Corso di Laurea in Informatica.
Corso di Algebra

Programma d'esame.

Anno Accademico 2023-24. Proff. Paolo Piazza e Gabriele Viaggi.

Libri di Testo:
[PC] Giulia Maria Piacentini Cattaneo: "Algebra un approccio algoritmico", ed Zanichelli.
[C] Giulio Campanella "Appunti di Algebra 1" ed Nuova Cultura.
[C2] Giulio Campanella "Appunti di Algebra 1. 200 esercizi svolti". Ed. Nuova Cultura.
[S-VG] René Schoof e Lambertus Van Geemen, "Algebra".
[A-dF] Marco Abate e Chiara de Fabritiis "Geometria Analitica con elementi di algebra lineare" edito da McGraw-Hill (terza edizione).

N.B.: per gli argomenti seguiti dal simbolo ($\diamond$) le dimostrazioni sono incluse nel programma d'esame; per gli argomenti seguiti dal simbolo ($*$) le dimostrazioni sono da considerarsi facoltative; per gli argomenti seguiti dal simbolo (†) le dimostrazioni sono da considerarsi omesse. In tutti i casi sono da includere definizioni ed enunciati.

Rapido ripasso di insiemestica. Relazione da un insieme A ad un insieme B. Esempi. Relazioni di equivalenza. Esempi. Classi di equivalenza. Partizione associata ad una relazione di equivalenza ($\diamond$). Relazione di equivalenza associata ad una partizione ($\diamond$) . Relazioni di ordine parziale. Esempi. Diagramma di Hasse. Assiomi di Peano per i numeri naturali. Definizione di ordine totale, somma e prodotto in una terna di Peano. Principio del buon ordinamento.[1] Relazione di congruenza tra interi e descrizione del quoziente. Relazione di divisibilità tra i naturali. Intersezioni e unioni di relazioni di equivalenza. Esempi di relazioni che falliscono esattamente una tra riflessività, simmetria, e transitività. Induzione matematica. Numeri interi ($\diamond$): motivazione e idea della costruzione di $\mathbb{Z}$ come quoziente di $\mathbb{N} \times \mathbb{N}$; descrizione delle classi di equivalenza; definizione di somma e prodotto; l'inclusione naturale di $\mathbb{N}$ in $\mathbb{Z}$ preserva le operazioni.

Strutture algebriche: semigruppo, gruppo, anello. Esempi e prime proprietà. Gli interi sono un anello commutativo unitario ed un dominio di integratà ($\diamond$). Semplici proprietà degli anelli: a0=0, a(-b)=-(ab)=(-a)b, (-a)(-b)=ab. ($\diamond$) Gruppo degli invertibili di un anello unitario ($\diamond$). Definizione di campo. Il campo dei numeri razionali: costruzione ($*$). Teorema: ogni gruppo G ammette una mappa iniettiva in S(G), il gruppo delle applicazione bigettive di G in sé, che preserva le operazioni. Idea e dimostrazione ($*$). Esempi tramite tabelle di moltiplicazione: discussione e classificazione dei gruppi con 3 e 4 elementi. $\mathbb{Z}_n$: buona definizione di somma e prodotto. $\mathbb{Z}_n$ è un anello commutativo con unità ($\diamond$). Se n non è primo allora $\mathbb{Z}_n$ ha divisori dello zero ($\diamond$). Divisori dello zero e legge di cancellazione in un anello commutativo unitario ($\diamond$). Numeri complessi: definizione e proprietà di campo. Teorema fondamentale dell'algebra (solo enunciato).

Divisione con resto in $\mathbb{Z}$. Massimo Comun Divisore di due interi. Identità di Bezout. Algoritmo euclideo. Equazioni Diofantee ax+by=c. Criterio di risolubilità ($\diamond$). Caratterizzazione delle soluzioni. Esempi. Discussione di risolubilità di ax=b

[1] Per i numeri naturali, solo definizioni ed enunciati

in $\mathbb{Z}_n$ e calcolo delle soluzioni $(*)$. Se n è primo allora $\mathbb{Z}_n$ è un campo $(\diamond)$.
Teorema: Sia A un anello unitario con finiti elementi e privo di divisori dello zero. Allora A è un anello di divisione. $(*)$
Il gruppo degli invertibili di $\mathbb{Z}_n$; calcolo della sua cardinalità mediante la funzione di Eulero. $(\diamond)$

Numeri primi. Teorema fondamentale dell'aritmetica $(\dagger)$. Esistono infiniti numeri primi $(*)$. MCD e mcm (minimo comun multiplo) utilizzando il teorema fondamentale dell'aritmetica $(*)$. Sistemi di equazioni congruenziali. Teorema cinese del resto $(\diamond)$. Sistemi riducibili ad un sistema cinese. Prodotto diretto di gruppi/anelli. Omomorfismi di gruppi/anelli. Seconda formulazione del teorema cinese del resto $(\diamond)$. Piccolo teorema di Fermat $(*)$. Teorema di Eulero $(*)$.

Gruppi e sottogruppi. Ordine di un elemento. Se G è finito allora l'ordine di g, $o(g)$, è finito per ogni g in G. Gli elementi $\{1, g, ..., g^{o(g)-1}\}$ sono a coppie distinti. Se $g^t = 1$ allora $o(g)$ divide t. L'ordine di g^s è uguale a $\mathrm{mcm}(o(g), s)/s$. Gruppi ciclici. Esempi. Caratterizzazione dei sottogruppi di $\mathbb{Z}$ e di $\mathbb{Z}_n$ $(\diamond)$. Teorema di struttura per i gruppi ciclici ed i loro sottogruppi $(\diamond)$. Se n è primo allora il gruppo moltiplicativo $\mathcal{U}(\mathbb{Z}_n)$ ed il gruppo additivo $\mathbb{Z}_{(n-1)}$ sono isomorfi $(*)$. Studio del reticolo dei sottogruppi di $\mathbb{Z}_{12}$. Generatori di un gruppo ciclico $(\diamond)$. Gruppi di ordine primo. $\mathcal{U}(\mathbb{Z}_{25}) = \mathbb{Z}_{20}$. Sottogruppo di torsione di un gruppo abeliano. Classificazione dei gruppi di ordine 6: $\mathbb{Z}_6$ e S_3.

Classi laterali destre e sinistre associate ad un sottogruppo H. aH è in generale differente da Ha. Partizione in classi laterali destre (sinistre) di G $(\diamond)$. Teorema di Lagrange $(\diamond)$. Relazione di equivalenza sinistra associata ad un sottogruppo $(\diamond)$. Relazione destra. Le due relazioni sono in generale differenti. Sottogruppo normale. Il nucleo di un omomorfismo è normale $(\diamond)$. Sottogruppi di indice 2 $(\diamond)$. Definizione di gruppo quoziente per un sottogruppo normale H, G/H $(\diamond)$. Automorfismi di un gruppo. Automorfismi interni. Descrizione del nucleo di $G \to \mathrm{Aut}(G)$ (centro di G) $(\diamond)$. $\mathrm{Aut}(\mathbb{Z}_n)$ è isomorfo a $\mathcal{U}(\mathbb{Z}_n)$. Teorema fondamentale di omomorfismo fra gruppi $(\diamond)$.

Gruppo simmetrico [2] definizione e notazioni. Permutazioni con supporto disgiunto commutano. Esempi: trasposizioni, cicli, ordine di un ciclo. Ogni permutazione si decompone unicamente, a meno di riordino dei fattori, in prodotto di cicli *disgiunti*. Esempi. Calcolo dell'ordine di una permutazione in termini della sua decomposizione in cicli. Problema di classificazione delle permutazioni a meno di coniugio. Invariante proveniente dalla decomposizione in cicli. Calcolo del coniugato di un ciclo. Dimostrazione che due permutazioni sono coniugate se e solo se hanno gli stessi invarianti (e calcolo di un elemento coniugante). Calcolo delle classi di coniugio di S_5. Ogni permutazione si scrive come prodotto di trasposizioni. La parità del numero di trasposizioni non dipende dalla decomposizione $(\dagger)$. Decomposizione esplicita in trasposizioni di un ciclo. Il gruppo alternante A_n. S_n è generato da (12) e $(12...n)$. A_n è generato dai 3-cicli.

Sistemi lineari di m equazioni in n incognite. Matrici. Lemma fondamentale $(\diamond)$. Metodo di Gauss per sistemi n per n. Sistemi $n \times n$ triangolari superiori: teorema

[2] Per il gruppo simmetrico si richiedono tutti gli enunciati visti a lezione; dimostrazioni facoltative se non specificato diversamente.

di esistenza e unicità ($*$). Definizione di spazio vettoriale. Lo spazio vettoriale dei segmenti orientati del piano con primo estremo in O, $\mathcal{V}_O^2$; lo spazio vettoriale dei segmenti orientati dello spazio con primo estremo in O, $\mathcal{V}_O^3$. Sottospazi di uno spazio vettoriale. Esempi in $\mathcal{V}_O^2$ e $\mathcal{V}_O^3$. Le soluzioni di un sistema lineare $m \times n$ omogeneo costituiscono un sottospazio vettoriale di $\mathbb{R}^n$ ($\diamond$). Combinazione lineare di k vettori. Span. Lo Span di k-vettori e' un sottospazio vettoriale ($\diamond$). Un sistema è risolubile se e solo se la colonna dei termini noti appartiene allo Span delle colonne della matrice dei coefficienti del sistema ($\diamond$). Dipendenza lineare; esempi ed osservazioni; base di uno spazio vettoriale finitamente generato; esempi; esistenza di una base (†); teorema del completamento (†); dimensione di uno spazio vettoriale. Coordinate associate ad una base. Dimensione di sottospazi. Intersezione e somma di sottospazi; formula di Grassmann (†); somma diretta; supplementari di un sottospazio.

Applicazioni lineari: esempi, proprietà di base; nucleo ed immagine. Iniettività e collegamento con il nucleo ($\diamond$). Teorema della dimensione ($\diamond$); conseguenze; esempi. Teorema di struttura per le soluzioni di un sistema non-omogeneo ($\diamond$). Teorema di Rouche'-Capelli ($\diamond$). $\mathrm{rg}(A) = \mathrm{rg}(A^T)$ (†) . Sistemi a scala; riduzione a scala ($\diamond$). Teorema fondamentale per i sistemi lineari e sue conseguenze ($\diamond$). Equazioni parametriche e cartesiane di sottospazi. $\mathrm{Hom}(V, W)$, anche denotato $\mathcal{L}(V, W)$, e sua struttura di spazio vettoriale. La composizione $\mathrm{Hom}(V, W) \times \mathrm{Hom}(W, Z) \to \mathrm{Hom}(V, Z)$ è bilineare. $\mathrm{End}(V)$ e sua struttura di anello unitario. Gli invertibili di $\mathrm{End}(V)$ sono $GL(V)$ =mappe lineari biunivoche. Caso finito dimensionale: calcolo di $\dim \mathrm{Hom}(V, W) = (\dim V)(\dim W)$. Caso $V = \mathbb{R}^n$ e $W = \mathbb{R}^m$. Corrispondenza biunivoca fra $\mathcal{L}(\mathbb{R}^n, \mathbb{R}^m)$ e $M_{mn}(\mathbb{R})$ (†): matrice associata a una mappa lineare $\mathbb{R}^m \to \mathbb{R}^n$ e mappa lineare associata a una matrice. Prodotto righe per colonne. Proprietà algebriche del prodotto righe per colonne di matrici. Anello delle matrici $n \times n$. Una matrice A è invertibile se e solo se le colonne sono linearmente indipendenti se e solo se le colonne generano $\mathbb{R}^n$. Formula per l'inversa di una matrice 2 x 2. Calcolo dell'inversa di una 3 x 3 tramite il metodo di Gauss.

Definizione di determinante, sue proprietà ($*$). Determinante di A e di una sua ridotta a scala. Sviluppo di Laplace secondo una riga e secondo una colonna. Determinante di una matrice triangolare. Unicità della funzione determinante ($*$). $\mathrm{rg}(A)$, $A \in M_{nn}(\mathbb{R})$, è minore di n se e solo $\det(A) = 0$. Teorema di Binet ($*$).

Matrice associata ad un'applicazione lineare $T : V \to W$ una volta fissata una base in partenza ed una base in arrivo. Notazione. Formula per la matrice di una composizione ($\diamond$). Cambiamento di base. Matrici simili.

Autovalori ed autovettori [3]. Operatori diagonalizzabili. Polinomio caratteristico. Sua struttura (con definizione di traccia). Molteplicità algebrica e geometrica di un autovalore. La molteplicità algebrica è sempre maggiore o uguale della molteplicità geometrica di un autovalore. Autovalori associati ad autovalori distinti sono linearmente indipendenti. Condizioni necessarie e sufficienti per la diagonalizzabilità.

Referenze bibliografiche dettagliate: vedere la pagina web del corso: `https://www1.mat.uniroma1.it/people/piazza/alg-info-23-24.htm`

[3]tutta la parte su autovalori ed autovettori comprende anche le dimostrazioni.