J. Austral. Math. Soc. (*Series A*) **27** (1979), 125–140

FINITE 2-GROUPS OF CLASS TWO WITH CYCLIC CENTRE

Y. K. LEONG

(Received 4 May 1978; revised 20 October 1978)

Communicated by H. Lausch

Abstract

In conjunction with an earlier work by Leong (1974a), this paper completes the solution of the isomorphism problem for finite nilpotent groups of class two with cyclic centre. A canonical decomposition for 2-groups of such type is obtained and proved.

Subject classification (*Amer. Math. Soc.* (*MOS*) *1970*): 20 D 15 (20 E 10).

1. Introduction

The structure of finite nilpotent groups of class two with cyclic centre was first discovered by Brady (1970) as part of his results in his Ph.D. thesis. His results were further exploited by Brady et al. (1969) and Leong (1974b) in their work on the subvarieties of $\mathfrak{A}_m(\mathfrak{N}_2 \wedge \mathfrak{B}_n)$ where m and n are coprime. In the latter work on the CREAM Conjecture of Higman (1967) for these subvarieties, it was found necessary to solve the isomorphism problem for the above-mentioned groups. This was solved by Leong (1974a) in the odd order case. The present work settles the remaining case of finite 2-groups, thereby completing the solution of the isomorphism problem for the above groups.

It is known, see Leong (1974a), that a finite q-group of nilpotency class two with cyclic centre is a central product either of two-generator subgroups with cyclic centre or of two-generator subgroups with cyclic centre and a cyclic subgroup, and that the finite q-groups of class two on two generators with cyclic centre

comprise the following list:

$$2r \leqslant n: \quad Q(n,r) = \langle a, b : a^{q^n} = b^{q^r} = 1, a^{q^{n-r}} = [a,b] \rangle;$$

$$r \leqslant n < 2r: \quad Q(n,r) = \langle a, b : a^{q^n} = b^{q^r} = 1, a^{q^r} = [a,b]^{q^{2r-n}},$$
$$[[a,b],a] = [[a,b],b] = 1 \rangle;$$

and if $q = 2$ we have as well

$$n \geqslant 1: \quad R(n) = \langle a, b : a^{2^{n+1}} = b^{2^{n+1}} = 1, a^{2^n} = [a,b]^{2^{n-1}} = b^{2^n},$$
$$[[a,b],a] = [[a,b],b] = 1 \rangle.$$

Again we use the notation $Q(n,0)$ for the cyclic group of order q^n, $n \geqslant 1$.

Leong (1974a) has shown that if q is an odd prime, then every finite q-group G of class two with cyclic centre has the central decomposition

$$G \cong Q(n_1, r_1) \dots Q(n_\alpha, r_\alpha) Q(l,l)^{\varepsilon_1} \dots Q(1,1)^{\varepsilon_l},$$

where $\alpha \geqslant 0$, $\varepsilon_i \geqslant 0$, $i = 1, \dots, l$,

$$n_1 > \dots > n_\alpha > l \geqslant 1, \quad n_\alpha > r_1 > \dots > r_\alpha \geqslant 0, \quad 0 < n_1 - r_1 < \dots < n_\alpha - r_\alpha,$$

and that this decomposition is unique up to isomorphism.

In this paper we will prove the following two theorems.

THEOREM A. *Every finite 2-group G of class two with cyclic centre either has the central decomposition*

$$G \cong Q(n_1, r_1) \dots Q(n_\alpha, r_\alpha) Q(l,l)^{\varepsilon_l} \dots Q(1,1)^{\varepsilon_1},$$

where $\alpha \geqslant 0$, $\varepsilon_i \geqslant 0$, $i = 1, \dots, l$,

$$n_1 > \dots > n_\alpha > l \geqslant 1, \quad n_\alpha > r_1 > \dots > r_\alpha \geqslant 0, \quad 1 < n_1 - r_1 < \dots < n_\alpha - r_\alpha,$$

or else it has the central decomposition

$$G \cong R(n) Q(l,l)^{\varepsilon_l} \dots Q(1,1)^{\varepsilon_1},$$

where $n \geqslant l \geqslant 1$, $\varepsilon_i \geqslant 0$, $i = 1, \dots, l$.

THEOREM B. *The canonical decomposition for finite 2-groups of class two with cyclic centre (as given in Theorem A) is unique up to isomorphism.*

We remark that an extra-special q-group P of order q^{2r+1} (see Gorenstein (1968), p. 204) may be written in our notations as

$$\text{if } q \text{ is odd}, \quad P \cong Q(1,1)^r \quad \text{or} \quad Q(2,1) Q(1,1)^{r-1};$$

$$\text{if } q = 2, \quad P \cong Q(1,1)^r \quad \text{or} \quad R(1) Q(1,1)^{r-1}.$$

https://doi.org/10.1017/S1446788700012052 Published online by Cambridge University Press

2. Reduction lemmas

In this section we give a series of lemmas which will be used to reduce a given central product of the $Q(n,r)$ and $R(m)$ to the canonical form. The first four lemmas are identical to those (see Leong (1974a)) required for the reduction of the odd order groups. Since their proofs are the same in both cases, we will merely state them. However, for the reduction of 2-groups, we need eight more lemmas, of which seven involve the factor $R(m)$.

LEMMA 2.1. *If either* $n_1 \geqslant n_2$ *and* $0 < r_1 \leqslant r_2$, *or* $n_1 \geqslant n_2$, $n_1 - r_1 \geqslant n_2 - r_2$ *and* $r_1 > r_2 > 0$, *then* $Q(n_1, r_1)\, Q(n_2, r_2) \cong Q(n_1, r_1)\, Q(r_2, r_2)$.

LEMMA 2.2. *If* $n_1 \leqslant r_2$ *or* $n_1 \leqslant n_2 - r_2$, *then* $Q(n_1, 0)\, Q(n_2, r_2) \cong Q(n_2, r_2)$.

LEMMA 2.3. *If* $n_1 \geqslant n_2$, *then* $Q(n_1, 0)\, Q(n_2, r_2) \cong Q(n_1, 0)\, Q(r_2, r_2)$.

LEMMA 2.4. *If* $r_1 \geqslant n_2$, *then* $Q(n_1, r_1)\, Q(n_2, r_2) \cong Q(n_1, r_1)\, Q(r_2, r_2)$

LEMMA 2.5. *If* $n \leqslant m$, *then* $Q(n, 0)\, R(m) \cong R(m)$.

PROOF. $Q(n, 0) = Z(Q(n, 0)) \leqslant Z(R(m))$.

LEMMA 2.6. *If* $n > m \geqslant 1$, *then* $Q(n, 0)\, R(m) \cong Q(n, 0)\, Q(m, m)$.

PROOF. Let z, c, d be canonical generators of $Q(n, 0)\, R(m)$ so that $z^{2^{n-m}} = [c, d]$. Put $x = cz^{-2^{n-m-1}}$, $y = dz^{-2^{n-m-1}}$. Then

$$\langle x, y \rangle \cong Q(m, m) \quad \text{and} \quad \langle z, c, d \rangle = \langle z \rangle . \langle x, y \rangle \cong Q(n\ 0)\, Q(m, m).$$

LEMMA 2.7. *For* $n \geqslant 1$, $Q(n+1, n) \cong Q(n, n)$.

PROOF. Let $Q(n, n) = \langle a, b \rangle$, and put $x = ab$, $y = b$. Then

$$\langle a, b \rangle = \langle x, y \rangle \cong Q(n+1, n).$$

LEMMA 2.8. *For* $m \geqslant 1$, $R(m)^2 \cong Q(m, m)^2$.

PROOF. Let a_1, b_1, a_2, b_2 be canonical generators of $Q(m, m)^2$. Put $x_1 = a_1 b_1$, $y_1 = b_1 a_2 b_2$, and $x_2 = a_2 b_2$, $y_2 = b_2 a_1 b_1$. Then $\langle x_1, y_1 \rangle \cong R(m) \cong \langle x_2, y_2 \rangle$. Moreover $[x_1, x_2] = [x_1, y_2] = [y_1, x_2] = 1$, and $[y_1, y_2] = [b_1, a_1]\, [a_2, b_2] = 1$. Hence

$$Q(m, m)^2 = \langle x_1, y_1 \rangle . \langle x_2, y_2 \rangle \cong R(m)^2.$$

https://doi.org/10.1017/S1446788700012052 Published online by Cambridge University Press

LEMMA 2.9. *If* $n > m \geqslant 1$, *then* $R(n)\,R(m) \cong R(n)\,Q(m,m)$.

PROOF. $Z = Z(R(n))$ is a 2^n-cycle containing $Z(R(m))$. Hence

$$R(n)\,R(m) = R(n)\,(Z\,.\,R(m)) \cong R(n)\,(Z\,.\,Q(m,m)) = R(n)\,Q(m,m)$$

in view of Lemma 2.6.

LEMMA 2.10. *If* $m \geqslant n > r \geqslant 1$, *then* $Q(n,r)\,R(m) \cong Q(r,r)\,R(m)$.

PROOF. There is a 2^n-cycle $C \leqslant Z(R(m))$, and

$$Q(n,r)\,R(m) = CQ(n,r)\,R(m) \cong CQ(r,r)\,R(m)$$

by Lemma 2.3. But $CQ(r,r)\,R(m) = Q(r,r)\,R(m)$.

LEMMA 2.11. *If* $n > r \geqslant 1$, $n-r > 1$ *and* $n > m \geqslant 1$, *then* $Q(n,r)\,R(m) \cong Q(n,r)\,Q(m,m)$.

PROOF. First we show that canonical generators a, b, c, d of $Q(n,r)\,R(m)$ may be chosen to satisfy the relations

$$a^{2^{n-1}} = [a,b]^{2^{r-1}} = c^{2^m} = d^{2^m}. \tag{1}$$

Now if $2r \leqslant n$, then $Z(Q(n,r)) = \langle a^{2^r} \rangle$ and is of order 2^{n-r}. The amalgamation in the central product $Q(n,r)\,R(m)$ may be chosen to be

$$a^{2^{n-m}} = [c,d] \quad \text{or} \quad a^{2^r} = [c,d]^{2^{m-n+r}}$$

according as $m < n-r$ or $m \geqslant n-r$. In either case, the above relations (1) hold. On the other hand, if $2r > n$, then $Z(Q(n,r)) = \langle [a,b] \rangle$ and is of order 2^r. The amalgamation may be chosen to be $[a,b]^{2^{r-m}} = [c,d]$ or $[a,b] = [c,d]^{2^{m-r}}$ according as $m < r$ or $m \geqslant r$. The relations (1) are then easily verified.

To prove the lemma, we consider three cases.

(i) $m < r$. Put $x = c[a,b]^{2^{r-m-1}}$, $y = d[a,b]^{2^{r-m-1}}$. Then in view of relations (1), $\langle x,y \rangle \cong Q(m,m)$. Thus $Q(n,r)\,R(m) = \langle a,b \rangle\,.\,\langle x,y \rangle \cong Q(n,r)\,Q(m,m)$ since $\langle x,y \rangle$ obviously centralizes $\langle a,b \rangle$.

(ii) $m < n-r$. Put $x = ca^{2^{n-m-1}}$, $y = da^{2^{n-m-1}}$. By relations (1), $\langle x,y \rangle \cong Q(m,m)$, and since $n-m-1 \geqslant r$, $\langle x,y \rangle$ centralizes $\langle a,b \rangle$. Hence

$$Q(n,r)\,R(m) = \langle a,b \rangle\,.\,\langle x,y \rangle \cong Q(n,r)\,Q(m,m).$$

(iii) $m \geqslant \max\{r, n-r\}$. It is clear that the amalgamation may be chosen so that

$$[a,b]^{2^{n-m-1}} = [c,d]^{2^{n-r-1}}. \tag{2}$$

https://doi.org/10.1017/S1446788700012052 Published online by Cambridge University Press

Now put $u = a$, $v = bc^{2^{n-r-1}} d^{2^{n-r-1}}$, $x = a^{2^{n-m-1}} c^{-1}$, $y = a^{2^{n-m-1}} d$. By relation (2), $\langle x, y\rangle$ centralizes $\langle u, v\rangle$, so that $Q(n,r)R(m)$ is the central product of $\langle u, v\rangle$ and $\langle x, y\rangle$. Moreover, $\langle x, y\rangle \cong Q(m,m)$. Bearing in mind that $n-r \geqslant 2$, $n \geqslant m+1$ and $n \geqslant 3$, we easily check that $\langle u, v\rangle \cong Q(n,r)$.

3. The canonical decomposition

The results of the preceding section enable us to obtain the canonical decomposition of a finite 2-group of class two with cyclic centre. Its uniqueness up to isomorphism will be proved in the next section.

Proof of Theorem A. Assume that G is non-trivial. By Theorem 2.1 and 2.2 of Brady et al. (1969), G has a decomposition as a central product of the $Q(n,r)$ and $R(m)$ which we arrange as

$$G \cong Q(n_1, r_1) \dots Q(n_\beta, r_\beta)\, Q(s,s)^{\lambda_s} \dots Q(1,1)^{\lambda_1} R(t)^{\mu_t} \dots R(1)^{\mu_1}, \tag{3}$$

where $n_1 \geqslant \dots \geqslant n_{\beta-1} \geqslant 1$, $n_i > r_i > 0$ $(1 \leqslant i \leqslant \beta-1)$, $n_\beta > r_\beta \geqslant 0$, and $r_\beta < 0$ implies $n_{\beta-1} \geqslant n_\beta$, and where $\lambda_1, \dots, \lambda_s$, $\mu_1, \dots, \mu_t \geqslant 0$, and $\lambda_s = 0$ (respectively $\mu_t = 0$) implies $\lambda_1 = \dots = \lambda_{s-1} = 0$ (respectively $\mu_1 = \dots = \mu_{t-1} = 0$) also.

First we show that the central decomposition (3) may be reduced to one of the following forms.

$$G \cong Q(n_1, r_1) \dots Q(n_\gamma, r_\gamma)\, Q(k,k)^{\delta_k} \dots Q(1,1)^{\delta_1}, \tag{4}$$

where $n_1 \geqslant \dots \geqslant n_\gamma \geqslant 1$, $n_i > r_i > 0$ $(1 \leqslant i \leqslant \beta-1)$, $n_\gamma > r_\gamma \geqslant 0$, and where $\delta_1, \dots, \delta_k \geqslant 0$, and $\delta_k = 0$ implies $\delta_1 = \dots = \delta_{k-1} = 0$ also;

$$G \cong R(t)\, Q(k,k)^{\delta_k} \dots Q(1,1)^{\delta_1}, \tag{5}$$

where $t \geqslant k$, $\delta_1, \dots, \delta_k \geqslant 0$.

Suppose that $\mu_i = 0$ in (3). If, moreover, $r_\beta = 0$ and $n_\beta > n_i$ for some $1 \leqslant i < \beta$, then by Lemma 2.3, $Q(n_\beta, 0)\, Q(n_i, r_i) \cong Q(n_\beta, 0)\, Q(r_i, r_i)$. So we may assume $n_\beta \leqslant n_{\beta-1}$, and G is then of the form (4).

So suppose that $\mu_t > 0$. If $\mu_t = 2j$ for some $j \geqslant 1$, then $R(t)^{\mu_t} = (R(t)^2)^j \cong Q(t,t)^{2j}$ by Lemma 2.8. If $\mu_t = 2j+1$ for some $j \geqslant 1$, then $R(t)^{\mu_t} = R(t)^{2j} R(t) \cong Q(t,t)^{2j} R(t)$ by Lemma 2.8. Hence we may assume $\mu_t = 1$. If $\mu_i > 0$ for some $1 \leqslant i < t$, then $R(t)\, R(i)^{\mu_i} \cong R(t)\, Q(i,i)^{\mu_i}$ by Lemma 2.9. Hence we may assume

$$\mu_i = 0, \quad i = 1, \dots, t-1.$$

https://doi.org/10.1017/S1446788700012052 Published online by Cambridge University Press

In view of Lemmas 2.5, 2.6, 2.10 and 2.11, we may assume $\beta = 0$. If, moreover, $\lambda_s = 0$, then G is of the form (5). So assume $\lambda_s > 0$. If $s > t$, then

$$Q(s,s)^{\lambda_s} R(t) \cong Q(s,s)^{\lambda_s} Q(t,t)$$

by Lemma 2.12. Hence we may assume $t \geqslant s$, and G will be of the form (5).

We prove by induction on γ that any group G of the form (4) has a decomposition of the first form asserted in the theorem. The case $\gamma = 0$ is easy. So suppose $\gamma > 0$ and that all groups of the form (4) with fewer than γ factors of the type $Q(n,r)$ with $n > r$ do have a decomposition of the first form asserted. If $n_1 - r_1 = 1$, then by Lemma 2.7, $Q(n_1, r_1) \cong Q(r_1, r_1)$, and hence G has a decomposition with $\gamma - 1$ factors of the type $Q(n,r)$ with $n > r$; so, by induction, we are done. We may now assume $n_1 - r_1 > 1$. The rest of the induction process is identical to that in the proof of Theorem 2.5 of Leong (1974a).

4. Uniqueness of the canonical decomposition

In this section, G and H will always denote finite 2-groups of class two with cyclic centre. For any finite group A, we use the notations

$$\Omega^i(A) = \langle x^{2^i} : x \in A \rangle, \quad i \geqslant 0,$$

$$d(A) = \text{minimal number of generators of } A \text{ if } A \neq 1,$$

$$d(A) = 0 \text{ if } A = 1.$$

As in Section 3 of Leong (1974a), we define the following isomorphism invariant $\rho_i(G)$, $i \geqslant 0$:

$$\rho_i(G) = d(\Omega^i(G/Z(G))).$$

The value of $\rho_i(G)$ is easily obtained from the following three lemmas, of which the first two are Lemmas 3.1 and 3.3 of Leong (1974a).

LEMMA 4.1. *Let GH be the central product of G and H with cyclic centre. Then $\rho_i(GH) = \rho_i(G) + \rho_i(H)$, $i \geqslant 0$.*

LEMMA 4.2. *Let $n \geqslant r \geqslant 0$. Then $\rho_i(Q(n,r)) = 2$ if $0 \leqslant i < r$, and zero if $i \geqslant r$.*

LEMMA 4.3. *Let $m \geqslant 1$. Then $\rho_i(R(m)) = 2$ if $0 \leqslant i < m$, and zero if $i \geqslant m$.*

PROOF. If $R(m) = \langle c, d \rangle$, then $c^{2^i}, d^{2^i} \in Z(R(m))$ if and only if $i \geqslant m$.

The method of enumeration of the cyclic subgroups of order 4 of an extra-special 2-group in Gorenstein (1968), pp. 205, 206, may be extended to give more

general results. In the following Lemmas 4.4 and 4.5,

$$n \geqslant 1, \quad l \geqslant 1 \quad \text{and} \quad Q = Q(l-1, l-1)^{\varepsilon_{l-1}} \dots Q(1,1)^{\varepsilon_1}, \quad \varepsilon_i \geqslant 0, \quad i = 1, \dots, l.$$

LEMMA 4.4. *The number of cyclic subgroups of order* 2^{l+1} *of* $Q(l,l)^n Q$ *is* $(2^{2ln-1} - 2^{(2l-1)n-1})\,|Q/Z(Q)|$.

PROOF. Write $G = Q_1 Q_2 \dots Q_n Q$ where each Q_i is isomorphic to $Q(l,l)$, and $Z = Z(G)$. Fix indices $1 \leqslant i_1 < i_2 < \dots < i_m \leqslant n$, and let X be the set of expressions $x = x_{i_1} x_{i_2} \dots x_{i_m} x_Q$, where $x_{i_j} \in Q_{i_j} - Z$, $j = 1, \dots, m$, $x_Q \in Q$, such that $\langle x \rangle$ is cyclic of order 2^{l+1}. Two expressions $x = x_{i_1} \dots x_{i_m} x_Q$ and $x' = x'_{i_1} \dots x'_{i_m} x'_Q$ are said to be the same if and only if $x_i = x'_{i_j}$, $j = 1, \dots, m$, and $x_Q = x'_Q$; otherwise x and x' are said to be different. Note that different expressions in X do not necessarily define distinct elements of G.

By a suitable choice of canonical generators a_i, b_i of Q_i, and $\langle z \rangle = Z(G) = Z(Q_i)$, $i = 1, \dots, n$, we have

$$x^{2^l} = z^{(\lambda_1 \mu_1 + \dots + \lambda_m \mu_m) 2^{l-1}},$$

where $x_{i_j} = a_{i_j}^{\lambda_j} b_{i_j}^{\mu_j} z^{\nu_j}$, $j = 1, \dots, m$. Call x_{i_j} odd if $\lambda_j \equiv 1 \equiv \mu_j \pmod 2$ and x_{i_j} even if $\lambda_j \mu_j \equiv 0 \pmod 2$. It is clear that $\langle x \rangle$ has order 2^{l+1} if and only if the number of odd x_{i_j} occurring in the expression $x = x_{i_1} \dots x_{i_m} x_Q$ is odd. Now the number of odd x_{i_j} in $Q_{i_j} - Z$ is equal to $p_0 = 2^{l-1} . 2^{l-1} . 2^l = 2^{3l-2}$, while the number of even x_{i_j} in $Q_{i_j} - Z$ is $p_e = (2^l . 2^l - 2^{l-1} . 2^{l-1} - 1)\, 2^l = (3 . 2^{2l-2} - 1)\, 2^l$. Hence the number of different expressions in X is

$$|X| = |Q| \sum \binom{m}{k} p_0^k p_e^{m-k},$$

where the summation is over all those odd integers k, $1 \leqslant k \leqslant m$, and so

$$|X| = \tfrac{1}{2} |Q| \{(p_e + p_0)^m - (p_e - p_0)^m\}.$$

For any odd integer γ and $x = x_{i_1} \dots x_{i_m} x_Q$, define x^γ to be the expression in X given by $x^\gamma = x_{i_1}^\gamma \dots x_{i_m}^\gamma x_Q^\gamma$. Now if $x, x' \in X$, then $\langle x \rangle = \langle x' \rangle$ if and only if $x' = x^\gamma$ for some odd integer γ. We show that if γ and δ are odd integers, then the expressions x^γ and x^δ are the same if and only if $\gamma \equiv \delta \pmod{2^{l+1}}$. Let $x_{i_j} = a_{i_j}^{\lambda_j} b_{i_j}^{\mu_j} [a_{i_j}, b_{i_j}]^{\nu_j}$, $j = 1, \dots, m$. If x^γ and x^δ are the same, then $x_{i_j}^\gamma = x_{i_j}^\delta$, $x_Q^\gamma = x_Q^\delta$, $j = 1, \dots, m$. Hence $\lambda_j \gamma \equiv \lambda_j \delta \pmod{2^l}$, $\mu_j \gamma \equiv \mu_j \delta \pmod{2^l}$, $j = 1, \dots, m$. Now for some $1 \leqslant k \leqslant m$, x_{i_k} is odd, and so $\gamma \equiv \delta \pmod{2^l}$. Write $\delta = \gamma + \gamma' 2^l$. Then

$$\tfrac{1}{2}\delta(\delta - 1) \equiv \tfrac{1}{2}\gamma(\gamma - 1) + \gamma\gamma' 2^{l-1} \pmod{2^l},$$

and

$$x_Q^\delta = x_Q^\gamma, \quad x_{i_j}^\delta = x_{i_j}^\gamma z^{\lambda_j \mu_j \gamma \gamma' 2^{l-1}}, \quad j = 1, \dots, m.$$

https://doi.org/10.1017/S1446788700012052 Published online by Cambridge University Press

We have

$$x^\delta = x^\gamma z^{(\lambda_1\mu_1+\ldots+\lambda_m\mu_m)\gamma\gamma' 2^{l-1}}.$$

Since $x^\delta = x^\gamma$ also, and $\lambda_1\mu_1+\ldots+\lambda_m\mu_m$ and γ are both odd, it follows that γ' is even, and hence $\delta \equiv \gamma \pmod{2^{l+1}}$. The converse is easy.

The following relation $\sim$ is an equivalence relation on X, where $x \sim x'$ if and only if $\langle x\rangle = \langle x'\rangle$. The number of different expressions in a given equivalence class is the number of different expressions of the form $x' = x^\gamma$ for some odd integer γ, where x is any representative of the given equivalence class. To compute this number, let $x = x_{i_1}\ldots x_{i_m}x_Q$ and $x' = x'_{i_1}\ldots x'_{i_m}x'_Q$. Then $x' = x^\gamma$ implies that

$$x'_Q = x_Q^\gamma z_Q, \quad x'_{i_j} = x_{i_j}^\gamma z_j, \quad j = 1,\ldots,m, \tag{6}$$

where $z_Q \in Z(Q)$, $z_j \in Z$, $j = 1,\ldots,m$, such that

$$z_1\ldots z_m z_Q = 1. \tag{7}$$

Clearly, z_1 is uniquely determined by $z_2,\ldots,z_m,z_Q$ in (7). Hence by the remarks in the preceding paragraph, the number of different expressions x' of the form $x' = x^\gamma$ for some odd integer γ is equal to $2^l|Z|^{m-1}.|Z(Q)| = 2^{lm}|Z(Q)|$.

Thus the number of distinct equivalence classes is

$$|X|/(2^{lm}|Z(Q)|) = \tfrac{1}{2}|Q/Z(Q)|(\alpha^m-\beta^m),$$

where $\alpha = (p_e+p_0)/2^l$, $\beta = (p_e-p_0)/2^l$. By taking all possible choices of indices $1 \leqslant i_1 < \ldots < i_m \leqslant n$, it follows that the number of distinct cyclic subgroups of order 2^{l+1} of G is equal to

$$\begin{aligned}\tfrac{1}{2}|Q/Z(Q)|\sum_{m=1}^{n}\binom{n}{m}(\alpha^m-\beta^m) &= \tfrac{1}{2}|Q/Z(Q)|\{(1+\alpha)^n-(1+\beta)^n\}\\ &= |Q/Z(Q)|(2^{2ln-1}-2^{(2l-1)n-1}).\end{aligned}$$

LEMMA 4.5. *The number of cyclic subgroups of order 2^{l+1} of $R(l)Q(l,l)^{n-1}Q$ is $(2^{2ln-1}+2^{(2l-1)n-1})|Q/Z(Q)|$.*

PROOF. Write $H = R(l)Q_1\ldots Q_{n-1}Q$ where $Q_i \cong Q(l,l)$, $i = 1,\ldots,n-1$, and $Z = Z(H)$. By Lemma 4.4, the number of cyclic subgroups $\langle x\rangle$ of order 2^{l+1} with $x \in Q_1\ldots Q_{n-1}Q$ is equal to $(2^{2l(n-1)-1}-2^{(2l-1)(n-1)-1})|Q/Z(Q)|$. So it remains to count the number of relevant subgroups $\langle x\rangle$ with $x \in H - Q_1\ldots Q_{n-1}Q$.

Fix indices $1 \leqslant i_1 < i_2 < \ldots < i_m \leqslant n-1$ where m may be zero. Let X_0 be the set of expressions $x = x_0x_{i_1}\ldots x_{i_m}x_Q$, where $x_0 \in R(l)-Z$, $x_{i_j} \in Q_{i_j}-Z$, $j = 1,\ldots,m$, $x_Q \in Q$, and $x = x_0x_Q$ if $m = 0$, and such that $\langle x\rangle$ is cyclic of order 2^{l+1}. Two expressions $x = x_0x_{i_1}\ldots x_{i_m}x_Q$ and $x' = x'_0x'_{i_1}\ldots x'_{i_m}x'_Q$ are said to be the same if $x_0 = x'_0$ $x_{i_j} = x'_{i_j}$, $j = 1,\ldots,m$, and $x_Q = x'_Q$; otherwise they are said to be different.

https://doi.org/10.1017/S1446788700012052 Published online by Cambridge University Press

It is easily checked that $\langle x_0 x_{i_1} \dots x_{i_m} x_Q \rangle$ is of order 2^{l+1} if and only if

$$(1+\lambda)(1+\mu)+\sum_{j=1}^{m}\lambda_j\mu_j \equiv 0 \pmod 2, \tag{8}$$

where $x_0 = c^\lambda d^\mu z^\nu$, $x_{i_j} = a_{i_j}^{\lambda_j} b_{i_j}^{\mu_j} z^{\nu_j}$, $j = 1, \dots, m$, with a suitable choice of canonical generators c, d and a_{i_j}, b_{i_j} for $R(l)$ and Q_{i_j} respectively, and $\langle z \rangle = Z$. To calculate the number of different expressions in X_0, we consider two cases: (i) $(1+\lambda)(1+\mu)$ is odd, (ii) $(1+\lambda)(1+\mu)$ is even. If we use the terminology introduced in the proof of Lemma 4.4, condition (8) is equivalent to the condition that the number of odd x_{i_j} occurring in the expression $x_0 x_{i_1} \dots x_{i_m} x_Q$ is odd or even according as we are in case (i) or case (ii). With the notations p_0, p_e used in the preceding proof, the number of different expressions in X_0 is then

$$|X_0| = \left\{(2^{l-1}.2^{l-1}-1)\,2^l \sum \binom{m}{k} p_0^k p_e^{m-k} + (2^l.2^l - 2^{l-1}.2^{l-1})\,2^l \sum \binom{m}{t} p_0^t p_e^{m-t}\right\} |Q|,$$

where the first summation is over all those odd integers k, $1 \leqslant k \leqslant m$, and the second summation is over all those even integers t, $0 \leqslant t \leqslant m$. Evaluating the sums, we have

$$|X_0|/|Q| = (2^{2l-1} - 2^{l-1})(p_e + p_0)^m + (2^{2l-2} + 2^{l-1})(p_e - p_0)^m.$$

As before, we may define an equivalence relation $\sim$ on X_0 by $x \sim x'$ if and only if $\langle x \rangle = \langle x' \rangle$. It is again easily shown that the number of different expressions in each equivalence class is equal to $2^{l(m+1)}|Z(Q)|$. Thus the number of distinct equivalence classes is

$$|Q/Z(Q)|\{(2^{2l-1} - 2^{-1})\,\alpha^m + (2^{2l-2} + 2^{-1})\,\beta^m\},$$

where $\alpha = (p_e + p_0)/2^l$, $\beta = (p_e - p_0)/2^l$. Hence the number of distinct cyclic subgroups $\langle x \rangle$ of order 2^{l+1} with $x \in H - Q_1 \dots Q_{n-1} Q$ is equal to

$$|Q/Z(Q)| \sum_{m=0}^{n-1} \binom{n-1}{m} \{(2^{2l-1} - 2^{-1})\,\alpha^m + (2^{2l-2} + 2^{-1})\,\beta^m\}$$

$$= |Q/Z(Q)|\{(2^{2l-1} - 2^{-1})\,2^{l(n-1)} + (2^{2l-2} + 2^{-1})\,2^{(2l-1)(n-1)}\}.$$

The lemma then follows from the remarks at the beginning of this proof.

We recapitulate some terminology from Leong (1974b). Let Z_{2^r} be the ring of integers modulo 2^r, $r \geqslant 1$. A finitely-generated Z_{2^r}-module U is said to be a symplectic module over Z_{2^r} if there is an alternating Z_{2^r}-bilinear form f defined on U. We write $V = V_1 \perp V_2$ if $V_i \subseteq U$, $i = 1, 2$, $V = V_1 \oplus V_2$ and $f(v_1, v_2) = 0$ for all $v_i \in V_i$, $i = 1, 2$. We denote by $\langle u_1, \dots, u_n \rangle$ the submodule of U generated by $u_1 \dots u_n$.

https://doi.org/10.1017/S1446788700012052 Published online by Cambridge University Press

For a submodule W of U, we write $W^{\perp} = \{u \in U : f(u, w) = 0 \text{ for all } w \in W\}$. The structure of non-degenerate symplectic modules over the ring of integers modulo q^r for any prime q and $r \geqslant 1$ is given in Leong (1974b). For our purposes we will only need the following two lemmas.

LEMMA 4.6. *Let U be a symplectic module over Z_{2^r}, $r \geqslant 1$, given by*

$$U = \langle u_1, v_1 \rangle \perp \ldots \perp \langle u_n v_n, \rangle$$

where $f(u_i, v_i) = 1 \quad i = 1, \ldots, n$.

If $u, v \in U$ such that $f(u, v) = 1$, then $U = \langle u\ v \rangle \perp U_1$ for some submodule U_1.

PROOF. Write $u = x_1 + \ldots + x_n$, $v = y_1 + \ldots + y_n$, where $x_i, y_i \in \langle u_i, v_i \rangle$, $i = 1, \ldots, n$. Then $f(u, v) = f(x_1, y_1) + \ldots + f(x_n, y_n)$. Since $f(u, v) = 1$, $f(x_i, y_i) \equiv 1 \pmod 2$ for some i. We may assume that $f(x_1, y_1) = 1$. Clearly then, $\langle u_1, v_1 \rangle = \langle x_1, y_1 \rangle$, so that $\{x_1, y_1, u_2, v_2, \ldots, u_n, v_n\}$ is a basis of U, and hence $\{u, v, u_2, v_2, \ldots, u_n, v_n\}$ is a basis of U. Now choose $w_3, w_4, \ldots, w_{2n-1}, w_{2n}$ such that

$$w_{2i-1} = \xi_i u + \eta_i v + u_i, \quad w_{2i} = \lambda_i u + \mu_i v + v_i \quad \text{and}$$

$$w_{2i-1}, \quad w_{2i} \in \langle u, v \rangle^{\perp}, \quad i = 2, 3, \ldots, n.$$

Clearly $\{u, v, w_3, w_4, \ldots, w_{2n}\}$ is again a basis of U, and hence $U = \langle u, v \rangle \perp U_1$, where $U_1 = \langle w_3, \ldots, w_{2n} \rangle$.

LEMMA 4.7. *Let U be the symplectic module as given in Lemma 4.6. Suppose $x_1, y_1, \ldots, x_n, \quad y_n \in U$ such that $f(x_i, y_i) = 1$, $f(x_i, x_j) \equiv f(x_i, y_j) \equiv f(y_i, y_j) \equiv 0 \pmod 2$, $i, j = 1, \ldots, n$ and $i \neq j$.*

Let $x \in U$ such that $f(x, x_i) \equiv 0 \equiv f(x, y_i) \pmod 2$, $i = 1, \ldots, n$. Then $f(x, u) \equiv 0 \pmod 2$ for all $u \in U$.

PROOF. The congruences here will be modulo 2. We use induction on n. Suppose $n = 1$. Then $U = \langle x_1, y_1 \rangle$. Write $x = \xi x_1 + \eta y_1$, so that $\xi \equiv \eta \equiv 0$, and hence $f(x, u) \equiv 0$ for all $u \in U$.

Now assume that the result in the lemma is true for symplectic modules of dimension $2k$, $k \geqslant 1$. Suppose now

$$V = \langle u_1, v_1 \rangle \perp \ldots \perp \langle u_{k+1}, v_{k+1} \rangle,$$

where $f(u_i, v_i) = 1$, $i = 1, \ldots, k+1$, and $x_1, y_1, \ldots, x_{k+1}, y_{k+1}$ are elements of V satisfying the conditions of the lemma. By Lemma 4.6, we may write

$$V = \langle x_{k+1}, y_{k+1} \rangle \perp W$$

https://doi.org/10.1017/S1446788700012052 Published online by Cambridge University Press

for some submodule W whose dimension is evidently $2k$. For $1 \leqslant i \leqslant k$, write $x_i = \lambda_i x_{k+1} + \mu_i y_{k+1} + w_i$, $y_i = \xi_i x_{k+1} + \eta_i y_{k+1} + z_i$, where $w_i, z_i \in W$. Now $f(x_i, x_{k+1}) \equiv f(x_i, y_{k+1}) \equiv 0$ imply $\lambda_i \equiv \mu_i \equiv 0$. Similarly, $\xi_i \equiv \eta_i \equiv 0$. If $1 \leqslant j \leqslant k$ and $i \neq j$, we have $f(x_i, x_j) \equiv f(w_i, w_j) \equiv 0$. We also have $f(w_i, z_j) \equiv f(z_i, z_j) \equiv 0$. Moreover, since $1 = f(x_i, y_i) \equiv f(w_i, z_i)$, we may assume that $f(w_i, z_i) = 1$. Thus the elements $w_1, z_1, \ldots, w_k, z_k$ of W satisfy the conditions of the lemma.

Let $x \in V$ and $x = v_0 + v_1$, where $v_0 \in \langle x_{k+1}, y_{k+1} \rangle$, $v_1 \in W$. If $f(x, x_i) \equiv 0 \equiv f(x, y_i)$, $i = 1, \ldots, k$, then $f(v_1, w_i) \equiv 0 \equiv f(v_1, z_i)$. Hence by the induction hypothesis, $f(v_1, w) \equiv 0$ for all $w \in W$. Since $f(x, x_{k+1}) \equiv 0 \equiv f(x, y_{k+1})$, we have $f(v_0, v') \equiv 0$ for all $v' \in \langle x_{k+1}, y_{k+1} \rangle$. It is then immediate that $f(x, v) \equiv 0$ for all $v \in V$. The induction is now complete.

We are in a position to prove the following crucial result.

LEMMA 4.8. *If G has the canonical decomposition*

$$G \cong Q(n_1, r_1) \ldots Q(n_\alpha, r_\alpha) Q(l, l)^{\varepsilon_l} \ldots Q(1, 1)^{\varepsilon_1},$$

where $\alpha > 0$, $r_\alpha > 0$, $l = n_\alpha - 1$ and $\varepsilon_l > 0$, then G has no subgroup isomorphic to $Q(r, r)^{\varepsilon_r + 1}$, $r = r_\alpha$.

PROOF. Let a_i, b_i be canonical generators of $Q(n_i, r_i)$, and c_{jk}, d_{jk}, $k = 1, \ldots, \varepsilon_j$ those of $Q(j, j)^{\varepsilon_j}$, $1 \leqslant j \leqslant l$. For convenience, we will use the additive notation in writing elements of G in terms of the canonical generators. An element x of G may be written in the form

$$x = \sum_{i=1}^{\alpha} (\lambda_i a_i + \mu_i b_i) + \sum_{j=1}^{l} \sum_{k=1}^{\varepsilon_j} (\lambda_{jk} c_{jk} + \mu_{jk} d_{jk}) + \nu z, \tag{9}$$

where $\langle z \rangle = Z(G)$.

Write $r = r_\alpha$. Then

$$2^r x = \sum_{i=1}^{\alpha} \{\lambda_i 2^r a_i + \mu_i 2^r b_i + \lambda_i \mu_i 2^{r-1}(2^r - 1)\,[b_i, a_i]\}$$

$$+ \sum_{j=1}^{l} \sum_{k=1}^{\varepsilon_j} \{\lambda_{jk} 2^r c_{jk} + \mu_{jk} 2^r d_{jk} + \lambda_{jk} \mu_{jk} 2^{r-1}(2^r - 1)\,[d_{jk}, c_{jk}]\} + \nu 2^r z.$$

If $2^r x = 0$, then taking commutators on both sides, we have

$$\lambda_i 2^r [a_i, b_i] = 0 = \mu_i 2^r [a_i, b_i], \quad i = 1, \ldots, \alpha,$$

$$\lambda_{jk} 2^r [c_{jk}, d_{jk}] = 0 = \mu_{jk} 2^r [c_{jk}, d_{jk},], \quad k = 1, \ldots, \varepsilon_j, \quad r+1 \leqslant j \leqslant l.$$

https://doi.org/10.1017/S1446788700012052 Published online by Cambridge University Press

Hence we have

$$\lambda_i = \lambda'_i 2^{r_i - r}, \quad \mu_i = \mu'_i 2^{r_i - r}, \quad i = 1, \ldots, \alpha,$$

$$\lambda_{jk} = \lambda'_{jk} 2^{j-r}, \quad \mu_{jk} = \mu'_{jk} 2^{j-r}, \quad k = 1, \ldots, \varepsilon_j, \quad r+1 \leqslant j \leqslant l.$$

Thus we have

$$(10) \qquad 0 = \sum_{i=1}^{\alpha-1} \lambda'_i 2^{r_i} a_i + \lambda'_\alpha 2^r a_\alpha + \lambda'_\alpha \mu'_\alpha 2^{r-1} [a_\alpha, b_\alpha] + \sum_{k=1}^{\varepsilon_r} \lambda_{rk} \mu_{rk} 2^{r-1} [c_{rk}, d_{rk}] + \nu 2^r z.$$

Now the amalgamation may be taken so that

$$[a_\alpha, b_\alpha] = [c_{rk}, d_{rk}] = 2^{l-r} z, \quad [c_{lk}, d_{lk}] = z, \quad k = 1, \ldots, \varepsilon_l,$$

$$2^{r_i} a_i = 2^{l - n_i + r_i} z, \quad i = 1, \ldots, \alpha,$$

The relation (10) becomes

$$0 \equiv \sum_{i=1}^{\alpha-1} \lambda'_i 2^{l - n_i + r_i} + \lambda'_\alpha 2^{r-1} + \lambda'_\alpha \mu'_\alpha 2^{l-1} + \sum_{k=1}^{\varepsilon_r} \lambda_{rk} \mu_{rk} 2^{l-1} + \nu 2^r \pmod{2^l}.$$

Since $(l - n_i + r_i) - (r-1) = n_\alpha - r_\alpha - n_i + r_i > 0$, $i = 1, \ldots, \alpha - 1$, and

$$(l-1) - (r-1) = n_\alpha - r_\alpha - 1 > 0,$$

it follows that $\lambda'_\alpha \equiv 0 \pmod 2$, and $\lambda_\alpha = \lambda'_\alpha = 2\lambda''_\alpha$.
Hence if $2^r x = 0$, then x has the form

$$x = \sum_{i=1}^{\alpha-1} (\lambda_i 2^{r_i - r} a_i + \mu_i 2^{r_i - r} b_i) + 2\lambda_\alpha a_\alpha + \mu_\alpha b_\alpha$$

$$+ \sum_{j=r+1}^{l} \sum_{k=1}^{\varepsilon_j} (\lambda_{jk} 2^{j-r} c_{jk} + \mu_{jk} 2^{j-r} d_{jk})$$

$$+ \sum_{j=1}^{r} \sum_{k=1}^{\varepsilon_j} (\lambda_{jk} c_{jk} + \mu_{jk} d_{jk}) + \nu z,$$

where we have suppressed the dashes of our previous notations. Let y be another element of G such that $2^r y = 0$, and let the corresponding integers in a similar expression of y be ρ_i, σ_i, ρ_{jk}, σ_{jk}, $i = 1, \ldots, \alpha$, $k = 1, \ldots, \varepsilon_j$, $1 \leqslant j \leqslant l$. Then

$$(11) \qquad [x, y] = \sum_{i=1}^{\alpha-1} (\lambda_i \sigma_i - \mu_i \rho_i) 2^{l + r_i - 2r} z + (\lambda_\alpha \sigma_\alpha - \mu_\alpha \rho_\alpha) 2^{l-r+1} z$$

$$+ \sum_{j=r+1}^{l} \sum_{k=1}^{\varepsilon_j} (\lambda_{jk} \sigma_{jk} - \mu_{jk} \rho_{jk}) 2^{l+j-2r} z$$

$$+ \sum_{j=1}^{r} \sum_{k=1}^{\varepsilon_j} (\lambda_{jk} \sigma_{jk} - \mu_{jk} \rho_{jk}) 2^{l-j} z.$$

https://doi.org/10.1017/S1446788700012052 Published online by Cambridge University Press

To prove the lemma, we consider two cases: (i) $\varepsilon_r = 0$, (ii) $\varepsilon_r > 0$. In the first case, if G has a subgroup isomorphic to $Q(r,r)$, then there exist elements x and y of G with $2^r x = 0 = 2^r y$, and $[x,y]$ is of order 2^r. But putting $\varepsilon_r = 0$ in (11) gives $2^{r-1}[x,y] = 0$, a contradiction.

So assume that $\varepsilon_r > 0$. If $x \in G$ is expressed as in (9), define $\hat{x} \in Q(r,r)^{\varepsilon_r}$ by

$$\hat{x} = \sum_{k=1}^{\varepsilon_r} (\lambda_{rk} c_{rk} + \mu_{rk} d_{rk}),$$

and define $\tilde{x}$ as the coset of $Q(r,r)^{\varepsilon_r}$ modulo its centre with representative $\hat{x}$. Now $Q(r,r)^{\varepsilon_r}$ induces a symplectic module U of dimension $2\varepsilon_r$ over Z_{2^r} with $U = Q(r,r)^{\varepsilon_r}/Z(Q(r,r)^{\varepsilon_r})$ and an alternating form f defined on U as follows: if u, $v \in Q(r,r)^{\varepsilon_r}$, then $f(\bar{u},\bar{v}) = \lambda$, where $\bar{u},\bar{v}$ are the corresponding cosets in U and $[u,v] = \lambda[c_{r1}, d_{r1}]$.

Suppose G has a subgroup isomorphic to $Q(r,r)^{\varepsilon_r+1}$. Then there are elements x_i, y_i, $i = 1,\ldots,\varepsilon_r+1$, of G such that $\langle x_i, y_i\rangle \cong Q(r,r)$, $1 = [x_i,x_j] = [x_i,y_j] = [y_i,y_j]$, $i,j = 1,\ldots,\varepsilon_r+1$ and $i \neq j$. Let $\tilde{x}_i$, $\tilde{y}_i$ be the elements of U corresponding to x_i, y_i, $i = 1,\ldots,\varepsilon_r+1$. It follows from (11) that

$$f(\tilde{x}_i,\tilde{y}_i) \not\equiv 0 \pmod 2 \quad \text{and} \quad f(\tilde{x}_i,\tilde{x}_j) \equiv 0 \equiv f(\tilde{x}_i,\tilde{y}_j) \equiv f(\tilde{y}_i,\tilde{y}_j) \pmod 2,$$
$$i,j = 1,\ldots,\varepsilon_r+1 \text{ and } i \neq j.$$

We may assume that $f(\tilde{x}_i,\tilde{y}_i) = 1$, $i = 1,\ldots,\varepsilon_r+1$. The elements $\tilde{x}_i$, $\tilde{y}_i$, $i = 1,\ldots,\varepsilon_r$, will then satisfy the conditions of Lemma 4.7. Since $f(\tilde{x}_t,\tilde{x}_i) \equiv 0 \equiv f(\tilde{x}_t,\tilde{y}_i) \pmod 2$, $i = 1,\ldots,\varepsilon_r$, where $t = \varepsilon_r+1$, Lemma 4.7 tells us that $f(\tilde{x}_t,\tilde{y}_t) \equiv 0 \pmod 2$, a contradiction. Hence G cannot have the supposed subgroup.

We will now prove the uniqueness of the canonical decomposition.

PROOF OF THEOREM B. A non-trivial finite 2-group of class two with cyclic centre will be said to be of the first or second type according as its canonical decomposition is of the first or second type as given in Theorem A. If G or H is of the first type, we write their canonical decompositions as

$$G = Q(n_1,r_1)\ldots Q(n_\alpha,r_\alpha)\,Q(l,l)^{\varepsilon_l}\ldots Q(1,1)^{\varepsilon_1},$$

$$H = Q(m_1,s_1)\ldots Q(m_\beta,s_\beta)\,Q(k,k)^{\delta_k}\ldots Q(1,1)^{\delta_1}.$$

If G or H is of the second type, we write their canonical decompositions as

$$G = R(n)\,Q(l,l)^{\varepsilon_l}\ldots Q(1,1)^{\varepsilon_1},$$

$$H = R(m)\,Q(k,k)^{\delta_k}\ldots Q(1,1)^{\delta_1}.$$

https://doi.org/10.1017/S1446788700012052 Published online by Cambridge University Press

It is trivial that $G \cong H$ if they are of the same type and either $\alpha = \beta$, $l = k$, $n_i = m_i$, $r_i = s_i$ $(i = 1, \ldots, \alpha)$, $\varepsilon_j = \delta_j$ $(j = 1, \ldots, l)$ or $n = m$, $l = k$, $\varepsilon_j = \delta_j$ $(j = 1, \ldots, l)$.

So assume $G \cong H$.

Step 1. We prove: G and H are of the same type.

If not, we may assume G to be of the first type and H of the second type. Suppose $\alpha = 0$. Then by considering the exponents of G and H, we have $l = m$. Since we may 'multiply' the isomorphism relation $G \cong H$ throughout by $Q(l, l)$, we may assume $k = l$. From the relations $\rho_i(G) = \rho_i(H)$, $i = 0, 1, \ldots, l-1$, and Lemmas 4.1, 4.2 and 4.3, we have $\varepsilon_l = 1 + \delta_l$, $\varepsilon_i = \delta_i$, $i = 1, \ldots, l-1$. Thus, with the notations of Lemma 4.4, $Q(l, l)^{e_l} Q \cong R(l) Q(l, l)^{e_l - 1} Q$, which is impossible since these two groups, by Lemmas 4.4 and 4.5, do not have the same number of cyclic subgroups of order 2^{l+1}.

Next suppose $\alpha > 0$. The exponents of G and H are respectively 2^{n_1} and 2^{m+1}. Hence $n_1 = m+1$. Furthermore, the exponents of the derived groups of G and H are respectively $2^{\max(r_1, l)}$ and 2^m since we may assume $\varepsilon_l > 0$. But $m = n_1 - 1 > r_1$; hence $l = m$ and $\alpha = 1$. It is clear that $\varepsilon_l = 1 + \delta_l$, $1 + \varepsilon_r = \delta_r$, $\varepsilon_i = \delta_i$, $i = 1, \ldots, l-1$ and $i \neq r$. We then have $G = Q(l+1, r) Q(l, l)^n Q$ and $H = R(l) Q(l, l)^{n-1} Q_0$, where $Q = Q(l-1, l-1)^{e_{l-1}} \ldots Q(1, 1)^{e_1}$, $Q_0 = Q \cdot Q(r, r)$ and $n = \varepsilon_l$.

We now compute the number $\Lambda(G)$ (respectively $\Lambda(H)$) of elements in G (respectively H) of order 2^{l+1}. Let a, b, a_i, b_i, $i = 1, \ldots, n = \varepsilon_l$ be canonical generators of $Q(l+1, r) Q(l, l)^{e_l}$, and $\langle z \rangle = Z(G)$. Let $x \in G$ and

$$x = a^{\lambda} b^{\mu} a_1^{\lambda_1} b_1^{\mu_1} \ldots a_n^{\lambda_n} b_n^{\mu_n} x_Q z^{\nu},$$

where $x_Q \in Q$ and $0 \leqslant \lambda, \mu < 2^r$, $0 \leqslant \lambda_i, \mu_i, \nu < 2^l$, $i = 1, \ldots, n$. Then x is of order 2^{l+1} if and only if

$$\lambda + \sum_{i=1}^{n} \lambda_i \mu_i \equiv 1 \pmod 2;$$

that is, if and only if the number of integers $1 \leqslant i \leqslant n$ for which $\lambda_i \mu_i \equiv 1 \pmod 2$ is odd or even according as λ is even or odd. If ω_0 (respectively ω_1) is the number of ordered pairs (λ', μ'), where $0 \leqslant \lambda', \mu' < 2^l$, such that $\lambda' \mu' \equiv 0 \pmod 2$ (respectively $\lambda' \mu' \equiv 1 \pmod 2$), then we have

$$\Lambda(G) = |Q/Z(Q)| \cdot 2^l \left\{ 2^{r-1} \cdot 2^r \sum \binom{n}{k} \omega_1^k \omega_0^{n-k} + 2^{r-1} \cdot 2^r \sum \binom{n}{t} \omega_1^t \omega_0^{n-t} \right\},$$

where the first summation is over all those odd integers k, $1 \leqslant k \leqslant n$, and the second summation is over all those even integers t, $0 \leqslant t \leqslant n$. Hence

$$\Lambda(G) = |Q/Z(Q)| 2^{l+2r-1} (\omega_0 + \omega_1)^n = |Q/Z(Q)| 2^{(2n+1)l+2r-1}.$$

Multiplying by 2^l the number of cyclic subgroups of H of order 2^{l+1} obtained from Lemma 4.5, we have

$$\Lambda(H) = |Q_0/Z(Q_0)|\{2^{(2n+1)l-1} + 2^{(2n+1)l-n-1}\}.$$

Since $|Q_0/Z(Q_0)| = |Q/Z(Q)|2^{2r}$, we have $\Lambda(H) > \Lambda(G)$, a contradiction. Hence G and H are of the same type.

Step 2. We prove: if G and H are both of the second type, then $n = m$, $l = k$, $\varepsilon_j = \delta_j$, $j = 1, \ldots, l$.

Clearly, $n = m$. We may assume that $\varepsilon_l > 0$, $\delta_k > 0$. Suppose $l > k$. Then by Lemmas 4.1, 4.2 and 4.3, $\rho_k(G) = 2 + 2(\varepsilon_t + \ldots + \varepsilon_{k+1}) > 2$, while $\rho_k(H) = 2$, a contradiction. Hence $l = k$. It follows easily from the relations $\rho_i(G) = \rho_i(H)$, $i = 0, \ldots, l-1$, that $\varepsilon_j = \delta_j$, $j = 1, \ldots, l$.

Step 3. We prove: if G and H are both of the first type and $\alpha = 0$, then $\beta = 0$, $l = k$, $\varepsilon_j = \delta_j$, $j = 1, \ldots, l$.

Suppose $\beta > 0$. We may assume $\varepsilon_l > 0$ and $\delta_k > 0$. Then by considering the exponents of G, G', H and H', we have $l+1 = m_1$, $l = \max\{s_1, k\}$. Since $\beta > 1$ implies that $m_1 - 1 > k$ and $m_1 - 1 > s$, we have $\beta = 1$ and $l = k = m_1 - 1$. Thus $G = Q(l,l)^n Q . Q(s,s)$ and $H = Q(l+1,s) Q(l,l)^n Q$, where $n = \varepsilon_1$, $s = s_1$, and $Q = Q(l-1,l-1)^{\delta_{l-1}} \ldots Q(1,1)^{\delta_1}$. If $\Lambda)G)$ and $\Lambda(H)$ have the same meaning as in the proof of Step 1, $\Lambda(H)$ may be obtained as in Step 1 and $\Lambda(G)$ obtained from Lemma 4.4. A comparison shows that $\Lambda(G) < \Lambda(H)$, a contradiction. Hence $\beta = 0$. Finally, as in Step 2, $l = k$, $\varepsilon_j = \delta_j$, $j = 1, \ldots, l$.

Henceforth we assume G and H are both of the first type with $\alpha > 0$ and $\beta > 0$.

Step 4. We prove: $n_1 = m_1$, $r_1 = s_1$.

It is clear that $n_1 = m_1$ and that $r_1 = 0$ implies $s_1 = 0$. If we now 'multiply' the relation $G \cong H$ throughout by $Q(n,n)$, where $n = n_1 - 1$, we obtain after the necessary reduction the following isomorphism relation

$$G_1 = Q(n_1, r_1) Q(n,n)^{\lambda_n} \ldots Q(1,1)^{\lambda_1} \cong Q(n_1, s_1) Q(n,n)^{\mu_n} \ldots Q(1,1)^{\mu_1} = H_1,$$

where $\lambda_n > 0$, $\mu_n > 0$. Suppose $r_1 > s_1$. From the relations $\rho_i(G_1) = \rho_i(H_1)$, $i = r_1 - 1$, r_1, we have $1 + \lambda_r = \mu_r$, $r = r_1$. Thus G_1 has a subgroup isomorphic to $Q(r,r)^{\lambda_r + 1}$, contradicting Lemma 4.8. Hence $r_1 = s_1$.

Step 5. We prove: $\alpha = \beta$, $n_i = m_i$, $r_i = s_i$, $i = 1, \ldots, \alpha$.

First we prove that if $n_i = m_i$, $r_i = s_i$, $i = 1, \ldots, \nu$, where $1 \leqslant \nu < \min\{\alpha, \beta\}$, then $n_{\nu+1} = m_{\nu+1}$, $r_{\nu+1} = s_{\nu+1}$. Suppose $n_{\nu+1} > m_{\nu+1}$. As in Step 4, we would then have the isomorphism $G_1 \cong H_1$, where

$$G_1 = Q(n_1, r_1) \ldots Q(n_\nu, r_\nu) Q(n_{\nu+1}, r_{\nu+1}) Q(n,n)^{\lambda_n} \ldots Q(1,1)^{\lambda_1},$$

$$H_1 = Q(n_1, r_1) \ldots Q(n_\nu, r_\nu) Q(n,n)^{\mu_n} \ldots Q(1,1)^{\mu_1},$$

https://doi.org/10.1017/S1446788700012052 Published online by Cambridge University Press

with $n = n_{\nu+1} - 1$ and $\lambda_n > 0$. The centres of G_1 and H_1 show that $r_{\nu+1} > 0$, and we conclude from the relations $\rho_i(G_1) = \rho_i(H_1)$, $i = r_{\nu+1} - 1$, $r_{\nu+1}$, that $\mu_r = 1 + \lambda_r$, $r = r_{\nu+1}$. Thus G_1 would have a subgroup isomorphic to $Q(r, r)^{\lambda_r+1}$, contradicting Lemma 4.8. Hence $n_{\nu+1} = m_{\nu+1}$. A similar argument shows that the supposition $r_{\nu+1} > s_{\nu+1}$ leads again to a contradiction of Lemma 4.8; and hence $r_{\nu+1} = s_{\nu+1}$. Together with the above remarks, Step 4 and a further application of the above argument in case $\alpha \neq \beta$ lead to the stated assertion.

Step 6. We prove: $l = k$, $\varepsilon_i = \delta_i$, $i = 1, \ldots, l$.

If $\varepsilon_l = 0$ and $\delta_k = 0$, we are done. If $\varepsilon_l > 0$ and $\delta_k = 0$, then

$$\rho_{l-1}(G) - \rho_{l-1}(H) = 2\varepsilon_l > 0,$$

a contradiction. Hence we may assume $\varepsilon_l > 0$ and $\delta_k > 0$. Suppose $l > k$; then again $\rho_{l-1}(G) = \rho_{l-1}(H) + 2\varepsilon_l$, which is impossible. Hence $l = k$. Finally, the relations $\rho_i(G) = \rho_i(H)$, $i = 0, 1, \ldots, l-1$, imply that $\varepsilon_i = \delta_i$, $i = 1, \ldots, l$. The proof is then complete.

Acknowledgement

The author would like to thank the referee for his useful comments and helpful suggestions.

References

J. M. Brady (1970), *Just-non-Cross varieties of groups* (Ph.D. Thesis, Australian National University).

J. M. Brady, R. A. Bryce and John Cossey (1969), 'On certain abelian-by-nilpotent varieties', *Bull. Austral. Math. Soc.* **1**, 403–416.

D. Gorenstein (1968), *Finite groups* (Harper and Row, New York, Evanston and London).

G. Higman (1967), 'The orders of relatively free groups', *Proc. Internat. Conf. on Theory of Groups*, Australian National University, Canberra, edited by L. G. Kovács and B. H. Neumann (Gordon and Breach, New York).

Y. K. Leong (1974a), 'Odd order nilpotent groups of class two with cyclic centre', *J. Austral. Math. Soc.* **17**, 142–153.

Y. K. Leong (1974b), 'The CREAM conjecture for the subvarieties of certain abelian-by-nilpotent varieties', *Bull. Austral. Math. Soc.* **10**, 429–451.

Department of Mathematics
University of Singapore
Singapore 10