Special topics course Algebra Fall 2025: Computational Methods in Algebraic Number theory, Algebraic Geometry, and Group Theory with Applications in Cryptography, MATH 518, Lux

Prerequisites: Algebra, MATH 511A/B.

The aim of this course is to give a survey of the algorithms and computational methods in Algebraic Number Theory, Algebraic Geometry, and Group theory. An essential part of the course will be the application of the methods as implemented in the state of the art computer algebra systems such as MAGMA and OSCAR.

Parts of the content of this course can be seen as a preparation for the upcoming Arizona Winter school 2026, which will be dedicated to computational aspects of arithmetic geometry and cryptography.

Following Cohen's book, we will start with a review of fundamental algorithms for finitely generated abelian groups, a highlight being the the famous LLL (Lenstra, Lenstra, Lovasz) algorithm for finding short vectors in a Euclidian lattice. The LLL algorithm is of fundamental importance for the analysis of (post quantum) cryptosystems based on lattices! We will then move on to study algorithmic aspects in algebraic number fields culminating in the discussion of algorithms determining the ideal class group and the group of units in the ring of algebraic integers of an algebraic number field.

In the second part we will analyze the fundamental notion of a Gröbner basis of an ideal in a multivariate polynomial ring and describe the Buchberger algorithm for computing a Gröbner basis. This will be followed by applications of Gröbner bases to problems in commutative algebra, and algebraic geometry, such as solving multivariate polynomial equations and a discussion of elliptic curve cryptography.

In the last part of the course, we will give an overview of the basic algorithms that allow one to analyze a group given either as a permutation group, by a presentation with generators and relations or as a matrix group over a finite field under the aspect of cryptography. We will have a look at a famous computational problem that arises in quantum computing called the hidden subgroup problem.

All three parts will involve hands-on computations using the computer algebra systems MAGMA and OSCAR.

Learning outcome:

Students should be able to solve problems in algebraic number theory, algebraic geometry and group theory using the computer algebra systems MAGMA and OSCAR, both interactively and in the form of scripts written in the MAGMA and OSCAR language. Students should also be aware of the underlying algorithms, their performance and limitations, since this is vital for cryptographic purposes. In addition, they will learn how to use the existing large data bases in MAGMA and OSCAR for their own research problems in the area of Number theory, Algebraic Geometry, and Group theory.

Approximate schedule:

1) Week 1 -6: Algorithms for finitely generated abelian groups, Chapter 2 in Cohen's book, and units and ideal classes, Chapter 4 in Cohen's book.
2) Week 7 - 12: Basic Theory of Gröbner Bases, Chapter 1 in Adams and Loustaunau's book and applications of Gröbner bases, Chapter 2 in Adams and Loustaunau's book.

3) Week 13: Algorithms for permutation groups: the Schreier-Sims method for determining the order of a permutation group.
4) Week 14: Algorithms for finitely presented groups: the Todd-Coxeter coset enumeration.
5) Week 15: Algorithms for matrix groups: The MeatAxe.

Literature:

1) Cohen, A Course In Computational Algebraic Number Theory. Graduate Texts in Mathematics. Vol. 138. Springer-Verlag, 1993.
2) Adams and Loustaunau, An Introduction to Gröbner Bases, AMS, Graduate Studies in Mathematics, Volume: 3, AMS, 1994.
3) Holt, Eick, O'Brien, Handbook of Computational Group Theory, CRC Press, 2005.

Software used:

1) W. Bosma, J. J. Cannon, C. Fieker, A. Steel (eds.), Handbook of Magma functions, Edition 2.16 (2010), 5017 pages.
2) Decker, Eder, Fieker, The Computer Algebra System OSCAR: Algorithms and Examples, Algorithms and Computation in Mathematics 32, Springer-Verlag, 2024
3) OSCAR – Open Source Computer Algebra Research system, Version 1.3.0-DEV, The OSCAR Team, 2025.