Algebra & Discrete Mathematics Courses 2018-2019

Period I

MS-A0401 Hakula
Diskreetin matematiikan perusteet 5cr

Diskreetillä matematiikalla tarkoitetaan äärellisiin ja numeroituvasti äärettömiin joukkoihin liittyvää matematiikkaa. Sen menetelmät ovat laajassa käytössä myös muilla tieteenaloilla, erityisesti tietojenkäsittelytieteissä.

Diskreetin matematiikan perusteet -kurssilla käydään läpi diskreetin matematiikan ja samalla koko yliopistomatematiikan perusrakenteita ja -menetelmiä kuten joukko-oppia, logiikkaa, kombinatoriikkaa ja lukuteoriaa. Lisäksi tutustutaan moderneihin sovelluksiin esimerkiksi tiedonsalaukseen ja verkkoteoriaan liittyen.

Kurssi sopii kaikille Aalto-yliopiston kandidaattiopiskelijoille, esitiedoiksi riittää lukion matematiikka.

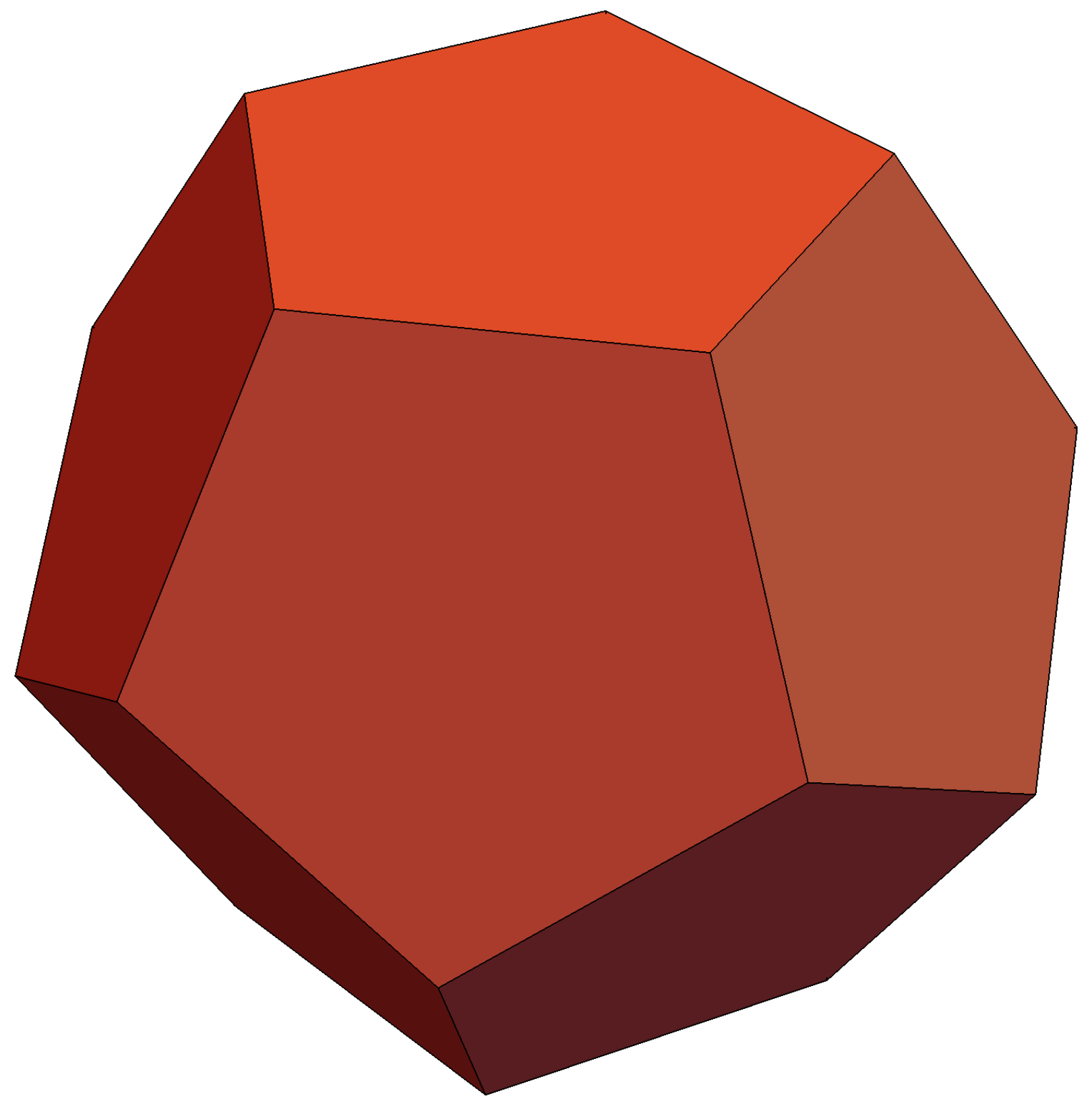
MS-E1050 Kohl
Graph Theory 5cr

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 and useful theorems, especially those related to colourings and regularity, and ends with a glimpse into current research topics.

The course is aimed at master's and doctoral students, so mathematical maturity comparable to a bachelor in computer science, mathematics or operational research is expected.

CS-E4320 Brzuska
Cryptography and Data Security 5cr

What does it mean for an encryption scheme to be secure? Can we prove that an encryption scheme is secure? In this course, we develop meaningful formal definitions of security for cryptographic primitives and learn that the existence of secure cryptography hinges on the P vs. NP question. We then show how to prove that the security of "simple" cryptography implies the security of complex crytography such as the TLS protocol, the security protocol underlying https and the main building block for secure communication on the internet. A background in computability and complexity theory is assumed.



Period II

MS-A0409 Metsalo
Grundkurs i diskret matematik 5cr

Efter kursen skall studenten:
-förstå matematiska bevis och behovet av dem
-känna till elementär mängdlära samt grundläggande egenskaper hos funktioner och relationer
-kunna använda centrala matematiska beteckningar
-behärska elementär kombinatorik, egenskaper hos heltalen samt moduläraritmetik
-kunna manipulera permutationsgrupper
-förstå vad som menas med algoritmhastighet
-behärska grunderna i grafteori.

MS-E1110 Hollanti
Number Theory 5cr

"Mathematics is the queen of sciences and number theory is the queen of mathematics." (cit. Gauss) We will prove the quadratic reprocity law, stated and proved by Gauss, when he was 17 years old, and refered to by himself as the golden theorem, and by others as one of the most beautiful theorems in all of mathematics.

We will get into at least one valuable application: the RSA public-key cryptosystem, used in, *e.g.*, 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 really is so...

MS-E1996 Gnilke
Coding Theory 5cr

Coding theory is the application of mathematics to problems in data transmission and storage. An error-correcting code enables the receiver of a faulty message to recover the original content.

We will cover the basics of linear error-correcting codes for the Hamming metric and prove bounds on their parameters. We will introduce several classical constructions of codes and shortly discuss decoding strategies. Furthermore we will introduce new avenues of coding theory, such as distributed storage, code-based cryptography, and network coding. A solid background in linear algebra and an interest in discrete mathematics are sufficient to follow the course.

Period III

MS-C1081 Greferath
Abstract Algebra 5cr

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 briefly applications to digital communications. This course provides background for more advanced courses such as Galois Theory, Algebraic Geometry, and Algebraic Number Theory.

Foundations of Discrete Mathematics or similar knowledge is recommended as a prerequisite.

MS-E1687 Brzuska
Advanced Topics in Cryptography 5cr

In this course, we learn how to argue rigorously about the security of complex systems. We will learn to model the security of complex systems and then show that, based on certain assumptions, a cryptographic construction is secure in the model. We study different proof methodologies such as (hand-written) reduction proofs as well as computer-assisted and/or computer-verified proofs. We also see how security is assessed in the absence of rigorous arguments. Topics include (but are not restricted to) secure messaging, white-box cryptography and obfuscation. Basic knowledge in cryptography (such as CS-E4320 Cryptography and Data Security) is assumed.

Period IV

MS-A0402 Greferath
Foundations of Discrete Mathematics 5cr

Discrete mathematics considers finite and countably infinite sets. Its methods are widely used in other disciplines, especially in computer science.

Foundations of discrete mathematics course provides the students with a multitude of basic techniques and theorems that are useful throughout later studies. It will cover topics in set theory, logics, combinatorics, and number theory. Also permutation groups and basics of graph theory will be introduced, as well a some more modern applications of discrete mathematics.

The course is suitable for all bachelor students, no specific background beyond high-school mathematics is required.

Period V

MS-E1995 Hollanti
Applications of Coding Theory in Security 5cr

The course consists of three main parts: 1) Study of algebraic lattices and their applications to physical layer security, referring to a scenario where the eavesdropper is allowed to have infinite computational power and the security lies on the randomness of the communication medium. 2) Study of storage codes used in distributed storage systems (e.g., Google, Facebook, various peer-to-peer networks) with emphasis on securing the stored files and guaranteeing privacy for a user retrieving files. 3) Students' own small projects on selected topics. The students should have taken Linear Algebra and Abstract Algebra (or similar courses), Galois Theory and especially Coding Theory are recommended but not necessary.

Thesis Topics and Projects

If you are interested in writing a thesis or special assignment related to algebra or discrete mathematics, we have many interesting topics. Contact Chris Brzuska, Alex Engström, Camilla Hollanti, Kaie Kubjas, 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/`