Universitat de Lleida

DEGREE CURRICULUM

ALGEBRA

Coordination: DALFO SIMO, CRISTINA

Academic year 2022-23

ALGEBRA 2022-23

Subject's general information

<table>
<tr><td>Subject name</td><td>ALGEBRA</td></tr>
<tr><td>Code</td><td>105005</td></tr>
<tr><td>Semester</td><td>1st Q(SEMESTER) CONTINUED EVALUATION</td></tr>
<tr><td>Typology</td><td>
<table>
<tr><th>Degree</th><th>Course</th><th>Character</th><th>Modality</th></tr>
<tr><td>Bachelor's Degree in Computer Engineering</td><td>1</td><td>COMMON/CORE</td><td>Attendance-based</td></tr>
</table>
</td></tr>
<tr><td>Course number of credits (ECTS)</td><td>6</td></tr>
<tr><td>Type of activity, credits, and groups</td><td>
<table>
<tr><th>Activity type</th><th>PRAULA</th><th>TEORIA</th></tr>
<tr><td>Number of credits</td><td>3</td><td>3</td></tr>
<tr><td>Number of groups</td><td>1</td><td>1</td></tr>
</table>
</td></tr>
<tr><td>Coordination</td><td>DALFO SIMO, CRISTINA</td></tr>
<tr><td>Department</td><td>MATHEMATICS</td></tr>
<tr><td>Teaching load distribution between lectures and independent student work</td><td>6 ECTS correspond to a workload of 60 h of lectures and assessments and 90 h of autonomous study work for each student.</td></tr>
<tr><td>Important information on data processing</td><td>Consult this link for more information.</td></tr>
<tr><td>Language</td><td>Catalan.</td></tr>
<tr><td>Distribution of credits</td><td>Theoretical lectures are combined with problem-solving sessions.
Lectures will be organized for 1 group (6ECTS, 4h/week).</td></tr>
</table>

ALGEBRA 2022-23

Teaching staff	E-mail addresses	Credits taught by teacher	Office and hour of attention
DALFO SIMO, CRISTINA	cristina.dalfo@udl.cat	6	

Subject's extra information

Previous knowledge/skills in basic mathematics (General Upper Secondary Education level) are recommended.
This subject is scheduled for the fall semester of the 1st year.
The knowledge and competencies acquired in this subject will be useful for following other subjects with contents related to logic, data structure, discrete mathematics, and the subjects in the specialization on Computation.

Learning objectives

- Appropiately use of 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 arising in the engineering field. Aptitude to apply knowledge of linear algebra; differential and integral calculus; numerical methods; algorithmic, numerical; statistics, and optimization.
- GII-FB3 - Capacity to understand and master the basic concepts of discreet mathematics, logical, algorithmic, and computational complexity, and its application to solve engineering problems.

Cross-disciplinary competences

- EPS1 - Capacity to solve problems and prepare and defend arguments inside the area of studies.
- EPS5 - Capacity for the abstraction 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 quotioent 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

ALGEBRA 2022-23

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. Studying for control.
6	Lesson 3	Lectures and problem sessions	4 hours. Study and problem-solving.
7	Lesson 3	Lectures and problem sessions	4 hours. Study and problem-solving.
8	Lesson 4	Lectures and problem sessions	6 hours. Study and problem-solving.
9		Partial 1 Assessment	8 hours. Studying for exams.
10	Lesson 4	Lectures and problem sessions	4 hours. Study and problem-solving.
11	Lesson 5	Control 2 and Evaluation of book reading	6 hours. Studying for control.
12	Lesson 5	Lectures and problem sessions	4 hours. Study and problem-solving.
13	Lesson 6	Lectures and problem sessions	4 hours. Study and problem-solving.
14	Lesson6	Lectures and problem sessions	4 hours. Study and problem-solving.
15	Lesson 6	Lectures and problem sessions	8 hours. Studying for exams.
16		Tutorials	8 hours. Studying for exams.
17		Partial 2 Assessment	8 hours. Studying for exams.
18		Tutorials	
19		Final assessment	

Evaluation

Acr.	Assessment activities	Weight	Minimum Mark	Resit
C1	Control 1. Lesson1.	10%	No	No
P1	Partial 1. Lessons 1, 2, 3.	40%	2.5 points	Yes
C2	Control 2. Lesson 2.	10%	No	No
P2	Partial 2. Lessons 4, 5, 6.	40%	2.5 points	Yes

AC	Complementary activities: complementary reading or watching mathematically related videos	5%	No	No
PCI	Participation	5%	No	No

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

The final mark will be computed after the resit of P1 and/or P2, if necessary.
Final Mark = 0.1·C1 + 0.4·P1 + 0.1·C2 + 0.4·P2 + 0.05·AC+ 0.05·PCI

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.
- 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

- Ronald S. IRVING. Integers, Polynomials, and Rings: a Course in Algebra. Springer. 2003.
- Kenneth ROSEN, Matemática Discreta y sus aplicaciones. McGraw-Hill Interamericana, 5a. edició, 2006.
- 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.
- Howard ANTON. Introducción al Álgebra Lineal. Ed. Limusa, 3a. edició, 1990.
- Wolgang 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.