4.1. *V possesses no nontrivial proper subgroups which are normal in G. In particular, V is an elementary abelian q-group.*

PROOF. Suppose the lemma is false and let $V_0 \neq \langle 1 \rangle$ be a normal subgroup of G which is properly contained in V. Then C_1, $V_0^{\#}$, $V - V_0$ are the p-regular classes in G. Clearly $|V - V_0|$ is divisible by q. On the other hand $|V - V_0| = |G : C_G(v)|$, where v is an element of $V - V_0$. But $C_G(v) \supseteq V$. Hence $|G : C_G(v)|$ is a power of p, a contradiction. Thus the lemma is proved.

We now assume V is of order q^{ℓ}, that is, $V \simeq E_{q^{\ell}}$ and denote by P a Sylow p-subgroup of G. Then $G \simeq E_{q^{\ell}} \rtimes P$. As $r_{p'}(G) = 3$, $V^{\#}$ consists of two conjugacy classes in G. We denote these conjugacy classes by Δ_1 and Δ_2, and set $|\Delta_1| = p^m$, $|\Delta_2| = p^n$, $m \leq n$. Then we have

$$q^{\ell} = 1 + p^m + p^n.$$

PROPOSITION 4.2. *Under the above notation, if $m = n$ then part (5), (6), (7) or (8) of Theorem B holds.*

PROOF. We distinguish two cases:

CASE 1. $p = 2$. We shall show that part (5) or (6) of Theorem B holds. Since $q^{\ell} - 1 = 2^{n+1}$, by [7, Lemma 19.3], one of the following holds:

(i) $q = 3$, $\ell = 2$ and $n = 2$.

(ii) $\ell = 1$, that is, $q = 2^{n+1} + 1$ is a Fermat prime.

Suppose first that (i) holds. Then we have $|\Delta_1| = |\Delta_2| = 4$, and so $|P|$ is divisible by 4. But P is contained isomorphically in $\mathrm{GL}(2, 3)$ because $V \simeq E_{3^2}$. Therefore $|P| = 4$, 8 or 16. Suppose $|P| = 4$. Then P acts semiregularly on $V^{\#}$, and hence $P \simeq \mathbb{Z}_4$. On the other hand, if $|P| = 8$ or 16 then $P \simeq \mathbb{Z}_8$, Q_8, D_8 or S_{16}. But if $P \simeq \mathbb{Z}_8$, Q_8 or S_{16} then P acts transitively on $V^{\#}$. This contradicts our assumption. Hence P must be isomorphic to D_8. Therefore, in this case, (5) holds. Suppose next that (ii) holds. Then $|\Delta_1| = |\Delta_2| = 2^n$, and so $|P|$ is divisible by 2^n. Further, as $V \simeq \mathbb{Z}_q$, we have $\mathrm{Aut}\, V \simeq \mathbb{Z}_{q-1} = \mathbb{Z}_{2^{n+1}}$. Hence $|P| = 2^n$ or 2^{n+1}. But if $|P| = 2^{n+1}$ then P acts transitively on $V^{\#}$, which contradicts our assumption. Thus we have $P \simeq \mathbb{Z}_{2^n}$, and (6) follows.

CASE 2. p is odd. We shall show that part (7) or (8) of Theorem B holds. Since P acts faithfully on V and acts $\frac{1}{2}$-transitively on $V^{\#}$, by [7, Theorem 19.6], P is cyclic and G is a Frobenius group. From the equality $q^{\ell} - 1 = 2p^n$, it follows at once that if $q = 3$ then $\ell \geq 2$. To complete the proof, we must show the converse implication. This will be proved in the following lemma.

LEMMA 4.3. *Let p be an odd prime and q a positive odd integer. If p, q satisfy the relation $q^{\ell} - 1 = 2p^n$, where $\ell \geq 2$, then $q = 3$.*

https://doi.org/10.4153/CJM-1991-034-2 Published online by Cambridge University Press

PROOF. Because of the equality

$$2p^n = q^\ell - 1 = (q-1)(q^{\ell-1} + q^{\ell-2} + \cdots + q + 1),$$

we may write

$$q - 1 = 2p^a, \quad q^{\ell-1} + q^{\ell-2} + \cdots + q + 1 = p^b,$$

where $a + b = n$. Hence $q^{\ell-1} + q^{\ell-2} + \cdots + q + 1$ is odd. But this is the sum of ℓ odd numbers. Hence ℓ is odd. We now set $\ell = 2k + 1$ and prove the lemma by induction on k. If $k = 1$, then $\ell = 3$ and

$$q - 1 = 2p^a, \quad q^2 + q + 1 = p^b.$$

We have to show that $a = 0$. Suppose otherwise. Then $p | (q-1)$, so that $p | (q^2 - 1)$. Hence we have

$$0 \equiv q^2 + q + 1 = (q^2 - 1) + (q - 1) + 3 \equiv 3 \pmod{p},$$

which implies that $p = 3$. Therefore $q = 2 \cdot 3^a + 1$, and so

$$3^b = q^2 + q + 1 = 3(4 \cdot 3^{2a-1} + 2 \cdot 3^a + 1).$$

Thus we have

$$4 \cdot 3^{2a-1} + 2 \cdot 3^a = 3^{b-1} - 1.$$

The left hand side of the above equality is divisible by 3, but the right hand side is not divisible by 3. This contradiction shows that $a = 0$ and hence $q = 3$. This proves the lemma for $k = 1$. Suppose next that $k > 1$ and that the lemma holds for $\ell' = 2k' + 1$ where $k' < k$. Assume by way of contradiction that $q > 3$, namely, $a \geq 1$. Then $p | (q-1)$, and so $p | (q^i - 1)$ for all $i \geq 1$. Therefore, for every positive integer e,

$$q^e + q^{e-1} + \cdots + q + 1 \equiv e + 1 \pmod{p}.$$

In particular,

$$0 \equiv q^{\ell-1} + q^{\ell-2} + \cdots + q + 1 \equiv \ell \pmod{p},$$

which forces $p | \ell$. We write $\ell = sp$. We now show that $s = 1$. Suppose otherwise. Then $q^p - 1$, being a proper divisor of $q^\ell - 1$, is expressible in the form $2p^c$, where $0 < c < n$. Therefore, by the induction hypothesis, we get $q = 3$, which contradicts our assumption. This proves that $s = 1$, namely, $\ell = p$. As $q = 2p^a + 1$, we have

$$\begin{aligned} p^b &= q^{p-1} + q^{p-2} + \cdots + q + 1 \\ &= (2p^a + 1)^{p-1} + (2p^a + 1)^{p-2} + \cdots + (2p^a + 1) + 1. \end{aligned}$$

It is easy to see that the above is written in the form

$$A(2p^a)^2 + \big(p(p-1)/2\big)2p^a + p,$$

where A is a positive integer. Hence

$$p^b = 4Ap^{2a} + (p-1)p^{a+1} + p.$$

But the right hand side of the above equality is not a power of p, and we reach a contradiction. This completes the proof of Lemma 4.3, and so Proposition 4.2 is proved.

https://doi.org/10.4153/CJM-1991-034-2 Published online by Cambridge University Press

5. **Proof of parts (9) and (10) of Theorem B.** Suppose that G is a p-nilpotent group and $V = O_{p'}(G)$ is abelian. We saw in Lemma 4.1 that V is an elementary abelian q-group. Suppose now that V is of order q^{ℓ}. In the preceding section, we determined the structure of G for the case that two p-regular classes Δ_1 and Δ_2 have the same cardinality. In this section, we consider the case where $|\Delta_1| = p^m < |\Delta_2| = p^n$. Our result which will be proved in this section is as follows:

PROPOSITION 5.1. *If $m < n$ then part (9) or (10) of Theorem B holds.*

First of all we prove the following

LEMMA 5.2. *Let $v \in V^{\#}$. Then every element of $\langle v\rangle^{\#}$ is conjugate to v in G.*

PROOF. Supppose the lemma is false and choose u in $\langle v\rangle^{\#}$ to be not conjugate to v. As $r_{p'}(G) = 3$, C_1, C_u, C_v are all p-regular classes in G. Because $u \in \langle v\rangle^{\#}$, $C_G(u) = C_G(v)$, and so $|C_u| = |C_v|$, which contradicts our assumption that $m < n$. Thus the result follows.

By making use of the preceding lemma, we verify the following

LEMMA 5.3. *The following hold:*
(1) $p = 2$.
(2) $\ell(q-1) \leq p^m = 2^m$.
(3) q is a Fermat prime.

PROOF. (1) Let $v \in V^{\#}$. Because $|V| = q^{\ell} = 1 + p^m + p^n$, clearly q is odd. Let P be a Sylow p-subgroup of G. By Lemma 5.2, we can choose x in P so that $v^x = v^{-1}$. Clearly x has even order. Hence P is a 2-group, proving (1).

(2) From Lemma 5.2, it follows that $C_v \cup \{1\}$ is a union of cyclic subgroups of V, and consequently $|C_v|$ is a multiple of $|\langle v\rangle^{\#}| = q-1$. Further, as $\langle C_v\rangle$ is a normal subgroup of G, we have $\langle C_v\rangle = V$ by Lemma 4.1. This shows that C_v contains a set of generators of V. Thus we have $|C_v| \geq \ell(q-1)$, and hence we have $2^m = |\Delta_1| \geq \ell(q-1)$, proving (2).

(3) We saw in the proof of (2) that $q-1$ is a divisor of $|\Delta_1|$. But $|\Delta_1|$ is a power of 2. Hence $q-1$ is a power of 2, proving (3).

LEMMA 5.4. *Let q be a positive integer of the form $2^e + 1$. Suppose that q satisfies the equality $q^{\ell} - 1 = 2^m + 2^n$, where $0 < m < n$ and $2^e \ell \leq 2^m$. Then one of the following holds:*
(1) $q = 3$ *and* $\ell = 4$.
(2) $q \neq 3$ *and* $\ell = 2$.

To prove this lemma we need some number-theoretical lemmas.

LEMMA 5.5. *Let s be a positive integer and let $2^a (a \geq 0)$ be the 2-part of s, that is, the highest power of 2 dividing s. Then the following hold:*
(1) If s is odd then $2^2 \| (3^s + 1)$ *and* $2 \| (3^s - 1)$.
(2) If s is even then $2 \| (3^s + 1)$ *and* $2^{a+2} \| (3^s - 1)$.

https://doi.org/10.4153/CJM-1991-034-2 Published online by Cambridge University Press

(3) *If q is an integer of the form 2^e+1 with $e > 1$ then $2 \| (q^s+1)$ and $2^{e+a} \| (q^s-1)$.*

PROOF. (1) This is trivial for $s=1$. If $s>1$ we have

$$\begin{aligned} 3^s+1 &= (2+1)^s+1 \\ &\equiv \big(s(s-1)/2\big)4+2s+2 \pmod 8, \end{aligned}$$

and so

$$3^s+1 \equiv 2(s^2+1) \pmod 8.$$

But $2 \| (s^2+1)$ because s is odd. Thus it follows at once that $2^2 \| (3^s+1)$. Further the equality

$$3^s-1 = (3-1)(3^{s-1}+3^{s-2}+\cdots+3+1)$$

implies that $2 \| (3^s-1)$ because $3^{s-1}+3^{s-2}+\cdots+3+1$ is odd. Thus (1) is proved.

(2) Suppose that s is even. Since $3^s+1=(2+1)^s+1$, we have

$$3^s+1 \equiv 2(s+1) \pmod 4.$$

As $s+1$ is odd, we get at once $2 \| (3^s+1)$. Next, we show $2^{a+2} \| (3^s-1)$ by induction on a. Let σ be the odd part of s, so that $s=2^a\sigma$. If $a=1$,

$$3^s-1 = 3^{2\sigma}-1 = (3^\sigma-1)(3^\sigma+1).$$

Hence, by (1), we have $2^3 \| (3^s-1)$, proving the first step of induction. Suppose next $a>1$. We already know that $2 \| (3^{2^{a-1}\sigma}+1)$. Hence from the equality

$$3^{2^a\sigma}-1 = (3^{2^{a-1}\sigma}-1)(3^{2^{a-1}\sigma}+1),$$

we get $2^{a+2} \| (3^{2^a\sigma}-1)$ by the induction hypothesis. Thus (2) is proved.

(3) Since $q^s+1=(2^e+1)^s+1 \equiv 2 \pmod{2^e}$, it follows at once that $2 \| (q^s+1)$. We next prove $2^{e+a} \| (q^s-1)$ by induction on a. If $a=0$ then from the equality

$$q^s-1 = (q-1)(q^{s-1}+q^{s-2}+\cdots+q+1),$$

we have $2^e \| (q^s-1)$ because $q^{s-1}+q^{s-2}+\cdots+q+1$ is odd. Suppose now $a>0$ and let σ be the odd part of s. As $2 \| (q^{2^{a-1}\sigma}+1)$, from the equality

$$q^{2^a\sigma}-1 = (q^{2^{a-1}\sigma}-1)(q^{2^{a-1}\sigma}+1)$$

and the induction hypothesis it follows that $2^{e+a} \| (q^{2^a\sigma}-1)$. Thus (3) is proved.

Let k be a positive integer. By the preceding lemma, the 2-part of $3^{2^k}-1$ is 2^{k+2} and the 2-part of $3^{2^k}+1$ is 2. Further, if q is an integer of the form 2^e+1 with $e>1$ then the 2-part of $q^{2^k}-1$ is 2^{e+k} and the 2-part of $q^{2^k}+1$ is 2. Concerning the odd parts of these numbers we have the following

LEMMA 5.6. *(1) Let s, t be the odd parts of* $3^{2^k}-1$ *and* $3^{2^k}+1$ *respectively. Then*

(a) $t-1=2^{k+1}s$, *and*

(b) if $k\geq 2$, $2^2\|(s-1)$.

(2) Let q be an integer of the form 2^e+1 *with* $e>1$ *and let u, v be the odd parts of* $q^{2^k}-1$ *and* $q^{2^k}+1$ *respectively. Then*

(a) $v-1=2^{e+k-1}u$, *and*

(b) $2^{e-1}\|(u-1)$.

PROOF. (1) Write $t-1=2^a\tau$, where τ is odd. Then

$$3^{2^k}+1=2t=2^{a+1}\tau+2,$$

which implies that

$$3^{2^k}-1=2^{a+1}\tau.$$

Thus we have $a=k+1$ and $\tau=s$, proving (a). To prove (b) we use induction on k. If $k=2$,

$$3^{2^k}-1=3^4-1=2^4\cdot 5.$$

Hence $s=5$. Thus (b) holds for $k=2$. Now let $k>2$ and set

$$3^{2^{k-1}}-1=2^{k+1}s',\quad 3^{2^{k-1}}+1=2t',$$

where s' and t' are odd. Then

$$3^{2^k}-1=(3^{2^{k-1}}-1)(3^{2^{k-1}}+1)=2^{k+2}s't'.$$

Hence $s=s't'$. We note that $t'-1=2^ks'$ by (a), and $s'-1=2^2\delta$, δ odd, by the induction hypothesis. Therefore

$$\begin{aligned} s-1&=s't'-1\\ &=2^{k+2}s'\delta+2^ks'+4\delta\\ &=4(2^ks'\delta+2^{k-2}s'+\delta), \end{aligned}$$

which implies that $2^2\|(s-1)$. Hence (b) holds for every $k\geq 2$.

We can prove (2) by an argument wholly analogous to the proof of (1), and we omit the proof.

LEMMA 5.7. *Let s and t be odd integers greater than 1. If* $st-1$ *is a power of 2, then the 2-part of* $s-1$ *coincides with that of* $t-1$.

PROOF. Write $s-1=2^a\sigma$, $t-1=2^b\tau$, where σ and τ are odd. Assume by way of contradiction that $a\neq b$. Without loss we may assume $a>b$. We set $st-1=2^\ell$. Then

$$2^\ell+1=st=(2^a\sigma+1)(2^b\tau+1),$$

and so

$$2^{a+b}\sigma\tau+2^a\sigma+2^b\tau=2^\ell.$$

Thus we have

$$2^a\sigma\tau+2^{a-b}\sigma+\tau=2^{\ell-b}.$$

This is impossible and the result follows.

https://doi.org/10.4153/CJM-1991-034-2 Published online by Cambridge University Press

LEMMA 5.8. *Let k be a positive integer and let q be an integer of the form 2^e+1 with $e > 1$.*

(1) $3^{2^k}-1$ is expressible as a sum 2^m+2^n for some m, n with $m < n$ only when $k = 2$.

(2) $q^{2^k}-1$ is expressible as a sum 2^m+2^n for some m, n with $m < n$ only when $k = 1$.

PROOF. (1) Suppose that $3^{2^k}-1$ is expressible as in the form stated in the lemma. Then it is trivial that $k \geq 2$. When $k = 2$ we have in fact

$$3^{2^k}-1 = 3^4-1 = 2^4+2^6.$$

Now suppose $k > 2$. By Lemma 5.5, we may write

$$3^{2^{k-1}}-1 = 2^{k+1}s, \quad 3^{2^{k-1}}+1 = 2t,$$

where s and t are odd. Then

$$3^{2^k}-1 = (3^{2^{k-1}}-1)(3^{2^{k-1}}+1) = 2^{k+2}st.$$

But $3^{2^k}-1 = 2^m(1+2^{n-m})$. Hence we have

$$st = 1+2^{n-m}.$$

As $k > 2$, $s \neq 1$; and it is trivial that $t \neq 1$. Therefore, by Lemma 5.7, the 2-part of $s-1$ coincides with that of $t-1$. Thus we have $2^2 = 2^k$ by Lemma 5.6, which contradicts our assumption $k > 2$. Thus (1) is proved.

We can prove (2) by an argument analogous to the proof of (1), and we omit the proof.

Now we are ready to prove Lemma 5.4.

PROOF OF LEMMA 5.4. To our end it suffices to prove that ℓ is a power of 2. Indeed if ℓ is a power of 2 then the result follows at once from Lemma 5.8. We now set $\ell = 2^a s$, s odd. We must prove that $a > 0$ and $s = 1$. Suppose first $a = 0$, that is, ℓ is odd. Then $2^e \| (q^\ell-1)$ by Lemma 5.5. This implies that $e = m$. Therefore we have $2^m\ell = 2^e\ell \leq 2^m$. This forces $\ell = 1$. But then $q^\ell - 1 = q-1 = 2^e$, which contradicts our assumption. We therefore obtain $a \neq 0$. We next prove $s = 1$. We distinguish two cases:

CASE 1. $e = 1$, that is, $q = 3$. By Lemma 5.5, we have $3^\ell - 1 = 1 = 2^{a+2}\sigma$, where σ is odd. Therefore

$$2^{a+2}\sigma = 2^m+2^n = 2^m(1+2^{n-m}),$$

which implies that $a+2 = m$. But then

$$2^{a+2} = 2^m \geq 2\ell = 2^{a+1}s,$$

and so $s \leq 2$. Thus we get $s = 1$ because s is odd.

CASE 2. $e > 1$. By Lemma 5.5, $2^{e+a} \| (q^\ell-1)$. From this it follows that $e+a = m$. Hence we have

$$2^{e+a} = 2^m \geq 2^e\ell = 2^{e+a}s.$$

https://doi.org/10.4153/CJM-1991-034-2 Published online by Cambridge University Press

This forces $s = 1$, and the proof is complete.

We are now in a position to prove Proposition 5.1.

PROOF OF PROPOSITION 5.1. In Lemmas 5.3, 5.4, we proved that $p = 2$ and one of the following holds:

(i) $V \simeq E_{3^4}$.

(ii) $V \simeq E_{q^2}$, where $q = 2^e + 1$ is a Fermat prime greater than 3.

We distinguish two cases:

CASE 1. $V \simeq E_{3^4}$. We shall show that part (9) of Theorem B holds. We may regard a Sylow 2-subgroup P of G as a subgroup of a Sylow 2-subgroup Q of $\mathrm{GL}(4,3)$. As $3^4 - 1 = 2^4 + 2^6$, $|\Delta_1| = 2^4$ and $|\Delta_2| = 2^6$. Hence $|P| \geq 2^6$. Let D be a Sylow 2-subgroup of $\mathrm{GL}(2,3)$ and set

$$U = \left\{ \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix} \mid c, d \in D \right\}.$$

Then U is a 2-group of order 2^8. Set

$$x = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

Then $U \rtimes \langle x \rangle$ has order 2^9, and so we may identify Q with $U \rtimes \langle x \rangle$. Write $V = V_1 \times V_2$ and $V_1 = \langle x_1 \rangle \times \langle x_2 \rangle$, $V_2 = \langle y_1 \rangle \times \langle y_2 \rangle$. We may assume that U acts on each of V_1 and V_2. From the form of Q, we have $C_{x_1} \subseteq V_1^\# \cup V_2^\#$. But then

$$2^4 = |\Delta_1| \leq |C_{x_1}| \leq |V_1^\# \cup V_2^\#| = 2^4.$$

We therefore have

$$\Delta_1 = C_{x_1} = V_1^\# \cup V_2^\#, \quad \Delta_2 = C_{x_1 y_1}.$$

We now claim that P is not contained in U. Indeed, if $P \subseteq U$, then $C_{x_1} \subseteq V_1^\#$, a contradiction. Hence we have $|P : P \cap U| = 2$ because $|Q : U| = 2$. Therefore we can choose h in $P - U$ so that $P = \langle P \cap U, h \rangle$. Let $g = \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix}$ lie in $P \cap U$. As h is of the form $\begin{pmatrix} 0 & a \\ b & 0 \end{pmatrix}$, $a, b \in D$, we have $g^h = \begin{pmatrix} d^b & 0 \\ 0 & c^a \end{pmatrix}$. This shows that the groups

$$U_1 = \left\{ c \mid \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix} \in P \cap U \right\}, \quad U_2 = \left\{ d \mid \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix} \in P \cap U \right\}$$

are isomorphic subgroups of D. But D is a semi-dihedral group S_{16}, and so we may regard $P \cap U$ as a subgroup of $S_{16} \times S_{16}$. Thus we see by the above that $P \cap U$ is a subdirect product $H_1 \times_s H_2$ of isomorphic subgroups H_1 and H_2 of S_{16}. Moreover, as $P \cap U$ acts transitively on $V_1^\#$, U_1 is isomorphic to $\mathbb{Z}_8$, Q_8 or S_{16}. Hence H_1 and H_2 are both isomorphic to $\mathbb{Z}_8$, Q_8 or S_{16}. Thus (9) follows because $|P| \geq 2^6$.

We show now that this situation does in fact occur. Let $g = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$, $h = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ be elements of GL(2, 3). Then $g^8 = h^2 = I$, the identity matrix, and $g^h = g^3$. Therefore $L = \langle g, h \rangle$ is a semi-dihedral group of order 16, that is, L is a Sylow 2-subgroup of GL(2, 3). Further it is easy to check that $M = \langle g^2, gh \rangle$ is a quaternion group of order 8. Now let $\Delta_{\langle g \rangle}$ and Δ_M be the subgroups of GL(4, 3) given by

$$\Delta_{\langle g \rangle} = \left\{ \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} \,\middle|\, x \in \langle g \rangle \right\}, \quad \Delta_M = \left\{ \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} \,\middle|\, x \in M \right\}.$$

Set

$$R_1 = \left\langle \Delta_{\langle g \rangle}, \begin{pmatrix} g^2 & 0 \\ 0 & I \end{pmatrix} \right\rangle, \quad R_2 = \left\langle \Delta_M, \begin{pmatrix} g^2 & 0 \\ 0 & I \end{pmatrix} \right\rangle.$$

Then each of R_1 and R_2 has order 2^5. Further R_1 is a subdirect product of $\langle g \rangle$ and $\langle g \rangle$; and R_2 is a subdirect product of M and M. By a direct computation, we see that $\begin{pmatrix} h & 0 \\ 0 & gh \end{pmatrix}$ normalizes the cyclic group generated by $\begin{pmatrix} g & 0 \\ 0 & g^3 \end{pmatrix}$, and the group

$$R_3 = \left\langle \begin{pmatrix} g & 0 \\ 0 & g^3 \end{pmatrix}, \begin{pmatrix} h & 0 \\ 0 & gh \end{pmatrix} \right\rangle$$

has order 2^5. It is easy to check that R_3 is a subdirect product of L and L. Therefore R_1, R_2 and R_3 are groups of type (a) in (9). We now set

$$P_1 = \left\langle R_1, \begin{pmatrix} 0 & g \\ I & 0 \end{pmatrix} \right\rangle, \quad P_2 = \left\langle R_2, \begin{pmatrix} 0 & gh \\ I & 0 \end{pmatrix} \right\rangle, \quad P_3 = \left\langle R_3, \begin{pmatrix} 0 & g \\ g & 0 \end{pmatrix} \right\rangle.$$

Then we have $|P_i : R_i| = 2$ for every i, $1 \leq i \leq 3$. Let P_i act on an abelian group V of type (3, 3, 3, 3). Then one can check directly that P_i has three orbits. This shows that $r_{2'}(V \rtimes P_i) = 3$.

We next show the existence of groups of type (b). Clearly the groups

$$R_4 = \left\{ \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} \,\middle|\, x, y \in \langle g \rangle \right\} \text{ and } R_5 = \left\{ \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} \,\middle|\, x, y \in M \right\}$$

are isomorphic to $\mathbb{Z}_8 \times \mathbb{Z}_8$ and $Q_8 \times Q_8$ respectively. Now set

$$\Delta_L = \left\{ \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} \,\middle|\, x \in L \right\}.$$

Then the group

$$R_6 = \left\langle \Delta_L, \begin{pmatrix} g^2 & 0 \\ 0 & I \end{pmatrix} \right\rangle$$

is a subdirect product of L and L and its order is 2^6. Therefore R_4, R_5 and R_6 are groups of type (b). Set

$$P_i = \left\langle R_i, \begin{pmatrix} 0 & g \\ I & 0 \end{pmatrix} \right\rangle, \quad i = 4, 5, 6.$$

Then $|P_i : R_i| = 2$ and one can check directly that an abelian group V of type $(3,3,3,3)$ is a union of three orbits under the action of P_i. Therefore we have $r_{2'}(V \rtimes P_i) = 3$.

A group of type (c) is given as follows. Set

$$R_7 = \left\langle \Delta_L, \begin{pmatrix} g & 0 \\ 0 & I \end{pmatrix} \right\rangle.$$

Then R_7 is a subdirect product of L and L and has order 2^7, that is, R_7 is a group of type (c). Setting

$$P_7 = \left\langle R_7, \begin{pmatrix} 0 & g \\ I & 0 \end{pmatrix} \right\rangle,$$

one can check that $|P_7 : R_7| = 2$ and an abelian group V of type $(3,3,3,3)$ is a union of three orbits under the action of P_7, and hence $r_{2'}(V \rtimes P_7) = 3$.

Finally, we give a group of type (d). Clearly the group

$$R_8 = \left\{ \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} \,\middle|\, x, y \in L \right\}$$

is isomorphic to $L \times L$ and hence this is a group of type (d). We note that the group

$$P_8 = \left\langle R_8, \begin{pmatrix} 0 & g \\ I & 0 \end{pmatrix} \right\rangle$$

is in fact a Sylow 2-subgroup of $\mathrm{GL}(4,3)$. It is easy to check that an abelian group V of type $(3,3,3,3)$ is a union of three orbits under the action of P_8. Therefore $r_{2'}(V \rtimes P_8) = 3$.

CASE 2. $V \simeq E_{q^2}$, where $q = 2^e + 1$ is a Fermat prime greater than 3. We shall show that part (10) of Theorem B holds. Since $q^2 - 1 = 2^{e+1} + 2^{2e}$, we have $m = e + 1$ and $n = 2e$. To our end, we need to find a Sylow 2-subgroup of $\mathrm{GL}(2,q)$. Clearly the group

$$\mathcal{T}_0(q) = \left\{ \begin{pmatrix} a & 0 \\ 0 & \pm a^{-1} \end{pmatrix}, \begin{pmatrix} 0 & a \\ \pm a^{-1} & 0 \end{pmatrix} \,\middle|\, 0 \neq a \in \mathrm{GF}(q) \right\}$$

has order $2^2(q-1) = 2^{e+2}$. Let γ be a generator of the multiplicative group of $\mathrm{GF}(q)$ and set $z = \begin{pmatrix} 1 & 0 \\ 0 & \gamma \end{pmatrix}$. Then $z^{2^{e-1}} \in \mathcal{T}_0(q)$ and so $Q = \langle \mathcal{T}_0(q), z \rangle$ has order 2^{2e+1}. Since $|\mathrm{GL}(2,q)| = q(2^{e-1}+1)2^{2e+1}$, Q is a Sylow 2-subgroup of $\mathrm{GL}(2,q)$. Setting

$$g = \begin{pmatrix} \gamma & 0 \\ 0 & \gamma^{-1} \end{pmatrix}, \quad s = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad t = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

we have $\mathcal{T}_0(q) = \big(\langle g \rangle \times \langle s \rangle\big) \rtimes \langle t \rangle$. Hence, noting that $s = z^{2^{e-1}} \in \langle z \rangle$, we see that Q is given by

$$Q = \big(\langle g \rangle \rtimes \langle t \rangle\big) \rtimes \langle z \rangle.$$

From this we see immediately that the commutator subgroup Q' of Q is equal to $\langle g \rangle$. Therefore Q/Q' is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_{2^e}$. We may regard a Sylow 2-subgroup P of

G as a subgroup of Q. But as $|P| \geq |\Delta_2| = 2^{2e}$, we have $|Q : P| \leq 2$. Suppose now $|Q : P| = 2$. Then, as $P \supseteq Q' = \langle g \rangle$, one of the following holds:

(i) $P = \langle g, t, z^2 \rangle = \langle \mathcal{T}_0(q), z^2 \rangle$.

(ii) $P = \langle g, z \rangle$.

(iii) $P = \langle g, tz \rangle$.

We now show that only case (iii) happens. So suppose first that (i) holds and let u, v be generators of V. Then we see immediately that Δ_1 is equal to $\langle u \rangle^{\#} \cup \langle v \rangle^{\#}$. Therefore $\Delta_2 = C_{uv}$. But t fixes uv. This is impossible because P must act regularly on Δ_2. On the other hand, if (ii) holds then clearly $\Delta_1 = \langle u \rangle^{\#}$, a contradiction. Thus P is a group of type (iii). In this case, as $tz = \begin{pmatrix} 0 & \gamma \\ 1 & 0 \end{pmatrix}$, we have

$$(tz)^i = \begin{cases} \begin{pmatrix} \gamma^k & 0 \\ 0 & \gamma^k \end{pmatrix} & \text{if } i = 2k, \\ \begin{pmatrix} 0 & \gamma^{k+1} \\ \gamma^k & 0 \end{pmatrix} & \text{if } i = 2k+1, \end{cases}$$

and so P is a group consisting of the matrices

$$\begin{pmatrix} a\gamma^k & 0 \\ 0 & a^{-1}\gamma^k \end{pmatrix}, \quad \begin{pmatrix} 0 & a\gamma^{k+1} \\ a^{-1}\gamma^k & 0 \end{pmatrix},$$

where $a \in \mathrm{GF}(q)$, $a \neq 0$ and $0 \leq k \leq 2^{e-1} - 1$. Therefore it follows at once that C_1, C_u and C_{uv} are the p-regular classes of G. Set $x = g$, $y = tz$. Then P is in fact a group given in (10)(b). Further it is clear that V is a union of three orbits under the action of Q and so the proof is complete.

6. **Proof of parts (11) and (12) of Theorem B.** In Sections 2 through 5, we proved that if G is either a p'-group or a p-nilpotent group then one of (1)–(10) in Theorem B holds. As remarked in Lemma 1.1, the p'-length of G is at most 2. Therefore, to complete the proof of Theorem B, it remains only to show the following:

PROPOSITION 6.1. *The case $G = O_{p'pp'}(G)$ does not occur.*

PROPOSITION 6.2. *If $G = O_{p'pp'p}(G)$ then part (11) or (12) of Theorem B holds.*

At first we prove Proposition 6.1.

PROOF OF PROPOSITION 6.1. Assume the proposition is false and let G be a group such that $G = O_{p'pp'}(G)$ and $r_{p'}(G) = 3$. Then we have $r_{p'}\big(G/O_{p'p}(G)\big) = 2$, and so $|G/O_{p'p}(G)| = 2$. This forces p to be odd. Set $V = O_{p'}(G)$. As $r_{p'}(G) = 3$, G acts transitively on $V^{\#}$, and so V is elementary abelian and has a complement, say T, in G ([2, Chap. VII, Lemma 15.4]). Further from $|T/O_p(T)| = 2$, it immediately follows that $V^{\#}$ is a union of at most two orbits under the action of $O_p(T)$, that is, $r_{p'}\big(O_{p'p}(G)\big) = 2$ or 3. We distinguish two cases:

CASE 1. $r_{p'}\big(O_{p'p}(G)\big) = 2$. In this case, Theorem A applies to $O_{p'p}(G)$. But, as p is odd, only (e) of the theorem is applicable. Hence V is a 2-group. Now let t be an involution of T. Then the p-regular classes of G are C_1, $V^{\#}$ and C_t. This implies that a Sylow 2-subgroup of G is of exponent 2, and so it is abelian, a contradiction.

CASE 2. $r_{p'}\big(O_{p'p}(G)\big) = 3$. Since p is odd and V is elementatry abelian, (7) and (8) of Theorem B apply to $O_{p'p}(G)$. If $O_{p'p}(G)$ is type (7), then V is a cyclic group. But then G/V is abelian, because G/V is contained isomorphically in Aut V, which is abelian. This is not the case. Suppose next $O_{p'p}(G)$ is type (8). Let P be a Sylow p-subgroup of T, so that $|T : P| = 2$. Let $v \in V^{\#}$. Clearly v is not inversed by any element of P. But T acts regularly on $V^{\#}$. We therefore can choose an involution t in $T - P$ so that $T = \langle P, t \rangle$ and $v^t = v^{-1}$ for every $v \in V^{\#}$. Then we have $v^{xt} = v^{tx}$ for every x in P, which shows that $xtx^{-1}t^{-1} \in C_T(v) = \langle 1 \rangle$. This shows that T is abelian, a contradiction. Thus Proposition 6.1 is proved.

We next prove Proposition 6.2.

PROOF OF PROPOSITION 6.2. Set $V = O_{p'}(G)$. As $r_{p'}(G) = 3$, G acts transitively on $V^{\#}$, and so V is an elementary abelian r-group for some prime $r \neq p$. By [2, Chap. VII, Lemma 15.4], V has a complement in G. We denote by T a complement of V and let W be a Hall p'-subgroup of T. Since $r_{p'}(G) = 3$, we have $r_{p'}\big(T/O_p(T)\big) = r_{p'}\big(G/O_{p'p}(G)\big) = 2$. Hence, by Theorem A, W is an elementary abelian q-group where q is either 2 or a Fermat prime. Clearly, the p-regular classes of G are C_1, $V^{\#}$ and C_w ($w \in W^{\#}$), and so the order of every element of $(VW)^{\#}$ is either q or r. We now claim that $q \neq r$. So assume $q = r$. Then VW is a nonabelian q-group of exponent q. Hence $q \neq 2$, and so q is a Fermat prime and $p = 2$ by Theorem A. Since the center $Z(VW)$ of VW is contained in V ([1, Theorem 6.3.3]), we see that $|V^{\#}|$ is a power of 2. This forces $|V|$ to be q or 3^2, that is, $V \simeq \mathbb{Z}_q$ or E_{3^2}. But if $V \simeq \mathbb{Z}_q$ then T is contained isomorphically in Aut $\mathbb{Z}_q$, and so T is abelian. This is not the case. Therefore $V \simeq E_{3^2}$. In this case, we have $T \simeq \mathrm{GL}(2,3)$. Because the nontrivial 2-regular classes of G are $V^{\#}$ and C_w, the set

$$\Delta_w = \{\, w^g \in VW \mid g \in G \}$$

coincides with $VW - V$. Hence $|\Delta_w| = 18$. Now let $g \in G$ and suppose $w^g \in VW$. Then it is clear that $g \in N_G(VW)$. Set $S = O_2(T)$ ($\simeq Q_8$). Then there is an involution s in G such that $T = \langle S, W, s \rangle$. Let t be an involution of S and v an element of $Z(VW)^{\#}$. Then $N = N_G(VW)$ and $C = C_N(w)$ are given by

$$N = \langle V, W, t, s \rangle, \quad C = \langle v, t \rangle.$$

Thus we have $|\Delta_w| = |N : C| = 6$. This contradicts the fact that $|\Delta_w| = 18$. This contradiction shows that $q \neq r$. Because every element of $(VW)^{\#}$ is either a q-element or an r-element, VW is a Frobenius group. Therefore W is a cyclic group, and so we have $|W| = q$. Hence, by Theorem A, $p = 2$ and $T/O_2(T) \simeq \mathbb{Z}_q \rtimes \mathbb{Z}_{2^n}$, where $q = 2^n + 1$. We set $S = O_2(T)$. Since T acts transitively on $V^{\#}$, S acts $\frac{1}{2}$-transitively on $V^{\#}$. Therefore, by [7, Theorem 19.6], one of the following holds:

(i) S is cyclic or generalized quaternion.

(ii) $|V| = r^2$, r is a Mersenne prime and S is dihedral or semi-dihedral.

https://doi.org/10.4153/CJM-1991-034-2 Published online by Cambridge University Press

(iii) $|V| = r^2$, r is a Fermat prime and $S \simeq \mathcal{T}_0(r)$.

(iv) $|V| = 3^4$, $S \simeq \mathcal{T}_0(3^2)$ or a central product of D_8 and Q_8.

Concerning part (iv), see also [7, p. 242] and [3, Theorem II]. We note that if S is cyclic, generalized quaternion of order greater than 8, dihedral, semi-dihedral or $\mathcal{T}_0(r)$ with $r = 2^\ell + 1$, then, with the exception of $\mathcal{T}_0(5)$, $\operatorname{Aut} S$ is an abelian group or a 2-group ([7, Theorem 9.1, Propositions 9.10, 19.7]). But $T/S = N_T(S)/C_T(S)$ is contained isomorphically in $\operatorname{Aut} S$ and T/S is neither an abelian group nor a 2-group. Hence we have one of the following possibilities:

(a) $S \simeq Q_8$.

(b) $V \simeq E_{5^2}$, $S \simeq \mathcal{T}_0(5)$.

(c) $V \simeq E_{3^4}$, S is a central product of D_8 and Q_8.

STEP 1. If case (a) holds then part (11) of Theorem B holds.

PROOF. As $\operatorname{Aut} Q_8 \simeq \Sigma_4$, $T/S \simeq \Sigma_3$. Hence $q = 3$ and $|V^\#| = 3 \cdot 8$ or $3 \cdot 16$, and so $V \simeq E_{5^2}$ or E_{7^2}. We now show that $V \simeq E_{7^2}$. Suppose otherwise and let P be a Sylow 2-subgroup of T. We distinguish two cases:

CASE 1. Suppose that P acts $\frac{1}{2}$-transitively on $V^\#$. Clearly P does not act semiregularly on $V^\#$, and so by [7, Theorem 19.6], P is isomorphic to $\mathcal{T}_0(5)$. Therefore $Z(P) \simeq \mathbb{Z}_4$; and by [1, Theorem 6.3.3], it is contained in $O_{2'2}(G) = VS$. This is impossible because $Z(S) \simeq \mathbb{Z}_2$.

CASE 2. Otherwise P does not act $\frac{1}{2}$-transitively on $V^\#$. Clearly $V^\#$ is a union of two orbits Δ_1, Δ_2 with $|\Delta_1| = 8$, $|\Delta_2| = 16$ under the action of P, which implies that $r_{2'}(V \rtimes P) = 3$. Hence (10) of Theorem B applies to $V \rtimes P$, and so P is given by

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

Again this contradicts [1, Theorem 6.3.3] because $Z(P) \simeq \mathbb{Z}_4$ and $Z(S) \simeq \mathbb{Z}_2$.

Thus we have $V \simeq E_{7^2}$. Let w be a generator of W, a cyclic group of order 3. Since w^{-1} is conjugate to w in G, there is an element x in $T - SW$ such that x^2 lies in S, $T = \langle SW, x \rangle$ and $w^x = w^{-1}$. But then $x^2 \in C_S(w) = Z(S)$, and so the order of x is at most 4. Because a Sylow 2-subgroup $\langle S, x \rangle$ of T acts semiregularly on $V^\#$, it is a generalized quaternion group of order 16, which implies that $x^2 \neq 1$, that is, the order of x is 4. This shows that G is a group stated in (11). We note that T is a group G_{48} given in [2, Chap. XII, Definition 8.4].

We show now that a group G which satisfies condition (11) does in fact exist. Let

$$s = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad t = \begin{pmatrix} 2 & 3 \\ 3 & -2 \end{pmatrix}, \quad w = \begin{pmatrix} -1 & 3 \\ 2 & 0 \end{pmatrix}, \quad x = \begin{pmatrix} 3 & 2 \\ 2 & -3 \end{pmatrix}$$

be elements of $\mathrm{GL}(2,7)$. Set $S = \langle s, t \rangle$. Then $S \simeq Q_8$; and the element w is of order 3 and normalizes S. Further $x^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \in Z(S)$ and x normalizes each of S and $\langle w \rangle$. Now let T be a group generated by S, w and x. Then, regarding E_{7^2} as a vector space over GF(7), we get a semidirect product $G = E_{7^2} \rtimes T$. This is a group of type (11) in Theorem B, and we can easily check that $r_{2'}(G) = 3$.

STEP 2. If case (b) holds then part (12) of Theorem B holds.

PROOF. Since W acts semiregularly on $V^\#$ and $|V^\#| = 3 \cdot 2^3$, we have $|W| = q = 3$ and $T/S \simeq \Sigma_3$. Let w be a generator of W. Then we can choose $x \in T - SW$ so that $T = \langle SW, x\rangle$, $x^2 \in S$ and $w^x = w^{-1}$. Clearly $x^2 \in C_S(w)$. Since the center $Z\big(\mathcal{T}_0(5)\big)$ of $\mathcal{T}_0(5)$ is a cyclic group $\left\langle \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \right\rangle$ of order 4, we see that $C_S(w) \supseteq Z(S)$. This together with Sylow's theorem implies that $C_S(w) = Z(S)$. Therefore the order of x is at most 8. We must show that the order of x is 8. We note that a Sylow 2-subgroup Q of GL(2, 5) is given by

$$Q = \left\langle \mathcal{T}_0(5), \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \right\rangle.$$

It is easy to check that if σ is an element of $Q - \mathcal{T}_0(5)$ such that $\sigma^2 \in Z\big(\mathcal{T}_0(5)\big)$ then the order of σ is 8. This implies that the order of x is in fact 8. Hence G is a group stated in (12).

We show now the existence of such a group. Let $w = \begin{pmatrix} -2 & 1 \\ 2 & 1 \end{pmatrix}$ be an element of GL(2, 5). Then w is of order 3 and normalizes $\mathcal{T}_0(5)$. Set $x = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$. Then $x^2 = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \in \mathcal{T}_0(5)$, and x normalizes each of $\langle w \rangle$ and $\mathcal{T}_0(5)$. Let T be a group generated by $\mathcal{T}_0(5)$, w and x. Then, regarding E_{5^2} as a vector space over GF(5), we get a semidirect product $G = E_{5^2} \rtimes T$. This is a group of type (12) in Theorem B, and one can check directly that $r_{2'}(G) = 3$.

STEP 3. Case (c) does not occur.

PROOF. Assume by way of contradiction that case (c) occurs and let G be a group which satisfies the condition stated in (c). Since W acts semiregularly on $V^\#$ and $|V^\#| = 5 \cdot 2^4$, we have $|W| = q = 5$ and $T/SW \simeq \mathbb{Z}_4$. Therefore we can choose an element x of $T - SW$ so that $x^4 \in S$ and $T = \langle SW, x\rangle$. Now we note that for every element v of $V^\#$, the length of the S-orbit containing v is 16, that is, $|C_S(v)| = 2$; and the length of the SW-orbit containing v is 80, that is, SW acts transitively on $V^\#$. Set $U = \langle S, W, x^2\rangle$. Then a Sylow 2-subgroup R of U does not act $\frac{1}{2}$-transitively on $V^\#$ ([7, Theorem 19.6]). Hence there exists an element v of $V^\#$ such that the length of the R-orbit containing v is 32, which implies that $C_R(v) = C_S(v)$. We can now choose an element y of $\langle S, x^2\rangle - S$ so that v^y is not contained in the S-orbit containing v. But, because SW acts transitively on $V^\#$, there exists $\sigma \in SW - S$ with $v^\sigma = v^y$. Then $\sigma y^{-1} \in C_U(v)$. Now set $\sigma = sw$, where $s \in S$, $w \in W^\#$. We then see that wy^{-1} is a 2-element because T/S is a Frobenius group. Hence $\sigma y^{-1} = s(wy^{-1})$ is contained in some Sylow 2-subgroup R of U, which contradicts the fact that $C_R(v) = C_S(v)$. This contradiction shows that case (c) does not occur. Thus we complete the proof of Proposition 6.2, and Theorem B is proved.

REFERENCES

1. D. Gorenstein, *Finite groups*. Harper & Row, New York, 1968.

2. B. Huppert and N. Blackburn, *Finite groups II, III*. Springer-Verlag, Berlin, 1982.

3. I. M. Isaacs and D. S. Passman, *Half-transitive automorphism groups*, Canad. J. Math. **18**(1966), 1243-1250.

4. S. Koshitani, *On group algebras of finite groups*, in Representation Theory II, Groups and Orders (Proc. 4th Int. Conf., Ottawa/Can. 1984), Lecture Notes Math. **1178** Springer-Verlag, Berlin, 1986, 109–128.

5. Y. Ninomiya and T. Wada, *Cartan matrices for blocks of finite p-solvable groups with two simple modules*, to appear in J. Algebra.

6. J. B. Olsson, *On 2-blocks with quaternion and quasidihedral defect groups*, J. Algebra **36**(1975), 212–241.

7. D. S. Passman, *Permutation groups*. Benjamin, New York, 1968.

Department of Mathematics
Faculty of Liberal Arts
Shinshu University
Matsumoto, 390
Japan