Canad. Math. Bull. Vol. **14** (1), 1971

QUASIGROUPS ORTHOGONAL TO A GIVEN ABELIAN GROUP

BY

CHARLES C. LINDNER

In this note we prove the following theorem, which does not seem to appear explicitly in the literature.

THEOREM. *Let A be a finite abelian group and p the smallest prime which divides $|A|$. Then there are $p-1$ mutually orthogonal quasigroups of order $|A|$, one of which is A.*

Proof. If $p=2$ there is nothing to prove. So we consider the case where $p\geq 3$. Let $i\in\{1,2,\ldots,p-1\}$. Then the mapping $\alpha_i: A\to A$ given by $a\alpha_i=a^i$ is an automorphism of A so that each element of A has a unique ith root.

We define groupoids $(A_1, o_1), (A_2, o_2),\ldots,(A_{p-1}, o_{p-1})$ as follows. $A=A_1=A_2=\cdots=A_{p-1}$, o_1 is the operation in A, which we will denote by juxtaposition, and $xo_iy=x^iy$.

Each (A_i, o_i) is a quasigroup. For if $xo_iy=xo_iz$, then $x^iy=x^iz$ gives $y=z$, and if $yo_ix=zo_ix$, then $y^ix=z^ix$ gives $y^i=z^i$ which implies $y=z$, since each element in A has a unique ith root.

The quasigroups $(A_1, o_1),\ldots,(A_{p-1}, o_{p-1})$ are mutually orthogonal. To see this let $x, y, z, w\in A$ with $x\neq z$ and $y\neq w$, and suppose that $xo_iy=zo_iw$ and $xo_jy=zo_jw$. We can assume $i<j$, so that $1\leq j-i\leq p-1$. But then $xo_jy=zo_jw$ gives $x^jy=z^jw$ gives $x^{j-i}(x^iy)=z^{j-i}(z^iw)$. Since $xo_iy=zo_iw$ we have $x^{j-i}=z^{j-i}$—a contradiction since each element of A has a unique $j-i$ root. This contradiction completes the proof of the theorem.

Added in proof. The referee has pointed out to the author the availability of the ideas developed in [1] to produce a proof of the theorem in this note. In particular, in terms of the concepts in [1] we have shown that if A is a finite abelian group and p is the smallest prime divisor of $|A|$, then the set of mappings $\alpha_1, \alpha_2,\ldots,\alpha_{p-1}$ is a set of mutually orthogonal orthomorphisms.

REFERENCE

1. D. M. Johnson, A. L. Dulmage and N. S. Mendelsohn, *Orthomorphisms of groups and orthogonal latin squares. I.* Canad. J. Math. **13** (1961), 356–372.

AUBURN UNIVERSITY,
AUBURN, ALABAMA