Algebra and Number Theory Seminar

Title: Finite congruence-simple semirings and their application to public-key cryptography

Speaker: Jens Zumbraegel (UCD/CSI)

Date: Mon 2nd February 2009 at 4:00PM

Location: Mathematical Sciences Seminar Room

Abstract: A set with two binary operations (R,+,*) is called a semiring if (R,+) is a commutative semigroup, (R,*) is a semigroup, and both distributive laws hold. We assume that R has always a zero-element which is neutral in (R,+) and absorbing in (R,*). Semirings arise in numerous occasions, the natural numbers (N=0,1,2,dots,+,*) probably being the most well-known example. The structure of a semiring is in a sense the most general over which matrix operations can be defined. Problems from graph theory like shortest path have concise descriptions using certain semirings.

Finite semirings can be applied in public-key cryptography to construct semigroup actions that may serve as a basis for generalised Diffie-Hellman and ElGamal cryptosystems. For cryptographic purposes it is important that the semiring in use is congruence-simple, meaning that it cannot be homomorphically mapped onto a smaller semiring. This leads to the question whether useful congruence-simple semirings exist.

In the talk a full classification of finite congruence-simple semirings will be presented

and the proof will be sketched. The result generalises the classical Wedderburn-Artin theorem on the classification of finite simple rings. A substantial notion in the proof is that of (strongly) irreducible semimodules over semirings. Key results are that 1) any finite congruence-simple semiring R admits an irreducible semimodule M, and 2) a density result stating that R is then a "dense" subsemiring of the endomorphism semiring End(M) of the commutative monoid (M,+).