



Universitat de Lleida

# DEGREE CURRICULUM

# **ALGEBRA**

Coordination: VALLS MARSAL, MA MAGDALENA

Academic year 2022-23

## Subject's general information

<b>Subject name</b>	ALGEBRA			
<b>Code</b>	102005			
<b>Semester</b>	1st Q(SEMESTER) CONTINUED EVALUATION			
<b>Typology</b>	<b>Degree</b>	<b>Course</b>	<b>Character</b>	<b>Modality</b>
	Bachelor's Degree in Computer Engineering	1	COMMON/CORE	Attendance-based
	Double bachelor's degree: Degree in Computer Engineering and Degree in Business Administration and Management	1	COMMON/CORE	Attendance-based
<b>Course number of credits (ECTS)</b>	6			
<b>Type of activity, credits, and groups</b>	<b>Activity type</b>	PRAULA		TEORIA
	<b>Number of credits</b>	3		3
	<b>Number of groups</b>	2		2
<b>Coordination</b>	VALLS MARSAL, MA MAGDALENA			
<b>Department</b>	MATHEMATICS			
<b>Teaching load distribution between lectures and independent student work</b>	6 ECTS correspond to a workload of 60 h of lectures and assesment and 90 h autonomous study work for each student.			
<b>Important information on data processing</b>	Consult <a href="#">this link</a> for more information.			
<b>Language</b>	Catalan.			
<b>Distribution of credits</b>	Theoretical lectures are combined with problem solving sessions. Lectures will be organized for 2 groups (6ECTS, 4h/week each).			

Teaching staff	E-mail addresses	Credits taught by teacher	Office and hour of attention
MIRET BIOSCA, JOSE MARIA	josepmaria.miret@udl.cat	6	
VALLS MARSAL, MA MAGDALENA	magda.vallsmarsal@udl.cat	6	

## Subject's extra information

Previous knowledge/skills on basic mathematics (General Upper Secondary Education level) are recommended.

This subject is scheduled in the fall semester of the 1st year.

The knowledge and competencies acquired in this subjects will be useful to follow other subjects with contents related with logics, data structure, discrete mathematics and the subjects in the especialization on Computation.

## Learning objectives

- Appropriately use set operations, both to simplify expressions or to prove equalities.
- Recognize equivalence and order relations (total and partial).
- Obtain the quotient set and the equivalence classes.
- Determine the characteristic elements in an ordered set.
- Distinguish injective, exhaustive and bijective maps.
- Manipulate the composition of maps and inverse maps.
- Apply mathematical induction to show different mathematical statements.
- Recognize the algebraic structures of group, ring and field.
- Adequately use the elements in modular arithmetic.
- Solve diophantine equations and linear congruencies.
- Encrypt and decrypt with the RSA cryptosystem.

## Competences

### Specific competences

- GII-FB1 - Capacity to solve mathematical problems arisen in the engineering field. Aptitude to apply knowledge on: linear algebra; differential and integral calculus; numerical methods; algorithmic, numerical; statistics and optimisation.
- GII-FB3 - Capacity to understand and master the basic concepts of discrete mathematics, logical, algorithmic and computational complexity, and its application to solve engineering problems.

### Cross-disciplinary competences

- EPS1 - Capacity to solve problems and prepare and defence arguments inside the area of studies.
- EPS5 - Capacity of abstraction and of critical, logical and mathematical thinking.

### University strategic competences

- CT5 - Acquire knowledge in scientific thinking.

## Subject contents

### I. SET THEORY

#### 1. Sets.

- Sets and elements. Subsets.
- Set operations.
- Laws of the algebra of sets.
- Partition of a set.
- Cartesian product.

#### 2. Relations

- Relations in a set: definitions and examples.
- Equivalence relations. Equivalence classes and quotient set.
- Order relations. Characteristic elements.
- Hasse diagram to represent an ordered set.

#### 3. Maps.

- Map between sets: definitions and examples.
- Injective, surjective and bijective maps.
- Composition of maps.
- Inverse map.

#### 4. Induction and denumerability

- Mathematical induction.
- Infinite sets and denumerable sets.

### II. ALGEBRAIC STRUCTURES AND ARITHMETIC

#### 5. Algebraic structures.

- Algebraic composition laws. Properties.

- Group structure: definitions, properties, examples.
- Ring and field structures: definitions, properties, examples.

## 6. Modular arithmetic.

- Division of integers. Divisors and multiples.
- Greatest Common Divisor. Euclidean algorithm. Bézout's identity.
- Linear diophantine equations.
- Prime numbers. Fundamental theorem of arithmetic.
- Congruences. Linear congruences.
- Modular exponentiation. Fermat's and Euler's Theorems.
- Introduction to cryptography: RSA cryptosystem

## Methodology

Theoretical and practical contents are mixed for the sake of combining basic aspects with illustrative examples and problem solving.

Problem solving combines joint resolution on the blackboard or individual resolution. Some sessions will be devoted to group problem solving. Proposed problems are either solved and presented by students, or collected to be assessed.

The students will be provided beforehand with the collection of problems to be solved, as well as the exams of previous years, which will be solved in groups.

## Development plan

Week	Lesson	Activities	Student workload
1	Introduction. Lesson 1	Lectures	4 hours. Study and problem solving.
2	Lesson 1	Lectures and problem sessions	4 hours. Study and problem solving.
3	Lesson 1	Lectures and problem sessions	4 hours. Study and problem solving.
4	Lesson 2	Lectures and problem sessions	4 hours. Study and problem solving.
5	Lesson 2	Control 1	6 hours. Study for control.
6	Lesson 3	Conferences attendance	4 hours. Study and problem solving.
7	Lesson 3	Lectures and problem sessions	4 hours. Study and problem solving.
8	Tema 4	Lectures and problem sessions	6 hours. Study and problem solving.

Week	Lesson	Activities	Student workload
9		Partial 1 Assessment	8 hours. Study for exams
10	Lesson 4	Lectures and problem sessions	4 hours. Study and problem solving.
11	Lesson 5	Control 2	6 hours. Study for control.
12	Lesson 5	Complementary book reading	4 hours. Study and problem solving. Reading complementary book.
13	Lesson 6	Lectures and problem sessions	4 hours. Study and problem solving. Reading complementary book.
14	Lesson 6	Lectures and problem sessions	4 hours. Study and problem solving. Reading complementary book.
15	Lesson 6	Complementary reading assessment	8 hours. Study for exams.
16		Tutorization	8 hours. Study for exams.
17		Partial 2 Assessment	8 hours. Study for exams.
18		Tutorization	
19		Final assessment	

## Evaluation

Acr.	Assessment activities	Weight	Minimum Mark	Resit
C1	Control 1. Lesson 1.	1 point	No	No
P1	Partial 1. Lessons 1, 2, 3.	4 points	1 point	Yes
C2	Control 2. Lesson 4.	1 point	No	No
P2	Partial 2. Lessons 4, 5, 6	4 points	1 point	Yes
AC	Complementary activities : complementary reading or attending mathematic-related conferences or exhibitions	0.5 points	No	No
PCL	Participation	0.5 points	No	No

A student with final mark below 5 or who has not reached the minimum marks required, can resit either P1, P2 or both.

$$\text{FinalMark} = C1 + P1 + C2 + P2 + AC + PCL$$

## Bibliography

### Books including problems

- Montse ALSINA; Claudi BUSQUÉ; Enric VENTURA, Problemes d'Àlgebra. Servei de Publicacions de

l'U.A.B., 1990.

- Nina BIJEDIC; Joan GIMBERT; Josep M. MIRET; Magda VALLS. Elements of Discrete Mathematical Structures for ComputerScience. Univerzittska knjiga Mostar, 2007.
- Javier León CÁRDENAS. Álgebra. Serie Universitaria Patria. 2014.
- Emilio ESPADA. Problemas Resueltos de Álgebra (Vol I,II). EDUNSA, 1989.
- Joan GIMBERT; Xavier HERNÁNDEZ; Nacho LÓPEZ; Josep M. MIRET; Ramiro MORENO; Magda VALLS. Curs Pràctic d'Àlgebra per a Informàtics, Col.lecció Eines, núm. 48. Edicions de la Universitat de Lleida,2004. En format ebook a <https://www.publicacions.udl.cat/distribucio/>

## Theory books

- Howard ANTON. Introducción al Álgebra Lineal. Ed. Limusa, 3a. edició, 1990.
- Manel CASTELLET; Irene LLERENA. Àlgebra Lineal i Geometria. Manuals de la Universitat Autònoma de Barcelona, 1979.
- Lindsay CHILDS. Concrete Introduction to Higher Algebra. Springer, 1a. edició, 1979.
- Ronald S. IRVING. Integers, Polynomials and Rings: a Course in Algebra. Springer. 2003.
- Gustavo LABBE MORALES. Curso Introductorio de Estructura Algebraicas. Ed. Patagonia. Universidad de La Serena. 2017.
- Serge LANG. Undergraduate algebra. Springer. 2010.
- Ramón RODRÍGUEZ VALLEJO. Conjuntos Numéricos, Estructuras Algebraicas y Fundamentos de Álgebra Lineal. Ed. Tébar. 2013.
- Kenneth ROSEN, Matemática Discreta y sus Aplicaciones. McGraw-Hill Interamericana, 5a. edició, 2006.
- Donald F. STANAT; David McALLISTER. Discrete Mathematics in Computer Science, Prentice-Hall, 1a. Edició.
- Wolfgang WILLEMS, Ismael GUTIÉRREZ GARCÍA. Una Introducción a la Criptografía de Clave Pública. Ed. Uninorte. 2010.

## Recommended reading

- Simon SINGH. Los Códigos Secretos. Ed. Debate, 2000.
- Joan GÓMEZ URGELLÉS. Matemáticos, Espías y Piratas Informáticos. Codificación y criptografía. National Geographic 2015.