A CLASS OF FINITE GROUPS WITH ZERO DEFICIENCY

by J. W. WAMSLEY

(Received 8th December 1972)

1. Introduction

Let G be a finite group generated by n elements and defined by m relations, then G has a presentation, $G = \{x_1, \ldots, x_n \mid R_1, \ldots, R_m\} = F/R$, where F is free on generators $x_1, \ldots, x_n$ and R is the normal closure in F of $R_1, \ldots, R_m$. The deficiency of this presentation is $n-m$. Since G is finite the deficiency is non-positive and the deficiency of G is the maximal over the deficiencies of all presentations for G.

The torsion part of $R/[F, R]$ is a presentation invariant and is known as the Schur multiplicator of G. It is an open question as to whether a finite p-group with trivial Schur multiplicator has zero deficiency. One way to obtain a finite p-group, G_p, with trivial multiplicator is to take a finite group, G, with zero deficiency and let G_p be the maximal p-factor of G.

One of the few known classes of finite groups with zero deficiency is given by Macdonald (**1**). A member of this class is presented by

$$G(\alpha, \beta) = \{a, b \mid c = a^{-1}b^{-1}ab,\ c^{-1}ac = a^{\alpha},\ cbc^{-1} = b^{\beta}\}.$$

In this paper we show that for p an odd prime, the maximal p-factor of $G(\alpha, \beta)$ has zero deficiency.

2. Preliminaries

In this section we give some results concerning the deficiency of factor groups of groups with zero deficiency. The following theorem (**2**, Theorem 2.1) is stated without proof.

Theorem 2.1. *Let G be a finite p-group with presentation $G = F/R$ and suppose the vector space $R/[F, R]R^p$ has dimension m. If we take any set of m elements $R_1, \ldots, R_m$, of R, linearly independent in R modulo $[F, R]R^p$ and let $K = F/S$, where S is the closure of $R_1, \ldots, R_m$ in F, then G is the maximal p-factor group of K, in the sense that if A is a finite p-group which is a factor group of K then A is a factor group of G.*

Corollary 2.2. *Let $M = \{x_1, \ldots, x_n \mid R_{i_1}, \ldots, R_{i_t}\}$ where $R_{i_1}, \ldots, R_{i_t}$ is a subset of $R_1, \ldots, R_m$. If M is a finite p-group then $G = K$.*

Proof. K is a factor of M and hence K is a finite p-group.

Lemma 2.3. *Let* $G = \{x_1, \ldots, x_n \mid R_1, \ldots, R_m\} = F/R$ *and*

$$G/N = \{x_1, \ldots, x_n \mid R_1, \ldots, R_m, S_1, \ldots, S_u\} = F/S$$

then if $R_{i_1}, \ldots, R_{i_t}$ *are linearly independent in* S *modulo* $[F, S]S^p$ *they are linearly independent in* R *modulo* $[F, R]R^p$.

Proof. The natural mapping $R/[F, R]R^p$ into $S/[F, S]S^p$ is a homomorphism and hence a linear transformation of the respective vector spaces.

Theorem 2.4. *Let* G *be a finite* p*-group with zero deficiency and* N *a normal subgroup of* G *contained in the derived group of* G*, then* G/N *has trivial multiplicator if and only if* $N = 1$.

Proof. Take presentations for G and G/N to be

$$G = \{x_1, \ldots, x_n \mid R_1, \ldots, R_n\} = F/R$$

and

$$G/N = \{x_1, \ldots, x_n \mid R_1, \ldots, R_n, S_1, \ldots, S_u\} = F/S,$$

where $S_i \in F'$, then $R_1, \ldots, R_n$ are linearly independent in S modulo $[F, S]S^p$ and hence if G/N has trivial multiplicator then G/N is the maximal p-factor of G. However, G is a finite p-group and therefore $G/N = G$. Conversely, if G/N does not have trivial multiplicator then $G/N \neq G$ and hence $N \neq 1$ and the theorem is proved.

Hence if we give a presentation with zero deficiency which defines a finite p-group, G, and we show that $G_p(\alpha, \beta)$ is a factor group of G and that

$$G/G' \cong G_p/G_v',$$

then $G = G_p(\alpha, \beta)$.

3. The Main Results

Let p be an odd prime and consider the maximal p-factor, G_p, of a Macdonald group, i.e.,

$$G_p = \{a, b \mid c = a^{-1}b^{-1}ab,\ c^{-1}ac = a^{1+jp^r},\ cbc^{-1} = b^{1+kp^s},\ a^{p^\alpha} = 1,\ b^{p^\beta} = 1,\}$$

where $(j, p) = 1$, $(k, p) = 1$, and r, s, α, β are some positive integers. We have for suitable u, v and w that

$$c^{-u}ac^u = a^{1+p^r},\ c^{-uv}bc^{uv} = b^{1+p^s} \quad \text{and} \quad c^u = a^{-uw}b^{-1}a^u b,$$

where $(u, p) = 1$, $(v, p) = 1$ and v is a power of a primitive root, γ, in the range $0 < \gamma < 2p$. Further since $a^{p^\alpha} = 1$, we may replace w with $y = w + \delta$ where p^α divides δ and v divides y. Note that $\alpha > r$.

Lemma 3.1. $y = 1 + tp^r$, *where* $1 + 2t \not\equiv 0$ *modulo* p.

Proof. We have that $(1 + jp^r)^u \equiv 1 + p^r$ modulo p^α. Hence $1 + ujp^r \equiv 1 + p^r$ modulo p^{r+1} giving that $uj \equiv 1$ modulo p. Also

$$b^{-1}a^u b = (ac)^u = c^u a^{(1+jp^r)((1+jp^r)^u - 1)/jp^r}$$

https://doi.org/10.1017/S0013091500015315 Published online by Cambridge University Press

and

$$a^{uw}c^u = c^u a^{(1+jp^r)^u uw}.$$

Equating right-hand sides gives that

$$(1+jp^r)^{u-1}uw \equiv ((1+jp^r)^u - 1)/jp^r \text{ modulo } p^\alpha.$$

Since $y \equiv w$ modulo p^{r+1} we have

$$(1+(u-1)jp^r)uy \equiv u+u(u-1)jp^r/2 \text{ modulo } p^{r+1},$$

whence $y \equiv 1$ modulo p^r. Let $y = 1+tp^r$ then substitution, cancellation and division by p^r yields $ut+u(u-1)j/2 \equiv 0$ modulo p, whence $2t \equiv j-uj \equiv j-1$ modulo p and we have $1+2t \equiv j \not\equiv 0$ modulo p which proves the lemma. Hence we may choose, with a change of generators, a presentation for G_p of the form

$$G_p = \{a,\ b \mid c = a^{-y}b^{-1}ab,\ c^{-1}ac = a^{1+p^r},\ c^{-v}bc^v = b^{1+p^s},\ a^{p^\alpha} = 1,\ b^{p^\beta} = 1\},$$

where $y = 1+tp^r$, $1+2t \not\equiv 0$ modulo p, $(v, p) = 1$, v divides y and the only primes dividing v lie in the range 0 to $2p$. Let

$$H = \{a, b \mid c = a^{-y}b^{-1}ab, c^{-1}ac = a^{1+p^r}, c^{-v}bc^v = b^{1+p^s}\},$$

then G is a factor group of H and by the previous section when we show that H is a finite p-group we have shown $G = H$ and hence G is a two generator-two relation finite p-group.

The following calculations are all in H.

Lemma 3.2. *a, b and c have finite orders.*

Proof. We have that $c^v = b^{-1}a^v ba^{-y(1+p^r)((1+p^r)^v-1)/p^r}$, $c^{-v}a^v c^v = a^{v(1+p^r)^v}$ and $c^{-v}bc^v = b^{1+p^s}$ whence by Section 4 of (3) a^v, b *and* c^v generate a finite group since v divides y.

Lemma 3.3. *The order of c divides the order of a.*

Proof. Suppose the order of a is m, then by raising the relation $b^{-1}ab = a^y c$ to the power m we have $c^m = a^{-y(1+p^r)((1+p^r)^m-1)/p^r}$, whence since the right-hand side commutes with c, the relation $c^{-1}ac = a^{1+p^r}$ gives that m divides

$$y(1+p^r)((1+p^r)^m-1).$$

However, the power of p which divides m also divides $((1+p^r)^m-1)/p^r$ and hence $c^m = 1$.

Lemma 3.4. *a has p-power order.*

Proof. Since $c^m = 1$, we have that m divides $((1+p^r)^m-1)/p^r$. Suppose q is the smallest prime dividing m and suppose $0<q<p$, then

$$(1+p^r)^m \equiv 1 \text{ modulo } q, \quad 1+p^r \not\equiv 1 \text{ modulo } q,$$

therefore some prime dividing $q-1$ divides m or $q = 2$. In either case $q = 2$

since q is the smallest prime dividing m. However, m is odd and therefore $q = p$. Therefore p is the smallest prime dividing m.

Similarly, if q is a prime dividing m and $0<q<2p$ then p divides $q-1$ or $p = q$ and hence $q = p$. Hence $(v, m) = 1$.

Finally, suppose q is the largest prime dividing m and that $q \neq p$. Let $m' = m/q$ then by Section 3 of (1) we have that m divides $(1+p^r)^{m'}-1)$ and hence m divides $(1+p^r)^{m'}-1)/p^r$ giving that $b^{-1}a^{m'}b = c^{m'}$. Therefore

$$bc^{m'}b^{-1} = a^{m'} = c^{m'}b^z$$

for some z. Conjugation by c and elimination of $c^{m'}$ gives that $a^{p^r m'} = b^{t'}$ for some t' whence $a^{p^r m'}$ is central and hence conjugation by c gives that $a^{p^{2r}m'} = 1$. However, this implies that $a^{m'} = 1$ and therefore $q = p$.

Lemma 3.5. *We may solve the equation* $c^x = a^{-x}b^{-1}a^xb$ *where* $(x, p) = 1$.

Proof. $b^{-1}a^xb = (a^yc)^x = c^xa^{y(1+p^r)((1+p^r)^x-1)/p^r}$ and $a^xc^x = c^xa^{x(1+p^r)x}$

Therefore, if the order of a is p^n, we need to solve the equation

$$x(1+p^r)^{x-1} \equiv y((1+p^r)^x-1)/p^r \text{ modulo } p^n.$$

This equation reduces to $f(x)p^r \equiv 0$ modulo p^n where $f(x) \equiv 2x(x-1-2t)$ modulo p. Note that $y = 1+tp^r$ where $1+2t \not\equiv 0$ modulo p. We show by induction on n that $f(x) \equiv 0$ modulo p^n has a solution coprime with p for any n. For $n = 1$ we have the solution $x = 1+2t$.

Assume that $f(x_i) \equiv 0$ modulo p^i, therefore $f(x_i) = kp^i$ for some k, where $f(x) = a_0+a_1x+a_2x^2+\ldots+a_mx^m$. We try $x = x_i+\delta p^i$ and we have

$$\begin{aligned} f(x) &= a_0+a_1(x_i+\delta p^i)+a_2(x_i+\delta p^i)^2+\ldots+a_m(x_i+\delta p^i)^m \\ &\equiv a_0+a_1x_1+a_2x_i^2+\ldots+a_mx_i^m \\ &\qquad +a_1\delta p^i+2a_2x_i\delta p^i+\ldots+ma_mx_i^{m-1}\delta p^i \text{ modulo } p^{i+1} \\ &\equiv kp^i+\delta p^if'(x_i) \text{ modulo } p^{i+1} \\ &\equiv (k+\delta 2(1+2t))p^i \text{ modulo } p^{i+1}. \end{aligned}$$

Hence we need to solve the equation

$$k+2\delta(1+2t) \equiv 0 \text{ modulo } p,$$

whence $\delta = -k/2(1+2t)$ will do.

Lemma 3.6. *H is a finite nilpotent group.*

Proof. H is generated by a^x and b with relations, $c^x = a^{-x}b^{-1}a^xb$,

$$c^{-x}a^xc^x = a^{x(1+p^r)x},$$

$c^{-x}bc^x = b^z$ for suitable z and hence H is a factor group of a Macdonald group and therefore nilpotent.

However H/H' is a finite p-group and therefore H is a finite p-group. Also $H/H' \cong G_p/G_p'$ and hence $H = G_p$ giving

Theorem 3.7. *The maximal p-factor of a Macdonald group is a group with zero deficiency.*

REFERENCES

(1) I. D. MACDONALD, On a class of finitely presented groups, *Canad. J. Math.* **14** (1962), 602-613.

(2) J. W. WAMSLEY, Minimal presentations for certain group extensions, *Israel J. Math.* **9** (1971), 459-463.

(3) J. W. WAMSLEY, A class of three-generator, three-relation, finite groups, *Canad. J. Math.* **22** (1970), 36-50.

THE FLINDERS UNIVERSITY OF SOUTH AUSTRALIA