SFB QMC

UNIVERSITÄT SALZBURG

Fachbereich Mathematik
Hellbrunnerstraße 34
5020 Salzburg

Gastvortrag

Montag, 20. Juni 2016
13.00 Uhr c.t.
Seminarraum II

Prof. Michel Lavrauw
University of Padova

Finite semifields, finite geometry and applications

Abstract:
The theory of finite semifields has received a lot of attention in recent years. The concept of a semifield was first studied by L. E. Dickson in 1905 (1). His motivation was purely algebraic: what happens if one omits the axiom of associativity for multiplication in the definition of a finite (skew)field? This question arose naturally after it had been shown that the axiom of commutativity for multiplication is redundant in the axiomatic definition of a finite field (the Wedderburn Theorem or Dickson-Wedderburn Theorem).

Nowadays these (non-associative) algebraic structures are called *semifields*, a notion introduced by Knuth (2).They turn up in various areas of mathematics related to finite fields, and play a key role in finite geometry (Galois geometry).

We will introduce the main concepts and explain recent developments in the theory of finite semifields, and will conclude with applications to cryptography and coding theory. We will follow the notation and terminology from (3).

(1) L. E. Dickson: Linear algebras in which division is always uniquely possible. *Trans. Amer. Math.Soc*, 7(3), 370--390, 1906.
(2) D. E. Knuth. Finite semifields and projective planes. *J. Algebra*, 2, 182--217, 1965.
(3) M. Lavrauw, O. Polverino: *Finite semifields*, Chapter 6 in Current research topics in Galois Geometry (J. De Beule and L. Storme, Eds.), NOVAAcademic Publishers, Pub. Date 2011

Einladender: Peter Hellekalek