

Program	Level		I cycle				
	Name of the program		Theoretical Computer Science				
COURSE							
Course title	Algebra for Computer Science						
Course code	Semester	Course status	ECTS	Contact hours (L+AE+LE)			
PMAT 290	IV	Mandatory course	5	3+2+0			
Lecturer							
Course Goals	The goal is to provide the knowledge in algebraic structures and their properties on the level needed for applications in computer science.						
Learning Outcomes	Student will gain the knowledge of algebra needed for applications in cryptography and coding theory.						
COURSE CONTENT							
Grupoid, semi groups, groups and subgroups. Lagrange theorem. Permutation groups. Quotient groups. Homomorphism.							
Ring, ideal, quotient ring. Polynomial ring. Euclidian domain. Greatest common divisor. Prime and irreducible elements.							
Extension fields. Finite fields. Arithmetic over finite fields.							
Boolean algebra. Use in cryptography, coding theory and generating of pseudo-random numbers.							
LITERATURE							
[1] D. S. Malik, John N. Mordeson, M.K.Sen, Fundamentals of Abstract Algebra, Mc Grew Hill							
[2] L. Gårding, T. Tambour, Algebra for Computer Science, Springer-Verlag							
[3] H. Jamak, Algebra, NIK Sezam doo Sarajevo, 2004.							
[4] P.B. Bhattacharya, S.S. Jain, S.R. Nagpaul, Basic Abstract algebra, Cambridge University Press, 1994.							
STUDENT WORKLOAD (hours in a semester)							
Lectures	45	Tutorial	30	Individual work	50	T o t a l	125
GRADING				REMARKS			
Criterion	Maximum points	Minimum points					
Midterm exams	50	25					
Homework assignment							
Project							
Laboratory assignments							
Final exam	50	25					
T o t a l	100	55					