Algebra n. 3

Prof.ssa Margherita Barile

a.a. 2021/2022

Gli argomenti indicati con * sono facoltativi per l'esame orale.

PARTE PRIMA .

Complementi sui gruppi

Sottogruppo generato da un sottoinsieme: definizione, caratterizzazione, caso dei gruppi simmetrici ed alterni. Secondo e terzo teorema di isomorfismo per gruppi. Gruppi risolubili: definizione, gruppi derivati, caratterizzazione mediante le catene normali, risolubilità di sottogruppi e gruppi quozienti, caso dei gruppi simmetrici, teorema di Galois-Jordan*, risolubilità dei p-gruppi, teoremi di Burnside* e di Feit-Thompson.

PARTE SECONDA .

Complementi su polinomi e campi

Unicità del campo di spezzamento, teoremi di estensione degli isomorfismi di campo: forma debole, forma forte*. Polinomi separabili, estensioni separabili, campi perfetti. Teorema dell'elemento primitivo. Immersioni di un'estensione separabile in una chiusura algebrica. Lemma di Dedekind. Estensioni algebriche semplici e finitezza dei campi intermedi. Teorema di Lüroth*. Polinomi simmetrici e polinomi simmetrici elementari, polinomi simmetrizzati per somma e per prodotto, funzioni razionali simmetriche, formule di Viète. Risultante di due polinomi: espressioni mediante la matrice di Sylvester e mediante le radici*. Discriminante di un polinomio: definizione tramite il risultante, calcolo mediante la matrice di Vandermonde, relazione con la molteplicità delle radici (caso particolare dei polinomi reali quadratici e cubici). Polinomi ciclotomici: definizione, formula ricorsiva, irriducibilità*, polinomi ciclotomici di ordine primo, applicazione alla dimostrazione del teorema di Wedderburn sui corpi finiti*.

PARTE TERZA . **Teoria di Galois**

Gruppo di Galois di un'estensione, campo fisso di un gruppo di automorfismi di campo. Estensioni normali e galoisiane: definizioni e caratterizzazioni. Teorema Fondamentale della Teoria di Galois, e sua applicazione al Teorema Fondamentale dell'Algebra*. Gruppo di Galois del prodotto di un'estensione galoisiana e di un'estensione algebrica*. Gruppo di Galois di un polinomio, suo studio per i polinomi di grado 2,3,4*, per i polinomi ciclotomici, per le equazioni binomie e l'equazione generale di grado n. Formule risolutive delle equazioni algebriche di grado 2, 3, 4, risolvente cubica di Ferrari e sua variante*. Estensioni radicali: definizione e caratterizzazione*. Criterio di risolubilità per radicali.

Segmenti costruibili con riga e compasso e numeri reali costruibili: definizione e criterio sufficiente. Trascendenza di π* secondo il teorema di Lindemann. Costruzioni impossibili. Numeri complessi costruibili: definizione e caratterizzazione*. Criterio di Gauss per la costruibilità dei poligoni regolari.

PARTE QUARTA . **Teoria algebrica dei numeri**

Generalità sui moduli sugli anelli commutativi unitari: definizione, sottomodulo generato da un sottoinsieme, moduli finitamente generati, moduli liberi e non liberi, rango di un modulo libero, moduli liberi su **Z** e loro sottomoduli*, omomorfismi di moduli, moduli quoziente. Anelli e moduli noetheriani: definizioni equivalenti, teorema della base di Hilbert*, quozienti, sottomoduli e somme

dirette finite di moduli noetheriani, moduli noetheriani su un anello noetheriano. Dimostrazione che ogni ideale di un anello commutativo unitario è contenuto in un ideale massimale*.
Elementi interi ed estensioni intere: definizione, caratterizzazione, interi algebrici (caratterizzazione, relazione con i numeri algebrici), criterio sufficiente per le estensioni intere, transitività delle estensioni intere, chiusure intere (dimostrazione di Milne che la chiusura intera è un anello*) , anelli integralmente chiusi, il caso di $\mathbf{Z}$ (e, più in generale, di un UFD). L'anello degli interi D_K di un campo numerico K: teorema di caratterizzazione nel caso di un campo quadratico, D_K come dominio di Dedekind. Relazione tra PID e UFD: caso generale e caso dei domini di Dedekind. Ideali frazionari. Relazione di divisibilità tra ideali. Fattorizzazione e gruppo moltiplicativo degli ideali non nulli di un dominio di Dedekind: criterio di fattorizzazione di Kummer*, numeri interi che sono primi in D_K. Norma, traccia e caratteristica di un elemento in un'estensione finita di campi. Norma di un ideale di D_K: definizione, confronto con le norme dei suoi elementi, proprietà moltiplicativa*.
Gruppo delle classi di ideali: due definizioni equivalenti, relazione con la proprietà di PID, numero delle classi di ideali ed applicazioni alla risolubilità di equazioni diofantee. Cenni alla teoria di Kummer.
Caratterizzazione dei PID mediante la norma di Hasse-Dedekind. Criterio necessario per i domini euclidei. Esempio di un PID che non è un dominio euclideo.
Residui quadratici modulo un primo: definizione, criterio di Eulero, Lemma di Gauss, legge di reciprocità quadratica.