Commentationes Mathematicae Universitatis Carolinae

N. J. Mutio

Complete metacyclic groups

Commentationes Mathematicae Universitatis Carolinae, Vol. 16 (1975), No. 3, 541--547

Persistent URL: http://dml.cz/dmlcz/105646

COMMENTATIONES MATHEMATICAE UNIVERSITATIS CAROLINAE

16,3 (1975)

COMPLETE METACYCLIC GROUPS

N.J. MUTIO, Nairobi

Abstract: In this paper it is shown (Theorem 1) that under certain conditions the order of a metacyclic group G divides the order of its automorphism group. The main result is Theorem 3 which gives both necessary and sufficient conditions for a (nonabelian) metacyclic group to be complete. This extends the known classes of finite groups G with the property that $|G|$ divides $|Aut(G)|$.

Key words and phrases: Split metacyclic group, complete group, innter, outer automorphisms, characteristic, conjugate, trivial intersection subgroup, Frobenius kernel, Frobenius complement.

AMS: 20D45 Ref. Ž.: 2.722.2

The purpose of this paper is to extend the known classes of finite groups G where the order $|G|$ of the group divides the order $|Aut(G)|$ of its automorphism group Aut(G). R. Davitt [2] has shown that if G is a noncyclic metacyclic p-group, p and odd prime, such that $|G| > p^2$, then $|G| \,\big|\, |Aut(G)|$. We shall show here that Davitt's result holds for certain metacyclic groups which are not necessarily p-groups. Necessary and sufficient conditions for G to be complete will also be given. An arbitrary group G is called <u>complete</u> if its center Z(G) is trivial and its automorphism group equals Inn(G), the group of its inner automorphisms. A group G is called <u>metacyclic</u> if it has a cyclic normal subgroup A such that G/A is also cyclic. Let $A = \langle a \rangle$ with $|a| = m$ and $G/A = \langle bA \rangle$ with $|bA| = s$. Denote by r the least positive integer for which $b^{-1}ab = a^r$. Then $(m,r) = 1$, $r^s \equiv 1 \pmod{m}$, and if u is the (multiplicative) order of r mod m, then $u \mid s$. A metacyclic group G therefore has a presentation of the form

$$G = \langle a,b : a^m = 1 ,\ b^s = a^t ,\ b^{-1}ab = a^r \rangle$$

and G is called <u>split</u> if $t = 0$. We will refer to the integers m, s, r, u and t as the <u>usual parameters</u> of G. The subgroup $\langle b \rangle$ will be denoted by B.

We remark here that all our groups will be assumed to be split, nonabelian and metacyclic so that $t = 0$ and $r > 1$.

For any $x \in G$ let $\underline{x}$ denote the innter automorphism of G determined by x. Using the above representation of G (G arbitrary metacyclic) it is easily shown that $Z(G) = \langle a^{m/d}, b^u \rangle$, where $d = (m, r-1)$, and

$$\mathrm{Inn}(G) = \langle \underline{a},\underline{b} : \underline{a}^{m/d} = 1 = \underline{b}^u,\ \underline{b}^{-1}\underline{ab} = \underline{a}^r \rangle .$$

Hence $|Z(G)| = mu/d = |\mathrm{Inn}(G)|$.

<u>Theorem 1</u>. Let G be a metacyclic group with the usual parameters such that $s = u$. Then $|G| \,\big|\, |\mathrm{Aut}(G)|$.

<u>Proof</u>: We construct a subgroup of $\mathrm{Aut}(G)$ of order $mu = |G|$. For each integer j, $1 \le j \le m$, define $\sigma(a^j) : G \longrightarrow G$ by

$$(b^k a^i)\,\sigma(a^j) = (ba^j)^k a^i = b^k a^{j(r^k-1)/(r-1)} a^i .$$

Then

$$[(b^k a^i)\ \sigma(a^j)]\,[(b^w a^v)\ \sigma(a^j)] = b^k a^{j(r^k-1)/(r-1)} a^i b^w a^{j(r^w - 1)/(r-1)} a^v$$

$$= b^{k+w} a^{j(r^{k+w})/(r-1)} a^{ir^w+v} \ .$$

On the other hand,

$$[(b^k a^i)(b^w a^v)]\ \sigma(a^j) = (b^{k+w} a^{ir^w+v})\ \sigma(a^j)$$

$$= b^{k+w} a^{j(r^{k+w})/(r-1)} a^{ir^w+v} \ .$$

Hence $\sigma(a^j)$ is an endomorphism of G which fixes A elementwise.

Now suppose that $(b^k a^i)\ \sigma(a^j) = 1$ for some positive integers k and i. Then $b^k a^{j(r^k-1)/(r-1)} a^i = 1$. Since G is split this yields $b^k = 1$ and consequently $a^i = 1$, finally yielding $b^k a^i = 1$. Thus $\sigma(a^j) \in \mathrm{Aut}(G)$ for each j.

Next we have that for any x and y in A,
$b(\sigma(x)\,\sigma(y)) = (b\,\sigma(x))\,\sigma(y) = (bx)\,\sigma(y) = b(xy) = b\,\sigma(xy)$.
Since $a\,\sigma(x) = a$ for every $x \in A$ we conclude that $\sigma :$
$: A \longrightarrow \mathrm{Aut}(G)$ is a homomorphism into. But $b\,\sigma(x) = b$ clearly implies that $x = 1$. Hence σ is a monomorphism. Furthermore it is clear that $\sigma(A) = \langle \sigma(a) \rangle$.

We investigate $\langle \sigma(a) \rangle \cap \mathrm{Inn}(G)$. So suppose that $\sigma(a^i) \in \mathrm{Inn}(G)$ for some i. Then $\sigma(a^i)$ is equivalent to conjugation by some power of a since it fixes A elementwise. So let $b\,\sigma(a^i) = b\underline{a}^z$ for some integer z. Then $b\,\sigma(a^i) = ba^{z(1-r)} = b(\sigma(a^{1-r}))^z$, yielding $\sigma(a^i) =$
$= (\sigma(a^{1-r}))^z$. We conclude that

$$\langle \sigma(a) \rangle \cap \mathrm{Inn}(G) = \langle \sigma(a^{1-r}) \rangle$$

and it is clear that $|\langle \sigma(a^{1-r})\rangle| = m/d$. Since $Inn(G) \lhd Aut(G)$ we have $\langle \sigma(a)\rangle \cdot Inn(G)$ is a subgroup of $Aut(G)$ of order $mu = |G|$ and the theorem is proved.

The following result asserts that under certain conditions G has no outer automorphisms. Let $\varphi(x)$ be the Euler phi-function.

<u>Lemma 2</u>. Let G be as in Theorem 1 such that the following hold :

1. $\varphi(m) = u$;
2. A is characteristic in G ;
3. B is conjugate to all its automorphic images.

Then $Inn(G) = Aut(G)$.

<u>Proof</u>: Since A is cyclic of order m we have that $|Aut(A)| = \varphi(m)$. On the other hand, the subgroup $\langle \underline{b}\rangle$ of $Aut(G)$ is of order u and each of its members restricts to an automorphism of A . Since $\varphi(m) = u$ we see that every automorphism of A is equivalent to conjugation of elements of A by some power of b . So let $\beta \in Aut(G)$. Since A is characteristic in G , $\beta|_A \in Aut(A)$, so that $\beta|_A = \underline{b}^k$ for some integer $k > 0$. On the other hand, since $B\beta$ is conjugate to B , we have that for some integer i , $1 \le i \le m$, $B\beta = \langle b\beta\rangle = \langle a^{-i}ba^{i}\rangle = \langle b\underline{a}^{i}\rangle$. Hence $a\beta = a\underline{b}^k$ and $b\beta = b\underline{a}^{i}$. It follows that $\beta = \underline{b}^k\underline{a}^{i} \in$ $\in Inn(G)$ and the lemma is proved.

We are now ready to give some necessary and sufficient conditions for a metacyclic group to be complete. This is

Theorem 3. Let G be as in Theorem 1. Then the following are equivalent:

1. G is complete.

2. (i) $d = (m, r-1) = 1$,

(ii) A is characteristic in G such that $\varphi(m) = u$,

(iii) B is conjugate to all its automorphic images.

Proof: $1 \Longrightarrow 2$: G complete implies that $Z(G) = \langle a^{m/d}, b^u \rangle = 1$, yielding $d = 1$ so that 2(i) holds. Next, G complete implies that all its automorphisms are inner of the form $\underline{b}^k\underline{a}^i$ for positive integers k and i . Hence $a(\underline{b}^k\underline{a}^i) = a^{r^k} \in A$. Hence every automorphism of G is an automorphism of A and A is characteristic in G . Furthermore, all the restrictions contribute exactly u distinct automorphisms of A , namely conjugations of elements of A by powers of b . But $|\mathrm{Aut}(A)| = \varphi(m)$ and $u \mid \varphi(m)$. Suppose $u < \varphi(m)$. For each integer n , $1 \leq n \leq m$ satisfying $(n,m) = 1$, define $\alpha_n : A \longrightarrow A$ by $a^i\alpha_n = a^{in}$, $1 \leq i \leq m$. Then it is clear that $\alpha_n \in \mathrm{Aut}(A)$ and these are the only automorphisms of A , so that they are $\varphi(m)$ in number. Since $u < \varphi(m)$, then there exists an integer n_o such that $(n_o, m) = 1$ and α_{n_o} is not equivalent to conjugation by a power of b . Now extend α_{n_o} to an automorphism of G by defining $b\alpha_{n_o} = b$. Then α_{n_o} , as an automorphism of G , is not inner, a contradiction since G is complete. Hence $\varphi(m) = u$. This completes the proof of 2(ii). Condition 2(iii) is obvious since all automorphisms of G are inner. This completes the proof of $1 \Longrightarrow 2$.

$2 \Longrightarrow 1$: First of all, since G is split, $b^u = 1$, and since $d = 1$ by 2(i), we have $Z(G) = 1$. Secondly, by the lemma above, conditions 2(ii) and 2(iii) imply that G has no outer automorphisms. This completes the proof.

Let G be any finite group. A subset B of G is called a T.I. set (trivial intersection set) if $g \in G$ implies that either $g^{-1}Bg = B$ or $(g^{-1}Bg) \cap B = 1$. A finite group G is called Frobenius if it has a nontrivial proper subgroup H which is a self-normalizing T.I. set. The subgroup H is called a Frobenius complement of G. If G is a Frobenius group then it is well known that there exists another subgroup M, popularly known as the Frobenius Kernel of G, and unique in G such that $H \cap M = 1$ and $(|H|,|M|) = 1$. A Frobenius group is clearly split.

Some Frobenius groups are complete as shown in the following corollary to the above theorem.

Corollary 4: Let G be a metacyclic Frobenius group with Frobenius complement $\langle b \rangle$ and order mu. If $(m,r-1) = 1$, $\varphi(m) = u$ and $\langle b \rangle$ is a p-subgroup, then G is complete.

Proof: First note that G is split metacyclic. Secondly, $\langle a \rangle$ is the Frobenius kernel and is therefore characteristic in G ([4], Corollary 17.5). Thirdly, since $\langle b \rangle$ is a p-subgroup such that $(|b|,|a|) = 1$, it follows that $\langle b \rangle$ is conjugate to all its automorphic images. Fourthly, since $(m, r-1) = 1$ and $\varphi(m) = u$, all the conditions of (2) of Theorem 3 are satisfied and the corollary follows.

Remark. An infinite class of complete metacyclic groups is easily constructed as follows. For any prime $p > 2$ let G be the group generated by a and b with defining relations $a^p = 1 = b^{p-1}$ and $b^{-1}ab = a^r$, where $1 < r < p$ and the multiplicative order of r modulo p is $p - 1$. Then G is metacyclic with $A = \langle a \rangle$ a characteristic subgroup. By Theorem 10.5 of [4] the subgroup $B = \langle b \rangle$ is conjugate to its automorphic images. Hence G is complete by Theorem 3 above.

Observe that S_3, the symmetric group on three letters belongs to this class.

References

[1] C. CURTIS and I. REINER: Representations of Finite Groups and Associative Algebras, Interscience, New York, 1966.

[2] R. DAVITT: The automorphism group of a finite metacyclic p-group, Proc. Amer. Math. Soc. 25(1970),876-879.

[3] R. DAVITT and A. OTTO: On the automorphism group of a finite p-group with the central quotient metacyclic, Proc. Amer. Math. Soc. 30(1971),467-472.

[4] D. PASSMAN: Permutation Groups, W.A. Benjamin, Inc., New York, 1968.

Kenyatta University College

Nairobi

Kenya

(Oblatum 6.2.1965)