Study programmes: Bachelor studies – Informatics

Course name: M140 - Algebra 1

Lecturers: Milan Bozić, Aleksandar Lipkovski, Dragana Todorić, Zoran Petrović

Status: Compulsory

ECTS: 6

Attendance prerequisites: M105, M106, M120

Course aims: Acquisition of general and specific knowledge of algebra.

Course outcome: Upon completion of the course, students have the basic knowledge of algebra. They have acquired the fundamental notions, main constructions and basic theorems of group theory, ring theory and elementary number theory. They are qualified to solve problems from the mentioned areas and follow other courses in which algebra plays an important part.

Course content:

-Elements of abstract algebra. Algebraic structures. Algebraic theories and varieties, examples. Homomorphisms of algebras, subalgebras and generating sets; direct product of algebras. Congruences and quotient algebras. Fundamental theorem on homomorphisms.

-Boolean algebras. Partially ordered sets and lattices. Axioms of Boolean algebras, examples, Boolean identities. Finite Boolean algebras.

-Groups. Semigroups, monoids, groups. Power of an element in a group, Lagrange's theorem, order of an element in a group. Cyclic groups; multiplicative group of integers modulo n and Euler's theorem; direct product of cyclic groups, multiplicativity of Euler's function. Normal subgroups and quotient groups; inner automorphisms of a group. First isomorphism theorem. Dihedral groups. Symmetric and alternating groups. Groups of order less than 8.

-Finitely generated abelian groups. Primary decomposition, invariant factor decomposition.

-Group actions. Class equation; Sylow theorems.

-Introduction to number theory. Congruences. Euclidean division and Euclidean algorithm. Ring of integers modulo n, finite fields, Fermat's little theorem, Wilson's theorem, Chinese remainder theorem. Multiplicative arithmetic functions.

-Rings. Consequences of axioms. Characteristic of a ring. Ideals and congruences. Quotient ring, ring of integers modulo n. Prime and maximal ideals. The isomorphism theorem for rings. Ring of polynomials over a field. Euclidean division and Euclidean algorithm for polynomials. Roots of polynomial and polynomial factorization into irreducible factors. Boolean algebras and rings.

-Fields. Consequences of axioms, characteristic. Finite fields. Field extensions, degree of a field extension. Gauss's lemma and irreducibility of polynomials over the rationals. Field of fractions. Algebraic and transcendental elements over a field, simple extensions. Compass-and-straightedge constructions. Kronecker's construction and splitting field of a polynomial. Viete's formulas.

Literature:

1. G. Kalajdžić, Algebra, Matematički fakultet, Beograd, 1998.
2. Ž. Mijajlović, Algebra, Milgor, Beograd, 1998.
3. N. Božović, Ž. Mijajlović, Uvod u teoriju grupa, Naučna knjiga, Beograd, 1990.
4. A. Clark, Elements of Abstract algebra, Dover Publ. Co., New York, 1984.
5. A. Baker, A concise introduction to the theory of numbers, Cambridge Univ. Press., 1984.

Number of hours:	**Lectures:**	**Tutorials:**		
5	3	2		

Teaching and learning methods: Frontal / Interactive / Tutorials / Lectures / Exercises

Assessment (maximal 100 points)

Course assignments	**points**	**Final exam**	**Points**

Lectures	-	Written exam	-
Exercises / Tutorials	-	Oral exam	-
Colloquia	30	Written-oral exam	70
Essay / Project	-		