DEGREE CURRICULUM

ÀLGEBRA

Coordination: Josep M. Miret

Academic year 2013-14

ALGEBRA 2013-14

Subject's general information

Subject name	ÀLGEBRA
Code	102005
Semester	1st
Typology	Compulsory
ECTS credits	6
Groups	GGA, GGB i GEIADE
Theoretical credits	0
Practical credits	0
Coordination	Josep M. Miret
Department	Matemàtica
Teaching load distribution between lectures and independent student work	1,5 independent study work for each 1-hour-lecture
Important information on data processing	Consult this link for more information.
Language	Catalan / spanish
Distribution of credits	Josep M. Miret Biosca GEI 6 crèdits Maria Magdalena Valls Marsal GEI 6 crèdits, GEIADE 6 crèdits
Office and hour of attention	Agree an appointment by e-mail.

ALGEBRA 2013-14

Josep M. Miret Biosca
Maria Magdalena Valls Marsal

Subject's extra information

The course as part of the academic plan

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

Learning objectives

See competences

Competences

Degree-specific competences

- Ability to resolve logical problems that can arise in engineering. Aptitude to apply knowledge about lineal algebra; differential and integral calculus; numeric methods, numeric algorithms; statistics and optimization.

Goals

- Distinguish injective, surjective and bijective maps.
- Obtain composed and inverse mappings.
- Adequately use elements in modular arithmetic.
- Solve diophantine equations and linear congruencies.
- Adequately use Fermat's and Euler's Theorems.
- Encrypt and decrypt with RSA.

- Ability to understand and master the basic concepts of discrete mathematics, logic, algorithm and computational complexity, and their application to the resolution of engineering problems.

Goals

- Appropiately use of set operations.
- Recognize equivalence and order relations.
- Obtain the quotient set and the equivalence classes.
- Determine the characteristic elements in a ordered set.
- Use of mathematical induction in mathematical proofs.
- Determine the properties of a given algebraic structure.
- Recognize groups, rings and fields.
- Adequately use the elements in modular arithmetic.
- Solve diophantine equations and linear congruencies.

Degree-transversal competences

- Ability for abstraction and critical, logical and logical reasoning.

Goals

- Recognize equivalence and order relations.
- Obtain the quotient set and equivalence classes.
- Determine the characteristic elements in a ordered set.
- Use mathematical induction in mathematical proofs.
- Determine the properties of a given algebraic structure.
- Recognize the algebraic structures of group, ring and field.

- Ability to resolve problems and elaborate and defend arguments inside their field of study.

Goals

- Solve diophantine equations and linear congruencies.
- Encrypt and decrypt with RSA.
- Use mathematical induction in mathematical proofs.

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.

• Maps composition.

• 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.

•Chinese remainder theorem.

•Modular exponentiantion. Fermat's and Euler's Theorems.

•Introduction to cryptography.

Methodology

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

Development plan

The following table shows the expected amount of hours devoted to each lesson:

Lesson	Theoretical concepts	Problem solving	Independent student work
1	5	3	12
2	4	4	12
3	3	3	9
4	2	2	6
5	5	6	15
6	6	6	18

Evaluation

Planned tests:

- C1 - Control 1:
  - Lesson 1.
  - Among 3rd and 5th weeks.
  - Value: 1 point
- P1 - Exam 1:
  - Lessons 1, 2, 3
  - 9th week
  - Value: 4 points
- C2 - Control 2:
  - Lesson 4.
  - Among 12h and 14h weeks.
  - Value: 1point
- P2 - Exam 2:
  - Lessons 4, 5 i 6
  - Among 16th and 17th weeks.
  - Value: 4 points.

To compute the final mark the minimum marks in P1 and P2 are: P1 >= 1 punt i P2 >= 1 punt.

The student can obtain an additional point to the final mark, according to the following concepts:

- Participation: 0.5 punts
- Complementary activitities : 0.5 points

Final Mark = C1 + P1 + C2 + P2 + AD

Bibliography

Books including problems

ALSINA, M; BUSQUÉ, C; VENTURA, E. Problemes d' Àlgebra. Servei de Publicacions de l'U.A.B., 1990.

BIJEDIC, N; GIMBERT, J; MIRET,J.M; VALLS, M. Elements of Discrete Mathematical Structures for ComputerScience. Univerzittska knjiga Mostar, 2007.

ESPADA, E. Problemas resueltos de Álgebra (Vol I,II). EDUNSA, 1989.

GIMBERT, J; HERNÁNDEZ, X; LÓPEZ, N; MIRET, J.M; MORENO, R; VALLS, M. CursPràctic d'Àlgebra per a Informàtics, Col.lecció Eines. Edicions de la Universitat de Lleida,2004.

Theory books

ANTON, H. Introducción al Álgebra Lineal. Ed. Limusa, 3a. edició, 1990.

CASTELLET, M; LLERENA, I. Àlgebra Lineal i Geometria. Manuals de la Universitat Autònomade Barcelona, 1979.

CHILDS, L. A Concrete Introduction to HigherAlgebra. Springer, 1a. edició, 1979.

STANAT, D.F.; McALLISTER, D.F. DiscreteMathematics in Computer Science, Prentice-Hall, 1a. Edició.

Recommended reading

SINGH, S. Los códigos secretos. Ed. Debate, 2000.