A PROPERTY OF FINITE SIMPLE NON-ABELIAN GROUPS

W. D. MAURER AND JOHN L. RHODES[1]

It has been proved by Fröhlich [1] that the collection of inner automorphisms of a finite simple non-abelian group G generates the group (under pointwise multiplication) of all functions from G into G leaving the identity fixed, and, conversely, that the only finite groups with this property are the simple non-abelian groups, Z_2, and $[e]$. It follows directly that the inner automorphisms and the constant functions of a simple non-abelian group into itself generate the entire group of functions from G into G. The purpose of this note is to prove the following generalization of this theorem.

THEOREM. *Let G be a finite group of order $\mathfrak{g} \geqq 3$, and let A be a finite set of order $\mathfrak{a} \geqq 3$. Let $F(A, G)$ be the group of all functions $f: A \to G$ under the operation $(f_1 \cdot f_2)(a) = f_1(a) \cdot f_2(a)$, and let H be a subgroup of $F(A, G)$ such that:*

(a) *$f^g \in H$, where $f^g(a) = g$, all $a \in A$, for each $g \in G$;*

(b) *if $x, y \in A$, there exists $f \in H$ with $f(x) \neq f(y)$.*

Then H is necessarily equal to $F(A, G)$ if and only if G is simple non-abelian.

PROOF. Let G be simple non-abelian. A j-tuple $(g_1, \cdots, g_j)$ of elements $g_i \in G, j \leqq \mathfrak{a}$, is called accessible if for every j-tuple $(a_1, \cdots, a_j)$ of distinct members of A there exists $f \in H$ such that $f(a_i) = g_i$, $1 \leqq i \leqq j$. We prove all j-tuples (in particular, all $\mathfrak{a}$-tuples) accessible by induction on j. All 1-tuples are accessible, by (a) above. It suffices to show that all j-tuples of the form $(g, e, \cdots, e)$ are accessible, since H is a subgroup. Let $\alpha = (a_1, \cdots, a_j)$ be a particular j-tuple of distinct members of A, and let $G_\alpha \subseteq G$ be the set of all $g \in G$ for which there exists $f \in H$, $f(a_1) = g$, $f(a_i) = e$, $2 \leqq i \leqq j$; since H is a subgroup of $F(A, G)$, G_α is a subgroup of G, and, in fact, it is seen to be a normal subgroup by considering $f^x \cdot f \cdot f^{x^{-1}}$. Since G is simple, it suffices to show that $G_\alpha \neq [e]$. For $j = 2$, this follows from (b) above; if $f(a_1) \neq f(a_2)$, then $f' = f \cdot f^z$, where $z = (f(a_2))^{-1}$, satisfies $f'(a_1) \neq e$, $f'(a_2) = e$. Now assume $j \geqq 3$. Let $g_1, g_2 \in G$ be such that $g_1 g_2 \neq g_2 g_1$. Such elements exist because G is non-abelian. Since all $(j-1)$-tuples are accessible, there exist $f_1, f_2 \in H$ such that the values of f_1 and f_2 on the elements

Received by the editors February 12, 1963 and, in revised form, January 3, 1964.

[1] The second-named author proved the corollary presented here by a somewhat complicated method assuming [1]. The first author obtained the present proof.

a_i are given by the following diagram:

$$\begin{array}{llllll} a = & a_1 & a_2 & a_3 & a_4 \cdots & a_n \\ f_1(a) = & g_1 & e & x & e & e \\ f_2(a) = & g_2 & y & e & e & e \end{array}$$

where x and y are (unspecified) elements of G. Then the values of $f_3 = f_1^{-1} \cdot f_2^{-1} \cdot f_1 \cdot f_2$ on the elements a_i are given by

$$\begin{array}{llllll} a = & a_1 & a_2 & a_3 & a_4 \cdots & a_n \\ f_3(a) = & [g_1g_2] & e & e & e & e, \end{array}$$

where $[g_1g_2] = g_1^{-1}g_2^{-1}g_1g_2$, which shows that $[g_1g_2] \in G_\alpha$ and, therefore, $G_\alpha \neq [e]$.

Conversely, suppose that G is either nonsimple or abelian. If G has a proper nontrivial normal subgroup N, then

$$H = \{f: A \to G \,|\, f(x)f(y)^{-1} \in N, \text{ all } x, y \in A\}$$

satisfies the requirements (a) and (b) of the theorem, and is a proper subset of $F(A, G)$. To prove H a subgroup, we note that if $f(x)f(y)^{-1} = h \in N$, $g(x)g(y)^{-1} = k \in N$, then

$$\begin{aligned} f(x)g(x)(f(y)g(y))^{-1} &= f(x)(g(x)g(y)^{-1})f(y)^{-1} = f(x)kf(y)^{-1} \\ &= f(x)kf(x)^{-1}f(x)f(y)^{-1} = f(x)kf(x)^{-1}h, \end{aligned}$$

and this is in N since $f(x)kf(x)^{-1}$ is a conjugate of k.

If G is abelian, then the order of the product of two subgroups of the abelian group $F(A, G)$ is less than or equal to the product of the orders. Hence, let $\mathfrak{a} \leqq \mathfrak{g}$, let G_1 be the subgroup consisting of the functions f^g, and let G_2 be the cyclic subgroup generated by any function f such that $f(a_1) \neq f(a_2)$ for all $a_1, a_2 \in A$. Then we may set $H = G_1 \cdot G_2$; the order of G_1 is $\mathfrak{g}$, and the order of G_2 is not greater than $\mathfrak{g}$, since $g_i^{\mathfrak{g}} = e$ for all $g_i \in G$. Thus the order of H is not greater than $\mathfrak{g}^2$, whereas the order of $F(A, G)$ is $\mathfrak{g}^{\mathfrak{a}}$, $\mathfrak{a} \geqq 3$. If $\mathfrak{a} > \mathfrak{g}$, $A' \subset A$ is of order $\mathfrak{g} \geqq 3$, and $H' \subset F(A', G)$ is a proper subgroup satisfying conditions (a) and (b) of the theorem, then the set H of functions whose restrictions to A' are in H' also satisfies conditions (a) and (b) and is also a proper subgroup. This completes the proof of the theorem.

If we set $A = G$, we obtain that the constant functions and the identity inner automorphism (which certainly satisfies condition (b) of the theorem) of a simple non-abelian group generate the entire group of functions from G into G. This generalizes Fröhlich's theorem mentioned above; in fact, from this, Fröhlich's theorem follows immediately. The collection G_K of constant functions on G normalizes the group G_I of pointwise products of inner automorphisms of G. If G_1 is the set of all functions on G fixing the identity, then $G_I = G_1$ if and only if the group generated by G_I and G_K is $F(G, G)$. Thus, if G is simple non-abelian, $G_I = G_1$.

If we set $A = G^n$, the direct product of G taken with itself n times, we obtain a result useful in the algebraic theory of machines. Let X_n be a set of n elements, and let $a_1, \cdots, a_k$ be elements of $G \cup X_n$ (disjoint union) for some finite group G. Then the *product function of n variables* mapping from G^n into G associated with $(a_1, \cdots, a_k)$ is defined as follows. If $X_n = [x_1, \cdots, x_n]$, then $f(g_1, \cdots, g_n) = b_1 \cdots b_k$, where

$$b_i = a_i \quad \text{for } a_i \in G,$$

$$b_i = g_j \quad \text{for } a_i = x_j \in X_n.$$

Thus we may associate a product function $f: G^n \to G$ with each sequence of elements of $G \cup X_n$. This correspondence is a homomorphism of the free semigroup of finite sequences of elements of $G \cup X_n$ into the group of functions from G^n into G under pointwise multiplication. Its image, as a subsemigroup of a finite group, is itself a group $F_n(G)$. Now the following result holds.

COROLLARY. *Every function $f: G^n \to G$, $n \geqq 1$, belongs to $F_n(G)$ if and only if G is a simple non-abelian group (or $G = [e]$).*

PROOF. For $G = [e]$ the theorem is obvious. It is easy to verify that $F_1(G)$ is generated by the inner automorphisms and the constant functions. Thus if $F_1(G)$ consists of all functions we have seen that G_I, the group of pointwise products of inner automorphism, consists of all functions fixing the identity and thus G can possess no proper nontrivial subgroups. In this situation G is simple non-abelian or $G = Z_p$, the integers modulo the prime p. However, $F_n(Z_p)$ is seen to have order strictly less than the order of $F(Z_p^n, Z_p)$ for all $n \geqq 2$ by performing a trivial calculation.

Now let G be simple non-abelian. The constant functions belong to $F_n(G)$ since they correspond to the sequences (g_i) of length 1. If $(g_1, \cdots, g_n)$ and $(g_1', \cdots, g_n')$ are distinct elements of G^n, there exists an index i for which $g_i \neq g_i'$, and the product function corresponding to the sequence (x_i) of length 1 satisfies condition (b) for this pair of elements of G^n. The corollary now follows immediately from the theorem.

BIBLIOGRAPHY

1. A. Fröhlich, *The near-ring generated by the inner automorphisms of a finite simple group*, J. London Math. Soc. **33** (1958), 95–107.

UNIVERSITY OF CALIFORNIA, BERKELEY