Academic subject: ALGEBRA 3			
Degree Class: LM-40 - Matematica		**Degree Course:** Mathematics	**Academic Year:** 2017/2018
		Kind of class: Mandatory/Optional depending on the Curriculum	**Year:** **Period:** 2
			ECTS: 7 divided into **ECTS lessons: 6,5** **ECTS exe/lab/tutor: 0,5**
Time management, hours, in–class study hours, out–of–class study hours lesson: 52 exe/lab/tutor: 8 in–class study: 60 out–of–class study: 115			
Language: Italian	**Compulsory Attendance:** no		
Subject Teacher: Margherita Barile	**Tel:** +39 080 5442204 **e–mail:** margherita.barile@uniba.it	**Office:** Department of Mathematics 2nd floor, room 23	**Office days and hours:** By appointment
Prerequisites: Fundamental concepts on finite groups, commutative rings, field extensions, polynomials.			
Educational objectives: Understanding the historical background, the theoretical motivations ad the practical applications of abstract algebra.			
Expected learning outcomes (according to Dublin Descriptors)	**Knowledge and understanding:** Recognizing abstract algebra as a unitary conceptual framework. **Applying knowledge and understanding:** Applying algebraic structures to problem solving. **Making judgements:** Assessing the practical utility of abstract algebra as a working tool. **Communication:** Acquire conciseness in presenting complex topics. **Lifelong learning skills:** Examining algebraic concepts in a historical perspective.		

Course program

Complements on groups

Subgroup generated by a subset: definition, characterization, the case of symmetric and alternating groups. Second and third isomorphism theorem for groups. Solvable groups: definition, derived groups, characterizations by means of normal chains, solvability of subgroups and quotient groups, the case of symmetric groups, Galois-Jordan Theorem*, solvability of p-groups, Burnside Theorem* and Feit-Thompson Theorem.

Complements on polynomials and groups

Uniqueness of the splitting field, the isomorphism extension theorem for fields: weak form, strong form*. Separable polynomials, separable extensions, perfect fields. The primitive element theorem. Embeddings of a separable extension in an algebraic closure. Dedekind's Lemma. Simple algebraic extensions and finiteness of intermediate fields. Lüroth's Theorem*. Symmetric polynomials and elementary symmetric polynomials, symmetrization by sum and product, symmetric rational functions, Viète's formulas. Resultant of two polynomials, expressed in terms of the Sylvester matrix and in terms of roots*. Discriminant of a polynomial: definition in terms of the resultant, computation by means of Vandermonde's matrix, relation with the multiplicity of roots (in the special cases of cubic and quartic polynomials). Cyclotomic polynomials: definition, recursive formula, irreducibility*, cyclotomic polynomials of prime order, application to the proof of Wedderburn's Theorem on finite division rings*.

Galois Theory

Galois group of an extension, fixed field of a group of field automorphisms. Normal and Galois extensions: definitions and characterizations. The Fundamental Theorem of Galois Theory and its application to the Fundamental Theorem of Algebra*. Galois group of the composite of an algebraic and a Galois extension*. The Galois group of a polynomial and its determination for polynomials of degree 2, 3, 4, for the cyclotomic polynomials, for binomials and for the general equation of degree n. Solutions of the algebraic equations of degree 2, 3, 4, Ferrari's cubic resolvent and its alternative form*. Radical extensions: definition and characterization*. Criterion for solvability by radicals.

Line segments constructible by ruler and compass and constructible real numbers. The transcendence of π according to Lindemann*. Impossible constructions. Constructible complex numbers: definition and characterization. Gauss' criterion for the constructibility of a regular polygon.

Algebraic number theory

Generalities on modules over commutative unit rings: definition, submodule generated by a subset, finitely generated modules, free modules over **Z** and their submodules*, module homomorphisms, quotient modules. Noetherian rings and modules: equivalent definitions, Hilbert's basis theorem*, quotient, submodules and finite direct sums of Noetherian modules, Noetherian modules over a Noetherian ring. Proof that every ideal of a commutative unit ring is contained in a maximal ideal*. Integral elements and integral extensions: definition, characterization, algebraic integers (characterization, relation with algebraic numbers), sufficient criterion for integral extensions, transitivity of integral extensions, integral closures (Dedekind's proof that the integral closure is a ring*) , integrally closed rings, the case of **Z** (and, more generally, of a UFD). The ring of integers D_K of a number field K: characterization theorem for quadratic fields, D_K as a Dedekind domain. Relation between PID and UFD in the general case and for Dedekind domains. Fractional ideals. Divisibility relation between ideals. Factorizations and the multiplicative group of nonzero ideals in a Dedekin domain: Kummer's factorization criterion*, integers that are prime in D_K. Norm, trace and characteristic of an element in a finite field extension. Norm of an ideal of D_K : definition, comparison with the norms of elements, multiplicative property*. Ideal class group: two equivalent definitions, relation with the PID property, the ideal class number and its applications to the resolution of Diophantine equations. Characterization of PIDs by means of the Hasse-Dedekind norm. A necessary criterion for Euclidean domains. An example of a PID that is not an Euclidean domain. Quadratic residues modulo a prime: definition, Euler's criterion, Gauss Lemma, the quadratic reciprocity law.

*the proof is optional

Teaching methods:
Lectures

Auxiliary teaching:
Complete lecture notes available on line:
http://www.dm.uniba.it/~barile/Rete2/indice_dispense.htm

Assessment methods:
Oral exam

Bibliography:

R. B. Ash, *A Course in Algebraic Number Theory*,
https://faculty.math.illinois.edu/~r-ash/ANT.html
R. B. Ash, *Abstract Algebra*, *The Basic Graduate Year*
https://faculty.math.illinois.edu/~r-ash/Algebra.html
M. F. Atiyah, I.G. Macdonald, *Introduzione all'algebra commutativa*, trad. di P. Maroscia, Feltrinelli, Milano, 1981.
M. Baker, *Algebraic Number Theory,*
http://people.math.gatech.edu/~mbaker/pdf/ANTBook.pdf
A. Caranti, S. Mattarei, *Introduzione alla Teoria di Galois*,
http://www.science.unitn.it/~caranti/Didattica/Galois/2005-06/Note/Galois.pdf
D. S. Dummit, R. M. Foote, *Abstract Algebra,* Wiley, New York, 1999.
S. Franciosi, F. de Giovanni, *Elementi di Algebra,* Aracne, Roma, 1992.
P. Grillet, *Algebra*, John Wiley & Sons, New York, 1999.
I. N. Herstein, *Algebra*, Editori Riuniti, Roma, 1994.
I. M. Isaacs, *Algebra. A Graduate Course,* Brooks/Cole, Pacific Grove, 1994.
J. S. Milne, *Algebraic Number Theory,*
http://www.jmilne.org/math/CourseNotes/ant.html
P. Morandi, *Field and Galois Theory,* Springer, New York, 1996.
J. Rotman, *Galois Theory,* Springer, New York, 1990