2EL1740 – Algebra and cryptology

Instructors: Remi Geraud
Department: DÉPARTEMENT MATHÉMATIQUES
Language of instruction: FRANCAIS
Campus: CAMPUS DE PARIS - SACLAY
Workload (HEE): 60
On-site hours (HPE): 35,00
Elective Category : Fundamental Sciences
Advanced level : No

Description

This lecture is an introduction to the tools and techniques of modern mathematics, with a view towards scientific and technological applications.

Exploring the crossroads where pure mathematics, computer science and information theory meet, we will address questions such as

- How do you communicate with a deep space probe?
- How can one assess the authenticity of a digital document?
- How does one find very large prime numbers? How can one factor large integers into their prime divisors?
- and many others

These questions will lead us to introduce algebraic structures (categories, groups, rings, modules, spectra...) and to study their relationships and symmetries, but it will also hint at us that otherwise familiar notions (points, spaces, functions, numbers...) can be thought in a radically new and unifying way.

Applications of these tools to code theory and cryptology in the 20th and 21st centuries will be the governing thread of these lectures.

This lecture aims at providing students with:

- A cultural overview of the evolution of mathematics during the 20th and 21st century, along with the language that will enable them to pursue in that field
- A strong command of computational algebra, especially in finite rings and fields, and elliptic curves (rational points and divisors)
- An understanding of the mathematical foundations underpinning modern cryptology

Quarter number

SG8

Prerequisites (in terms of CS courses)

This lecture does not require an advanced mathematical background, but some fluency in computer programming is recommended.

That being said this lecture comes with a heavy workload necessary to develop an intuition of the discussed notions.

Syllabus

(Note: this syllabus is subject to last-minute changes and does not necessarily follow the lectures' order)
If you need any additional information, or are unsure about some aspect of this course, please contact the lecturer.

- Cyclic groups, finite fields, euclidean alattices and ideals, spectra
- Algorithmic number theory
- Finite and projective geometries, varieties
- Theory of elliptic curves over finite fields
- Theory of linear and AG codes
- Applications and cryptographic constructions

Class components (lecture, labs, etc.)

Blackboard lectures (notes will be provided to the attendance).
Exercises are provided, some of which will be solved in detail. (Optional) homework assignments will be given.
A textbook is provided which complements lectures, and additional references will be given for specific aspects.
Tutorials : 10,5 h
lectures : 21h

Grading

Evaluation will be hybrid: students will have regular, small graded tests to ensure they master the basic notions of this course, then will be asked to produce a more complex final project involving these notions.

Course support, bibliography

- David Eisenbud, *Commutative Algebra (with a View Toward Algebraic Geometry)*
- Robin Hartshorne, *Algebraic Geometry*
- William Fulton, *Algebraic curves: An Introduction to Algebraic Geometry*

- Henning Stichtenoth, *Algebraic Function Fields and Codes*
- Michel Demazure, *Cours d'algèbre*
- Joseph H. Silverman, *The Arithmetic of Elliptic Curves*
- Joseph H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*
- Jean-Pierre Serre, *Cours d'arithmétique*
- Michael Tsfasman, Serge Vlăduţ, Dmitry Nogin, *Algebraic Geometric Codes: Basic Notions*

Resources

Lectures will mostly rely on the blackboard, with computer tools being used in later exercises. Relevant software will be provided as needed.

Teaching staff: Rémi Géraud-Stewart.

Learning outcomes covered on the course

At the end of this course, the students will be able to

- Recognise the presence of underlying algebraic structures in engineering problems
- Understand the issues addressed by cryptology and code theory, know and recognise their leading industrial applications
- Master the mathematical language in which algebraic questions are formulated and analysed

Description of the skills acquired at the end of the course

1. Recognise the presence of underlying algebraic structures in engineering problems

- C.1.2 : identify the structures that were discussed during lectures
- C.6.1 : invoke the relevant technological tools

2. Understand the issues addressed by cryptology and code theory, know and recognise their leading industrial applications

- C.6.7 : understand the technical aspects and difficulties related to communication and information transfer
- C.3.6 : evaluate technical solutions against specific needs and constraints
- C.6.1 and C.1.4 : introduce relevant tools and correct configurations

3. Master the mathematical language in which algebraic questions are formulated and analysed.

- C.2.3 : practice acquiring new skills to approach a given problem