SOME AUTOMORPHISMS OF FINITE NILPOTENT GROUPS

by J. C. HOWARTH

(Received 12 February, 1960)

1. Introduction. This note extends the concept of the inner automorphism, but here applies only to those finite groups G for which some member of the lower central series is Abelian. In general (e.g. when G is metabelian) the construction yields an endomorphism semigroup, but in the special case where G is nilpotent (and may therefore, for our present purposes, be considered as a p-group) a group of automorphisms results.

2. Construction. Employing the notation

$$[s, t] = s^{-1}t^{-1}st$$

for any two elements s and t of a group G, we first list the identities

$$[xy, zt] = y^{-1}[x, t]t^{-1}[x, z]y[y, z]t, \qquad (2.1)$$

$$[[x, y], z] = [y, x][z, x][x, yz]. \qquad (2.2)$$

We denote by

$$(G =)\, G_1 \supseteq G_2 \supseteq \dots$$

the lower central series of G, so that $G_2 = [G, G]$ and $G_i = [G_{i-1}, G]$. The use of (2.1) yields the result that, if the subgroup G_k of G is Abelian, then for $g \in G$, $h \in G_{k-1}$ and $c \in G_k$,

$$[gc, h] = [g, h][c, h]. \qquad (2.3)$$

Concerning endomorphisms, we clearly have the following criterion.

LEMMA 2.4. *If, with each element g of G is associated an element a_g, then the mapping*

$$\alpha: \quad g\alpha = ga_g$$

is an endomorphism if and only if, for all pairs g, h of elements of G,

$$a_g h a_h = h a_{gh}.$$

THEOREM 2.5. *If the subgroup G_k is Abelian, then for arbitrary elements $a_1, \dots, a_m$ chosen from G_{k-1}, the mapping*

$$\theta: \quad g\theta = g[g, a_1] \dots [g, a_m]$$

is an endomorphism of G, the set of all such endomorphisms being closed under multiplication.

Should G be also a p-group, then θ defines, in all cases, an automorphism, the complete set resulting in a p-group.

Proof. Since, for each i, the mapping $g \to g[g, a_i]$ is an inner automorphism, then, by Lemma 2.4,

$$[g, a_i]h[h, a_i] = h[gh, a_i].$$

Thus, writing $u_i = [u, a_i]$ for any element u of G, we have, since elements of the form x_i, y_j commute,

$$\begin{aligned} g_1 \dots g_m h h_1 \dots h_m &= g_2 \dots g_m g_1 h h_1 \dots h_m \\ &= g_2 \dots g_m h (gh)_1 h_2 \dots h_m \\ &= g_3 \dots g_m h (gh)_1 (gh)_2 h_3 \dots h_m \\ &= \dots \\ &= h (gh)_1 \dots (gh)_m. \end{aligned}$$

Hence, by Lemma 2.4, θ is an endomorphism.

If the elements $b_1, \dots, b_n$ of G_{k-1} define a second endomorphism

$$\phi: \quad g\phi = g[g, b_1] \dots [g, b_n],$$

then use of the identities (2.3) and (2.2) gives

$$\begin{aligned} g\theta\phi &= g \prod_i [g, a_i] \prod_j [g[g, a_1] \dots [g, a_m], b_j] \\ &= g \prod_i [g, a_i] \prod_j [g, b_j] \prod_{i,j} [[g, a_i], b_j] \\ &= g \prod_i [g, a_i] \prod_j [g, b_j] \prod_{i,j} [a_i, g][b_j, g][g, a_i b_j] \end{aligned}$$

i.e.,
$$g\theta\phi = g \prod_{i,j} [g, a_i b_j] \prod_i [a_i, g]^{n-1} \prod_j [b_j, g]^{m-1}, \qquad (2.6)$$

which is of the required form.

The fact that θ is invariably an automorphism in the case where G is a p-group, is due to a result of Burnside. See P. Hall [**1**, pp. 35–6]. Since the Frattini subgroup F of G contains the commutator subgroup G', then if elements $x_1, \dots, x_r$ form a minimal set of generators of G (so that the cosets $\bar{x}_i = x_i F$ form a basis of G/F), it follows that each $\bar{x}_i = (x_i\theta)F$. This implies that $x_1\theta, \dots, x_r\theta$ generate G, or that θ is an automorphism.

Since θ belongs to the p-group consisting of those automorphisms of G which reduce to the identity on G/F [**1**, pp. 37–8], then the set of all automorphisms θ must also form a p-group.

3. Some identities. Suppose that G is a p-group. We choose first an element a from the subgroup G_{k-1}, then an integer c (not necessarily positive) and for $g \in G$, write θ for the automorphism

$$g\theta = g[g, a]^c. \qquad (3.1)$$

It is easily verified that use of the formula (2.6) yields, for any positive integer q,

$$g\theta^q = g[g, a]^{c_1}[g, a^2]^{c_2} \dots [g, a^q]^{c_q},$$

where
$$c_i = c^i(1-c)^{q-i}\binom{q}{i}.$$

The use of this formula, together with certain elementary congruence properties listed below, makes it possible to derive some identities involving automorphisms of a type similar to θ.

O

https://doi.org/10.1017/S2040618500034171 Published online by Cambridge University Press

LEMMA 3.2. *In the following, a, b, m and n are integers, m and n being positive, and r is an integer in the range* $0 \leqslant r \leqslant n$.

(i) $a^{p^n} \equiv a^{p^{n-1}} \pmod{p^n}$.

(ii) *If b is prime to p and satisfies* $1 \leqslant b \leqslant p^{n-r}$, *then* $\binom{p^n}{bp^r} \equiv 0 \pmod{p^{n-r}}$.

(iii) *If* $a \equiv b \pmod{p^n}$, *then* $a^p \equiv b^p \pmod{p^{n+1}}$.

From (iii), we have immediately

(iv) *If* $a \equiv b \pmod{p^n}$, *then* $a^{p^m} \equiv b^{p^m} \pmod{p^{m+n}}$.

Denoting the exponent of any group H by $\exp H$, let $p^s = \exp G_k$ and write $w = p^{s-1}$.

THEOREM 3.3. *Let* θ *be the automorphism* (3.1). (i) *If* $n \geqslant s$, *then* $\theta^p = \phi^w$, *where* $g\phi = g[g, a^{p^{n-s+1}}]^c$. (ii) *If* $g\psi = g[g, a]^b$, *then* $c \equiv b \pmod{p^t}$ *implies that* $\psi^v = \theta^v$, *where* $v = p^{s-t}$.

Proof. (i) Writing γ for the automorphism $g\gamma = g[g, a^p]^c$, it is clearly sufficient to establish that, for $n \geqslant s$, $\theta^{p^n} = \gamma^{p^{n-1}}$. We have, putting $q = p^n$ and $r = p^{n-1}$,

$$g\theta^q = g[g, a]^{c_1} \dots [g, a^q]^{c_q}, \quad g\gamma^r = g[g, a^p]^{d_1} \dots [g, a^q]^{d_r},$$

where
$$c_i = c^i(1-c)^{q-i}\binom{q}{i}, \quad d_j = c^j(1-c)^{r-j}\binom{r}{j}.$$

Since $p^s = \exp G_k$ divides q, then, for i prime to p, we have, by Lemma 3.2,

$$c_i \equiv \binom{q}{i} \equiv 0 \pmod{p^s}$$

and hence we may rewrite

$$g\theta^q = g[g, a^p]^{e_1} \dots [g, a^{pr}]^{e_r},$$

where
$$e_j = c^{pj}(1-c)^{p(r-j)}\binom{pr}{pj}.$$

Let p^d be the highest power of p dividing j; then $0 \leqslant d \leqslant n-1$ and

$$\binom{pr}{pj} \equiv 0, \quad \binom{r}{j} \equiv 0 \pmod{p^{n-d-1}},$$

$$c^{pj} \equiv c^j \pmod{p^{d+1}}, \quad (1-c)^{(r-j)p} \equiv (1-c)^{r-j} \pmod{p^{d+1}}.$$

Hence $d_j \equiv e_j \pmod{p^n}$, and since $\exp G_k$ divides p^n, the result is established.

(ii) We have

$$g\theta^v = g[g, a]^{f_1} \dots [g, a^v]^{f_v}, \quad g\psi^v = g[g, a]^{h_1} \dots [g, a^v]^{h_v},$$

where
$$f_i = c^i(1-c)^{v-i}\binom{v}{i}, \quad h_i = b^i(1-b)^{v-i}\binom{v}{i}.$$

If p^d, where $0 \leqslant d \leqslant s-t$, is the highest power of p dividing i, then

$$\binom{v}{i} \equiv 0 \pmod{p^{s-t-d}}, \quad c^i \equiv b^i \pmod{p^{t+d}},$$

and
$$(1-c)^{v-i} \equiv (1-b)^{v-i} \pmod{p^{t+d}}.$$

Together these congruences yield $f_i \equiv h_i \pmod{p^s}$, which completes the proof.

This result provides an upper bound for the order of the automorphism θ of (3.1). If we examine first the case for which the integer c is arbitrary, Theorem 3.3 (i) yields the result:

COROLLARY 3.4. *If the inner automorphism of G with respect to the element a has order p^m then θ has order dividing p^{m+s-1}.*

Should the integer c be divisible by $p^t (0 \leqslant t \leqslant s)$, then, by repeated applications of (ii) we have, putting $v = p^{s-t}$,

$$\theta^v = \theta_1^v = \theta_2^v = \ldots,$$

where, writing $c_i = c^{p^i}$, $g\theta_i = g[g, a]^{c_i}$. However, if $t \geqslant 1$, c_i is divisible by $p^{p^i t}$ and hence θ^v is the identity automorphism.

COROLLARY 3.5. *If the integer c is divisible by $p^t (1 \leqslant t \leqslant s)$, then the order of the automorphism θ divides p^{s-t}.*

REFERENCE

1. P. Hall, Groups of prime power order, *Proc. London Math. Soc.* (2) **36** (1934) 29–95.

THE UNIVERSITY
GLASGOW