Arch. Math., Vol. 45, 111–115 (1985)

0003-889X/85/4502-0111 $ 2.50/0

Two results on wreath products

By

L. G. Kovács

Among the familiar basic facts concerning unrestricted permutational wreath products (sketched in the first few paragraphs of the last section of Cossey, Kegel, and Kovács [2]), the Embedding Theorem has the central role. It asserts the existence of an embedding; the proof is a construction which involves arbitrarily chosen coset representatives, with the effect that the embedding constructed may vary by an inner automorphism induced by an element of the base group. The theorem becomes even more useful once we rule out the possibility that a totally different construction could yield "equally natural" embeddings beyond this range of variation. The first result to be presented here achieves this in a somewhat more general context. Its essence first appeared as a special case of the last part of Theorem 3.1 in Gross and Kovács [3] (re-stated as Theorem 3.02 in [4] and extensively used there as well). A full statement is given here and proved from first principles. It leads to the second result which concerns centralizers of certain subgroups in wreath products and has an application in the context of primitive permutation groups.

1. The Uniqueness Theorem. The following notation and conventions will be found convenient. Permutations will be written on the left, homomorphisms on the right, and composites formed accordingly. If A is a group and I a set, the elements of the cartesian power A^I will be thought of as the functions $f\colon I \to A$, $i \mapsto f(i)$. If $\varrho\colon P \to \operatorname{Sym} I$ is a permutation representation of a group P, one obtains an action of P on A^I by setting $f^p(i) = f((p\varrho)\,i)$ for all f in A^I, p in P, and i in I. The semidirect product PA^I formed with this action may be called $A\,Wr\,\varrho$ or just W; its natural projection onto the distinguished copy of P in W is denoted π; and for each element w of W we write $w = (w\pi)f_w$ (so $f_w \in A^I$). Let 0 be an element of I and P_0 its stabilizer $\{p \in P \mid (p\varrho)\,0 = 0\}$ in P, with ϱ_0 the permutation representation of P_0 on $I \setminus \{0\}$: then $P_0 A^I$ has a natural direct decomposition as $A \times (A\,Wr\,\varrho_0)$; the corresponding projection of $P_0 A^I$ onto A will be called π_0. Explicitly, $w\pi_0 = f_w(0)$ whenever $w \in P_0 A^I$. We shall have several occasions to calculate this when w is given as $y^{-1}uv$ (with $y, u, v \in W$): then

$$(0) \qquad w\pi_0 = f_y(0)^{-1} f_u((v\pi\varrho)\,0)\, f_v(0),$$

because $f_w = f_y^{-w\pi} f_u^{v\pi} f_v$ is readily confirmed and $(w\pi\varrho)\,0 = 0$ by assumption.

[Traditionally, in forming wreath products one only used representations ϱ which were both faithful and transitive. In most contexts, faithfulness can be dispensed with at no

cost, and even transitivity is only needed to prevent an already complicated setting from becoming distractingly tedious.]

Uniqueness Theorem. *Let γ and γ' be homomorphisms of a group G into W, and suppose that $G\gamma\pi\varrho$ is transitive.*

If $f \in A^I$,

$$(1) \qquad f(0) = a, \quad \text{and}$$

$$(2) \qquad g\gamma' = (g\gamma)^f \quad \text{for all } g \text{ in } G,$$

then

$$(3) \qquad \gamma'\pi = \gamma\pi, \quad \text{and}$$

$$(4) \qquad h\gamma'\pi_0 = (h\gamma\pi_0)^a \quad \text{for all } h \text{ in } G_0$$

where G_0 is the stabilizer of 0 (the complete inverse image of $G\gamma\pi \cap P_0$) in G.

Conversely, if $a \in A$ and (3), (4) *hold, then there is a unique f in A^I satisfying* (1) *and* (2)*; namely, that defined by* (5) *below.*

Proof. Since π is a homomorphism and $(A^I)\pi = 1$, (2) certainly implies (3). Application of (0) with $y = v = f$, $u = h\gamma$ shows directly that (1) and (2) also imply (4).

Suppose that (3), (4) hold. Take immediate advantage of (3) by easing notation; for $(g\gamma\pi\varrho)i$ write simply gi, noting that also $(g\gamma'\pi\varrho)i = gi$. To each i in I, choose an element g_i in G such that $g_i 0 = i$ (this is how the transitivity assumption is exploited); for further simplicity, set $g_i\gamma = p_i f_i$ and $g_i\gamma' = p_i f_i'$ (with $p_i \in P$, $f_i, f_i' \in A^I$). By another application of (3), one may re-write (2) as $f^{g\gamma\pi} f_{g\gamma'} = f_{g\gamma} f$. The two sides being functions, their equality means agreement at each i: so (2) is now equivalent to

$$(2') \qquad f(gi) f_{g\gamma'}(i) = f_{g\gamma}(i) f(i) \quad \text{for all} \quad g \text{ in } G,\ i \text{ in } I.$$

Substitute 0 for i in (2′), and then g_i for g in the resulting equation; if (1) also holds, the result is

$$(5) \qquad f(i) = f_i(0)\, a\, f_i'(0)^{-1} \quad \text{for all} \quad i \text{ in } I.$$

This defines the only function f which can possibly satisfy (1) and (2); we must still prove that it does satisfy them.

First, recall that $g_0 \in G_0$ and apply (4) with $h = g_0$, to see that $i = 0$ in (5) yields (1). Next, check that $g_{gi}^{-1} g g_i \in G_0$ and apply (4) with $h = g_{gi}^{-1} g g_i$, using (0) once for $w = h\gamma'$ and once for $w = h\gamma$: the result is

$$f_{gi}'(0)^{-1} f_{g\gamma'}(i) f_i'(0) = a^{-1} f_{gi}(0)^{-1} f_{g\gamma}(i) f_i(0)\, a.$$

When the two values of f in (2′) are substituted from the definition (5), (2′) becomes equivalent to the equation we just derived. This completes the proof.

[The intransitive variant of the Uniqueness Theorem is not too hard to state, and the proof needs no new ideas. The role of 0 is to be given to a complete set J of representatives of the orbits of $G\gamma\pi\varrho$, and that of a is to be played by a mapping $J \to A, j \mapsto a(j)$. Thus (1) becomes

$$f(j) = a(j) \quad \text{for all} \quad j \text{ in } J,$$

and (4) is replaced by

$$h\gamma'\pi_j = (h\gamma\pi_j)^{a(j)} \quad \text{for all} \quad j \text{ in } J \quad \text{and all} \quad h \text{ in } G_j$$

where the π_j are the obvious analogues of π_0 and G_j denotes the stabilizer of j in G: (2) and (3) remain unchanged.]

2. The Centralizer Theorem. The second result will describe the centralizer C of a subgroup G in an unrestricted permutational wreath product $A\,Wr\,\varrho$ where $P = \mathrm{Sym}\, I$ and ϱ is the identitiy mapping. We shall use γ for the inclusion of G in W, and suppress these two maps throughout. As before, 0 is an arbitrary element of I; for each i in I, G_i is the corresponding stabilizer $\{g \in G \mid (g\pi)i = i\}$. *Assume that $G\pi$ is transitive*: so to each i we have an element g_i in G such that $g_i = p_i f_i$ and $p_i 0 = i$. The role of $\pi_0\colon P_0 A^I \twoheadrightarrow A$ is unchanged.

Let C_0 denote the set of those elments x in the normalizer $\mathbb{N}_G(G_0)$ to which there exist $a(x)$ in A such that

(6) $$(h^x)\pi_0 = (h\pi_0)^{a(x)} \quad \text{for all} \quad h \text{ in } G_0:$$

these $a(x)$ will then form a coset of the centralizer $\mathbb{C}_A(G_0\pi_0)$. If $x \in G_0$ then $a(x) = x\pi_0$ will always do, so $G_0 \leqq C_0$. If $x \in C_0$ then of course x must normalize $G_0 \cap \ker \pi_0$ as well. One could also say that the elements of $\mathbb{N}_A(G_0\pi_0)$ induce, by conjugation, a group $\mathrm{Aut}_A\, G_0\pi_0$ of automorphisms on $G_0\pi_0$; that π_0 yields a homomorphism from $\mathbb{N}_G(G_0) \cap \mathbb{N}_G(G_0 \cap \ker \pi_0)$ into $\mathrm{Aut}\, G_0\pi_0$; and that C_0 is the complete inverse image of $\mathrm{Aut}_A\, G_0\pi_0$ under this homomorphism. (This second description shows incidentally that C_0 is a subgroup.)

Centralizer Theorem. *The map $c \mapsto g_{(c\pi)0}^{-1} G_0$ is a homomorphism of C onto C_0/G_0, and π_0 maps the kernel of this homomorphism isomorphically onto $\mathbb{C}_A(G_0\pi_0)$. Conversely, for each x in C_0 and for each $a(x)$ in A satisfying* (6), *define a permutation p by*

(7) $$p\,i = p_i(x\pi)0 \quad \textit{for all} \quad i \textit{ in } I,$$

and an element f of A^I by

(8) $$f(i) = f_i(0)\,a(x)\,f_i((x\pi)0)^{-1} \quad \textit{for all} \quad i \textit{ in } I:$$

C is the set of all the quotients $c f^{-1}$ so obtained.

The proof will exploit the fact that the restriction of π is a transitive permutation representation of G. Thus $i \mapsto g_i G_0$ is a bijection of I onto the set of the left cosests of G_0 in G, such that $(g\pi)i$ corresponds to $g\,g_i G_0$ whenever $g \in G$. [Beware: if $p \notin G$ then $p\,i$ does not correspond to $p\,g_i G_0$; indeed, this coset does not even lie in G. What it corresponds to is, of course, $g_{pi} G_0$.] Further, the stabilizer G_i is $g_i G_0 g_i^{-1}$, equal to G_0 if and only if $g_i \in \mathbb{N}_G(G_0)$.

If $p \in \mathbb{C}_P(G\pi)$ then in particular p must leave invariant the fixed point set of $G_0\pi$; so $p\,0$ is fixed by G_0, whence $G_{p0} = G_0$ and so $g_{p0} \in \mathbb{N}_G(G_0)$ follow. Moreover, as each p_i lies in $G\pi$,

(7′) $$p\,i = p\,p_i 0 = p_i\,p\,0 \quad \text{for each} \quad i \text{ in } I.$$

Conversely, if $g_{p0} \in \mathbb{N}_G(G_0)$ then

$$p_{(g\pi)i}^{-1}(g\pi)p_i \in G_0 = G_{p0} \quad \text{for all} \quad g \text{ in } G,$$

so if (7′) also holds then

$$p(g\pi)i = p_{(g\pi)i}\,p\,0 = (g\pi)p_i\,p\,0 = (g\pi)\,p\,i \quad \text{whenever} \quad g \in G, i \in I$$

shows that $p \in \mathbb{C}_P(G\pi)$. Thus $p \mapsto g_{p0}\,G_0$ is a bijection of $\mathbb{C}_P(G\pi)$ onto $\mathbb{N}_G(G_0)/G_0$. In fact, this map is an anti-isomorphism: for, if $p, q \in \mathbb{C}_P(G\pi)$ then, as p_{q0} lies in $G\pi$ and so commutes with p,

$$p_{q0}\,p_{p0}\,0 = p_{q0}\,p\,0 = p\,p_{q0}\,0 = p\,q\,0,$$

whence $g_{q0}\,g_{p0} \in g_{pq0}\,G_0$.

Since π obviously maps C into $\mathbb{C}_P(G\pi)$, it follows that $c \mapsto g_{(c\pi)0}^{-1}\,G_0$ is a homomorphism of C into $\mathbb{N}_G(G_0)/G_0$, with kernel $C \cap A^I$. The Uniqueness Theorem applied with $\gamma' = \gamma$ tells us that π_0 maps $C \cap A^I$ isomorphically onto $\mathbb{C}_A(G_0\pi_0)$.

An element p of P lies in $C\pi$ if and only if there is an f in A^I satisfying (2) with $\gamma' \colon g \mapsto p^{-1}gp$. By the Uniqueness Theorem, this is the case if and only if (3) holds and there is an a in A satisfying (4); moreover, the relevant f are then defined, in terms of these a, by (5). With this choice of γ', (3) amounts to $p \in \mathbb{C}_P(G\pi)$ and is therefore equivalent to $g_{p0} \in \mathbb{N}_G(G_0)$ and (7′), so suppose these hold. Let $x \in g_{p0}\,G_0$; then $(x\pi)\,0 = p\,0$, so (7′) becomes (7) and (5) becomes (8). It remains to verify that there exist a satisfying (4) if and only if there exist $a(x)$ satisfying (6). This is a direct consequence of the fact that

$$(p^{-1}hp)\,\pi_0 = f_x(0)\,(h^x)\,\pi_0\,f_x(0)^{-1} \quad \text{for all} \quad h \text{ in } G_0$$

whenever $x \in \mathbb{N}_G(G_0)$ and p is defined by (7). The last equation is verifed by two applications of (0): one with $w = p^{-1}hp$, the other with $w = x^{-1}hx$. This completes the proof.

Finally, note that it is not hard to find examples in which $C_0 \neq G_0$ or $C_0 \neq \mathbb{N}_G(G_0)$, so the complexity of the Centralizer Theorem seems unavoidable. For instance, let G be an extension of the elmentary abelian group A_4' of order 4 by a group of order 3 (so G is either the alternating group A_4 or the relevant direct product). The Embedding Theorem yields an embedding of G into $W = A\,Wr\,S_3$ where $A = A_4'$ and S_3 is the symmetric group of degree 3. In each case, the projection of G in S_3 is transitive, G_0 has order 4 and is normal in G; but while $C_0 = G_0$ when G is alternating, $C_0 = G$ when G is abelian. (This example will be exploited further at the end of the next section.)

3. An application to primitive groups. We close by sketching the application which motivated the Centralizer Theorem.

It follows readily from Lemma 5.1 of [4] that the primitive permutation groups which have a disjoint pair of (nontrivial) normal subgroups are precisely the groups constructed as follows. Take a nonabelian characteristically simple group, say M, and a subgroup G of Aut M containing Inn M large enough to ensure that Inn M is minimal normal in G. Let G^* be the subgroup of the direct square $G \times G$ of G consisting of the (g_1, g_2) with $g_1, g_2 \in G$ and $g_1 \equiv g_2$ modulo Inn M; then (Inn $M) \times 1$ and $1 \times ($Inn $M)$ are disjoint normal subgroups of G^*. The corefree maximal subgroups of G^* are precisely the diagonal copies

$$G_\alpha = \{(g, \alpha^{-1}g\alpha) \mid g \in G\}$$

of G formed with automorphisms α of M such that

$$g \equiv \alpha^{-1} g \alpha \quad \text{modulo} \quad \text{Inn}\, M \quad \text{for all} \quad g \text{ in } G:$$

in other words, such that the coset $\bar{\alpha}$ of α in Out $M = (\text{Aut}\, M)/(\text{Inn}\, M)$ centralizes $\bar{G} = G/(\text{Inn}\, M)$. Since one also has that G_α is conjugate to G_β in G^* if and only if $\bar{\alpha} = \bar{\beta}$, *the set of equivalence types of faithful primitive permutation representations of G^* is bijective with the centralizer of $\bar{G}$ in* Out M.

When M is a cartesian power S^I, with finite I, of some nonabelian simple group S (as it must be whenever M is finite), one has that $\text{Aut}\, M = (\text{Aut}\, S)\, Wr (\text{Sym}\, I)$, $\text{Out}\, M = (\text{Out}\, S)\, Wr (\text{Sym}\, I)$, and the condition that Inn M be minimal normal in G is equivalent to the transitivity of the projection of G (or $\bar{G}$) in Sym I. Thus in this case the Centralizer Theorem (applied with $\bar{G}$ in place of G) enables us to account for the equivalence types of faithful primitive permutations representations of G^*.

That account may also be translated into the language of G itself, as follows. Identify S with the direct factor of M corresponding to the index 0, and let G_0 be the "normalizer" of S in G; restriction to S maps G_0 into Aut S, and then the natural map into Out S. The image $\text{Out}_G\, S$ of G_0 under the composite map will play the role of $\bar{G}_0 \pi_0$. On the other hand, let C_0 consist of those elements x of $\mathbb{N}_G(G_0)$ to which there exist automorphisms $\alpha(x)$ of S such that, for each h in G_0, the restriction of h^x to S is congruent modulo Inn S to the conjugate of the restriction of h by $\alpha(x)$.

Corollary. *The centralizer of $\bar{G}$ in* Out M *has a homomorphism onto C_0/G_0 with kernel isomorphic to $\mathfrak{C}_{\text{Out}\, S}(\text{Out}_G\, S)$.*

In view of Out $A_6 \cong A_4'$, the example at the end of the previous section suggests that the complexity of this result is also unavoidable.

Corefree maximal subgroups in finite groups form the subject of the paper [1] by Aschbacher and Scott; I am indebted for the opportunity to see a pre-publication copy. For the relevant case, see part B) of their Theorem 1.

References

[1] M. Aschbacher and L. Scott, Maximal subgroups in finite groups. J. Algebra (to appear).
[2] John Cossey, O. H. Kegel, and L. G. Kovács, Maximal Frattini extensions. Arch. Math. **35**, 210–217 (1980).
[3] Fletcher Gross and L. G. Kovács, On normal subgroups which are direct products. J. Algebra **90**, 133–168 (1984).
[4] L. G. Kovács, Maximal subgroups in composite finite groups. J. Algebra (to appear).

Eingegangen am 30. 8. 1984

Anschrift des Autors:

L. G. Kovács
Department of Mathematics
Australian National University
Canberra, A.C.T. 2601
Australia