Groups which are not (right) multiplication groups of loops

Gábor P. Nagy (University of Szeged, Hungary)

Let G be a permutation group acting transitively on the finite set Q. We are interested in the following questions:

Question 1: Is there a loop operation on Q such that the multiplication group is contained in G?

Question 2: Is there a loop operation on Q such that the right multiplication group is contained in G?

Questions 1' and 2': What about equality?

Concerning Question 1, there are negative results by Vesanen and Drápal on classical linear groups. Moreover, Drápal asked in 2001 if in dimension $k \geq 3$, any group G with $PSL(k,q) \leq G \leq P\Gamma L(k,q)$ can be realized as multiplication group of a loop. We show that the answer is yes for all $k \geq 3$ and prime power q. The constructions come from finite geometry: we use the multiplicative loops of finite nearfields modulo their centers.

Beside these results, very little is known. In particular, there are no theoretical methods which could exclude large families of groups. We present a computer program which can deal with groups where $|Q|$ is small and for which a small integer d exists such that the stabilizer of d elements in G is small. For example, the Mathieu group M_{22} of degree 22 can be handled.

Question 2 is usually formulated in the language of sharply transitive sets. The subset S of G is said to be sharply transitive if for any $x, y \in Q$, there is an element $s \in S$ such that s maps x to y. Clearly, the set of right multiplication maps of a quasigroup (loop) is a sharply transitive set (with $1 \in S$). Here, computers can be used for groups of order < 5000. The presently known theoretical tools for showing that a finite permutation group G does not contain a sharply transitive set are following: Lorimer's enumeration method, O'Nan's contradicting subgroup method, and character theoretical methods by Grundhöfer and P. Müller. We will try to give an idea of the latter and show some examples which are still open.

Both questions are even harder if there is a loop whose (right) multiplication group is properly contained in the group G and one wants to show that there is no loop with (right) multiplication group G. The situation gets better if G has not many transitive subgroup. For example, this is the case when G consists of semilinear transformations of a vector space.