ODD ORDER NILPOTENT GROUPS OF CLASS TWO WITH CYCLIC CENTRE

Dedicated to the memory of Hanna Neumann

Y. K. LEONG

(Received 5 July 1972)

Communicated by M. F. Newman

1. Introduction

The isomorphism problem for finite groups of odd order and nilpotency class 2 with cyclic centre will be solved using some results of Brady [1], [2]. Since a finite nilpotent group is the direct product of its Sylow subgroups, we only need to consider finite q-groups where q is a prime. It has been shown in [1] and [2] that a finite q-group of nilpotency class 2 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 q-groups of class 2 on two generators with cyclic centre comprise the following list:

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

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

and if $q = 2$ we have as well

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

We shall also use the notation $Q(n,0)$ for the cyclic group of order q^n, $n > 0$. For the definition of a central product, see [3]. A central product of the $Q(n,r)$ and $R(n)$ depends, of course, on the way the common subgroup is amalgamated. However, Brady [1] has shown that all central products with cyclic centre of a given finite set of the $Q(n,r)$ and $R(n)$ are, in fact, isomorphic.

In the next two sections, we shall assume that q is odd and show that while a q-group of class 2 with cyclic centre may have many decompositions as a central

https://doi.org/10.1017/S1446788700016724 Published online by Cambridge University Press

product of centrally indecomposable factors, there is a canonic type of decomposition to which an analogue of the Krull-Schmidt Theorem for direct products applies. Our results should be compared with those in [4], [5] and [6].

This work forms part of my Ph. D. thesis submitted to the Australian National University. I thank my supervisor, Dr. R. A. Bryce, for suggesting the problem and his guidance and supervision.

2. The canonic decomposition

Henceforth $Q(n_1, r_1) \cdots Q(n_\alpha, r_\alpha)$ will always denote the central product with cyclic centre of the $Q(n_i, r_i)$, $i = 1, \cdots, \alpha$. We say that the elements a, b are *canonic generators* of $Q(n, r)$, $r > 0$, if they generate $Q(n, r)$ and satisfy the defining relations in the preceding section. We also say that the elements a_i, b_i, $i = 1, \cdots, \alpha$, are *canonic generators* of $Q(n_1, r_1) \cdots Q(n_\alpha, r_\alpha)$, where $r_i > 0$, $i = 1, \cdots, \alpha$, if a_i, b_i are canonic generators of $Q(n_i, r_i)$, $i = 1, \cdots, \alpha$. We say that $Q(n, r)$ is of *Type* I or of *Type* II according as $2r \leqq n$ or $2r > n$.

We first investigate the different ways a finite q-group of class 2 with cyclic centre decomposes.

LEMMA 2.1. *$Q(n_1, r_1)Q(n_2, r_2) \cong Q(n_1, r_1)Q(r_2, r_2)$ if either $n_1 \geqq n_2$ and $0 < r_1 \leqq r_2$, or $n_1 \geqq n_2$, $n_1 - r_1 \geqq n_2 - r_2$ and $r_1 > r_2 > 0$.*

PROOF. We consider the first case only; the second is similar. Let

$$G = Q(n_1, r_1)Q(n_2, r_2).$$

First we show that canonic generators a_i, b_i of $Q(n_i, r_i)$, $i = 1, 2$, may be chosen such that

$$a_1^{q^{n_1-n_2+r_2}} = a_2^{q^{r_2}}, \tag{1}$$

$$[a_1, b_1] = [a_2, b_2]^{q^{r_2-r_1}}. \tag{2}$$

(i) $1 \leqq r_1 \leqq r_2 \leqq [\frac{1}{2}n_2] \leqq [\frac{1}{2}n_1]$.

Both $Q(n_1, r_1)$ and $Q(n_2, r_2)$ are of Type I, so that $Z(Q(n_i, r_i)) = \langle a_i^{q^{r_i}} \rangle$, $i = 1, 2$. Moreover, $n_1 - r_1 \geqq n_2 - r_2$ since $n_1 - n_2 \geqq 0 \geqq r_1 - r_2$. Thus,

$$Z(Q(n_2, r_2)) \leqq Z(Q(n_1, r_1)).$$

The amalgamation may be chosen to give $a_2^{q^{r_2}} = a_1^{q^{n_1-n_2+r_2}}$. Since

$$r_1 + r_2 \leqq 2[\tfrac{1}{2}n_2] \leqq n_2,$$

we have

$$[a_1, b_1] = a_1^{q^{n_1-r_1}} = (a_1^{q^{n_1-n_2+r_2}})^{q^{n_2-r_1-r_2}} = a_2^{q^{n_2-r_1}} = (a_2^{q^{n_2-r_2}})^{q^{r_2-r_1}}$$
$$= [a_2, b_2]^{q^{r_2-r_1}}.$$

(ii) $[\frac{1}{2}n_2] \leqq [\frac{1}{2}n_1] < r_1 \leqq r_2 \leqq n_2 \leqq n_1$.

Both $Q(n_1, r_1)$ and $Q(n_2, r_2)$ are of Type II, so that $Z(Q(n_i, r_i)) = \langle [a_i, b_i] \rangle$, $i = 1, 2$. The amalgamation may be given by

$$[a_1, b_1] = [a_2, b_2]^{q^{r_2 - r_1}}.$$

Since $r_1 + r_2 > 2[\frac{1}{2}n_1] \geqq n_1 - 1 \geqq n_2 - 1$, we have

$$\begin{aligned} a_2^{q^{r_2}} = [a_2, b_2]^{q^{2r_2 - n_2}} &= ([a_2, b_2]^{q^{r_2 - r_1}})^{q^{r_1 + r_2 - n_2}} = [a_1, b_1]^{q^{r_1 + r_2 - n_2}} \\ &= ([a_1, b_1]^{q^{2r_1 - n_1}})^{q^{n_1 - r_1 + r_2 - n_2}} = a_1^{q^{n_1 - n_2 + r_2}}. \end{aligned}$$

(iii) $1 \leqq r_1 \leqq [\frac{1}{2}n_1]$, $[\frac{1}{2}n_2] < r_2 \leqq n_2$.

$Q(n_1, r_1)$ is of Type I, and $Q(n_2, r_2)$ is of Type II. The centres of $Q(n_1, r_1)$, $Q(n_2, r_2)$ are $\langle a_1^{q^{r_1}} \rangle$, $\langle [a_2, b_2] \rangle$ respectively. If $n_1 - r_1 \geqq r_2$, the amalgamation may be given by $a_1^{q^{n_1 - r_2}} = [a_2, b_2]$, so that

$$\begin{aligned} a_2^{q^{r_2}} = [a_2, b_2]^{q^{2r_2 - n_2}} = a_1^{q^{n_1 - n_2 + r_2}}, \text{ and } [a_1, b_1] = a_1^{q^{n_1 - r_1}} &= (a_1^{q^{n_1 - r_2}})^{q^{r_2 - r_1}} \\ &= [a_2, b_2]^{q^{r_2 - r_1}}. \end{aligned}$$

However, if $n_1 - r_1 < r_2$, the amalgamation may be given by $a_1^{q^{r_1}} = [a_2, b_2]^{q^{r_1 + r_2 - n_1}}$, so that $a_2^{q^{r_2}} = ([a_2, b_2]^{q^{r_1 + r_2 - n_1}})^{q^{n_1 - n_2 + r_2 - r_1}} = a_1^{q^{n_1 - n_2 + r_2}}$, and $[a_1, b_1] = a_1^{q^{n_1 - r_1}} = (a_1^{q^{r_1}})^{q^{n_1 - 2r_1}} = [a_2, b_2]^{q^{r_2 - r_1}}$.

Hence the relations (1) and (2) are valid. Finally, put

$$x_1 = a_1, \ y_1 = b_1 b_2^{q^{n_1 - n_2 + r_2 - r_1}}, \ x_2 = a_1^{q^{n_1 - n_2}} a_2^{-1}, \ y_2 = b_2.$$

Then $[x_2, y_1] = 1$, from relation (2). Hence $\langle x_1, y_1 \rangle$ and $\langle x_2, y_2 \rangle$ centralize each other. From relation (1), we deduce that $\langle x_2, y_2 \rangle \cong Q(r_2, r_2)$. Also, $\langle x_1, y_1 \rangle \cong Q(n_1, r_1)$ and $G = \langle x_1, y_1 \rangle \cdot \langle x_2, y_2 \rangle$. Therefore, $G \cong Q(n_1, r_1)Q(r_2, r_2)$.

Lemma 2.2. *$Q(n_1, 0)Q(n_2, r_2) \cong Q(n_2, r_2)$ if $n_1 \leqq r_2$ or $n_1 \leqq n_2 - r_2$.*

Proof. For, $Q(n_1, 0) = Z(Q(n_1, 0)) \leqq Z(Q(n_2, r_2))$.

Lemma 2.3. *$Q(n_1, 0)Q(n_2, r_2) \cong Q(n_1, 0)Q(r_2, r_2)$ if $n_1 \geqq n_2$.*

Proof. Let $Q(n_1, 0) = \langle a_1 \rangle$, and let a_2, b_2 be cannonic generators of $Q(r_2, r_2)$. The amalgamation may be given by $a_1^{q^{n_1 - r_2}} = [a_2, b_2]$. Put $x_2 = a_1^{q^{n_1 - n_2}} a_2$, $y_2 = b_2$. Then

$$\langle a_1, a_2, b_2 \rangle = \langle a_1 \rangle \cdot \langle x_2, y_2 \rangle,$$

where $\langle a_1 \rangle$ centralizes $\langle x_2, y_2 \rangle \cong Q(n_2, r_2)$.

Lemma 2.4. *$Q(n_1, r_1)Q(n_2, r_2) \cong Q(n_1, r_1)Q(r_2, r_2)$ if $r_1 \geqq n_2$.*

https://doi.org/10.1017/S1446788700016724 Published online by Cambridge University Press

Proof. There is a q^{n_2}-cycle $C \leqq Z(Q(n_1, r_1))$. Hence

$$\begin{aligned} Q(n_1, r_1)Q(n_2, r_2) &= Q(n_1, r_1)CQ(n_2, r_2) \cong Q(n_1, r_1)CQ(r_2, r_2) \\ &= Q(n_1, r_1)Q(r_2, r_2), \text{ by Lemma 2.3.} \end{aligned}$$

We can now give the *canonic decomposition* of a finite q-group of class 2 with cyclic centre when q is an odd prime. Its uniqueness will be proved in the next section.

Theorem 2.5. *Let q be an odd prime. Then every finite q-group G of class 2 with cyclic centre has the central decomposition,*

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

where $\alpha \geqq 0$, $\varepsilon_i \geqq 0$, $i = 1, \cdots, l$,

$$n_1 > \cdots > n_\alpha > l,\ n_\alpha > r_1 > \cdots > r_\alpha \geqq 0,\ 0 < n_1 - r_1 < \cdots < n_\alpha - r_\alpha.$$

Proof. We may suppose that G is non-trivial. Then by 2.1 and 2.2 of [2], G has a decomposition as a central product of $Q(n, r)$'s which we arrange as

$$(*) \qquad G \cong Q(n_1, r_1) \cdots Q(n_\beta, r_\beta)Q(k, k)^{\lambda_k} \cdots Q(1, 1)^{\lambda_1},$$

where $n_1 \geqq \cdots \geqq n_\beta > 0$, $n_i > r_i > 0$ $(1 \leqq i \leqq \beta - 1)$, $n_\beta > r_\beta \geqq 0$, and where $\lambda_1, \cdots, \lambda_k \geqq 0$, and $\lambda_k = 0$ implies $\lambda_1 = \cdots = \lambda_{k-1} = 0$ also.

We prove by induction on β that G has a decomposition of the type asserted. The case $\beta = 0$ is easy; so suppose $\beta > 0$ and that all groups with a decomposition of the type (*) with fewer than β factors of the form $Q(n, r)$ with $n > r$ do satisfy the statement of the theorem.

First suppose there exists $1 \leqq i \leqq \beta$ such that $n_i = n_{i+1}$. Then, from Lemmas 2.1 or 2.3, we have

$$Q(n_i, r_i)Q(n_{i+1}, r_{i+1}) \cong Q(n_i, r)Q(s, s)$$

where $r = \min\{r_i, r_{i+1}\}$, $s = \max\{r_i, r_{i+1}\}$.

Hence G has a decomposition with $\beta - 1$ factors of the form $Q(n, r)$ with $n > r$ and so, by induction, we are done. We may therefore suppose that

$$n_1 > \cdots > n_\beta > 0.$$

If, for some $1 \leqq i \leqq \beta$, either $r_i \leqq r_{i+1}$; or $r_i > r_{i+1}$ but $n_i - r_i \geqq n_{i+1} - r_{i+1}$, then using Lemmas 2.1 or 2.2, we again give G a decomposition with fewer than β $Q(n, r)$'s with $n > r$. Hence we may suppose that

$$r_1 > \cdots > r_\beta \geqq 0,\ 0 < n_1 - r_1 < \cdots < n_\beta - r_\beta.$$

Finally, if $\lambda_k \neq 0$ and $n_\beta \leqq k$, then by Lemma 2.4,

$$Q(n_\beta, r_\beta)Q(k, k) \cong Q(k, k)Q(r_\beta, r_\beta),$$

https://doi.org/10.1017/S1446788700016724 Published online by Cambridge University Press

and we can again use induction. Hence we may suppose that $n_\beta > k$. And if $n_\alpha \leqq r_1$, use Lemma 2.4 again. The induction is now complete.

3. Uniqueness of the canonic decomposition

In this section G and H will always denote finite q-groups of class 2 with cyclic centre. We write $G = G_* G_0$ where $G_* = Q(n_1, r_1) \cdots Q(n_\alpha, r_\alpha)$ and $G_0 = Q(l, l)^{\varepsilon_l} \cdots Q(1, 1)^{\varepsilon_1}$, satisfying the conditions of the canonic decomposition in Theorem 2.5. Note that $G_* = 1$ if $\alpha = 0$. Similar comments apply to the notation $H = H_* H_0$. For any finite q-group A, we use the notations:

$$\Omega^i(A) = \langle x^{q^i} : x \in A \rangle, \ i \geqq 0,$$

$$d(A) = \text{minimal number of generators of } A.$$

For $i \geqq 0$, we define the numbers $\rho_i(G)$ and $\sigma_i(G)$ as follows:

$$\rho_i(G) = \begin{cases} d(\Omega^i(G/Z(G))) & \text{if } \Omega^i(G/Z(G)) \neq 1, \\ 0 & \text{if } \Omega^i(G/Z(G)) = 1; \end{cases}$$

$$\sigma_i(G) = \begin{cases} d(\Omega^i(G)/\Omega^i(G')) & \text{if } \Omega^i(G)/\Omega^i(G') \neq 1, \\ 0 & \text{if } \Omega^i(G)/\Omega^i(G') = 1. \end{cases}$$

These numbers are clearly isomorphism invariants and will play an important role in the proof of the uniqueness of the canonic decomposition. We can easily calculate $\rho_i(G)$ from the following three lemmas.

LEMMA 3.1. *Let GH be the central product of G and H with cyclic centre. Then*

$$\rho_i(GH) = \rho_i(G) + \rho_i(H), \qquad i \geqq 0.$$

PROOF. Since the centre of GH is cyclic, we may assume that $Z(G) \geqq Z(H)$. If $GH = G$, then $H \leqq Z(G)$ and so H is cyclic. By definition, $\rho_i(H) = 0$ and hence $\rho_i(GH) = \rho_i(G) + \rho_i(H)$. Similarly when $GH = H$.

So assume that $GH \neq G$ and $GH \neq H$. Then

$$\Omega^i(GH \,/\, Z(GH)) = \Omega^i(G \,/\, Z(G)).\ \Omega^i(HZ(G) \,/\, Z(G)).$$

We claim that $\Omega^i(G/Z(G)) \cap \Omega^i(HZ(G)/Z(G)) = 1$. For if $\bar{x}$ belongs to this intersection, then $\bar{x} = g^{q^i} Z(G) = h^{q^i} Z(G)$ for some $g \in G$, $h \in H$, and hence $h^{q^i} \in G \cap H = Z(H) \leqq Z(G)$, and so $\bar{x} = 1$. Also, $HZ(G)/Z(G) \cong H/H \cap Z(G) = H/Z(H)$. Since all the factor groups dealt with are abelian q-groups, we have the required result.

LEMMA 3.2. *For $i \geqq 0, j \geqq 1$,*

$$\rho_i(Q(n_1, r_1) \cdots Q(n_j, r_j)) = \rho_i(Q(n_1, r_1)) + \cdots + \rho_i(Q(n_j, r_j)).$$

https://doi.org/10.1017/S1446788700016724 Published online by Cambridge University Press

PROOF. This follows from Lemma 3.1 by an easy induction.

LEMMA 3.3.

$$\rho_i(Q(n,r)) = \begin{cases} 2 & \text{if } 0 \leqq i < r, \\ 0 & \text{if } i \geqq r. \end{cases}$$

PROOF. If $r = 0$, there is nothing to prove. So suppose $r > 0$. Let $G = Q(n,r) = \langle a, b \rangle$. Then, for $0 \leqq i < r$,

$$a^{q^i}, b^{q^i} \notin Z(G), \text{ and } \langle a^{q^i} Z(G) \rangle \cap \langle b^{q^i} Z(G) \rangle = 1,$$

so that

$$\Omega^i(G/Z(G)) = \langle a^{q^i} Z(G) \rangle \times \langle b^{q^i} Z(G) \rangle.$$

However, for $i \geqq r$, $a^{q^i} \in Z(G)$ and $b^{q^i} = 1$, and hence $\Omega^i(G/Z(G)) = 1$.

The calculation of $\sigma_i(G)$ is more complicated, and it is useful to introduce the auxiliary constants $\sigma_i(G_*)$, $\sigma_i(G_0)$, $i \geqq 0$, corresponding to each G, defined by:

$$\sigma_i(G_*) = \begin{cases} d(\Omega^i(G_*)\Omega^i(G')/\Omega^i(G')) & \text{if } \Omega^i(G_*)\Omega^i(G')/\Omega^i(G') \neq 1, \\ 0 & \text{if } \Omega^i(G_*)\Omega^i(G')/\Omega^i(G') = 1; \end{cases}$$

$$\sigma_i(G_0) = \begin{cases} d(\Omega^i(G_0)/\Omega^i(G_0')) & \text{if } \Omega^i(G_0)/\Omega^i(G_0') \neq 1, \\ 0 & \text{if } \Omega^i(G_0)/\Omega^i(G_0') = 1; \end{cases}$$

their relevance is given by the next lemma.

LEMMA 3.4. *For $i \geqq 0$, $\sigma_i(G) = \sigma_i(G_*) + \sigma_i(G_0)$.*

PROOF. The result is trivial if $G_0 = 1$. So suppose $G_0 \neq 1$. Write $N = \Omega^i(G')$, $A = \Omega^i(G_*)N/N$, $B = \Omega^i(G_0)N/N$, so that $\Omega^i(G)/\Omega^i(G') = AB$.

We claim that $A \cap B = 1$. Let $\bar{x} = xN \in A \cap B$ and we may suppose $x \in \Omega^i(G_0)$. Then x is central in G, and hence $x \in \Omega^i(G_0) \cap Z(G_0)$. If we could show that

$$(*) \qquad \Omega^i(G_0) \cap Z(G_0) \leqq \Omega^i(G_0'),$$

then $\bar{x} = 1$. To do this, let

$$Q(j,j)^{\varepsilon_j} = \langle a_{jk}, b_{jk} \colon k = 1, \cdots, \varepsilon_j \rangle, \qquad j = 1, \cdots, l;\ \varepsilon_l > 0.$$

Let $y \in \Omega^i(G_0)$. Then

$$y = \left(\prod_{j=i+1}^{l} \prod_{k=1}^{\varepsilon_j} a_{jk}^{\lambda_{jk} q^i} b_{jk}^{\mu_{jk} q^i} \right) [a_{l1}, b_{l1}]^{\nu q^i}.$$

If $y \in Z(G_0)$, then commuting with a_{jk} and b_{jk}, we get $1 = [a_{jk}, b_{ik}]^{\lambda_{jk} q^i} = [a_{jk}, b_{jk}]^{\mu_{jk} q^i}$. Hence q^j divides $\lambda_{jk} q^i$ and $\mu_{jk} q^i$, and so $y = [a_{l1}, b_{l1}]^{\nu q^i} \in \Omega^i(G_0')$. Therefore (*) is proved.

Finally, $B \cong \Omega^i(G_0) / \Omega^i(G_0) \cap N$, and it can be shown as in above that $\Omega^i(G_0) \cap N = \Omega^i(G_0')$. Since AB is an abelian q-group, we have the lemma.

https://doi.org/10.1017/S1446788700016724 Published online by Cambridge University Press

We require a few preliminary results whose proofs are similar to that of Lemma 2.1, so we omit them.

LEMMA 3.5. *Let $n_1 > n_2 > r_1 > r_2 > 0$, $n_1 - r_1 < n_2 - r_2$. Then canonic generators a_i, b_i, $i = 1, 2$, of $Q(n_1, r_1)Q(n_2, r_2)$ can be chosen such that*

$$a_1^{q^{r_1}} = a_2^{q^{n_2-n_1+r_1}}, \ [a_1, b_1]^{q^{r_1-r_2}} = [a_2, b_2].$$

LEMMA 3.6. *Let $n_1 > n_2 > r_1 > 0$, $n_1 - r_1 < n_2$. Let $Q(n_2, 0) = \langle a_2 \rangle$. Then canonic generators a_1, b_1 of $Q(n_1, r_1)$ can be chosen such that the following relation holds in $Q(n_1, r_1)Q(n_2, 0)$*

$$a_1^{q^{r_1}} = a_2^{q^{n_2-n_1+r_1}}.$$

In the rest of this section, we denote the canonic generators of $G* = Q(n_1, r_1) \cdots Q(n_\alpha, r_\alpha)$ by a_i, b_i, $i = 1, \cdots, \alpha$. If $r_\alpha = 0$, we set $b_\alpha = 1$.

LEMMA 3.7. *Let $r \geqq n_{i+1} - n_i + r_i$, $1 \leqq i < \alpha$. Then*

$$\Omega^r(G_*) = \Omega^r(Q(n_1, r_1) \cdots Q(n_i, r_i)).$$

PROOF. Let $1 \leqq i < j \leqq \alpha$. We have, by Lemmas 3.5 and 3.6, that the canonic generators may be chosen so that $a_i^{q^{r_i}} = a_j^{q^{n_j-n_i+r_i}}$. Since $r \geqq n_{i+1} - n_i + r_i \geqq n_j - n_i + r_i$, we have

$$a_j^{q^r} = a_i^{q^{r+n_i-n_j}} \in \Omega^r(Q(n_i, r_i)).$$

Also, $r \geqq n_{i+1} - n_i + r_i > r_{i+1} \geqq r_j$ and hence $b_j^{q^r} = 1$. Therefore $\Omega^r(Q(n_j, r_j)) \leqq \Omega^r(Q(n_i, r_i))$.

COROLLARY 3.8. *Let $r \geqq r_{i+1}$, $0 \leqq i < \alpha$. Then $\Omega^r(G_*) = \Omega^r(Q(n_1, r_1) \cdots Q(n_{i+1}, r_{i+1}))$.*

PROOF. If $i = \alpha - 1$, there is nothing to prove. If $i < \alpha - 1$, then $r_{i+1} > n_{i+2} - n_{i+1} + r_{i+1}$ and the corollary follows from Lemma 3.7.

LEMMA 3.9. *Let $r \geqq 0$. If $a_i^{q^r} \neq 1$, then $a_i^{q^r} \notin \Omega^r(G')$.*

PROOF. $G' = G'_*$ or G'_0 according as $r_1 \geqq l$ or $r_1 < l$. Hence $|\Omega^r(G')| = 1$ or q^{m-r}, where $m = \max\{r_1, l\}$, according as $r \geqq m$ or $r < m$.

If $r \geqq m$, clearly $a_i^{q^r} \notin \Omega^r(G')$. If $r < m$, suppose $a_i^{q^r} \in \Omega^r(G')$; then $a_i^{q^m} = (a_i^{q^r})^{q^{m-r}} = 1$, which is a contradiction since $m < n_i$, $i = 1, \cdots, \alpha$. Hence $a_i^{q^r} \notin \Omega^r(G')$.

We can now calculate $\sigma_i(G_*)$, $\sigma_i(G_0)$, $i \geqq 0$.

https://doi.org/10.1017/S1446788700016724 Published online by Cambridge University Press

LEMMA 3.10.

$$\sigma_r(G_0) = \begin{cases} 2(\varepsilon_l + \cdots + \varepsilon_{r+1}) & \text{if } l > r \geqq 0, \\ 0 & \text{if } \quad r \geqq l. \end{cases}$$

PROOF. Recall that $G_0 = Q(l,l)^{\varepsilon_l} \cdots Q(1,1)^{\varepsilon_1}$, $\varepsilon_i \geqq 0$, $i = 1, \cdots, l$. We may assume that $\varepsilon_l > 0$. If $r \geqq l$, then $\Omega^r(G_0) = 1 = \Omega^r(G_0')$ and hence $\sigma_r(G_0) = 0$.

So suppose $0 \leqq r < l$. Write

$$Q_i = Q(i,i)^{\varepsilon_i} = \langle x_{ij}, y_{ij} : j = 1, \cdots, \varepsilon_i \rangle, \; i = 1, \cdots, l.$$

Then $\Omega^r(G_0) = \Omega^r(Q_l \cdots Q_{r+1})$, $\Omega^r(G_0') = \Omega^r(Q_l')$. Write $P_i = \Omega^r(Q_i)\Omega^r(Q_l')/\Omega^r(Q_l')$, $i = 1, \cdots, l$. Clearly $P_i = 1$ for $i \leqq r$. We now show that

$$P_i \cong \Omega^r(Q_i)/\Omega^r(Q_i'), \; \mathrm{i} = 1, \cdots, l.$$

We may suppose $i > r$. It is sufficient to prove that

$$\Omega^r(Q_i) \cap \Omega^r(Q_l') = \Omega^r(Q_i').$$

Let $x \in \Omega^r(Q_i) \cap \Omega^r(Q_l')$, where

$$x = \left(\prod_{j=1}^{\varepsilon_i} x_{ij}^{\lambda_j q^r} y_{ij}^{\mu_j q^r} \right) [x_{il}, y_{il}]^{\nu q^r} \; .$$

Then x is central in Q_i. Commuting with x_{ij} and y_{ij}, we have

$$1 = [x_{ij}, y_{ij}]^{\lambda_j q^r} = [x_{ij}, y_{ij}]^{\mu_j q^r}.$$

Hence q^i divides $\lambda_j q^r$ and $\mu_j q^r$ and so $x = [x_{il}, y_{il}]^{\nu q^r} \in \Omega^r(Q_i')$. The opposite inclusion is obvious.

Finally, we claim that for $r < i \leqq l$,

$$P_i \cap P_l \cdots P_{i+1} P_{i-1} \cdots P_{r+1} = 1.$$

For let $\bar{y}$ belong to this intersection, where we may assume that $y \in \Omega^r(Q_i)$, so that y is central in Q_i. As in above, we see that $y \in \Omega^r(Q_i')$, and hence $\bar{y} = 1$.

It is clear that for $r < i \leqq l$,

$$\Omega^r(Q_i)/\Omega^r(Q_i') = \langle \bar{x}_{il}^{q^r} \rangle \times \langle \bar{y}_{il}^{q^r} \rangle \times \cdots \times \langle \bar{x}_{i\varepsilon_i}^{q^r} \rangle \times \langle \bar{y}_{i\varepsilon_i}^{q^r} \rangle,$$

and hence $d(P_i) = 2\varepsilon_i$, $i = r+1, \cdots, l$. Since

$$\Omega^r(G_0)/\Omega^r(G_0') = P_l \times P_{l-1} \times \cdots \times P_{r+1},$$

we have the required result.

LEMMA 3.11. *Let* $n_{i+1} - n_i + r_i \leqq r < r_i$, $1 \leqq i < \alpha$. *Then*

$$\sigma_r(G_*) = 2i.$$

PROOF. By Lemma 3.7,

$$\Omega^r(G_*) = \Omega^r(Q(n_1, r_1) \cdots Q(n_i, r_i)).$$

https://doi.org/10.1017/S1446788700016724 Published online by Cambridge University Press

Write

$$P = \Omega^r(G_*)\Omega^r(G')/\Omega^r(G') = \langle \bar a_1^{q^r}, \bar b_1^{q^r}, \cdots, \bar a_i^{q^r}, \bar b_i^{q^r} \rangle.$$

We claim that the set $S = \{\bar a_j^{q^r}, \bar b_j^{q^r}, j = 1, \cdots, i\}$ is a minimal set of generators for P. If not, we can eliminate at least one element x from S. Suppose $x = \bar b_j^{q^r}$ for some $1 \leqq j \leqq i$. Then x can be expressed in terms of the other generators, and since $\Omega^r(G') \leqq Z(G)$, we have $1 = [a_j, b_j^{q^r}] = [a_j, b_j]^{q^r}$, which is impossible as $r < r_i \leqq r_j$. Similarly if $x = \bar a_j^{q^r}$ for some $1 \leqq j \leqq i$. Hence S is a minimal set. Since P is an abelian q-group, we have $d(P) = 2i$.

LEMMA 3.12. *Suppose $r_\alpha > 0$. Let $0 \leqq r < r_\alpha$. Then*

$$\sigma_r(G_*) = 2\alpha.$$

PROOF. This is similar to that of the preceding lemma.

LEMMA 3.13. *Let $r_{i+1} \leqq r < n_{i+1} - n_i + r_i$, $0 \leqq i < \alpha$, where we set $n_0 = r_0 = 0$. Then*

$$\sigma_r(G_*) = 2i + 1.$$

PROOF. By Corollary 3.8,

$$\Omega^r(G_*) = \Omega^r(Q(n_1, r_1) \cdots Q(n_{i+1}, r_{i+1})).$$

Write

$$P = \Omega^r(G_*)\Omega^r(G') / \Omega^r(G')$$
$$= \langle \bar a_1^{q^r}, \cdots, \bar a_{i+1}^{q^r}, \bar b_1^{q^r}, \cdots, \bar b_i^{q^r} \rangle.$$

We claim that the set $S = \{\bar a_1^{q^r}, \cdots, \bar a_{i+1}^{q^r}, \bar b_1^{q^r}, \cdots, \bar b_i^{q^r}\}$ is a minimal set of generators for P. If not, we can delete at least one element x from S. Suppose that $x = \bar a_j^{q^r}$ or $\bar b_j^{q^r}$ for some $1 \leqq j \leqq i$. Then x can be expressed in terms of the other generators, and since $\Omega^r(G') \leqq Z(G)$, we have that $[a_j, b_j]^{q^r} = 1$ in either case. This is impossible since $r < n_{i+1} - n_i + r_i < r_i \leqq r_j$. So suppose $x = \bar a_{i+1}^{q^r}$. We then proceed as follows. We would have

$$a_{i+1}^{q^r} = a_1^{\lambda_1 q^r} \cdots a_i^{\lambda_i q^r} b_1^{\mu_1 q^r} \cdots b_i^{\mu_i q^r} c$$

for some $c \in \Omega^r(G')$. Commuting both sides with a_j and b_j, $1 \leqq j \leqq i$, we have

$$1 = [a_j, b_j]^{\lambda_j q^r} = [a_j, b_j]^{\mu_j q^r}.$$

Hence q^{r_j} divides $\lambda_j q^r$ and $\mu_j q^r$, and so we can write

$$\lambda_j = \lambda_j' q^{r_j - r}, \ \mu_j = \mu_j' q^{r_j - r}, \qquad j = 1, \cdots, i.$$

Then

$$a_{i+1}^{q^r} = a_1^{\lambda'_1 q^{r_1}} \cdots a_i^{\lambda'_i q^{r_i}} c.$$

By Lemmas 3.5 and 3.6, we may suppose that

$$a_j^{q^{r_j}} = a_{i+1}^{q^{n_{i+1} - n_j + r_j}}, \qquad j = 1, \cdots, i.$$

https://doi.org/10.1017/S1446788700016724 Published online by Cambridge University Press

Hence

$$(a_{i+1}^{\lambda})^{q^r} \in \Omega^r(G'),$$

where

$$\lambda = 1 - \lambda_1' q^{n_{i+1}-n_1+r_1-r} - \cdots - \lambda_i' q^{n_{i+1}-n_i+r_i-r}.$$

Since $r < n_{i+1} - n_i + r_i < \cdots < n_{i+1} - n_1 + r_1$, it follows that λ is prime to q, and hence $a_{i+1}^{q^r} \in \Omega^r(G')$, which contradicts Lemma 3.9 since $a_{i+1}^{q^r} \neq 1$. Thus we have proved the minimality of S, and so $d(P) = 2i + 1$.

We shall be concerned only with the parity of $\sigma_r(G)$. This is given by

THEOREM 3.14. *If* $n_{i+1} - n_i + r_i \leqq r < r_i$, $1 \leqq i < \alpha$, *or if* $0 \leqq r < r_\alpha$ (*when* $r_\alpha > 0$), *then* $\sigma_r(G)$ *is even.*

If $r_{i+1} \leqq r < n_{i+1} - n_i + r_i$, $0 \leqq i < \alpha$, *where we set* $n_0 = r_0 = 0$, *then* $\sigma_r(G)$ *is odd.*

PROOF. Since for all $r \geqq 0$,

$$\sigma_r(G) = \sigma_r(G_*) + \sigma_r(G_0)$$

and $\sigma_r(G_0)$ is even, by Lemmas 3.4 and 3.10, it follows that $\sigma_r(G)$ and $\sigma_r(G_*)$ are of the same parity. The theorem then follows from Lemmas 3.11, 3.12 and 3.13.

Since $\sigma_r(G)$, $r \geqq 0$, are isomorphism invariants, the next lemma is clear.

LEMMA 3.15. *If* $G \cong H$, *then* $\sigma_r(G)$ *and* $\sigma_r(H)$ *are of the same parity for* $r \geqq 0$.

We can now prove the uniqueness of the canonic decomposition of the preceding section.

THEOREM 3.16. *The canonic decomposition for finite q-groups of class 2 with cyclic centre (as given in Theorem 2.5) is unique up to isomorphism.*

PROOF. Let G and H be non-trivial finite q-groups of class 2 with cyclic centre expressed in canonic decompositions

$$G = Q(n_1, r_1) \cdots Q(n_\alpha, r_\alpha) Q(l, l)^{\varepsilon_l} \cdots Q(1, 1)^{\varepsilon_1} = G_* G_0,$$

$H = Q(m_1, s_1) \cdots Q(m_\beta, s_\beta) Q(k, k)^{\delta_k} \cdots Q(1, 1)^{\delta_1} = H{*}H_0$. It is trivial that $G \cong H$ if $\alpha = \beta$, $l = k$, $n_i = m_i$ and $r_i = s_i$ for $i = 1, \cdots, \alpha$, and $\varepsilon_i = \delta_i$ for $i = 1, \cdots, l$. So assume that $G \cong H$.

Step 1. $\alpha = 0$. In this case, $G_* = 1$. Suppose $\beta > 0$. Then, by Lemma 3.10, $\sigma_{s_1}(G)$ is even while, by Lemma 3.14, $\sigma_{s_1}(H)$ is odd, contradicting Lemma 3.15. Hence $\beta = 0$.

We may then assume that $\varepsilon_l > 0$, $\delta_k > 0$. Suppose $l > k$; then, by Lemmas 3.2 and 3.3,

$$\rho_k(G) = 2(\varepsilon_l + \cdots + \varepsilon_{k+1}) > 0 = \rho_k(H),$$

which is a contradiction since $\rho_k(G)$ is an isomorphism invariant. Hence $l = k$. From the relations $\rho_i(G) = \rho_i(H)$, $i = 0, 1, \cdots, l-1$, we have

$$\varepsilon_l + \cdots + \varepsilon_1 = \delta_l + \cdots + \delta_1,$$

$$\varepsilon_l + \cdots + \varepsilon_2 = \delta_l + \cdots + \delta_2,$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$\varepsilon_l = \delta_l.$$

Hence $\varepsilon_i = \delta_i$, $i = 1, \cdots, l$.

In the rest of this proof, we assume $\alpha > 0$.

Step 2. We prove: $n_1 = m_1$, $r_1 = s_1$.

By Step 1, β cannot be zero and so $\beta > 0$. Clearly $q^{n_1} = q^{m_1} =$ exponent of G and hence $n_1 = m_1$. If $r_1 \neq s_1$, we may suppose $r_1 > s_1$. Then either $r_\alpha > s_1$ or $r_\gamma > s_1 \geqq r_{\gamma+1}$ for some $1 \leqq \gamma < \alpha$. If $r_\alpha > s_1$, then by Theorem 3.14, $\sigma_{s_1}(G)$ is even and $\sigma_{s_1}(H)$ is odd, contradicting Lemma 3.15. However, if $r_\gamma > s_1 \geqq r_{\gamma+1}$ for some $1 \leqq \gamma < \alpha$, let $s = \max\{n_{\gamma+1} - n_\gamma + r_\gamma, s_1\}$ so that $s_1 \leqq s < m_1$ and $n_{\gamma+1} - n_\gamma + r_\gamma \leqq s < r_\gamma$. Hence by Theorem 3.14, $\sigma_\varepsilon(H)$ is odd and $\sigma_s(G)$ is even, again contradicting Lemma 3.15. Hence $r_1 = s_1$.

Since we shall be referring frequently to Theorem 3.14 and Lemma 3.15 and it is clear from the context that one or the other is being invoked, we shall, for brevity, omit references to them.

Step 3. We prove: if $n_i = m_i$, $r_i = s_i$, $i = 1, \cdots, v$, where $v < \min\{\alpha, \beta\}$, then $n_{v+1} = m_{v+1}$, $r_{v+1} = s_{v+1}$.

First we show that $r_{v+1} = s_{v+1}$. If not, assume that $r_{v+1} > s_{v+1}$.

Claim A: $n_{v+1} = m_{v+1}$.

Let $u = n_{v+1} - n_v + r_v$, $v = m_{v+1} - m_v + s_v$. Now $s_v > r_{v+1} > s_{v+1}$ and $s_v > v > s_{v+1}$. Either $s_v > r_{v+1} \geqq v$ or $v > r_{v+1} > s_{v+1}$. In the first case, $\sigma_{r_{v+1}}(H)$ is even and $\sigma_{r_{v+1}}(G)$ is odd: a contradiction. We must then have $s_v > v > r_{v+1} > s_{v+1}$, or $r_v > v > r_{v+1}$ since $r_v = s_v$. Also, $r_v > u > r_{v+1}$. If $r_v > v > u > r_{v+1}$, then $\sigma_u(G)$ is even and $\sigma_u(H)$ is odd: a contradiction. However, if $r_v > u > v > r_{v+1}$, then $\sigma_v(G)$ is odd and $\sigma_v(H)$ is even: a contradiction. Hence $u = v$, and so $n_{v+1} = m_{v+1}$.

Claim B: $r_\lambda > s_{v+1} \geqq r_{\lambda+1}$ for some $v < \lambda < \alpha$.

This is clear if $r_\alpha = 0$. So assume that $r_\alpha > 0$. If the claim is false, then $r_\alpha > s_{v+1}$, so that $\sigma_{s_{v+1}}(G)$ is even and $\sigma_{s_{v+1}}(H)$ is odd: a contradiction.

Finally, we show that Claim B leads to a contradiction. Let $w = n_{\lambda+1} - n_\lambda + r_\lambda$. Then $w < u = v$ for we have $u - w = (n_{v+1} - n_{\lambda+1}) + (n_\lambda - n_v + r_v - r_\lambda) > 0$

since $v < \lambda$. Now $r_\lambda > w > r_{\lambda+1}$ and $r_\lambda > s_{v+1} \geqq r_{\lambda+1}$. Either $r_\lambda > s_{v+1} \geqq w$ or $w > s_{v+1} \geqq r_{\lambda+1}$. The first case implies that $\sigma_{s_{v+1}}(G)$ is even and $\sigma_{s_{v+1}}(H)$ is odd. The other case implies that $\sigma_w(H)$ is odd and $\sigma_w(G)$ is even. Both cases lead to contradictions. Hence we must have $r_{v+1} = s_{v+1}$.

To complete Step 3, we now prove that $n_{v+1} = m_{v+1}$. If not, assume that $n_{v+1} > m_{v+1}$. Then, with u and v defined as in the proof of Claim A, we have $u > v > s_{v+1} = r_{v+1}$. Thus $\sigma_v(G)$ is odd and $\sigma_v(H)$ is even: a contradiction. Hence $n_{v+1} = m_{v+1}$.

Step 4. We prove: $\alpha = \beta$.

If not, assume that $\alpha > \beta$. By Step 3, we have $n_i = m_i$, $r_i = s_i$ for $i = 1, \cdots, \beta$. Thus $r_{\beta+1} < s_\beta$, and hence $\sigma_{r_{\beta+1}}(G)$ is odd and $\sigma_{r_{\beta+1}}(H)$ is even: a contradiction. Of course, if $s_\beta = 0$, then $r_\beta = 0$ and so α must be equal to β.

At this point of the proof, we have $\alpha = \beta$, $n_i = m_i$, $r_i = s_i$, $i = 1, \cdots, \alpha$, or $G_* \cong H_*$.

Step 5. We prove: $l = k$, $\varepsilon_i = \delta_i = i = 1, \cdots, l$.

First we show that $G_0 = 1$ implies $H_0 = 1$. For if $H_0 \neq 1$, we may suppose $\delta_k > 0$, and since $G_* \cong H_*$, we have by Lemma 3.1, $\rho_0(G_0) = \rho_0(H_0)$, and so by Lemmas 3.2 and 3.3, $2(\delta_k + \cdots + \delta_1) = 0$, which is a contradiction. Hence $H_0 = 1$.

Lastly, we may assume that $\varepsilon_l > 0$, $\delta_k > 0$. As in Step 1, it is easily shown that $l = k$, $\varepsilon_i = \delta_i$, $i = 1, \cdots, l$. The proof is then complete.

References

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

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

[3] B. H. Neumann, *Lectures on topics in the theory of infinite groups* (Tata Institute of Fundamental Research, Bombay, 1960).

[4] M. F. Newman, 'On a class of nilpotent groups', *Proc. London Math. Soc.* (3) 10 (1960), 365–375.

[5] Marlene Schick, 'On central decompositions of groups I, II' (to appear).

[6] C. Y. Tang, 'On uniqueness of central decompositions of groups', *Pacific J. Math.* 33 (1970), 749–761.

Australian National University
Canberra, A. C. T. 2600

Present address:

Department of Mathematics
University of Singapore, Singapore.

https://doi.org/10.1017/S1446788700016724 Published online by Cambridge University Press