2-1995

An Elementary Proof that Finite Groups Lack Unique Product Structures

Matthew Cushman
Rose-Hulman Institute of Technology

MSTR 95-02

AN ELEMENTARY PROOF THAT FINITE GROUPS LACK UNIQUE PRODUCT STRUCTURES

Matthew Cushman

MS TR 95-02

February 1995

Department of Mathematics
Rose-Hulman Institute of Technology
Terre Haute, IN 47803

FAX(812) 877-3198 Phone: (812) 877-8391

An Elementary Proof that Finite Groups Lack Unique Product Structures

Matthew Cushman

February 20, 1995

Abstract

A group G is said to have a unique m-element product structure if there is a subset S of G such that the product map $\phi : S^m \to G$ is a bijection. In [1], it is proved using character theory that no nontrivial finite group has a unique m-element product structure for $m \geq 2$. We provide an elementary proof of this fact.

DEFINITION. Let m be a positive integer. We say that a group G has a *unique m-element product structure* if there is a subset S of G such that the product map $\phi : S^m \to G$ defined by $\phi(a_1, a_2, \ldots, a_m) = a_1 a_2 \ldots a_m$ is a bijection.

THEOREM. If G is a nontrivial finite group and $m \geq 2$, then G does not have a unique m-element product structure.

PROOF. Suppose we have $S \subset G$ for which the above ϕ is a bijection. Clearly $|G| = |S|^m$. Let $p > m$ be a prime and let

$$X = \{(a_1, \ldots, a_p) \in S^p \mid a_1 a_2 \cdots a_p = e\}$$

For each $(a_1, \ldots, a_{p-m}) \in S^{p-m}$ there is a unique $(a_{p-m+1}, \ldots, a_p) \in S^m$ such that $(a_1, \ldots, a_p) \in X$. Therefore, $|X| = |S|^{p-m}$.

Notice that if $(a_1, a_2, \ldots, a_p) \in X$, then $(a_p, a_1, \ldots, a_{p-1}) \in X$. Thus $\langle g \rangle$, the cyclic group of order p, acts on X by $g(a_1, \ldots, a_p) = (a_p, a_1, \ldots, a_{p-1})$. The size of each orbit divides p, and thus each orbit is either a singleton or has cardinality p. We now consider two cases:

Case 1. There is an orbit with one element, say $(a_1, \ldots, a_p)$. Clearly, all of the a_i are equal, so $a_1^p = e$. Since $e \notin S$, $a_1 \neq e$. Thus, a_1 is an element of order p, so $p \mid |G|$.

Case 2. Every orbit has p elements. Then $p \mid |S|^{p-m}$, so $p \mid |S|$. Consequently, $p \mid |G|$.

In either case, $p \mid |G|$. Since this holds for infinitely many p, we have a contradiction.

The author would like to acknowledge useful conversations with Gary Sherman of Rose-Hulman Institute of Technology and Phil Bradley of Rice University.

References

[1] D. Dimovski, Groups with Unique Product Structures, *Journal of Algebra* **146** (1992), 205-209.

Address of author

Department of Mathematics
Carnegie Mellon University
Pittsburgh PA 15213-3890