Chin. Ann. of Math.
5B (1) 1984

A THEOREM ON METABELIAN p-GROUPS AND SOME CONSEQUENCES

XU MINGYAO (徐明曜)
(*Beijing University*)

Abstract

This paper introduces a new characteristic subgroup $\zeta(G)$ for a finite p-group G, called the p-center of G (Definition 1). A property of p-centers for metabelian p-groups (Theorem 1) is proved. Applying this theorem to regular and p-abelian p-groups, we obtain several known results for these groups once again (Theorems 2, 3 and 6).

The notation and terminology used here are standard. (See [1].) But we use

$$G=G_1>G_2>\cdots>G_{c+1}=1 \tag{1}$$

to denote the lower central series of a nilpotent group G, $c=c(G)$ being the nilpotence class of G. And for commutators we use round brackets, e. g., (a, b), $(a_1, \cdots, a_n)$, and use square brackets to denote the p-commutators defined as follows

$$[a, b]=b^{-p}a^{-p}(ab)^p. \tag{2}$$

It is obvious that

$$(ab)^p=a^pb^p \Leftrightarrow [a, b]=1. \tag{3}$$

We call a group G metabelian if $G''=1$, or equivalently, if G' is abelian.

Some formulas of commutator calculation used in this paper are collected without proof as follows, and their proofs can be found in [1] III § 1, [2], or [3].

Let G be an arbitrary group and $a, b, c\in G$, then

$$(a, b)=(b, a)^{-1}, \tag{4}$$

$$(ab, c)=(a, c)^b(b, c)=(a, c)(a, c, b)(b, c), \tag{5}$$

$$(a, bc)=(a, c)(a, b)^c=(a, c)(a, b)(a, b, c). \tag{6}$$

And let G be a metabelian group. Suppose $a, b, c\in G$, $d\in G'$, then

$$(ad, b)=(a, b)(d, b), \tag{7}$$

$$(d^i, a)=(d, a)^i, \text{ for } i \text{ an integer}, \tag{8}$$

$$(d, a, b)=(d, b, a). \tag{9}$$

For brevity of writing we make the convention that

$$(ia, jb)=(a, b, \overbrace{a, \cdots, a}^{i-1}, \overbrace{b, \cdots, b}^{j-1}),$$

Manuscript received January 26, 1981.

where i, j are positive integers. Owing to (9), any simple commutator with entries a and b in a metabelian group can be reduced to the form (ia, jb) or (jb, ia).

In order to prove the main result of the paper, we also need the following formulas, mentioned as lemmas below.

Lemma 1. *Let G be a nilpotent group of class c. Assume that $a_1, \cdots, a_c \in G$ and $i_1, \cdots, i_c$ are positive integers. Then*

$$(a_1^{i_1}, \cdots, a_c^{i_c}) = (a_1, \cdots, a_c)^{i_1 \cdots i_c}.$$

Proof Using (5) and (6), it is easily proved that if $x, y \in G_s$, $1 \leqslant s < c$, and $z \in G$, then

$$(xy, z) \equiv (x, z)(y, z) \pmod{G_{s+2}}, \tag{10}$$

and if $x \in G_s$, $1 \leqslant s < c$, and $y, z \in G$, then

$$(x, yz) \equiv (x, y)(x, z) \pmod{G_{s+2}}. \tag{11}$$

Applying (10) and (11), the conclusion can be obtained by induction on $i_1 + \cdots + i_c$. The details are omitted.

Lemma 2. *Let G be a metabelian group, and $a, b \in G$, n a positive integer. Then we have*

$$(a, b^n) = \prod_{i=1}^{n} (a, ib)^{\binom{n}{i}}.$$

Proof By induction on n. The case $n=1$ is trivial. Now we suppose $n>1$. From (6) and the induction hypothesis we have

$$\begin{aligned}(a, b^n) &= (a, b^{n-1}b) = (a, b)(a, b^{n-1})(a, b^{n-1}, b) \\ &= (a, b) \prod_{i=1}^{n-1} (a, ib)^{\binom{n-1}{i}} \left(\prod_{i=1}^{n-1} (a, ib)^{\binom{n-1}{i}}, b \right) \\ &= (a, b) \prod_{i=1}^{n-1} (a, ib)^{\binom{n-1}{i}} \prod_{i=1}^{n-1} (a, (i+1)b)^{\binom{n-1}{i}} \qquad \text{(by (8))} \\ &= (a, b)(a, b)^{n-1} \prod_{i=2}^{n-1} (a, ib)^{\binom{n-1}{i}} \prod_{i=2}^{n} (a, ib)^{\binom{n-1}{i-1}} \\ &= (a, b)^n \prod_{i=2}^{n-1} (a, ib)^{\binom{n-1}{i} + \binom{n-1}{i-1}} (a, nb) = \prod_{i=1}^{n} (a, ib)^{\binom{n}{i}}.\end{aligned}$$

Lemma 3. *Let G be a metabelian group, and let $a, b \in G$, n a positive integer. Then we have*

$$(ab^{-1})^n = a^n \prod_{i+j \leqslant n} (ia, jb)^{\binom{n}{i+j}} b^{-n}.$$

Proof By induction on n. The case $n=1$ is trivial. Now suppose $n>1$. Applying the induction hypothesis, Lemma 2 and the formula

$$xy = yx(x, y),$$

we have

$$
\begin{aligned}
(ab^{-1})^n &= (ab^{-1})^{n-1}ab^{-1} = a^{n-1} \prod_{i+j\leqslant n-1} (ia,\ jb)^{\binom{n-1}{i+j}} b^{-(n-1)}ab^{-1} \\
&= a^{n-1} \prod_{i+j\leqslant n-1} (ia,\ jb)^{\binom{n-1}{i+j}} a(a,\ b^{n-1})b^{-n}, \ (\text{by } b^{-(n-1)}a = a(a,\ b^{n-1})b^{-(n-1)}) \\
&= a^n \prod_{i-j\leqslant n-1} [(ia,\ jb)((i+1)a,\ jb)]^{\binom{n-1}{i+j}} (a,\ b^{n-1})b^{-n} \\
&= a^n \prod_{j=1}^{n-2} (a,\ jb)^{\binom{n-1}{j+1}} \prod_{\substack{i+j\leqslant n-1\\ i>1}} (ia,\ jb)^{\binom{n-1}{i+j}} \prod_{\substack{i+j\leqslant n\\ i>1}} (ia,\ jb)^{\binom{n-1}{i+j-1}} \prod_{j=1}^{n-1} (a,\ jb)^{\binom{n-1}{j}} b^{-n} \\
&= a^n \prod_{j=1}^{n-2} (a,\ jb)^{\binom{n-1}{j+1}+\binom{n-1}{j}} (a,\ (n-1)b) \\
&\quad \times \prod_{\substack{i+j\leqslant n-1\\ i>1}} (ia,\ jb)^{\binom{n-1}{i+j}+\binom{n-1}{i+j-1}} \prod_{\substack{i+j=n\\ i\geqslant 1}} (ia,\ jb)b^{-n} \\
&= a^n \prod_{\substack{i+j\leqslant n-1\\ i=1}} (a,\ jb)^{\binom{n}{j+1}} \prod_{\substack{i+j\leqslant n-1\\ i>1}} (ia,\ jb)^{\binom{n}{i+j}} \prod_{i+j=n} (ia,\ jb)b^{-n} \\
&= a^n \prod_{i+j\leqslant n-1} (ia,\ jb)^{\binom{n}{i+j}} \prod_{i+j=n} (ia,\ jb)^{\binom{n}{n}} b^{-n} = a^n \prod_{i+j\leqslant n} (ia,\ jb)^{\binom{n}{i+j}} b^{-n}.
\end{aligned}
$$

Definition 1. *Let G be a finite p-group. Suppose*

$$\zeta(G) = \{a \in G \mid [a,\ x] = [x,\ a] = 1,\ \forall x \in G\}.$$

It is easily proved that $\zeta(G)$ is a characteristic subgroup of G. We call $\zeta(G)$ the p-center of G.

Lemma 4. *Let G be a finite p-group. Suppose $a \in \zeta(G)$ and $x \in G$. Then $(a,\ x^p) = 1$. From this it follows that $\zeta(G) \leqslant C_G(\mho_1(G))$, where $\mho_1(G) = \langle g^p \mid g \in G\rangle$.*

Proof Since $a \in \zeta(G)$, we have

$$a^{-1}x^pa = (a^{-1}xa)^p = a^{-p}(xa)^p = a^{-p}x^pa^p,$$

hence $a^{-(p-1)}x^pa^{p-1} = x^p$, i. e., $a^{p-1} \in C_G(x^p)$. Since $(p-1,\ p) = 1$, we have $\langle a^{p-1}\rangle = \langle a\rangle$. Hence $a \in C_G(x^p)$, i. e., $(a,\ x^p) = 1$ as desired.

Theorem 1. *Let G be a finite metabelian p-group. Suppose $a \in \zeta(G)$ and $x \in G$. Then $\langle a,\ x\rangle'$ is an elementary abelian group and $c(\langle a,\ x\rangle) < p$.*

Proof It will be proved by contradiction. Let G be a minimal counter-example. Then there exist $a \in \zeta(G)$ and $x \in G$ such that $\langle a,\ x\rangle'$ is not elementary abelian or $c(\langle a,\ x\rangle) \geqslant p$. From the minimality of G, we have $\langle a,\ x\rangle = G$. Since to be p-abelian is reserved under homomorphisms, if $\overline{G}$ is a homomorphic image of G, we can deduce $\bar{a} \in \zeta(\overline{G})$ from $a \in \zeta(G)$. Thus we claim that $c(G) \leqslant p$. If it is not the case, we have $c(G) > p$, $G_{p+1} \neq 1$. Writing $\overline{G} = G/G_{p+1}$, we have $|\overline{G}| < |G|$ and $c(\overline{G}) = p$. This contradicts the minimalty of G.

Next we prove that G' is elementary abelian. Since $a \in \zeta(G)$, we have $(a,\ x^p) = 1$ by Lemma 4. According to Lemma 2, it follows that

$$(a,\ x^p) = \prod_{i=1}^{p} (a,\ ix)^{\binom{p}{i}} = 1.$$

For $c(G) \leqslant p$, we have $(a,\ px) = 1$. Hence

$$(a,\ x)^p(a,\ 2x)^{\binom{p}{2}}\cdots(a,\ (p-1)x)^{\binom{p}{p-1}}=1,$$

where all exponents of the commutators are multiples of p. Now we claim that $(a,\ x)^p=1$. If not, we can choose $i>1$ such that $(a,\ ix)^{\binom{p}{i}}\neq 1$, but $(a,\ jx)^{\binom{p}{j}}=1$ for each j, $i<j\leqslant p-1$, hence we have

$$(a,\ x)^p(a,\ 2x)^{\binom{p}{2}}\cdots(a,\ ix)^{\binom{p}{i}}=1. \tag{12}$$

Furthermore, since $1<i<j\leqslant p-1$, we have $p\Big|\binom{p}{j}$. Thus we have $(a,\ jx)^p=1$ from $(a,\ jx)^{\binom{p}{j}}=1$. Making repeatedly commutator operations by x $i-1$ times in (12) we obtain

$$(a,\ ix)^p(a,\ (i+1)x)^{\binom{p}{2}}\cdots(a,\ (2i-1)x)^{\binom{p}{i}}=(a,\ ix)^p=1.$$

This contradicts $(a,\ ix)^{\binom{p}{i}}\neq 1$. Thus we've proved that $(a,\ x)^p=1$. Applying [1] III, 1.11a), we have $G'=\langle (a,\ x)^g\,|\,g\in G\rangle$. Therefore $\exp G'\leqslant p$, i. e., G' is an elementary abelian p-group.

Finally we shall deduce $c(G)<p$ and get a contradiction. Since $G=\langle a,\ x\rangle$ and $G_{p+1}=1$, using [1] III, 1.11b) and formulas (9), (1) and (8), we have

$$G_p=\langle ((p-j)a,\ jx)\,|\,j=1,\ \cdots,\ p-1\rangle\leqslant Z(G).$$

Because $a\in\zeta(G)$, we have $(ax^{-s})^p=a^px^{-sp}$ for each s, $1\leqslant s<p-1$. Applying Lemma 3, we have

$$(ax^{-s})^p=a^p\prod_{i+j\leqslant p}(ia,\ jx^s)^{\binom{p}{i+j}}x^{-sp}.$$

Note that $\exp G'\leqslant p$ and $G_p\leqslant Z(G)$, we get

$$(ax^{-s})^p=a^px^{-sp}\prod_{i+j=p}(ia,\ jx^s),$$

$$\prod_{j=1}^{p-1}((p-j)a,\ jx^s)=1.$$

And using Lemma 1, we obtain

$$\prod_{j=1}^{p-1}((p-j)a,\ jx)^{s^j}=1,\ \text{for } s=1,\ \cdots,\ p-1.$$

These equations, if written in the additive notation, can be viewed as a system of linear equations over the field GF(p) with $p-1$ "unknowns" $((p-j)a,\ jx)$, whose coefficient determinant is a Vandermonde determinant

$$\begin{vmatrix} 1 & 2 & \cdots & p-1 \\ 1^2 & 2^2 & \cdots & (p-1)^2 \\ \cdots & \cdots & \cdots & \cdots \\ 1^{p-1} & 2^{p-1} & \cdots & (p-1)^{p-1} \end{vmatrix}\neq 0.$$

This forces that all the "unknowns" $((p-j)a,\ jx)=1$. Therefore $G_p=1$ and $c(G)<p$. The proof is completed.

Remarks. It is well known that from $\exp G'\leqslant p$ and $c(G)<p$ it can be deduced that G is p-abelian, i. e., $\zeta(G)=G$. Thus Theorem 1 implies that a 2-generator

metabelian p-group must be p-abelian, if one of the generators is contained in $\zeta(G)$. This result is not trivial. The following example shows that for $p\neq 2$, p-commutativity is quite different from commutativity in that 2-generator metabelian p-groups need not be p-abelian even if the two generators are p-commutative. (But for $p=2$, because being 2-abelian is equivalent to being abelian, the situation is, of course, very simple.)

Besides, for a non-metabelian p-group $G=\langle a, x\rangle$, if $a\in\zeta(G)$, we can also prove that G is p-abelian. To save space, no proof will be given.

Example 1. Let G be a Sylow p-subgroup of the symmetric group S_{p^2}. Then G is a semi-direct product of an elementary abelian p-group $N=\langle a_1\rangle\times\cdots\times\langle a_p\rangle$ by a cyclic subgroup $\langle b\rangle$ of order p, where $N\lhd G$ and the following relations hold:

$$a_1^b=a_2,\ a_2^b=a_3,\ \cdots,\ a_{p-1}^b=a_p,\ a_p^b=a_1.$$

Therefore $G=\langle a_1, b\rangle$ and $G'\leqslant N$, i. e., G is a 2-generator metabelian p-group. Write $x=b^2a_1^{-1}$ and $y=a_1b^{-1}$, then it is obvious that $G=\langle x, y\rangle$. Now we have

$$y^p=(a_1b^{-1})^p=a_1^p\prod_{i+j=p}(ia_1,\ jb)b^{-p}=(a_1,\ (p-1)b),$$

$$x^{-p}=(a_1b^{-2})^p=a_1^p\prod_{i+j=p}(ia_1,\ jb^2)b^{-2p}=(a_1,\ (p-1)b^2)=(a_1,\ (p-1)b)^{2^{p-1}}.$$

By Fermat's theorem, $2^{p-1}\equiv 1\pmod p$ if $p\neq 2$; hence

$$x^{-p}=(a_1,\ (p-1)b)=y^p.$$

It follows that

$$x^py^p=1\quad\text{and}\quad y^px^p=1.$$

Moreover, $xy=b$, $yx=a_1ba_1^{-1}$, and hence

$$(xy)^p=b^p=1\quad\text{and}\quad(yx)^p=(a_1ba_1^{-1})^p=1.$$

Therefore $(xy)^p=x^py^p$ and $(yx)^p=y^px^p$, but $G=\langle x, y\rangle$ is not p-abelian.

As a direct consequence of Theorem 1, we mention

Theorem 2. *A finite metabelian p-group G with two generators is p-abelian if and only if $\exp G'\leqslant p$ and $c(G)<p$.*

This theorem is equivalent to the following theorem, first published by W. Brisley and I. D. Macdonald[2]*.

Theorem 3. *A finite metabelian p-group G is regular if and only if for every 2-generator subgroup H of G, it holds that $H_p\leqslant\mho_1(H')$.*

Using Theorem 1 we can also deduce the following theorem which gives a connection between the p-centers and the upper central series of metabelian p-groups.

Theorem 4. *Let G be a finite metabelian p-group. Then $\zeta(G)\leqslant Z_p(G)$, where $Z_p(G)$ is the $(p+1)$-th term of the upper central series of G.*

In order to prove this theorem, we need the following result due to N. D. Gupta

* In 1964, the author also proved this theorem in his thesis "On finite regular p-groups" § 2 at Peking University. But that paper was not published.

and M. F. Newman. (cf. [3] Lemma 2.2.)

Lemma 5. *Let G be a metabelian group, and let $d\in G'$, n a positive integer. If $(d, na)=1$, $\forall a\in G$, then $(d, b, (n-1)a)^{n!}=1$, $\forall a, b\in G$.*

Proof of Theorem 4 Suppose $a\in\zeta(G)$. We must show $a\in Z_p(G)$; and this is equivalent to $(a, x_1, \cdots, x_p)=1$ for all $x_1, \cdots, x_p\in G$. Since $a\in\zeta(G)\triangleleft G$, we have $(a, x_1)\in\zeta(G)$. Thus $((a, x_1), (p-1)x_p)=1$ by Theorem 1. Using Lemma 5 we get

$$(a, x_1, x_2, (p-2)x_p)^{(p-1)!}=1.$$

Because $((p-1)!, p)=1$, we get

$$((a, x_1, x_2), (p-2)x_p)=1.$$

Using Lemma 5 again, we get

$$(a, x_1, x_2, x_3, (p-3)x_p)^{(p-2)!}=1,$$

and

$$(a, x_1, x_2, x_3, (p-3)x_p)=1.$$

Applying Lemma 5 repeatedly as above, we finally obtain $(a, x_1, \cdots, x_p)=1$ as required.

For any finite p-group G, $\bar{G}=G/G''$ is metabelian. From Theorem 4 we have $\zeta(\bar{G})\leqslant Z_p(\bar{G})=Z_p(G)G''/G''$, and since $\zeta(G)\leqslant\zeta(\bar{G})$, we obtain the following

Theorem 5. *Let G be a finite p-group, then $\zeta(G)\leqslant Z_p(G)G''$.*

Applying Theorem 4 to the metabelian p-abelian p-groups, we obtain the following noteworthy result.

Theorem 6. *Let G be a finite metabelian p-abelian p-group, then $c(G)\leqslant p$.*

Proof Since G is p-abelian, then $\zeta(G)=G$. But by Theorem 4, we have $\zeta(G)\leqslant Z_p(G)$. Therefore $Z_p(G)=G$ and $c(G)\leqslant p$.

Acknowledgment

The author is indebted to professor Tuan Hsio-Fu for his suggestions and help.

References

[1] Huppert, B., Endliche Gruppen I, Springer-Verlag, 1967.
[2] Brisley, W. & Macdonald, I. D., Two classes of metabelian p-groups, *Math. Z.*, **112** (1969), 5—12.
[3] Gupta, N. D. & Newman, M. F., On metabelian groups, *J. Aus. Math. Soc.*, **6** (1966), 362—368.