SUB-QUASIGROUPS OF FINITE QUASIGROUPS

DRURY W. WALL

1. Introduction. Lagrange's theorem for finite groups (that the order of a sub-group divides the order of the group) does not hold for finite quasigroups in general. However, certain relationships can be obtained between the order of the quasigroup and the orders of its sub-quasigroups. This note will give some of these relationships.

DEFINITION. A set of elements Q and a binary operation "$\circ$" form a *quasigroup* $(Q, \circ)$ if and only if the following are satisfied:

I. If $a, b \in Q$ then there exists a unique $c \in Q$ such that $a \circ b = c$.

II. If $a, b \in Q$ then there exist $x, y \in Q$ such that $a \circ x = b$ and $y \circ a = b$.

III. If $a, x, y \in Q$ then either $a \circ x = a \circ y$ or $x \circ a = y \circ a$ implies $x = y$.

If $(Q, \circ)$ is a quasigroup and S is a subset of Q then $(S, \circ)$ is a sub-quasigroup of $(Q, \circ)$ if $(S, \circ)$ is a quasigroup.

Throughout this note the quasigroup operation will be written multiplicatively, that is, "ab" will be written for "$a \circ b$". Also, "Q" will be written to denote the quasigroup "$(Q, \circ)$". By quasigroup will be meant finite quasigroup, since only finite quasigroups will be considered. The order of a finite set X is the number of elements in X. For subsets X and Y of Q the symbols $X \cap Y$, $X \cup Y$ and $X \setminus Y$ will be used to denote the point set intersection, union and relative complement of X with Y, respectively.

The following elementary properties of a finite quasigroup Q will be of use.

P1. *If $X \subset Q$ and $a \in Q$ then X, aX and Xa have the same order.*

P2. *If $S \subset Q$ and S satisfies I then S is a sub-quasigroup of Q.*

Proof. To prove II, let $a, b \in S$. Since S satisfies I, $aS \subset S$ and by P1, $aS = S$. Thus, since $b \in S$ there exists an $x \in S$ such that $ax = b$. III is inherited from Q.

P3. *If S is a sub-quasigroup of Q then $a \in S$ and $b \notin S$ imply $ab \notin S$.*

2. Relationship of the order of any sub-quasigroup to the order of the quasigroup. The order of a sub-quasigroup need not divide the order of the quasigroup; in fact, these orders may be relatively prime. An example is given by Garrison [1, page 476] of a quasigroup of order 5 with a sub-quasigroup of order 2.

Received February 27, 1957, and in revised from June 15, 1957. Presented to the American Mathematical Society, August, 21, 1956.