

## SUBJECT TEACHING GUIDE

### G92 - Commutative Algebra

#### Double Degree in Physics and Mathematics Degree in Mathematics

Academic year 2023-2024

1. IDENTIFYING DATA					
Degree	Double Degree in Physics and Mathematics Degree in Mathematics			Type and Year	Compulsory. Year 4 Compulsory. Year 3
Faculty	Faculty of Sciences				
Discipline	Subject Area: Algebra Module: Compulsory Subjects				
Course unit title and code	G92 - Commutative Algebra				
Number of ECTS credits allocated	6	Term	Semester based (2)		
Web					
Language of instruction	Spanish	English Friendly	No	Mode of delivery	Face-to-face

Department	DPTO. MATEMATICAS, ESTADISTICA Y COMPUTACION				
Name of lecturer	LUIS MIGUEL PARDO VASALLO				
E-mail	luis.pardo@unican.es				
Office					
Other lecturers					

3.1 LEARNING OUTCOMES
- Have a wide collection of paradigmatic examples of groups, rings, domains, etc. and discern the properties algebraic that they have.
- Know how to operate in commutative rings with unit, as a generalization of polynomial rings.
- Know the elementary vocabulary of algebraic varieties as a generalization of the set of roots of an algebraic equation.
- Connect the ideas and terms of Commutative Algebra and Algebraic Geometry.
- Rings of polynomials and field of rational functions.
- Introduction to the elementary language of Algebraic Geometry, Commutative Algebra and Algebraic Number Theory. algebraic varieties. Commutative rings with unity. Ideals. Modules. Primes and primaries. Algebraic integers in a field of numbers. Algorithms.

#### 4. OBJECTIVES

Know the notion of determinant of an endomorphism between modules of finite rank and know how to prove its properties, among which the Hamilton-Cayley Theorem must be.

Know and know how to prove properties of Euclidean domains, domains of main ideals and domains of unique factorization. Know examples from Number Theory or Algebraic Geometry.

Know and know how to demonstrate the existence of Schmidt's Normal Form and its implications in the classification of groups finitely generated abelians, in Endomorphism Theory and in the resolution of diophantine linear equations.

Know the general form of the Chinese Remainder Theorem and its implications in Number Theory and in the existence of Jordan's Canonical Form.

Know some elementary demonstration of the Nullstellensatz and its geometric meaning.

Know basic notions and demonstrations of Noetherian rings. Know some proof of the Lasker-Noether Theorem.

The main goal is to learn some basics in Commutative Algebra, as a supplement to previous formation in Algebra.

There is also an attempt to form students in writing and reading abstract mathematical notions, statements and proofs as a scientific language, with contents related to the general scope of Commutative Algebra and its applications.

Learn by experience the need of patience and effort to deeply understand mathematical methodology.

6. COURSE ORGANIZATION	
CONTENTS	
1	Notions of ring, ideal and module over a ring- Euclidean domains. Remainder Theorem. Structure of residue rings. Prime fields. $R$ -algebra morphisms. theorems of Isomorphy. Abelian groups and modules. Endomorphism theory: annihilator ideal and minimal polynomial. Rings of polynomials in several variables and power series rings. Notions as the language of Geometry "à la Grothendieck". Notions as a basis for Algebraic Number Theory: quadratic extensions of $Z$ . Rings and modules in other contexts: continuous functions, differential and analytic functions and their corresponding rings and modules.
2	Determinant. Group action on a set: orbits, transitive and faithful actions. Example: Cayley graphs. Symmetric groups and its generators: cycles of any order. Index as group morphism. Determinant of a matrix with coordinates in a commutative ring. Generalized Laplace Formula: the general linear group $GL(n,R)$ . Determinant as a group morphism. Unimodular matrices. Hamilton-Cayley Theorem. Csanky-Leverrier-Fadeev-Souriau algorithm for computing characteristic polynomials..
3	Most elementary rings. Prime and maximal ideals. Zorn's Lemma and existence of maximal ideals. Zero divisors. Definition and presence in different contexts (continuous functions, differential functions, analytic functions). Euclidean domains. Bézout Identity with bounds. Euclid's algorithm. Euclid's algorithm in $Z$ : Lamé's Theorem. Classic univariate Elimination theory: Sylvester matrix and resultant. principal ideal domains. Bézout's Identity. Existence of factorization in Principal Ideal Domains and Euclidean Domains. Unique factorization domains. Gauss Lemma and factorization in polynomial rings. Applications: RSA cryptosystem, factorization of univariate polynomials over finite fields (Berlekamp's method), error correcting codes and Hamming distance..
4	Torsion. Equivalence of finitely generated torsion free modules and finitely generated free modules over a principal ideal domain. Smith Normal Form: algorithms and existence. Solving linear Diophantine equations. First Structure Theorem on Finitely Generated Abelian Groups. Companion matrix of a polynomial and tensor of the residue ring. Frobenius form of an endomorphism and cyclic decomposition of $K[X]$ -modules. Schwartz-Zippel Zero test: Fast algorithms to compute minimal polynomials of an endomorphism.
5	Chinese remainder Theorem. Applications: Secret Sharing, 2nd Structure Theorem for finitely generated Abelian Groups: elementary divisors. Modular Algorithms, Hadamard Inequality. Algebraically closed fields. Jordan forma of an endomorphism and CRT. Algorithms that compute the greatest common divisor of univariate polynomials in intrinsic dimension.
6	Nullstellensatz. Nilradical and Jacobson's radical. Zariski's topology. Algebraically closed fields (notion and main properties). Rings and ideals in Geometry. Ring of polynomial (also regular) functions ( $K[V]$ ), ring of rational functions ( $K(V)$ ), ideal of a variety ( $I(V)$ ):Local and semi-local rings. Localization. An elementary proof of Hilbert's Nullstellensatz. Bézout Identity in $K[X_1, \dots, X_n]$ . The language of categories: natural equivalence among categories. Examples in other contexts: Urysohn's Lemma and Tietze's Extension Theorem, Nullstellensatz of Banach-Stone-Cech, compactification through maximal spectra and Zariski topology.
7	Noetherian condition. Noetherian condition and partially ordered sets, assuming the Weak Election Axiom. Quasi-compact topological spaces. Noetherian rings and modules. Hilbert's Basissatz. Zariski's topology is quasi-compact and consequence: irreducible components and primes. NAK's Lemma (Nakayama, Azumaya, Kronecker). Irreducible modules and primary submodules. Primary decomposition. Lasker-Noether existence Theorem of primary decomposition. Associated, support and annihilator: first Uniqueness theorem. The graph of the spectrum of a ring: Krul's dimension. Noetherian condition and unique factorization (Nagat's Lemma). Introduction to standard and Groebner basis (Dixon's lemma and Buchberger algorithm).
8	Final exam

### 7. ASSESSMENT METHODS AND CRITERIA

Description	Type	Final Eval.	Reassessn	%
The student has to develop either some topic or some problems and exercise. The value of this part ins 40 % of the final qualification.	Work	No	Yes	40,00
Several questions and problems related to contents of the course. Its value is 60% of the final qualification.	Written exam	Yes	Yes	60,00
TOTAL				100,00
Observations				
In the Final examination of the Ordinary evaluation , there will be some specific questions for those students that didn't pass continuous evaluation.Extraordinary evaluation evaluation is 100% the results of the final examination.				
Observations for part-time students				
Part-time students will be evaluated by the same method described for full-time students.				

### 8. BIBLIOGRAPHY AND TEACHING MATERIALS

#### BASIC

M.F. Atiyah, I.G. Macdonald, Introducción al álgebra conmutativa, ed. reverté 1973