TRANSITIVE SETS OF HOMOMORPHISMS

W. R. SCOTT

The following remarks were inspired by the discussion in Zassenhaus [1, pp. 51–52] of multiply transitive holomorphs of groups. Theorems 1, 2, and 3 below generalize Theorem 6, Theorem 7, and an untheoremed statement, respectively, in [1]. Additional relevant theorems are given in [2].

Let G and H be groups. Let $o(G)$ denote the order of G. Consider the following statements.

(A_n) $o(G) \geqq n+1$, $o(H) \geqq n+1$, and if $a_i \in G$, $x_i \in H$, $i=1, \cdots, n$, $a_i \neq a_j$, and $x_i \neq x_j$ for $i \neq j$, $a_i \neq e_G$, and $x_i \neq e_H$, then there exists a homomorphism σ of G into H such that $a_i\sigma = x_i$, $i=1, \cdots, n$.

(B_n) $o(G) \geqq n+1$, $o(H) \geqq n+1$, and if $b_i \in G$ and $y_i \in H$, $i=1, \cdots$, $n+1$, $b_i \neq b_j$ and $y_i \neq y_j$ for $i \neq j$, then there exists an $h \in H$ and a homomorphism σ of G into H such that $h(b_i\sigma) = y_i$, $i=1, \cdots, n+1$.

The equivalence of (A_n) and (B_n) is first proved. Then conditions for the validity of (A_n) are investigated. For $n=1$ the results are incomplete, but for $n \geqq 2$ they are complete. The proofs are all trivial.

We use the notation Q for commutator subgroup, and the term *infinitely divisible* for a group H such that if $h \in H$ and n is a positive integer, then there exists an $x \in H$ such that $x^n = h$.

LEMMA. *The statements* (A_n) *and* (B_n) *are equivalent.*

PROOF. Suppose (B_n) is true. Let $(a_1, \cdots, a_n)$ and $(x_1, \cdots, x_n)$ with the properties listed in (A_n) be given. Let $b_i = a_i$ and $y_i = x_i$, $i=1, \cdots, n$, while $b_{n+1} = e_G$ and $y_{n+1} = e_H$. Then h, σ exist as in (B_n). But $h = e_H$, hence (A_n) is satisfied.

If (A_n) holds, and $(b_1, \cdots, b_{n+1})$ and $(y_1, \cdots, y_{n+1})$ as in (B_n) are given, let $a_i = b_{n+1}^{-1}b_i$, $x_i = y_{n+1}^{-1}y_i$, $i=1, \cdots, n$. Let σ be the homomorphism guaranteed by (A_n) and let h be such that $h(b_{n+1}\sigma) = y_{n+1}$. Then

$$h(b_i\sigma) = y_{n+1}(b_{n+1}^{-1}\sigma)(b_i\sigma) = y_{n+1}(a_i\sigma) = y_i, \qquad i = 1, \cdots, n,$$

and (B_n) holds also.

It is clear that in the above theorem homomorphism may be replaced throughout by anti-homomorphism or by isomorphism, while into may be replaced by onto. This follows immediately from the above proof except that for anti-homomorphisms, we let $a_i = b_ib_{n+1}^{-1}$ in

Received by the editors April 22, 1952 and, in revised form, June 1, 1952.

the second half of the proof.

In Theorems 1 and 2, (A_n) may be replaced by (B_n).

THEOREM 1. *If* (A_1) *is true and* G *is not torsion free, then all elements of* G *and* H *(except* e_G *and* e_H*) have the same prime order* p*; and if, furthermore,* H *is finite, then* G *is the direct product of groups of order* p*. Conversely if* $o(G)>1$, $o(H)>1$, *and* G *is the direct product of groups of prime order* p *while all elements of* H *are of order* p, *then* (A_1) *is true.*

PROOF. Since G is not torsion free, there is an $a\in G$ of prime order p. Then if $x\in H$, $x\neq e$, we have $a\sigma=x$ for some σ, hence $o(x)=p$ also. If $b\in G$, $b^p\neq e$, then $b^p\sigma=x$ for some $x\neq e$ and some σ, while $b^p\sigma=(b\sigma)^p=e$, a contradiction.

Next, let H be finite. If G were non-Abelian, there would exist an $a\in Q(G)$, $a\neq e$, and, since H is a finite p-group, an $x\in H-Q(H)$, and finally a σ such that $a\sigma=x$. But $Q(G)\sigma\subseteq Q(H)$ for all homomorphisms (and anti-homomorphisms). Hence G is Abelian, and therefore the direct product of groups of order p.

The converse is obvious and the proof will be omitted.

REMARK 1. In the converse, if both G and H are direct products of groups of order p, then additional requirements may be laid upon σ as follows: (i) if $o(G)\geqq o(H)$, then $G\sigma=H$, and (ii) if $o(G)\leqq o(H)$, then σ is an isomorphism of G into H.

REMARK 2. If G is torsion free and (A_1) holds, then H is infinitely divisible. For if $a\in G$, $a\neq e$, $x\in H$, $x\neq e$, then for any n there exists a σ such that $a^n\sigma=x=(a\sigma)^n$.

THEOREM 2. (A_2) *holds if and only if either* (i) G *and* H *are both direct products of groups of order* 2, *or* (ii) H *is a group of order* 3 *while* G *is a direct product of groups of order* 3.

PROOF. If H is of order 3, then by Theorem 1 and Remark 2, G is the direct product of groups of order 3.

Let $o(H)>3$. Suppose that $x\in H$, $x^2\neq e$. Then there exists a $y\in H$ such that $y\neq e$, x, or x^2. If $a\in G$, $a\neq e$, then by Theorem 1, $a^2\neq e$. By (A_2) there exists a σ such that $a\sigma=x$, $a^2\sigma=y$, a contradiction. Hence $x^2=e$ for all $x\in H$. By Theorem 1 and Remark 2, $a^2=e$ for all $a\in G$. Thus (A_2) implies (i) or (ii).

Conversely the required homomorphisms are of standard construction. Again the additional conditions given in Remark 1 may be imposed on σ.

THEOREM 3. (A_3) *holds for loops* G *and* H *if and only if* H *is the direct product of two groups of order* 2 *while* G *is the direct product of at least* 2 *groups of order* 2.

PROOF. Suppose (A_3) holds. If $o(H)>4$, then there exist $x, y, z\in H$ with $x\neq e, y\neq e$ or $x, z\neq e, x, y$, or xy. There exist $a, b\in G$ such that $a\neq e, b\neq e$ or a, and $ab\neq e$. Then there is a σ such that $a\sigma=x, b\sigma=y$, and $(ab)\sigma=z$, a contradiction. Hence $o(H)=4$. But a loop of order 4 is a group. If, for $a, b, c\in G$ we have $(ab)c\neq a(bc)$, then (even though one of these products may equal e_G) there is a σ such that $((ab)c)\sigma \neq (a(bc))\sigma$, i.e.,

$$((a\sigma)(b\sigma))(c\sigma) \neq (a\sigma)((b\sigma)(c\sigma)),$$

a contradiction since H is a group. Hence G is associative and therefore a group. It follows from Theorem 2 that G and H have the stated forms. (The proof for anti-homomorphisms is similar.)

The converse is again proved by exhibiting an obvious homomorphism.

COROLLARY. (A_n) *does not hold for loops for* $n>3$.

BIBLIOGRAPHY

1. H. Zassenhaus, *The theory of groups*, New York, 1949.

2. R. H. Bruck, *Loops with transitive automorphism groups*, Pacific Journal of Mathematics vol. 1 (1951) pp. 481–483.

UNIVERSITY OF KANSAS