Braces over a field and regular subgroups of the affine group

Francesco Catino, Università del Salento, Italy

The problem of determining all regular subgroups of an affine group has been raised explicitly by Liebeck, Praeger and Saxl in [4] and it is still open. Among the results in this area, Rizzo and I [2] establish a link between regular subgroups of an affine group and braces over a field: a vector space \( V \) over a field \( F \) with an operation \( \circ \) is called a brace over \( F \) or \( F \)-brace if the structure \((V, +, \circ)\) is a brace and \( \mu(a \circ b) = a \circ (\mu b) + (\mu - 1)b \), for all \( a, b \in V \) and \( \mu \in F \). Fixed a vector space \( V \), there exists a bijective correspondence between the class of all \( F \)-braces on the underlying vector space \( V \) and regular subgroups of the affine group \( \text{AGL}(V) \). This result extends a previous description of all abelian regular subgroups of an affine group in terms of commutative associative radical algebras obtained by Caranti, Dalla Volta and Sala in [3]. Besides the theoretical appeal of this subject, the interest in the topic is nowadays strongly motivated by applications to Cryptography, where such objects are used to insert and detect algebraic trapdoors in block ciphers, as discussed in [1].

In the talk I will introduce the relationship between regular subgroups of an affine group and \( F \)-braces, to then move to detail the most recent constructions of the latter ones. Throughout the talk, I will also introduce and review selected open problems and challenges in the field.

References