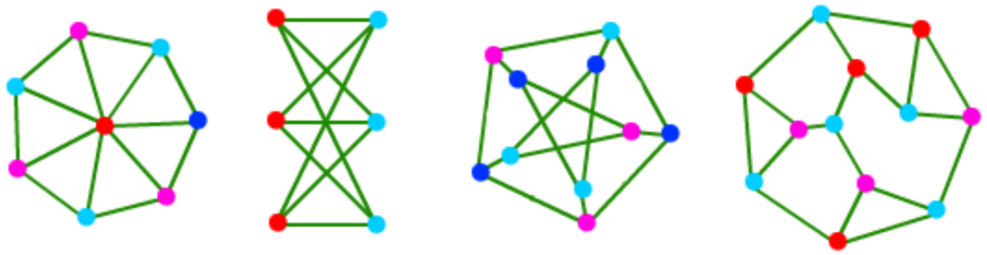
Courses in Algebra and Discrete Mathematics, Aalto University, Fall 2017 & Spring 2018

Bachelor students with a high level of mathematical maturity may well benefit from courses at the MSc level (MS-Exxxx), and advanced students are also welcome to take courses at the BSc level (MS-A/Cxxxx). N = period N.

I I IV MS-A040X: Grundkurs i diskret matematik (Swedish) / 5cr / Diskreetin matematiikan perusteet (Finnish)

Björn Ivarsson
Riikka Kangaslampi

Discrete mathematics refers to the mathematics of finite and enumerably-infinite sets. Its methods are widely used in other disciplines, especially in computer science. This course introduces basic structures and methods of discrete mathematics that are useful in later studies of mathematics and computer science, as well as in everyday work of an engineer or scientist. Modern applications for example in data encryption and graph theory will also be discussed. The course is suitable for all bachelor students as the first course in discrete mathematics.



I MS-E1050: Graph theory, 5cr

Riikka Kangaslampi

Graph theory, as most parts of math, is learned and understood by solving problems and proving theorems. Even though some notation and definitions are necessary to start working, the focus of the course is on doing graph theory. The course starts with basic properties in graph theory, continues with some important theorems, especially those related to colourings and regularity, and ends with a glimpse into current research topics. It is aimed at master's and doctoral students, so mathematical maturity comparable to a bachelor in computer science, mathematics or operations research is expected.

II MS-E1110: Number theory, 5cr

Piermarco Milione

"*Mathematics is the queen of sciences and number theory is the queen of mathematics.*" (cit. Gauss) We will prove the *Quadratic Reciprocity Law*, stated and proved by Gauss, when he was 17 years old, and referred to by himself as the "Golden Theorem".

We will get into at least one valuable application: the *RSA public-key cryptographic system,* used in daily-life bank transactions, and based on a theorem of Euler from 1736.
We will understand why it is considered secure, and ask if this is really so...

III MS-E1996: Matroid theory, 5cr

Thomas Westerbäck

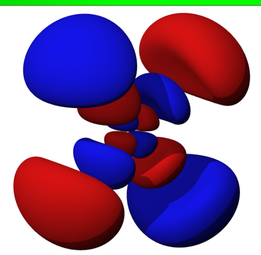
Matroid theory is a discrete theory that tries to capture the concept of independence. Two examples of matroids are a set of vectors in a vector space with the notion of linear independence, and the set of edges of a graph with the notion of cycle free. However, not all matroids come from vectors or graphs. Matroids play a significant role in many areas of research such as coding theory, graph theory, tropical geometry, optimization, topological and algebraic combinatorics. This course will cover the basics as well as some modern aspects and use of matroids.

III MS-E1997: Symmetries, 5cr

David Radnell

Symmetries, in a very general sense, are a central part of mathematics and is applications. For example, they appear in the geometry of everyday objects, in art and architecture, and in classical, quantum, and particle physics. Within mathematics they touch every area, from differential equations to number theory.

This course will introduce the abstract notions of *groups, Lie groups and Lie algebras* and focus on the study of their *representation theory.* Some applications will be discussed.



III MS-C1080: Introduction to abstract algebra, 5cr

Marcus Greferath

Abstract algebra describes numerous mathematical structures. For example the integers are a concrete realization of the abstract concept of a ring. These notions are useful in many branches of mathematics such as combinatorics, statistics, and geometry. They are important in many applications, including coding theory, cryptography, and physics. This course introduces groups, rings, ideals, integral domains and fields, and brief applications to digital communication. This course provides background for more advanced courses such as Galois Theory, Algebraic Geometry, and Algebraic Number Theory.

IV MS-E1111: Galois theory, 5cr

Oliver Gnilke

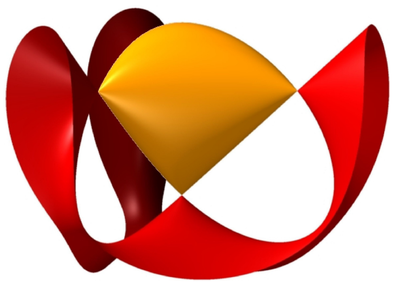
Although quite accessible, by studying polynomials and the structure of their roots, Galois theory is an interesting introduction to modern algebra.
This course introduces field extensions, their automorphisms and Galois groups. These are used to prove well-known theorems such as the non-existence of a closed formula for solutions to general polynomial equations of degree 5 or higher, or the impossibility of trisecting a general angle with ruler and compass. We will closely follow the book by Stewart on the topic.
The course MS-C1080 is a recommended prerequisite.

IV V MS-E1140 & 1141: Algebraic geometry I & II, 5cr & 5cr

Alexander Engström

MS-E1140: You will get a basic understanding of schemes.
The contents are a review of preliminaries in category theory and sheaf theory; definitions of affine, projective and general schemes; and basic properties of schemes.

The study material is Chapters 3-5 in "The Rising Sea: Foundations of Algebraic Geometry" by Vakil, with the necessary preliminaries of Chapters 1-2 to start off with. The prerequisites are some advanced algebra, geometry and topology. Mathematical maturity is much more important than specifics.
Prospective students are encouraged to take a glance at the study material.



MS-E1141: You will get a basic understanding of morphisms of schemes. The contents are the definition of morphisms of schemes and some useful classes; closed embeddings and related notions; fibered products of schemes and base change; separated and proper morphisms; and varieties. We use Chapters 6-10 in the same book. MS-E1140 is a prerequisite.

V MS-E1998: Algebraic number theory, 5cr

Laia Amorós

In 1839 Lamé claimed to have a proof of Fermat's Last Theorem (FLT), a famous conjecture from 1670. This proof revealed itself to be false, and the reason was that Lamé believed that certain rings of integers are unique factorization domains. A few weeks later, Kummer wrote a correct proof for a certain set of primes. FLT was finally proved in 1995 by A. Wiles. In this course we will build the necessary background to give Kummer's proof and understand why Lamé's proof was not correct. We will learn about number fields and their ring of integers, with special attention on quadratic number fields and cyclotomic fields.

Theses and special assignments

If you are interested in writing a thesis or a special assignment related to algebra or discrete mathematics, we have many interesting topics. Contact Alex Engström, Camilla Hollanti, Riikka Kangaslampi, Kalle Kytölä, any of the course instructors, or other members of the algebra and discrete mathematics group for further information. www.math.aalto.fi/en/research/discrete/