Lecturer: Ivan Arzhantsev

Classes: Ivan Arzhantsev, Roman Avdeev, Nikita Medved

Title of a Course: Algebra

Prerequisites: the course is based on knowledge of numerical systems and functions studied in high school, as well as on the basic concepts of the courses on Linear Algebra and Geometry, Calculus and Discrete Mathematics in the first three modules.

Course Type: compulsory

Abstract: the course is a gentle introduction to the theory of algebraic structures, including Groups, Rings and Fields, with applications to Algorithms, Cryptography and Coding Theory. The course provides professional background for further courses related to Discrete Mathematics, Formal Languages, Game Theory and Information Security.

Learning Objectives

- Introduction of main algebraic structures with explicit examples, motivations and applications
- Practice in basic computations with groups, rings and fields
- Forming students' skills in using matrix and polynomial techniques to formalize and solve applied problems, including economic and financial ones
- Study of the algorithmic aspects of the theory of finite groups and finite fields
- Formalization for further applications in programming, public-key cryptography and information theory

Learning Outcomes: Students who successfully pass the course will be able, along with other things, to classify all abelian groups of order 100, to find the sum of squares of the roots of a given polynomial, to explain why there exists no field with 6 elements, to realize error correcting linear codes and to implement basic cryptographic protocols.

Course Plan

- Binary operations
- Semigroups and groups: basic definitions and examples
- Cyclic groups. Cosets, normal subgroups and factor groups
- Direct sums and products
- Finite abelian groups
- Applications to cryptography: Diffie-Hellman Key Exchange and ElGamal Encryption
- Group actions: orbits and stabilizers
- Rings and algebras. Matrix algebras. Zero divisors, invertible elements and nilpotents
- Polynomial in several variables. Symmetric polynomials and Vieta's Formulas
- Fields. Field extensions. Structure of finite fields
- Applications to information transmission: linear codes and perfect codes

The course consists of 10 lectures and 10 classes during the 4^{th} module of the 1^{st} year.

Reading List

Required: [1] Notes provided by the lecturer

[2] Э.Б.Винберг. Курс алгебры. М.: МЦНМО, 2014 (English transl.: Ernest Vinberg. A Course in Algebra. Graduate Studies in Math. 56, Amer. Math. Soc., 2003)

[3] Сборник задач по алгебре под редакцией А.И.Кострикина. Новое издание. М.: МЦНМО, 2015 (English transl.: Exercises in Algebra. Edited by A. Kostrikin, CRC Press, 1996)

Optional: [4] Serge Lang. Algebra. Revised Third Edition. Graduate Texts in Math. 211, Springer, 2002

Grading System and Guidelines for Knowledge Assessment

During the module students have to complete home assignments weekly. Professors and assistants can ask students to present their written solutions orally. Each of the first five assignments contains 4 problems, while each of the last four assignments contains 5 problems. A solution of each problem is charged from 0 to 2 points. The total grade (H) for the home assignment is 0.15 times the sum of all points obtained by the student.

After the last class all students pass through a written test (T) with 6 problems evaluated as 0, 1 or 2 points for each problem. The final exam (E) is oral and is evaluated in points from 0 to 10.

The cumulative grade is computed as C= 0,6*H + 0,4*T

The grades H, T and C are in the range of 0 to 12.

The final course grade is given by F = min {0,5*C + 0,5*E, 10}.

Grades in all formulas are rounded according to the standard rule: if the fractional part of the grade A lies within the interval [0, 0.5), then A is rounded off downward, i.e. to the greatest integer less than or equal to A, and if the fractional part of the grade A lies within the interval [0.5, 1), then A is rounded off upward.