On the automorphism groups of certain wreath products

By C. H. HOUGHTON (Manchester)

§ 1. Introduction

The problem considered here is the determination of the structure of the automorphism group of the standard wreath product[1]) W of two groups A and B. B. H. NEUMANN and HANNA NEUMANN have shown (cf. [1]) that the automorphism group of W contains subgroups isomorphic to the automorphism groups of A and of B, while an unpublished result of PETER M. NEUMANN states that except when B is of order 2 and A is a dihedral group of order $4m+2$ or is of order 2, the base group is a characteristic subgroup of the wreath product. Using these results, one can describe completely the way in which the automorphism group of the unrestricted wreath product is built up from certain distinguished subgroups whose choice arises naturally from the way in which the wreath product is formed from its component groups.

Beyond that, the automorphism group of W naturally depends on the nature of the groups A and B. In the case when A is abelian and B is finite and cyclic, the automorphism group of W turns out to be soluble of length at most three. Using a method suggested by the work of DAYKIN [2], the automorphism group can be described completely when both A and B are finite and cyclic. We shall give no more than an indication of the method, which involves tedious computation, but only describe the result. In the particular case where A and B are both cyclic, of orders 2^r and 2^s respectively, the automorphism group is itself a 2-group and therefore nilpotent. When B is just a 2-cycle and A is of order 2^r with $r>1$, the class can also be computed without much trouble and shows the existence of a 2-group of class $r+1$ whose automorphism group is itself a 2-group and of class r.

This paper arose out of a thesis presented to the University of Manchester for the degree of Master of Technical Science. I thank my supervisors DR. HANNA NEUMANN and DR. JAMES WIEGOLD for their continual help and encouragement while I was doing this work and in the preparation of this paper.

§ 2. Preliminaries

We denote the order of a set S by $|S|$. If H is a subgroup of G, we write $H \leqq G$ and, when H is normal in G, $H \lhd G$. The commutator $h^{-1}k^{-1}hk$ of two elements h, k of a group G is denoted by $[h, k]$. We write Aut (G) for the automorphism group of a group G.

[1]) Throughout this paper we shall refer to the standard wreath product as the wreath product; no other wreath product is considered.

The wreath product of two groups A and B, which are assumed throughout this paper to be non-trivial, is defined as follows. Let F_1 be the group of functions on B taking values in A with multiplication of $f, g \in F_1$ defined by

$$fg(x) = f(x)g(x) \quad \text{for all } x \in B.$$

Then F_1 is the unrestricted direct product of $|B|$ isomorphic copies of A. The subgroup F_2 of F_1, consisting of all those $f \in F_1$ such that $f(x) = 1$ for all but a finite number of $x \in B$, is the corresponding restricted direct product. We denote both these groups by F, distinguishing between the unrestricted and the restricted direct product when necessary.

If $f \in F$ and $b \in B$, we define $f^b \in F$ by

$$f^b(x) = f(xb^{-1}) \quad \text{for all } x \in B.$$

The group of automorphisms of F defined by

$$f \to f^b \quad \text{for all } f \in F,$$

is isomorphic to B and we shall identify it with B. The wreath product W of A and B is defined as the splitting extension of F by this group of automorphisms; that is, W is generated by B and F with the relations

$$b^{-1}fb = f^b \quad \text{for all } b \in B \text{ and } f \in F.$$

If F is unrestricted, we call W the unrestricted wreath product of A and B, written A Wr B. If F is restricted, W is called the restricted wreath product of A and B, written A wr B. We shall refer to F as the base group of W. As mentioned in the introduction, we have the following result.

2. 1. *Except when B has order two and A is a dihedral group of order $4m+2$ or is of order two, the base group is characteristic in W.*

The subgroup of F consisting of all constant functions is the diagonal subgroup. It is necessarily trivial when W is restricted and B is infinite. Otherwise it is clearly isomorphic to A. Since we are naturally interested in the characteristic subgroups of the wreath product, the following result is important to us.

2. 2. *The centre of W coincides with the centre of the diagonal subgroup of W.*

This is easily confirmed; cf. also Baumslag [3]. To complete the preparations, we determine the derived group W' of W in the case when A and B are abelian and W is restricted. Clearly W' lies in the base group as W/F is isomorphic to B and so is abelian. Now we have the following result.

2. 3. *If A and B are both abelian and W is their restricted wreath product then a function $f \in F$ belongs to W' if and only if the product of its non-trivial values is the unit element of A.*

Proof. To prove the necessity of the condition we need only show that it is necessary for the generators of W' because A, and hence F, is abelian. If $f \in F$ is such a generator then $f = [bg, ch]$ for some $b, c \in B$, $g, h \in F$. So

$$f = g^{-1}g^c(h^b)^{-1}h,$$

and, as is quickly checked, the product of its non-trivial values is 1.

Suppose conversely that $f \in F$ and satisfies the condition of the theorem. For each non-trivial $b \in B$ for which $f(b) \neq 1$ we define $g_b \in F$ by:

$$g_b(1) = f(b), \quad g_b(x) = 1 \qquad \text{for non-trivial } x \in B.$$

Then,

$$f = \prod (g_b^b)(g_b)^{-1} = \prod [b, g_b^{-1}],$$

where the product is taken over all non-trivial $b \in B$ for which $f(b) \neq 1$.

A consequence of this theorem is that, if A and B are finite abelian groups, then $|W'| = |A|^{|B|-1}$.

§ 3. The automorphism group of the unrestricted wreath product

In view of 2. 1., we assume from now on that when B has order 2, A is not of the type specified there, so that the base group is characteristic in the wreath product. In [1], extensions of automorphisms of A and B to automorphisms of their wreath product W were constructed as follows.

3. 1. *If $\alpha \in \mathrm{Aut}(A)$, we define $\alpha^* \in \mathrm{Aut}(W)$ by $(bf)^{\alpha^*} = bf^{\alpha^*}$ for all $b \in B$, $f \in F$, where $f^{\alpha^*}(x) = (f(x))^\alpha$ for all $x \in B$.*

The group A^* of all such automorphisms is isomorphic to $\mathrm{Aut}(A)$.

3. 2. *If $\beta \in \mathrm{Aut}(B)$, we define $\beta^* \in \mathrm{Aut}(W)$ by $(bf)^{\beta^*} = b^\beta f^{\beta^*}$ for all $b \in B$, $f \in F$, where $f^{\beta^*}(x) = f(x^{\beta^{-1}})$ for all $x \in B$.*

The group B^* of all such automorphisms is isomorphic to $\mathrm{Aut}(B)$. It follows easily from these definitions that A^* and B^* permute elementwise in the automorphism group of W. In the next theorem we describe the structure of this automorphism group, assuming from now on that W is unrestricted.

Theorem 3. 3. (a) *The automorphism group*[2]) *of the wreath product W of two groups A and B can be expressed as a product,*

$$\mathrm{Aut}(W) = KI_1B^*,$$

where (1) *K is the subgroup of* $\mathrm{Aut}(W)$ *consisting of those automorphisms which leave B elementwise fixed,* (2) *I_1 is the subgroup of* $\mathrm{Aut}(W)$ *consisting of those inner automorphisms corresponding to transformation by elements of the base group F,* (3) *B^* is defined as in* 3. 2.

(b) *The group K can be written as A^*H, where* (4) *A^* is defined as in* 3. 1., (5) *H is the subgroup of* $\mathrm{Aut}(W)$ *consisting of those automorphisms which leave both B and the diagonal elementwise fixed.*

(c) *The subgroups A^*HI_1, HI_1B^*, HI_1, and I_1 are normal in* $\mathrm{Aut}(W)$ *and* $\mathrm{Aut}(W)$ *is the splitting extension of A^*HI_1 by B^*. Furthermore, A^* intersects HB^* trivially.*

[2]) The automorphism group described here does in fact occur in the cases excluded in 2. 1., the whole automorphism group being an extension of this by a 2-cycle, as is well known for $C_2 W_r C_2 \cong D_8$.

Proof. For the proof we write $L=\mathrm{Aut}(W)$ for convenience.

Proof of (a). Let α be an automorphism of W. If $b\in B$ then $b^\alpha\equiv b'$ (mod F) for some $b'\in B$. Since W is a splitting extension of F by B, the mapping $\beta: B\to B$ defined by $b^\beta=b'$, all $b\in B$, is an automorphism of B. Let $\beta'\in B^*$ be the extension of β^{-1} to an automorphism of W by the construction 3. 2. Then $b^{\beta'\alpha}\equiv b$ (mod F) and so $b^{-1}b^{\beta'\alpha}\in F$. We denote this function by f_b, so that for each $b\in B$ we have a function $f_b\in F$ given by $b^{\beta'\alpha}=bf_b$. Now we define a function[3] $g\in F$ which takes, at each argument $x\in B$, the same value as the function f_x takes at x, that is $g(x)=f_x(x)$ for each x. Then for each $b\in B$,

$$b^{-1}g^{-1}bg=(g^b)^{-1}g \text{ and } \big((g^b)^{-1}g\big)(x)=\big(g(xb^{-1})\big)^{-1}g(x)$$

for $x\in B$. At xb^{-1}, g takes the same value as $(xb^{-1})^{-1}(xb^{-1})^{\beta'\alpha}$. But this is

$$bx^{-1}x^{\beta'\alpha}(b^{\beta'\alpha})^{-1}=(x^{-1}x^{\beta'\alpha})^{b^{-1}}b(b^{\beta'\alpha})^{-1}.$$

So

$$g(xb^{-1})=f_x(x)\big(f_b(x)\big)^{-1}=g(x)\big(f_b(x)\big)^{-1},$$

and the value of $b^{-1}g^{-1}bg$ at x is the same as the value of f_b. Thus $b^{\beta'\alpha}=g^{-1}bg$. If $i\in I_1$ is the inner automorphism defined by $w^i=gwg^{-1}$ for all $w\in W$, then $b^{\beta'\alpha i}=b$ and so $\beta'\alpha i\in K$ and we have $L=KI_1B^*$.

Proof of (b). If $f\in F$ then f is in the diagonal D if and only if $f^b=f$ for all $b\in B$. Now if $\gamma\in K$, $b\in B$ and $f\in F$,

$$(f^b)^\gamma=(b^{-1}fb)^\gamma=b^{-1}f^\gamma b=(f^\gamma)^b,$$

so the diagonal is mapped onto itself by γ, and γ restricted to D is an automorphism γ_0 of D. As W is unrestricted, the diagonal is isomorphic to A under the mapping taking an element of D into its value in A. So γ_0 corresponds to an automorphism γ_1 of A defined by $\big(f(x)\big)^{\gamma_1}=f^{\gamma_0}(x)$ for all $f\in D$, $x\in B$. If $\gamma'\in A^*$ is the extension of γ_1^{-1} to an automorphism of W by the construction 3. 1. then $\gamma'\gamma$ leaves D elementwise fixed and therefore lies in H. So $K=A^*H$.

Proof of (c). A simple argument shows that the automorphisms in B^* leave the diagonal elementwise fixed. One can then check that the subgroups A^*HI_1, HI_1B^*, HI_1 and I_1 consist respectively of all those automorphisms with the following properties:

A^*HI_1 : for some $g\in F$, $b\to g^{-1}bg$ for all $b\in B$;

HI_1B^* : for some $g\in F$, $f\to g^{-1}fg$ for all $f\in D$;

HI_1 : for some $g\in F$, $b\to g^{-1}bg$ for all $b\in B$ and $f\to g^{-1}fg$ for all $f\in D$;

I_1 : for some $g\in F$, $w\to g^{-1}wg$ for all $w\in W$.

It is immediate from the first of these statements, together with 3. 2., that $A^*HI_1\cap B^*=1$. The proofs that the subgroups mentioned above are normal in

[3]) This function may have infinitely many non-trivial values even if the functions f_b do not.

L and of the assertions about A^* are now straightforward computations and will be omitted.

We now have two series of normal subgroups of $\mathrm{Aut}(W)$:

$$\mathrm{Aut}(W) = KI_1B^* \supseteqq KI_1 \supseteqq HI_1 \supseteqq I_1 \supseteqq 1,$$

and

$$\mathrm{Aut}(W) = A^*HI_1B^* \supseteqq HI_1B^* \supseteqq HI_1 \supseteqq I_1 \supseteqq 1.$$

Let I be the group of inner automorphisms of the wreath product and let I_2 be the subgroup consisting of those which correspond to transformation by elements of B. If B is abelian then I_2 lies in H and we have:

$$HI_1 \supseteqq I \supseteqq I_1 \supseteqq 1.$$

Since the centre of the wreath product is the centre of the diagonal, we know the structure of I_1. As B^* is isomorphic to $\mathrm{Aut}(B)$, we now turn our attention to the subgroup K. We know that if $\gamma \in K$, $b \in B$, and $f \in F$, then $(f^b)^\gamma = (f^\gamma)^b$. Suppose now that α is an automorphism of the base group F such that $(f^b)^\alpha = (f^\alpha)^b$ for all $b \in B$, $f \in F$. We can extend this to an automorphism $\gamma \in K$ by defining $(bf)^\gamma = bf^\alpha$ for all $b \in B$, $f \in F$. Thus we have the following.

3. 4. *The group K is isomorphic to the group of those automorphisms of the base group which commute with the inner automorphisms induced by elements of B.*

We also denote this group by K without risk of confusion.

§ 4. The group Aut (W) when A and B are finite and cyclic

When A and B are cyclic, the automorphism groups A^* and B^* are well known. So the results of the last section show that it is only the group K which has to be determined. To start with, we only assume that A is cyclic and B is finite abelian. Then A has a representation as the additive group of a ring R, namely the ring of integers if A is infinite or the ring of integers modulo $|A|$ if A is finite; in the latter case we identify each residue class modulo $|A|$ with the least positive integer it contains. If A is generated by a then we define $f_0 \in F$ by

$$f_0(1) = a, \quad f_0(b) = 1 \qquad \text{for all non-trivial } b \in B.$$

Then every element f of the base group F has a unique representation of the form

$$f = \prod_{b \in B} (f_0^b)^{r(b)} \text{ where } r(b) \in R.$$

Let S be the group ring of B over R. Then we can represent the base group faithfully as a one-dimensional S-module as follows. If $s = \sum_{b \in B} r(b)b \in S$, where $b \in B$ and $r(b) \in R$ then we define f_0^s to be $\prod_{b \in B} (f_0^b)^{r(b)}$.

If E is the ring of those endomorphisms α of the base group which commute with the group of automorphisms induced by elements of B then $\alpha \in E$ is completely determined by the image f_0^α of f_0. Now we construct a mapping θ between E and S which one can easily check to be a ring isomorphism; if $\alpha \in E$ and $f_0^\alpha = f_0^s$, where $s \in S$, then we define θ by putting $\alpha\theta = s$. In this set up, K is the multiplicative group of invertible elements of E, so it is isomorphic to the multiplicative group of invertible elements of S, which is abelian. Thus we have the following.

4. 1. *When A is cyclic and B is finite and abelian, then the group K* (cf. 3. 4.) *is abelian.*

Combining this with 3. 3 (a) we get the next theorem.

Theorem 4. 2. *The automorphism group of the wreath product of a cyclic group by a finite abelian group is soluble of length at most three.*

Now we specialise further and consider the group K arising when A is a cycle of order m and B is a cycle of order n; we shall denote it by $K(m, n)$. That is, $K(m, n)$ is the multiplicative group of invertible elements of the group ring of a cycle of order n over the ring of integers modulo m.

If m is written as a product of prime factors $m = p_1^{r_1} \dots p_t^{r_t}$, where $p_1, \dots, p_t$ are distinct, one can show without difficulty that $K(m, n)$ is isomorphic to the direct product of the groups $K(p_i^{r_i}, n)$ for $i = 1, \dots, t$. The determination of the groups $K(p^r, n)$ can be achieved by applying standard methods of ring theory and vector space theory. The details are tedious and complicated and so we merely state the results.

4. 31. *If p is a prime and $n = p^s h$, where h is not divisible by p, then the group $K(p^r, n)$ is the direct product of $K(p, h)$ and a p-group P.*

To describe the two factors, let φ be Euler's function and, for an integer d, let $M(d; p)$ be the order of p modulo d.

4. 32. *The group $K(p, h)$ is the direct product of $\sum_{d|h} \varphi(d)/M(d, p)$ cyclic groups, there being $\varphi(d)/M(d, p)$ factors of order $p^{M(d,p)} - 1$ for each divisor d of h.*

4. 33. *The group P contains a subgroup P_1 whose factor group P/P_1 is the direct product of $h(p-1)$ cycles of order p^s and $hp^{s-u-1}(p-1)^2$ cycles of order p^u, for $u = 1, \dots, s-1$. When $p \neq 2$, P_1 is the direct product of n cycles of order p^{r-1}; when $p = 2$, P_1 is the direct product of $n - \sigma$ cycles of order 2^{r-1}, σ cycles of order 2^{r-2} and σ cycles of order 2, where $\sigma = \sum_{d|h} \varphi(d)/M(d, 2)$.*

In conjunction with Theorem 3. 3. this immediately gives the first part of the following result.

Theorem 4. 4. *The automorphism group of the wreath product of a cycle of order 2^r by a cycle of order 2^s is a 2-group and therefore nilpotent. When $s = 1$ and $r > 1$, its class is r.*

PROOF. To prove the second part of the theorem we first note that the class of the wreath product is $r + 1$, (cf. LIEBECK [4]). Thus the class of its automorphism group is at least r. Now the group of inner automorphisms corresponding to transformation by elements of the base group is cyclic of order 2^r, generated by δ, say. A simple calculation shows that the derived group of the automorphism group lies in the group generated by δ^2 and hence the nilpotency class is exactly r.

References

[1] B. H. Neumann and Hanna Neumann, Embedding theorems for groups, *Journal London Math. Soc.* **34** (1959), 465–479.

[2] D. E. Daykin, On the rank of the matrix $f(A)$ and the enumeration of certain matrices over a finite field, *Journal London Math. Soc.* **35** (1960), 36–42.

[3] G. Baumslag, Wreath products and p-groups, *Proc. Cambridge Phil. Soc.* **55** (1959), 224–231.

[4] Hans Liebeck, Concerning nilpotent wreath products, *Proc. Cambridge Phil. Soc.* **58** (1962), 443–451.

(*Received September 13, 1962.*)