



UNIVERSITÄT DES SAARLANDES
Fachrichtung 6.1 Mathematik
Prof. Dr. R. Schulze-Pillot

Universität des Saarlandes, E2 4, Zi. 318 - email: schulzep@math.uni-sb.de

In the summer semester 2011 I will give a course with the title

Integral Quadratic Forms and Euclidean Lattices.

The course has been announced with two weekly hours (3 credit points) (Mo 10-12 Hs. 4, E2 4), I am considering to upgrade it to 4 weekly hours (6 credit points) and possibly to include problem sessions (3 credit points), this will depend on participants. Also depending on participants the course language will be english or german.

People interested in this course should contact me asap to facilitate planning.

The lecture course is concerned with a number theoretic subject with close links to coding theory, geometry (in particular sphere packing) and with applications in cryptography. In view of these links the course can be of interest to students of Informatik.

Euclidean lattices are \mathbb{Z} -lattices L in euclidean space \mathbb{R}^n equipped with the standard scalar product, in the simplest case $L = \mathbb{Z}^n$ one obtains the quadratic form $Q(x_1, \dots, x_n) = \sum_{j=1}^n x_j^2$. For more general L one looks for short vectors and for lattice bases consisting of short vectors, this leads to reduction theory, LLL-algorithm and related complexity problems. More general one admits other, not necessarily positive definite symmetric bilinear forms on \mathbb{R}^n . In all cases one studies classification problems, automorphism groups and solution numbers of equations $Q(\mathbf{x}) = t$ in the lattice L .

Prerequisites are linear algebra and some familiarity with the basic concepts of elementary number theory.

Literature: (Further literatur will be discussed in the first lecture)

- J. Conway, N.J.A. Sloane: Sphere Packings, Lattices and Groups
- J. Martinet: Perfect Lattices in Euclidean Spaces
- J. W. S. Cassels: Rational Quadratic Forms