ON A CLASS OF FINITELY PRESENTED GROUPS

I. D. MACDONALD

The groups in question are generated by elements A and B subject to the relations

$$A^{[A,B]} = A^{\alpha}, \qquad B^{[B,A]} = B^{\beta},$$

in which α and β are fixed integers. We prove:

THEOREM. *Each group of the class just presented is finite when neither α nor β equals* 1, *and is nilpotent. Its order is a factor of* $27(\alpha-1)(\beta-1)\epsilon^8$ *where ϵ is the greatest common divisor of $\alpha - 1$ and $\beta - 1$, and its nilpotency class is at most* 8.

We denote the commutator $X^{-1}Y^{-1}XY$ by $[X, Y]$, and $Y^{-1}XY$ by X^Y. If $X_1, X_2, \ldots, X_r$ are elements of some group then $\{X_1, X_2, \ldots, X_r\}$ will mean the subgroup which they generate. The terms $Z_i(G)$ of the ascending central series of the group G are defined by taking $Z_1(G)$ to be the centre, and $Z_{i+1}(G)$ to be the subgroup such that $Z_{i+1}(G)/Z_i(G)$ is the centre of $G/Z_i(G)$ for $i = 1, 2, \ldots$.

1. In this section we make some elementary remarks in preparation for the calculations by which the theorem will be proved. The group $\{A, B\}$ defined above will be called $G(\alpha, \beta)$, the number ϵ will be as explained in the theorem, and C will denote the commutator $[A, B]$ throughout. Thus the defining relations of $G(\alpha, \beta)$ become

$$A^C = A^{\alpha}, \tag{1.1}$$

$$B^{C^{-1}} = B^{\beta}. \tag{1.2}$$

It is easy to see that $G(\alpha, \beta)$ is isomorphic to $G(\beta, \alpha)$, which implies that in discussing the various cases that arise we lose nothing in taking $\alpha \geqslant \beta$. As the group $G(\alpha, \alpha)$ has an automorphism of order 2 interchanging A and B, these two elements must have the same order.

The group $G(0, \beta)$ (and likewise $G(\alpha, 0)$), is easily treated. For here we have $A = 1$, $C = 1$ and $B = B^{\beta}$; the group is finite cyclic, and certainly nilpotent, when $\beta \neq 1$. In the case $\beta = 1$ we again have a cyclic group. Therefore we shall always assume that $\alpha \neq 0$ and $\beta \neq 0$.

If we add the relation $C = 1$ to those defining $G(\alpha, \beta)$ we obtain $A^{\alpha-1} = B^{\beta-1} = 1$, and this clearly gives an abelian group of order $(\alpha-1)(\beta-1)$ which is a factor group of $G(\alpha, \beta)$. Therefore if $\alpha \neq 2$ and $\beta \neq 2$ we see that

Received July 31, 1961; improved form March 14, 1962.

$G(\alpha, \beta)$ has order greater than 1; if this order is finite and p is a prime dividing $(\alpha - 1)(\beta - 1)$, then the Sylow p-subgroup of $G(\alpha, \beta)$ is non-trivial.

Next we establish rules of computation for later use. We have

$$(A^u C^v)^w = C^{wv} A^{u\alpha^v \alpha'} \tag{1.3}$$

where $v \geqslant 0$, $w > 0$ and $\alpha' = 1 + \alpha^v + \ldots + \alpha^{(w-1)v}$; for

$$\begin{aligned}(A^u C^v)^w &= C^{wv} . C^{-wv} A^u C^{wv} \ldots C^{-2v} A^u C^{2v} . C^{-v} A^u C^v \\ &= C^{wv} A^{u\alpha^{wv}} \ldots A^{u\alpha^{2v}} A^{u\alpha^v}\end{aligned}$$

by (1.1). In particular we have

$$(A^w)^B = C^w A^{\alpha(1+\alpha+\ldots+\alpha^{w-1})} \tag{1.4}$$

for $w > 0$, since $(A^w)^B = (A^B)^w = (AC)^w$ and (1.3) may be applied to this with $u = v = 1$.

There is a further relation

$$(B^u C^{-v})^w = C^{-wv} B^{u\beta^v \beta'} \tag{1.5}$$

where $v \geqslant 0$, $w > 0$ and $\beta' = 1 + \beta^v + \ldots + \beta^{(w-1)v}$. This may be proved similarly, and leads to

$$(B^w)^A = C^{-w} B^{\beta(1+\beta+\ldots+\beta^{w-1})} \tag{1.6}$$

for $w > 0$.

At this point it would be possible to prove that if A, B, and C are all of finite order then every element of $G(\alpha, \beta)$ can be expressed as $A^p B^q C^r$ for suitable integers p, q, r, and so $G(\alpha, \beta)$ would be finite. We omit this proof as finiteness of $G(\alpha, \beta)$ will be established by other means. Let us note that if $A^m = 1$ or even if A^m lies in the centre $Z_1(G)$ of $G(\alpha, \beta)$ for some positive integer m, and $\alpha \neq 1$, then C has finite order; for (1.4) with $w = m$ gives $C^m = A^\theta$, for some θ, so

$$C^m = A^\theta = (A^\theta)^C = A^{\alpha\theta} = C^{\alpha m}$$

by (1.1), and $C^{(\alpha-1)m} = 1$. A similar result holds if B has finite order modulo $Z_1(G)$.

The main relation to which the calculations will be applied is

$$[A, B^\beta]^C = [A^\alpha, B], \tag{1.7}$$

which is an immediate consequence of (1.1) and (1.2).

It may be of interest to discuss briefly the group $G(1, \beta)$ before starting on the proof of the theorem. This is an infinite group as an infinite cyclic factor group is obtained by adding the relation $B = 1$ to the defining pair. But the group is nilpotent, for (1.7) gives

$$[A, B^\beta] = [A, B]^{C^{-1}} = [A, B]$$

and so $A^{-1}B^{-\beta}AB^\beta = A^{-1}B^{-1}AB$, which proves that A and $B^{\beta-1}$ commute. Therefore the centre $Z_1(G)$ of $G(1, \beta)$ contains $B^{\beta-1}$. We have $Z_2(G) \geqslant \{B^{\beta-1}, C\}$ and $Z_3(G) = G$. Thus the nilpotency class is at most 3.

2. In this section our aim is to prove that the elements A and B in $G(\alpha, \beta)$ have finite orders, provided that $\alpha \neq 1$ and $\beta \neq 1$. The calculations differ slightly in the several cases specified by the signs of α and β; we recall our assumption $\alpha \geqslant \beta$.

CASE 1. $\alpha > 1$ *and* $\beta > 1$.

On putting $w = \beta$ in (1.6) we find that

$$(B^{\beta})^{A} = C^{-\beta}B^{\beta(1+\beta+\ldots+\beta^{\beta-1})},$$

and so we have

$$\begin{aligned}[A, B^{\beta}]^{C} &= C^{-1}(B^{-\beta})^{A}B^{\beta}C \\ &= C^{-1}B^{-\beta(1+\beta+\ldots+\beta^{\beta-1})}C^{\beta}B^{\beta}C \\ &= B^{\delta}C^{\beta}\end{aligned} \tag{2.1}$$

by (1.2), where

$$\delta = \beta^{\beta} - (1 + \beta + \ldots + \beta^{\beta-1}). \tag{2.2}$$

Similarly (1.4) with $w = \alpha$ gives

$$\begin{aligned}[A^{\alpha}, B] &= A^{-\alpha}(A^{\alpha})^{B} \\ &= A^{-\alpha}C^{\alpha}A^{\alpha(1+\alpha+\ldots+\alpha^{\alpha-1})} \\ &= C^{\alpha}A^{-\alpha\gamma}\end{aligned} \tag{2.3}$$

by (1.1), where

$$\gamma = \alpha^{\alpha} - (1 + \alpha + \ldots + \alpha^{\alpha-1}). \tag{2.4}$$

Now (1.7), (2.1), and (2.3) give

$$B^{\delta}C^{\beta} = C^{\alpha}A^{-\alpha\gamma}. \tag{2.5}$$

We transform both sides of (2.5) by C^{-1}:

$$B^{\beta\delta}C^{\beta} = C^{\alpha}A^{-\gamma}. \tag{2.6}$$

On eliminating C^{α} from (2.5) and (2.6) we obtain

$$C^{-\beta}B^{(\beta-1)\delta}C^{\beta} = A^{(\alpha-1)\gamma},$$

and on eliminating C^{β} from the same equations

$$B^{(\beta-1)\delta} = C^{\alpha}A^{(\alpha-1)\gamma}C^{-\alpha};$$

hence

$$C^{\alpha-\beta}A^{(\alpha-1)\gamma}C^{\beta-\alpha} = A^{(\alpha-1)\gamma}. \tag{2.7}$$

Now (2.7) and (1.1) give, since $\alpha - \beta \geqslant 0$,

$$\begin{aligned}A^{(\alpha-1)\gamma} &= (A^{(\alpha-1)\gamma})^{C^{\alpha-\beta}} = A^{(\alpha-1)\gamma\alpha^{\alpha-\beta}}, \\ A^{(\alpha-1)(\alpha^{\alpha-\beta}-1)\gamma} &= 1.\end{aligned} \tag{2.8}$$

And similarly

$$B^{(\beta-1)(\beta^{\alpha-\beta}-1)\delta} = 1. \tag{2.9}$$

https://doi.org/10.4153/CJM-1962-051-5 Published online by Cambridge University Press

When $\alpha > \beta > 1$, it is clear that γ and δ are positive and that A and B have finite orders.

Let us next consider the case $\alpha = \beta > 1$. The relation (2.5) gives

$$C^{-\alpha}B^{\gamma}C^{\alpha} = A^{-\alpha\gamma}.$$

But (1.2) gives

$$B^{\gamma} = C^{-\alpha}B^{\alpha^{\alpha}\gamma}C^{\alpha} = (C^{-\alpha}B^{\gamma}C^{\alpha})^{\alpha^{\alpha}}.$$

When $C^{-\alpha}B^{\gamma}C^{\alpha}$ is eliminated between the last two relations we have

$$A^{-\alpha^{\alpha+1}\gamma} = B^{\gamma}.$$

Therefore both $A^{-\alpha^{\alpha+1}\gamma}$ and B^{γ} lie in the centre of $G(\alpha, \beta)$, and commute with C; so use of (1.1) gives

$$A^{-\gamma} = B^{\gamma}, \tag{2.10}$$

$$A^{\gamma} = (A^{\gamma})^{C} = A^{\alpha\gamma},$$

$$A^{(\alpha-1)\gamma} = 1. \tag{2.11}$$

Similarly we have

$$B^{(\alpha-1)\gamma} = 1. \tag{2.12}$$

Again A and B have finite orders.

Because of the importance which the case $\alpha > 1$ and $\beta > 1$ will later assume, we shall derive some more relations from those listed above. As remarked earlier we have proved enough to establish that C has finite order, hence the element CAC^{-1} is a power of A which will be written as $A^{\alpha^{-1}}$. Thus (2.5) becomes

$$B^{\delta} = A^{-\alpha^{1-\alpha}\gamma}C^{\alpha-\beta} \tag{2.13}$$

after the use of (1.1), and transformation by C^{-1} and then elimination of $C^{\alpha-\beta}$ yields

$$B^{(\beta-1)\delta} = A^{(\alpha-1)\gamma\alpha^{-\alpha}} \tag{2.14}$$

Transformations with C according to (1.1) give

$$A^{(\alpha-1)\gamma} = B^{(\beta-1)\delta}. \tag{2.15}$$

We further find that

$$A^{(\alpha-1)\gamma} = (A^{(\alpha-1)\gamma})^{C} = A^{\alpha(\alpha-1)\gamma}, A^{(\alpha-1)^2\gamma} = 1,$$

and as each term in (2.15) similarly has order dividing $\beta - 1$, there results

$$A^{\epsilon(\alpha-1)\gamma} = B^{\epsilon(\beta-1)\delta} = 1. \tag{2.16}$$

The expression obtained by raising both sides of (2.13) to the power $\beta - 1$ may be simplified by means of (1.3), and this with (2.15) shows that $C^{(\beta-1)(\alpha-\beta)} \in \{A\}$; similarly $C^{(\alpha-1)(\alpha-\beta)} \in \{B\}$. Thus

$$C^{(\alpha-1)(\beta-1)(\alpha-\beta)} = 1, \tag{2.17}$$

and we have by (1.1)

https://doi.org/10.4153/CJM-1962-051-5 Published online by Cambridge University Press

$$A = A^{C^{(\beta-1)(\alpha-\beta)}} = A^{\alpha^{(\beta-1)(\alpha-\beta)}};$$

hence and similarly

$$A^{\alpha^{(\beta-1)(\alpha-\beta)}-1} = B^{\beta^{(\alpha-1)(\alpha-\beta)}-1} = 1. \tag{2.18}$$

CASE 2. $\alpha < 0$ *and* $\beta < 0$.

By putting $w = -\beta$ in (1.6) we obtain

$$(B^{-\beta})^A = C^\beta B^{\beta(1+\beta+\ldots+\beta^{-\beta-1})}, \tag{2.19}$$

$$\begin{aligned}[A, B^\beta]^C &= C^{-1}(B^{-\beta})^A B^\beta C \\ &= C^{-1+\beta} B^{\beta(2+\beta+\ldots+\beta^{-\beta-1})} C \\ &= C^\beta B^\eta\end{aligned}$$

by (1.2), where

$$\eta = 2 + \beta + \ldots + \beta^{-\beta-1}. \tag{2.20}$$

Similarly (1.4) with $w = -\alpha$ gives

$$(A^{-\alpha})^B = C^{-\alpha} A^{\alpha(1+\alpha+\ldots+\alpha^{-\alpha-1})}, \tag{2.21}$$

$$\begin{aligned}[A^\alpha, B] &= A^{-\alpha}(A^\alpha)^B \\ &= A^{-\alpha\xi} C^\alpha\end{aligned}$$

where

$$\xi = 2 + \alpha + \ldots + \alpha^{-\alpha-1}. \tag{2.22}$$

Now (1.7), (2.19), and (2.21) give

$$B^\eta C^{-\alpha} = C^{-\beta} A^{-\alpha\xi}. \tag{2.23}$$

We note the similarity between equations (2.5) and (2.23). Indeed, (2.23) may be developed just as (2.5) was earlier to yield the fact that A and B are of finite orders in general—we omit the details of this process. However, closer attention is necessary when $\alpha - \beta = 0$ or $\xi = 0$ or $\eta = 0$, for these are circumstances in which the general argument given in case 1 would here break down. Elementary algebra shows that $\xi = 0$ only if $\alpha = -2$, hence $\eta = 0$ only if $\beta = -2$.

Let us consider the case $\alpha = \beta < 0$. If in addition $\alpha \neq -2$, it will be found that the argument for $\alpha = \beta > 1$ may be adapted to show that A and B have finite orders, as required. When $\alpha = \beta = -2$ we abandon (1.7) in favour of the relation

$$[A, B^4]^{C^2} = [A^4, B],$$

which we simplify by means of the following consequences of (1.6) and (1.4):

$$(B^4)^A = C^{-4}B^{10}, \qquad (A^4)^B = C^4 A^{10}.$$

Thus we obtain

$$C^{-2}B^{-10}C^4B^4C^2 = A^{-4}C^4A^{10},$$

and some applications of (1.1) and (1.2) reduce this to

$$B^{27}C^4 = C^4A^{-27}.$$

https://doi.org/10.4153/CJM-1962-051-5 Published online by Cambridge University Press

Now we proceed as when $\alpha = \beta > 1$, and obtain

$$A^{-27} = B^{27}.$$

This shows that A and B both have order dividing 81.

Next we examine the situation when $\alpha = -2$. We may suppose that $\beta < -2$. The relation (2.23), still valid, gives

$$B^{\eta} = C^{-\beta-2}, \tag{2.24}$$

$$B^{\eta} = (B^{\eta})^{C^{-1}} = B^{\beta\eta},$$

$$B^{(\beta-1)\eta} = C^{(\beta-1)(\beta+2)} = 1. \tag{2.25}$$

Now application of (1.1) shows that

$$A = A^{C^{(\beta-1)(\beta+2)}} = A^{(-2)^{(\beta-1)(\beta+2)}}, \tag{2.26}$$

$$A^{(-2)^{(\beta-1)(\beta+2)}-1} = 1.$$

Again A and B have finite orders.

Lastly we must consider what happens when $\beta = -2$, and so $\alpha = -1$. As $\xi = 2$ and $\eta = 0$, (2.23) becomes $C = A^2$; so $A = A^C = A^{-1}$, $A^2 = C = 1$. Next $B = B^{C^{-1}} = B^{-2}$, which gives $B^3 = 1$. Therefore $G(-1, -2)$ is cyclic of order 6.

CASE 3. $\alpha > 1$ *and* $\beta < 0$.

Defining η and γ as in (2.20) and (2.4) respectively, we find that

$$[A, B^{\beta}]^C = C^{\beta}B^{\eta},$$

$$[A^{\alpha}, B] = C^{\alpha}A^{-\alpha\gamma};$$

these relations are found just as (2.19) and (2.3) were. Now (1.7) becomes

$$B^{\eta} = C^{\alpha-\beta}A^{-\alpha\gamma}. \tag{2.27}$$

On transforming this by C^{-1} and eliminating $C^{\alpha-\beta}$ we find

$$A^{(\alpha-1)\gamma} = B^{(\beta-1)\eta}. \tag{2.28}$$

This relation may be treated like (2.10) to yield

$$A^{(\alpha-1)^2\gamma} = B^{(\alpha-1)(\beta-1)\eta} = 1. \tag{2.29}$$

We see that A and B are elements of finite order except perhaps when $\eta = 0$. Then (2.27) becomes

$$A^{\alpha\gamma} = C^{\alpha+2}, \tag{2.30}$$

since $\beta = -2$. This relation may be treated as (2.24) was, giving

$$A^{(\alpha-1)\gamma} = B^{(-2)^{(\alpha-1)(\alpha+2)}-1} = 1. \tag{2.31}$$

Therefore, whenever $\alpha > 1$ and $\beta < 0$, A and B are of finite orders.

This completes the proof of the fact that the orders of A and B are finite if $\alpha \neq 1$ and $\beta \neq 1$. The consequence that C has finite order was noted earlier.

3. The present section is devoted to a result in number theory which seems necessary to prove nilpotence and which also serves to establish finiteness of $G(\alpha, \beta)$.

LEMMA.* *Suppose m divides $n^m - 1$ where m is some positive integer and $n \neq 1$ is some integer. If $m = q_1 q_2 \ldots q_k$ for primes q_i such that $q_1 \leqslant q_2 \leqslant \ldots \leqslant q_k$ and $m_i = q_1 q_2 \ldots q_i$ for $1 \leqslant i \leqslant k$, with $m_0 = 1$, then*

(i) *m_i divides $n^{m_{i-1}} - 1$ for $1 \leqslant i \leqslant k$; and*

(ii) *m_i divides $(n^{m_i} - 1)/(n - 1)$ for $1 \leqslant i \leqslant k$.*

Proof. We may neglect the simple case which arises when $n = -1$ and $q_1 = 2$. By Fermat's theorem and by hypothesis we have

$$n^{q_i - 1} \equiv 1 \qquad \text{and} \qquad n^m \equiv 1 \pmod{q_i}$$

for $1 \leqslant i \leqslant k$; so the choice of the primes q_i now ensures that $n^{m_{i-1}} \equiv 1 \pmod{q_i}$. Another useful fact is that $(n^{m_i} - 1)/(n^{m_{i-1}} - 1)$ is divisible by q_i where $1 \leqslant i \leqslant k$, for the number in question is equal to the sum of q_i powers of $n^{m_{i-1}}$ and we have just proved that $n^{m_{i-1}} \equiv 1 \pmod{q_i}$.

The proof of (i) is by induction on i. The case $i = 1$, that is, the statement that q_1 divides $n - 1$, has already been established. We assume inductively that m_i is a factor of $n^{m_{i-1}} - 1$, which of course divides $n^{m_i} - 1$, for $1 \leqslant i < k$; and as q_{i+1} also divides $n^{m_i} - 1$, we have shown that $m_{i+1} = m_i q_{i+1}$ is a factor provided that $q_i \neq q_{i+1}$. But when $q_i = q_{i+1}$ an earlier remark shows that q_{i+1} divides $(n^{m_i} - 1)/(n^{m_{i-1}} - 1)$, so again $m_i q_{i+1}$ divides $n^{m_i} - 1$. This completes the inductive proof of (i).

We may again use induction for (ii). There is no difficulty when $i = 1$ as the required fact was proved earlier. In general we consider $(n^{m_{i+1}} - 1)/(n - 1)$, with inductive hypothesis that m_i divides $(n^{m_i} - 1)/(n - 1)$, and since q_{i+1} is known to divide $(n^{m_{i+1}} - 1)/(n^{m_i} - 1)$ for $1 \leqslant i \leqslant k$, we see that $m_i q_{i+1}$ divides $(n^{m_{i+1}} - 1)/(n - 1)$. This completes the inductive proof of (ii).

COROLLARY. *If q_k does not divide $n - 1$, then m divides $(n^{m/q_k} - 1)/(n - 1)$.*

4. In this section we consider supersolubility and finiteness of $G(\alpha, \beta)$ along with the question of what primes divide the group order, always assuming that $\alpha \neq 1$ and $\beta \neq 1$.

Let us suppose that A and B have orders μ and ν respectively. Application of (1.4) with $w = \mu$ gives

$$1 = (A^\mu)^B = C^\mu A^{\alpha\mu'}$$

where $\mu' = (\alpha^\mu - 1)/(\alpha - 1)$, so $C^\mu \in \{A\}$, and (1.1) gives

$$A = A^{C^\mu} = A^{\alpha^\mu}, \qquad A^{\alpha^\mu - 1} = 1.$$

*This lemma together with the proof of the nilpotence of $G(\alpha, \beta)$ is due to the referee, to whom I record my thanks.

Since it now appears that μ divides $\alpha^{\mu} - 1$, the lemma asserts that μ divides μ', and so we have $C^{\mu} = 1$; similarly we can prove that $C^{\nu} = 1$. If λ is the greatest common factor of μ and ν then $C^{\lambda} = 1$.

We shall examine the case $\mu = \nu$ first, taking the common order of A and B to be m. This case arises when $\alpha = \beta$, and the more general case will be reduced to it. Then m divides $\alpha^m - 1$, the conditions of the lemma are satisfied, and we adopt the definitions of q_i and m_i therein.

Next we define certain subgroups of $G(\alpha, \beta)$:

$$\begin{aligned} U_i &= \{A^{m_{i-1}}, B^{m_{i-1}}, C^{m_{i-1}}\}, \\ V_i &= \{A^{m_i}, B^{m_{i-1}}, C^{m_{i-1}}\}, \\ W_i &= \{A^{m_i}, B^{m_i}, C^{m_{i-1}}\} \end{aligned}$$

for $1 \leqslant i \leqslant k$. Thus

$$G(\alpha, \beta) = U_1 \geqslant \ldots \geqslant U_i \geqslant V_i \geqslant W_i \geqslant U_{i+1} \geqslant \ldots \geqslant W_k \geqslant 1.$$

Now (1.4) with $w = m_i$ gives

$$(A^{m_i})^B = C^{m_i} A^{\alpha m_i'}$$

where m_i divides $m_i' = (\alpha^{m_i} - 1)/(\alpha - 1)$ by the lemma. Therefore, and similarly,

$$(4.1) \qquad (A^{m_i})^B \in \{A^{m_i}, C^{m_i}\},$$

$$(4.2) \qquad (B^{m_i})^A \in \{B^{m_i}, C^{m_i}\}.$$

By (1.1) we have

$$(C^{m_i})^A = C^{m_i} A^{m_i''}$$

where m_{i+1} divides $m_i'' = 1 - \alpha^{m_i}$ by the lemma for $0 \leqslant i < k$. Thus we have

$$(4.3) \qquad (C^{m_i})^A \in \{A^{m_i+1}, C^{m_i}\},$$

$$(4.4) \qquad (C^{m_i})^B \in \{B^{m_i+1}, C^{m_i}\}.$$

Because A and B have finite orders and because (4.1)–(4.4) hold, every conjugate of the three given generators of U_i lies in U_i. Thus U_i, and similarly V_i and W_i, are all normal subgroups of $G(\alpha, \beta)$.

Since it follows that each of the factor groups U_i/V_i, V_i/W_i and W_i/U_{i+1} has order q_i or 1, (we take $U_{k+1} = 1$), the group $G(\alpha, \beta)$ is finite and supersoluble.

In the case $\mu \neq \nu$ we have $C^{\lambda} = 1$ and so in the usual way $A^{\alpha^{\lambda}-1} = 1$. Therefore $\alpha^{\lambda} - 1$ is divisible by μ, which in turn is divisible by λ; the lemma shows that $\lambda' = (\alpha^{\lambda} - 1)/(\alpha - 1)$ is divisible by λ. Now (1.4) with $w = \lambda$ gives

$$(A^{\lambda})^B = C^{\lambda} A^{\alpha\lambda'} \in \{A^{\lambda}\},$$

that is, $\{A^{\lambda}\}$ is normal in $G(\alpha, \beta)$. Similarly $\{B^{\lambda}\}$ is normal. Putting $N = \{A^{\lambda}, B^{\lambda}\}$, we examine the orders μ_0 and ν_0 of A and B respectively modulo N.

Clearly μ_0 and ν_0 divide λ. Since $A^{\mu_0} \in N$ we have $A^{\mu_0} \in \{B^\lambda\}$, say $A^{\mu_0} = B^{r\lambda}$; similarly $B^{\nu_0} = A^{s\lambda}$. Hence

$$A^{\mu_0\nu_0} = B^{r\lambda\nu_0} = A^{rs\lambda^2},$$

and we have $\mu_0 = \nu_0 = \lambda$. Since the two obvious generators of $G(\alpha, \beta)/N$ have equal orders we know that $G(\alpha, \beta)/N$ is finite supersoluble by earlier reasoning, so $G(\alpha, \beta)$ has the same properties.

We shall now prove that the only primes dividing μ are factors of $\alpha - 1$. Considering the case $\mu = \nu$, we suppose that q_i is not a factor of $\alpha - 1$ and that $q_i \neq q_{i+1}$ or $i = k$, and we let A have order σ modulo U_{i+1}. If q_i divides the order of A, we have by (1.4)

$$(A^{\sigma/q_i})^B = C^{\sigma/q_i}A^{\alpha\sigma'}$$

where $\sigma' = (\alpha^{\sigma/q_i} - 1)/(\alpha - 1)$ is divisible by σ, because of the corollary to the lemma. Thus

$$(A^{\sigma/q_i})^B \equiv C^{\sigma/q_i} \qquad (\text{modulo } U_{i+1}).$$

But it may be deduced from (1.2) that

$$(C^{\sigma/q_i})^B = B^{\sigma''}C^{\sigma/q_i}$$

where $\sigma'' = \beta^{\sigma/q_i} - 1$ is divisible by σ, by the lemma. As A and B have the same order modulo U_{i+1} we have proved that

$$A^{\sigma/q_i} \equiv C^{\sigma/q_i} \text{ (modulo } U_{i+1}).$$

Use of (1.1) in the usual way shows that $A^{(\alpha-1)\sigma/q_i} \in U_{i+1}$, so $A^{\sigma/q_i} \in U_{i+1}$ as q_i is prime to $\alpha - 1$. This contradicts the assumption that A has order σ modulo U_{i+1}. The conclusion is that the prime divisors of μ and ν are factors of $\alpha - 1$ and $\beta - 1$ respectively.

When $\mu \neq \nu$ the above argument applied to $G(\alpha, \beta)/N$ shows that if a prime factor p of μ does not divide $\alpha - 1$ then p divides the order of N, that is, p divides μ/λ. We have from (1.4) with $w = \mu/p$

$$(A^{\mu/p})^B = C^{\mu/p}A^{\alpha\mu'},$$

where $C^{\mu/p} = 1$ because $C^\lambda = 1$, and $\mu' = (\alpha^{\mu/p} - 1)/(\alpha - 1)$. The fact that μ divides $\alpha^\lambda - 1$ shows that both μ and μ/p divide $\alpha^{\mu/p} - 1$. At this point the lemma shows that μ/p divides μ'. Since μ divides both $(\alpha - 1)\mu'$ and $p\mu'$, and $\alpha - 1$ is prime to p, we see that μ divides μ', and so $A^{\mu/p} = 1$, a contradiction. Again we have shown that the only primes dividing the order of A are factors of $\alpha - 1$; and a similar result about B and $\beta - 1$ is clearly true. These are the only primes dividing the order of $G(a, \beta)$ as is clear from the proof of supersolubility.

5. In order to prove that $G(\alpha, \beta)$ is nilpotent and to find a bound on the class, only the case $\alpha > 1$ and $\beta > 1$ need be considered. For if μ and ν are the orders of A and B, the relations

$$A^C = A^{\alpha+2\mu}, \qquad B^{C^{-1}} = B^{\beta+2\nu}$$

https://doi.org/10.4153/CJM-1962-051-5 Published online by Cambridge University Press

are satisfied, which shows that $G(\alpha, \beta)$ is a factor group of $G(\alpha + 2\mu, \beta + 2\nu)$. Here $\alpha + 2\mu > 1$ and $\beta + 2\nu > 1$ as $\mu \geqslant |\alpha - 1|$ and $\nu \geqslant |\beta - 1|$. Hence if $G(\alpha, \beta)$ is nilpotent for $\alpha > 1$ and $\beta > 1$, then every $G(\alpha, \beta)$ is nilpotent; and if there is a $G(\alpha, \beta)$ of class precisely c we may take it that $\alpha > 1$ and $\beta > 1$.

We consider a prime p dividing the order of A, note that p divides $\alpha - 1$, and ask what power of p divides $(\alpha - 1)\gamma$, which is associated with the order of A. Let us suppose for the moment that $\alpha - 1$ is prime to 6, and put $\alpha = 1 + kp^n$ where k and p are coprime. By (2.4) we have

$$\begin{aligned}(\alpha - 1)\gamma &= 1 + (\alpha - 2)\alpha^\alpha \\ &= 1 + (\alpha - 2)\{1 + \tbinom{\alpha}{1}(\alpha - 1) + \tbinom{\alpha}{2}(\alpha - 1)^2 + \tbinom{\alpha}{3}(\alpha - 1)^3 + \ldots\} \\ &= (\alpha - 1)^3 + (\alpha - 2)\tbinom{\alpha}{2}(\alpha - 1)^2 + (\alpha - 2)\tbinom{\alpha}{3}(\alpha - 1)^3 + \ldots \\ &= \{1 + \tfrac{1}{2}(\alpha - 2)\alpha\}(\alpha - 1)^3 + \tfrac{1}{6}(\alpha - 2)^2(\alpha - 1)^4\alpha + \ldots \quad .\end{aligned}$$

But here we have

$$2 + (\alpha - 2)\alpha = 2 + (-1 + kp^n)(1 + kp^n) \equiv 1 \pmod p.$$

Thus the assumption on $\alpha - 1$ shows that p^{3n} but not p^{3n+1} divides $(\alpha - 1)\gamma$. A similarly elementary calculation, which is omitted, shows that this result holds whatever the nature of $\alpha - 1$, with these exceptions:

(i) if $p = 2$ the required power is 2^{3n-1};

(ii) if $p^n = 3$ and $k \equiv 2 \pmod 3$, the required power is 3^4.

A similar result holds for $(\beta - 1)\delta$.

In order to prove nilpotence when $\alpha - 1$ and $\beta - 1$ are both prime to 6 a number of congruences will be needed. These are stated without detailed proof as they are easily deduced from binomial expansions:

$$\alpha\{(\alpha^{(\alpha-1)^3} - 1)/(\alpha - 1)\} \equiv (\alpha - 1)^3 \pmod{(\alpha - 1)^4}; \tag{5.1}$$

$$\alpha\{(\alpha^{\epsilon^3} - 1)/(\alpha - 1)\} \equiv \epsilon^3 \pmod{(\alpha - 1)\epsilon^3}; \tag{5.2}$$

$$\alpha\{(\alpha^{\epsilon^2} - 1)/(\alpha - 1)\} \equiv \epsilon^2 \pmod{\epsilon^3}; \tag{5.3}$$

$$\alpha\{(\alpha^{\epsilon} - 1)/(\alpha - 1)\} \equiv \epsilon \pmod{\epsilon^2}; \tag{5.4}$$

$$\alpha^{(\alpha-1)\epsilon^2} - 1 \equiv (\alpha - 1)^2\epsilon^2 \pmod{(\alpha - 1)^3\epsilon}. \tag{5.5}$$

The result about $(\alpha - 1)\gamma$ proved above and (2.16) give

$$A^{(\alpha-1)^3\epsilon} = 1 \tag{5.6}$$

while (2.14) shows that $A^{(\alpha-1)^3} \in Z_1(G)$. Thus by (1.4) with $w = (\alpha - 1)^3$ and by (5.1) we have

$$A^{(\alpha-1)^3} = (A^{(\alpha-1)^3})^B = C^{(\alpha-1)^3}A^{(\alpha-1)^3},$$

and so $C^{(\alpha-1)^3} = 1$; similarly $C^{(\beta-1)^3} = 1$. Hence

$$C^{\epsilon^3} = 1, \tag{5.7}$$

and A commutes with $C^{(\alpha-1)\epsilon^2}$. Application of (1.1) shows that the order of A is a factor of $\alpha^{(\alpha-1)\epsilon^2} - 1$, and so, by (5.6) and (5.5), also a factor of $(\alpha - 1)^2\epsilon^2$. Because A commutes with C^{ϵ^3} by (5.7) its order divides $\alpha^{\epsilon^3} - 1$ and also $(\alpha - 1)\epsilon^3$ as we now see from (5.2). Therefore, and similarly,

$$A^{(\alpha-1)\epsilon^3} = B^{(\beta-1)\epsilon^3} = 1. \tag{5.8}$$

We can now show that A^{ϵ^3} is central in $G(\alpha, \beta)$, for (1.4), (5.8), (5.2), and (5.7) give

$$(A^{\epsilon^3})^B = C^{\epsilon^3}A^{\epsilon^3} = A^{\epsilon^3}.$$

Therefore, and similarly,

$$\{A^{\epsilon^3}, B^{\epsilon^3}\} \leqslant Z_1(G). \tag{5.9}$$

Next we prove that $C^{\epsilon^2} \in Z_2(G)$:

$$[A, C^{\epsilon^2}] = A^{\phi},$$
$$\phi = \alpha^{\epsilon^2} - 1 \equiv 0 \pmod{\epsilon^3}$$

by (1.1) and (5.3). Similarly $[B, C^{\epsilon^2}] \in Z_1(G)$.

This enables us to prove that $A^{\epsilon^2} \in Z_3(G)$. For

$$(A^{\epsilon^2})^B = C^{\epsilon^2}A^{\psi},$$
$$\psi = \alpha\{(\alpha^{\epsilon^2} - 1)/(\alpha - 1)\} \equiv \epsilon^2 \pmod{\epsilon^3}$$

by (1.4) and (5.3). Thus $Z_3(G) \geqslant \{A^{\epsilon^2}, B^{\epsilon^2}, C^{\epsilon^2}\}$.

We summarize the remaining steps as they present no further difficulty. We find that $C^{\epsilon} \in Z_4(G)$ by (5.4) and then that $Z_5(G) \geqslant \{A^{\epsilon}, B^{\epsilon}, C^{\epsilon}\}$ by (5.4) again. It follows easily that $C \in Z_6(G)$ and that $Z_7(G) = G(\alpha, \beta)$, that is, the group is nilpotent of class 7 or less.

It is convenient to deduce the bound on the order of $G(\alpha, \beta)$ here. Take a prime p such that p^n but no higher power of p divides ϵ and consider the Sylow p-subgroup. In consequence of (2.14) we have that $A^{p^{3n}} \in \{B\}$ or $B^{p^{3n}} \in \{A\}$, while (2.16) and (5.7) give $A^{p^{4n}} = B^{p^{4n}} = 1$ and $C^{p^{3n}} = 1$ respectively. The order of the Sylow p-subgroup is a factor of p^{10n}. Hence the order of $G(\alpha, \beta)$ is a factor of $(\alpha - 1)(\beta - 1)\epsilon^8$.

A number of other cases which will not be examined in detail here arise when we drop the restriction that $\alpha - 1$ and $\beta - 1$ are prime to 6. The class may be as high as 8 for some groups and the bound on the order should be increased to $27(\alpha - 1)(\beta - 1)\epsilon^8$. We do not go into the proofs as they are essentially similar to the case already considered.

Nor do we settle the complicated question of the precise order and class of every $G(\alpha, \beta)$. In many cases these are much less than our bounds, as may be seen from (2.13), (2.17), and (2.18) when $\alpha \neq \beta$ and from (2.10) otherwise. To determine whether the bounds are attained would involve construction of the groups by means of extension theory, for instance, and the groups

$G(\alpha, \beta)$ are awkward in this respect; the extensions would not normally split. We note that a likely group of class 8 is $G(34, 7)$.

Only a few of the groups $G(\alpha, \beta)$ are well known. If α and β are such that $\epsilon = 1$ then it follows that $C = 1$ and $G(\alpha, \beta)$ is cyclic of order $(\alpha - 1)(\beta - 1)$. In particular $G(\alpha, 2)$ is cyclic of order $\beta - 1$ and $G(2, 2)$ is trivial. It is easy to show that the groups $G(3, 3)$, $G(3, -1)$ and $G(-1, -1)$ are all isomorphic to the generalized quaternion group of order 16. Again, after construction of $G(1 + p^n, 1 + p^n)$ as an extension of its commutator subgroup, it appears that this group has order p^{7n} and class 5 if p is an odd prime.

Part of this work was done while the author held grants from the University of Aberdeen and from the Carnegie Trust for the Universities of Scotland. To the authorities of both these bodies I express my sincere thanks.

The University, Sheffield