Graduate Seminar on Topics in Algebra & Computation

Prof. Dr. Nitin Saxena

Sommersemester 2010: From Monday, 19th April 2010.
Monday 1200-1400, LWK 0.008, Endenicher Allee 60.
Friday 1400-1600, LWK 0.008.

Background:
Students who are aware of the basics of computation and basic algebra will find the seminar especially interesting.

Outline:
This seminar will study some advanced topics in computational algebra. The highlights of the course are *Gröbner basis*, *Algebraic-P/NP question* and *Elliptic curves.*

The students will be expected to present at least two lectures during the semester. Some topics to choose from are given below (see Reference). To send your choices or to ask for more details contact `ns@hcm.uni-bonn.de`

- Black-box Factoring of multivariate polynomials.
- Gröbner basis and the Ideal Membership problem.
- Hilbert's Nullstellensatz and Quantifier Elimination.
- Algebraic settings for the P=NP question.
- Three algebraic lower bounds: Strassen's, Ben-Or's & Mulmuley's.
- Elliptic Curves - Divisors & Lines.
- - Group Laws, Torsion points & Derivation.
- - Division Polynomials, Ramification & Endomorphisms.
- - Weil Pairing, Hasse's Theorem & Schoof's Algorithm.

Reference - 1) "Algebra and Computation", Madhu Sudan. Lecture notes at `http://people.csail.mit.edu/madhu/teaching.html`

2) "An Elementary Introduction to Elliptic Curves", L. S. Charlap & D. P. Robbins. Report available at `http://www.idaccr.org/reports/reports.html`