Algebra & Discrete Mathematics Courses Spring 2023

Period III

Advanced Topics in Cryptography — 5cr
MS-E1687 — Russell Lai

This is an introductory course on lattice-based cryptography intended for advance undergraduates and graduate students. We will begin with a general overview of lattice-based cryptography and introducing the short integer solution (SIS) problem and the learning with errors (LWE) problem. We then briefly study the connections of these problems with conjectured hard problems over lattices as well as attack strategies. The main focus of the course will be on building various cryptographic primitives based on the hardness of the SIS and LWE problems and their variants.

There are **no mandatory prerequisites** for this course. Assume familiarity with basic security notions, e.g. one-wayness, pseudorandomness, IND-CPA-security, and the concept of security reduction, taught in CS-E4340 Cryptography. This knowledge can also be acquired in self-study. We will also assume basic understanding of matrices and modular arithmetic.

Geometry of Numbers (Periods II–III) — 5cr
MS-EV0006 — Tapani Matala-Aho

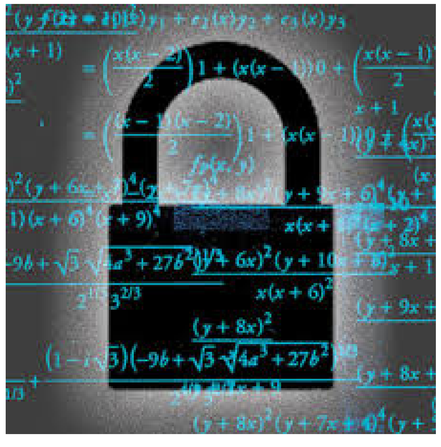
Geometry of Numbers studies number theoretic problems by the use of geometric methods. The main theory was formulated by H. Minkowski in 1896. We will study e.g. lattices, convex bodies, linear transformations, Blichfeldt's theorem, Minkowski's convex body theorems, linear forms and their approximations, and Dirichlet's theorems. It is still possible to join the course on Period III.

Prerequisites: Linear Algebra.

Algebraic Methods in Data Science — 5cr
MS-E1622 — Kaie Kubjas

In this course, one learns the main algebraic methods used in data science. Examples of such methods are matrix and tensor decompositions, topological data analysis, graphical models and numerical algebraic geometry. At the end of the course, the student can apply these methods and recognize problems in data science that can be solved using algebraic methods.

Prerequisites: First Course in Probability and Statistics, Linear Algebra.



Period IV

Commutative Algebra — 5cr
MS-EV0013 — Milo Orlich

Commutative algebra is the study of commutative rings and modules over them, which is a more general story than that of vector spaces over a field. Commutative algebra is in particular a fundamental tool in algebraic geometry and algebraic number theory. This course will cover in particular classical cornerstone results by Hilbert and Noether, and interactions of commutative algebra with geometry and combinatorics.

Prerequisites: Abstract Algebra

Galois Theory — 5cr
MS-E1111 — Camilla Hollanti

Galois theory provides a beautiful connection between groups and fields. We will (mainly) work with number fields, i.e., subfields of the complex numbers. We construct field extensions by polynomials, and study the related relative structures both from a group theoretic viewpoint and from the viewpoint of field extensions.

We prove a one-to-one correspondence between the so-called Galois groups and field extensions, which allows us to prove that polynomial equations of degree 5 or higher don't have general solution formulas.

Prerequisites: Abstract Algebra

Period V

Algebraic Number Theory — 5cr
MS-E1998 — Iván Blanco Chacón

The main goal of this course is to understand Kummer's proof of Fermat's Last Theorem (in the so-called regular case). In this course you will acquire the basics of this discipline: rings of integers, norms, traces and discriminants, factorisation in Dedekind domains, ramification and inertia, units and cyclotomic fields.

Prerequisites: Linear Algebra, Abstract Algebra, Galois Theory. Useful but not mandatory: Number Theory

Real Algebraic Geometry — 5cr
MS-EV0014 — Tobias Boege

This course deals with the solution sets of polynomial equations and inequalities over the real numbers. These are important geometric spaces which appear in statistics, optimization and various applications. We begin with ordered and real-closed fields, ideals and cones in their polynomial rings and finally prove two of the gems of the theory: the Tarski–Seidenberg theorem and the Positivstellensatz. We will explore computational aspects of this theory in the exercises.

Prerequisites: Participants should have encountered ideals in polynomial rings, for example in Abstract Algebra or (Computational) Algebraic geometry.

Summer

Elliptic Curve Cryptography — 5cr
MS-EV0012 — Iván Blanco Chacón

The main focus of this course is to become familiar with the main ideas and operations with elliptic curves, with a focus over those defined over finite fields. We will study Weierstrass equations, the addition law, ordinary and supersingular curves. In the second part, we will study the Hasse bound, the Schoof's algorithm and the Elliptic Curve Discrete Logarithm Problem.

Prerequisites: Linear Algebra, Abstract Algebra. Useful but not mandatory: Number Theory, Algebraic Number Theory

Codes over Nonstandard Alphabets — 5cr
MS-EV0011 — Marcus Greferath

Coding Theory has originally evolved as a kind of finite-field combinatorial linear algebra with a number of metrical and probability related aspects. Later in the development, the role of the integers modulo 4 was discovered, and hence, coding theory expanded its alphabet concept to rings and modules.

A further expansion of the alphabet notion is suggested by the integration of Group Testing into this framework: in fact, considering traditional Group Testing as coding theory over the binary semi-field, the most general is based on the idea of an alphabet carrying the structure of a semi-ring. This lecture series will address a selection of highlights of this development.

Prerequisites: Linear Algebra, Abstract Algebra