Proposal for a special topics course on Computational Methods in Algebra, by K. Lux, Fall 2017.

Prerequisites: an acquaintance with basic algebraic structures as covered in the core course MATH 511A/B.

Goal of the course: an introduction to the standard algorithms in algebraic number theory, group theory, and commutative ring theory. Computational approaches in algebra are essential both in pure mathematics and real world applications for example:

1) the Cohen-Lenstra prediction for the distribution of class groups of number fields and its refinements,

3) the construction of sporadic simple groups,

4) cryptography based on non-commutative groups,

5) algebraic cryptanalysis,

6) the decoding of linear codes.

Method: We will try to emphasize practical experience with the algorithms discussed in class. In particular, we will study the use of various computer algebra systems. Moreover, there will be ample opportunity to experiment with our own implementations of some of the algorithms discussed in class.

Outline of the syllabus: We plan to start with a survey of the algorithms in Linear Algebra as covered in Chapter 2 of H.Cohen, "A Course in Computational Algebraic Number Theory", Graduate Text in Mathematics,138, Springer, see `https://link.springer.com/chapter/10.1007/978-3-662-02945-9_2`.

We will then continue by covering more advanced algorithms in

1. algebraic number theory again following H. Cohen's book,
2. commutative algebra, Groebner bases and the Buchberger algorithm,
3. group theory, the Schreier-Sims algorithm, the Todd-Coxeter algorithm, the MeatAxe.

As an integral part of the course we are going to make use of various computer algebra systems such as

a) GAP, see `https://www.gap-system.org/`, and MAGMA, see `http://magma.maths.usyd.edu.au/magma/`. Both cover very nicely algorithms in group theory. MAGMA is also a very powerful tool for doing computations in commutative algebra and algebraic number theory.

b) SINGULAR, see `https://www.singular.uni-kl.de/`, which offers implementations of the standard algorithms (and more) in commutative algebra and algebraic geometry.