ALGEBRA PER INFORMATICI 2018-19
ELENCO DEGLI ARGOMENTI TRATTATI DURANTE LE LEZIONI

1. Martedì 25 settembre 2018

Informazioni sul corso. Linguaggio: insiemi, elementi, appartenenza, sottoinsiemi, inclusione. Unione, intersezione, differenza, differenza simmetrica e prodotto cartesiano di insiemi. L'insieme vuoto. Applicazioni: concetto; composizione di applicazioni. Esempi di applicazioni: identità, inclusione, altri esempi. La composizione di applicazioni è associativa ma non è commutativa. Applicazioni iniettive, suriettive, invertibili; varie riformulazioni di iniettività e invertibilità. Inversa di un'applicazione invertibile.

2. Mercoledì 26 settembre 2018

Aritmetica modulo 10. Gruppi abeliani, anelli, anelli commutativi, anelli con unità. $\mathbb{Z}$ e $\mathbb{Z}_{10}$ sono anelli commutativi con unità. Relazioni su insieme. Relazioni riflessive, simmetriche, transitive, di equivalenza. Esempi. La congruenza modulo 10 è una relazione di equivalenza.

Classi di equivalenza. $a \sim b \iff a \in [b] \iff [a] = [b]$. Ogni elemento appartiene a qualche classe di equivalenza; classi di equivalenza diverse sono disgiunte. Ogni relazione di equivalenza induce una partizione; ogni partizione induce una relazione di equivalenza. Classi di congruenza modulo 10.

Congruenze modulo $n > 1$. Congruenza modulo 2: le classi di congruenza sono i numeri pari e i numeri dispari.

3. Venerdì 28 settembre 2018

Richiami: $\mathbb{Z}_n$ è un anello commutativo con unità; una relazione di equivalenza su un insieme X induce una partizione di X in classi di equivalenza; insieme quoziente $X/\sim$. Nella lezione precedente abbiamo ricostruito $\mathbb{Z}_n$ come insieme. Operazioni su un insieme quoziente $X/\sim$ indotte da operazioni su X: possono essere ben definite o mal definite. Esempi di buona e cattiva definizione. Le operazioni di $\mathbb{Z}$ ben definiscono operazioni su $\mathbb{Z}_n = \mathbb{Z}/\equiv_n$. Calcolo delle tavole di addizione e moltiplicazione per $\mathbb{Z}_n$ per $n = 2, 3, 4, 5$. Divisione euclidea: $\mathbb{Z}_n$ possiede esattamente n elementi.

Corpi e campi. Esempi di campi: $\mathbb{Q}, \mathbb{R}, \mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_5$. $\mathbb{Z}$ e $\mathbb{Z}_4$ non sono campi. In un campo vale la legge di annullamento del prodotto, pertanto $\mathbb{Z}_n$ non è un campo se n è un numero composto. Se $\mathrm{MCD}(a, n) \neq 1$, allora $[a]$ non è invertibile in $\mathbb{Z}_n$. Esempi.

Calcolo del MCD con l'algoritmo euclideo. Un esempio.

4. Martedì 2 ottobre 2018

L'algoritmo euclideo per il calcolo del MCD: se $a = qb+r$ è una divisione euclidea, allora $\mathrm{MCD}(a, b) = \mathrm{MCD}(b, r)$; di conseguenza l'ultimo resto non nullo nell'algoritmo euclideo fornisce il Massimo Comun Divisore.

L'identità di Bézout: tutti i resti che compaiono durante l'algoritmo euclideo per il calcolo di $\mathrm{MCD}(a, b)$ sono della forma $ha + kb$, dove $h, k \in \mathbb{Z}$; di conseguenza, $\mathrm{MCD}(a, b)$ è di questa forma. Un elemento $[a] \in \mathbb{Z}_n$ è invertibile se e solo se $\mathrm{MCD}(a, n) = 1$; il suo inverso si ottiene calcolando l'identità di Bézout per a ed n. L'anello $\mathbb{Z}_n$ è un campo non appena n sia un numero primo. Il numero degli elementi invertibili in $\mathbb{Z}_n$ si indica con $\varphi(n)$.

Risoluzione di congruenze lineari. Il caso $ax \equiv b \mod n$ quando a è invertibile modulo n. Cosa accade se a non è invertibile?

5. Mercoledì 3 ottobre 2018

Risoluzione di congruenze lineari: caso generale. Varie formulazioni equivalenti per una congruenza lineare e diversi tipi di risposta. Esempi vari.

Il teorema cinese dei resti. Un esempio di risoluzione di un sistema di congruenze in forma standard. Le ipotesi del teorema sono necessarie: esempi di non esistenza e non unicità delle soluzioni. Una dimostrazione concettuale del teorema cinese dei resti.

6. Venerdì 5 ottobre 2018

Alcune conseguenze dell'identità di Bézout: se a divide bc e $\mathrm{MCD}(a, b) = 1$, allora a divide c; se un numero primo p divide bc, allora p divide almeno uno tra a e b; se a, b dividono c e $\mathrm{MCD}(a, b) = 1$, allora ab divide c; se una funzione $f : \mathbb{R} \to \mathbb{R}$ è sia $a-$periodica che $b-$periodica, allora è anche $\mathrm{MCD}(a, b)-$periodica.

Il concetto di omomorfismo. La proiezione al quoziente $\mathbb{Z} \to \mathbb{Z}_n$ è un'omomorfismo di anelli; quando $\mathrm{MCD}(m, n) = 1$, la bigezione $\mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ è un omomorfismo di anelli se sul prodotto cartesiano definiamo operazioni componente per componente.

Gruppi: definizione e prime proprietà. Esempi da anelli. Il gruppo simmetrico: definizione. Esercizio: S_3 non è abeliano.

7. Martedì 9 ottobre 2018

Ancora sul gruppo simmetrico: elenco degli elementi di S_3 e vari esempi di composizione. Il gruppo S_3 non è abeliano. Proprietà dell'inverso: $1^{-1} = 1, (a^{-1})^{-1} = a, (ab)^{-1} = b^{-1}a^{-1}$. Verifica in alcuni casi. Potenze di un elemento: $g^m g^n = g^{m+n}, g^0 = 1, (g^m)^n = g^{mn}$.

Notazione ciclica di permutazioni e sua (non) unicità. Calcolo della composizione e dell'inverso. Permutazioni che insistono su sottoinsiemi disgiunti commutano tra loro. Il gruppo simmetrico S_n ha ordine $n!$.

Gruppi: esempi già visti; prodotto diretto di gruppi e suo ordine; due realizzazioni isomorfe di V_4. Sottogruppi: due definizioni equivalenti. Esempi di sottogruppi: sottogruppi banali; i numeri pari costituiscono un sottogruppo di $(\mathbb{Z}, +)$; sottogruppo (g) generato da un elemento $g \in G$. Il sottogruppo generato da un elemento può essere finito.

8. Mercoledì 10 ottobre 2018

Richiami. L'intersezione di sottogruppi è un sottogruppo; l'unione di sottogruppi non è necessariamente un sottogruppo. Sottogruppo generato da un sottoinsieme; nel caso di un sottoinsieme contenente un singolo elemento, coincide con il concetto di sottogruppo generato da un elemento.

Sottogruppi di $(\mathbb{Z}, +)$: sono tutti della forma (n) per qualche $n \geq 0$. Se $(a) \cap (b) = (m)$, allora m è il minimo comune multiplo tra a e b. Somma tra sottogruppi di $(\mathbb{Z}, +)$: se $(a) + (b) = (d)$, allora $d = \mathrm{MCD}(a, b)$.

Congruenza modulo un sottogruppo $H < G$: definizione; è una relazione di equivalenza; le classi di congruenza sono le classi laterali sinistre aH. Analogia con la congruenza modulo n negli interi.

Omomorfismi di gruppi: definizione e prime proprietà. Vari esempi. Nucleo e immagine di omomorfismi: sono sottogruppi del gruppo di partenza e del gruppo di arrivo.

9. Venerdì 12 ottobre 2018

Richiami della lezione precedente. Un'omomorfismo $f : G_1 \to G_2$ è suriettivo se e solo se $\mathrm{Im}\, f = G_2$ ed è iniettivo se e solo se $\ker f = \{1\}$; più precisamente, $f(x) = f(y)$ esattamente quando $x \equiv y \mod \ker f$. Indice di un sottogruppo: se $f : G_1 \to G_2$ è un omomorfismo di gruppi, allora $|\mathrm{Im}\, f| = [G_1 : \ker f]$.

Ordine di elementi in un gruppo. Se $g \in G$ l'applicazione $f : (\mathbb{Z}, +) \to G$ definita da $f(n) = g^n$ è un omomorfismo di gruppi la cui immagine è (g). L'elemento $g \in G$ ha ordine finito d se e solo se (g) ha ordine d; g ha ordine infinito se e solo se (g) ha ordine infinito.

Il teorema di Lagrange. Enunciato. Preliminari: le classi di congruenza modulo H sono una partizione di G, e tutti i laterali di H in G hanno la stessa cardinalità; H è un laterale di H. $G = [G : H]|H|$.

Conseguenze del teorema di Lagrange: se $H < G$, allora sia $|H|$ che $[G : H]$ sono divisori di $|G|$. L'ordine di $g \in G$ divide $|G|$. Vari esempi.

10. Martedì 16 ottobre 2018

Gruppi isomorfi. Gruppi ciclici; un gruppo ciclico è isomorfo a $(\mathbb{Z}, +)$ se è infinito, e a $(\mathbb{Z}_n, +)$ se ha ordine n. Gruppi di ordine primo sono ciclici. I gruppi ciclici sono abeliani.

Classificazione dei gruppi di ordine ≤ 7. Alcune premesse: un gruppo in cui ogni elemento ha ordine 1 o 2 è abeliano; ogni gruppo di ordine pari possiede elementi di ordine 2.

I gruppi di ordine $2, 3, 5, 7$ sono ciclici. Gruppi di ordine 4: sono ciclici se possiedono elementi di ordine 4 oppure isomorfi a V_4 se hanno solo elementi di ordine 1 e 2. Gruppi di ordine 6: hanno sempre elementi di ordine 2; sono ciclici se hanno elementi di ordine 6; devono possedere elementi di ordine 3; sono isomorfi a $(\mathbb{Z}_6, +)$ oppure a S_3.

Se $g \in G$, allora $g^{|G|} = 1$. Due esempi, di cui uno interessante. Se $\mathrm{MCD}(a, n) = 1$; allora $a^{\varphi(n)} \equiv 1 \mod n$. I casi $n = 7$ e $n = 15$.

11. Mercoledì 17 ottobre 2018

Piccolo teorema di Fermat: se p è primo, allora $a^p \equiv a \mod p$. Vari esercizi: calcolo di $2^{1234} \mod 23$; $2019^{2019} \mod 100$ in due modi; $2018^{2018} \mod 100$ utilizzando il teorema cinese dei resti. Ordine di $[6]$ in $\mathbb{Z}_{25}^{\times}$; ordine di $[6]$ e di $[15]$ in $(\mathbb{Z}_{25}, +)$.

Crittografia RSA.

12. Venerdì 19 ottobre 2018

Gruppo diedrale D_n dell'n-agono regolare: possiede $2n$ elementi; contiene il sottogruppo ciclico C_n costituito dalle n rotazioni; contiene anche n simmetrie rispetto a rette. Se r è un generatore di C_n e s è una (qualsiasi) simmetria, allora le rotazioni sono gli elementi $r^i, i = 0, \ldots, n-1$ mentre le simmetrie sono gli elementi $sr^i, i = 0, \ldots, n-1$. Si ha $r^i s = sr^{-i}$ e $s^{-1} = s$. Tavola moltiplicativa. Il gruppo diedrale non è abeliano.

Segno di permutazioni. Il segno di una permutazione σ dipende dal numero di inversioni di σ. L'applicazione che associa a ciascuna permutazione il suo segno è un omomorfismo di gruppi. Segno di trasposizioni; segno di n-cicli. Segno di una permutazione espressa in notazione ciclica. Permutazioni pari e dispari. Sottogruppo alterno $A_n < S_n$ composto dalle sole permutazioni pari: contiene $n!/2$ elementi. In generale, se $f : G \to H$ è un omomorfismo di gruppi, allora $|\mathrm{Im}\, f| = [G : \ker f]$.

13. MARTEDÌ 23 OTTOBRE 2018

Richiami. Calcolo del segno di una permutazione. Calcolo dell'ordine di una permutazione attraverso la sua struttura ciclica.

Una lunga divagazione: gruppi quozienti e sottogruppi normali. Se $\sim$ è una relazione di equivalenza su un gruppo G tale che $[a][b] = [ab]$ sia ben definita, allora $\sim$ è la congruenza modulo un sottogruppo normale. Esempi di sottogruppi normali: i sottogruppi banali sono normali; ogni sottogruppo di un gruppo abeliano è normale; i nuclei di omomorfismi sono normali. Formulazioni equivalenti della normalità di un sottogruppo. Il sottogruppo alterno $\mathrm{A}_n < \mathrm{S}_n$ è normale. Un sottogruppo di indice 2 è necessariamente normale; $\mathrm{C}_n < \mathrm{D}_n$ è normale.

Relazione di coniugio: è di equivalenza. Un sottogruppo è normale se e solo se è unione di classi di coniugio.

14. MERCOLEDÌ 24 OTTOBRE 2018

Prime proprietà della relazione di coniugio: un elemento è centrale se e solo se è coniugato solo a se stesso; elementi coniugati hanno lo stesso ordine. Classi coniugate in S_3; classi coniugate in un gruppo abeliano.

Centralizzatore $Z(x)$ di un elemento $x \in G$ e centro $Z(G)$ di un gruppo G: sono sottogruppi di G. Due elementi $a, b \in G$ coniugano x nello stesso elemento se e solo se giacciono nella stessa classe di congruenza modulo $Z(x)$ in G. Il numero di coniugati di x in G è $[G : Z(x)]$; in particolare, divide $|G|$. Centralizzatore di elementi in S_3. Classi coniugate in D_5. Esercizio: calcolare le classi coniugate in D_n, distinguendo n pari da n dispari.

Prodotto diretto di sottogruppi. G si dice prodotto diretto dei suoi sottogruppi H, K se: sono entrambi normali; $H \cap K = \{1\}$; $HK = G$. In tal caso, G è isomorfo a $H \times K$. Esempio: $\mathbb{Z}_6$ è isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_3$. Prossimamente: gruppi con p^2 elementi, quando p è un numero primo.

15. VENERDÌ 26 OTTOBRE 2018

Prodotto diretto di sottogruppi: se G è un gruppo finito, $|H||K| = |G|$ è equivalente a verificare che $HK = G$, se $H \cap K = \{1\}$.

Gruppi di ordine p^2: le classi di coniugio contengono un solo elemento se sono centrali e p elementi se non lo sono; il centro ha ordine multiplo di p; il centro non può contenere solo p elementi; un gruppo di ordine p^2 è abeliano. Gruppi abeliani di ordine p^2: sono isomorfi a $\mathbb{Z}_{p^2}$ se ciclici; sono isomorfi a $\mathbb{Z}_p \times \mathbb{Z}_p$ se non ciclici.

Classi di coniugio in S_n: due permutazioni sono coniugate se e solo se hanno la stessa struttura ciclica. Classi coniugate in S_4 e S_5 e loro cardinalità; sottogruppi normali di S_4 e S_5.

16. MERCOLEDÌ 31 OTTOBRE 2018

Teorema di Cauchy per gruppi abeliani finiti. Classi di coniugio nei gruppi alterni.

17. MARTEDÌ 6 NOVEMBRE 2018

Correzione della prova di esonero

18. MERCOLEDÌ 7 NOVEMBRE 2018

Primo esonero.

19. VENERDÌ 9 NOVEMBRE 2018

Algoritmo probabilistico di primalità di Solovay-Strassen: congruenze quadratiche; simbolo di Legendre; legge di reciprocità quadratica; simbolo di Jacobi; teorema di Solovay-Strassen.

20. MARTEDÌ 13 NOVEMBRE 2018

Un campo con quattro elementi. In un campo finito, tutti gli elementi $\neq 0$ hanno lo stesso ordine primo p. L'ordine di un campo finito è p^n, dove p è primo e $n \geq 1$.

Un esempio di riscaldamento: il campo $\mathbb{Q}(\sqrt{2})$. Numeri complessi. Somma e prodotto di numeri complessi. Coniugazione complessa, norma complessa. Rappresentazione grafica dei numeri complessi nel piano di Argand-Gauss. Interpretazione geometrica della somma e del prodotto di numeri complessi. Ogni numero complesso non nullo ha un inverso moltiplicativo. I numeri complessi formano un campo.

21. VENERDÌ 16 NOVEMBRE 2018

Ancora sui numeri complessi. Norma e argomento. Radici cubiche di 1. Radici quadrate di i. Il teorema fondamentale dell'algebra: varie formulazioni equivalenti.

Algebra lineare: due esempi motivanti. Definizione di K-spazio vettoriale; $\mathbb{R}^n$ è uno spazio vettoriale reale.

22. MARTEDÌ 20 NOVEMBRE 2018

Vari esempi di spazi vettoriali e di applicazioni lineari. Corrispondenza tra applicazioni lineari $K^m \to K^n$ e matrici $n \times m$ a coefficienti in K. Somma, multiplo e composizione di applicazioni lineari sono lineari. La matrice associata alla somma di applicazioni lineari è la somma, coefficiente per coefficiente, delle matrici associate agli addendi; la matrice associata a cT si ottiene da quella associata a T moltiplicando tutti i coefficienti per c. Matrice associata alla composizione di applicazioni lineari: un esempio.

23. Mercoledì 21 novembre 2018

.

La composizione tra applicazioni lineari si traduce nel prodotto righe per colonne delle corrispondenti matrici. Proprietà del prodotto righe per colonne: $A(BC) = (AB)C, A(B+C) = AB + AC, (A+B)C = AC + BC$. Matrice identità I: $AI = IA = A$.

Sottospazi vettoriali: definizione; sottospazi banali; retta generata da un elemento $\neq 0$; sottospazi vettoriali di $\mathbb{R}^2$ e $\mathbb{R}^3$. Nucleo e immagine di un'applicazione lineare: sono sottospazi vettoriali; un'applicazione lineare è iniettiva se e solo se il nucleo contiene soltanto il vettore nullo.

Il calcolo del nucleo di un'applicazione lineare $K^m \to K^n$ è equivalente alla risoluzione di un sistema lineare omogeneo di n equazioni in m incognite. Un esempio.

24. Venerdì 23 novembre 2018

Risoluzione di sistemi lineari attraverso il procedimento di eliminazione di Gauss-Jordan: vari esempi. Procedimento di eliminazione su matrici: pivot, forma a scala. Il numero dei pivot è limitato sia dal numero delle righe che da quello delle colonne.

Se c'è un pivot sulla colonna dei termini noti, il sistema non ammette soluzioni. Se non c'è un pivot sulla colonna dei termini noti, il sistema ammette sempre soluzioni, e queste sono parametrizzate dalle incognite relative a colonne che non contengono pivot.

25. Martedì 27 novembre 2018

Il concetto di combinazione lineare. Generatori (lineari) di sottospazi vettoriali; sottospazio vettoriale generato da elementi dati. Alcuni insiemi di generatori sono più economici di altri: dipendenza e indipendenza lineare. Concetto di base. Modi per costruire una base: da ogni insieme di generatori si estrae una base; ogni insieme di vettori linearmente indipendenti si completa ad una base.

26. Mercoledì 28 novembre 2018

Concetto di dimensione di uno spazio vettoriale: due basi dello stesso spazio vettoriale hanno lo stesso numero di elementi. Affermazione tecnica: se $v_1, \dots, v_n$ è una base di V e $w_1, \dots, w_k, k \leq n$ sono elementi linearmente indipendenti di V; allora posso sostituire k degli elementi della base, opportunamente scelti, con i k vettori $w_1, \dots, w_k$ in modo da ottenere un'altra base di V. Il caso $k = 1$; passo induttivo. Se $\dim V = n$, più di n elementi di V devono essere linearmente dipendenti, e meno di n elementi di V non lo generano. Se $\dim V = n$, n elementi di V lo generano se e solo se sono linearmente indipendenti se e solo se sono una base.

27. Venerdì 30 novembre 2018

Riassunto delle ultime lezioni. Come si verifica se degli elementi di $\mathbb{R}^n$ sono linearmente indipendenti: mettendoli in colonna in una matrice e controllando se sono tanti quanti i pivot al termine dell'eliminazione di Gauss. Osservazione: anche se sono linearmente dipendenti, quelli nelle colonne corrispondenti alle posizioni dei pivot sono linearmente indipendenti.

Teorema della dimensione: se $T : V \to W$ è lineare, allora $\dim \ker T + \dim \operatorname{Im} T = \dim V$. Applicazione al caso $T : \mathbb{R}^m \to \mathbb{R}^n$: $\dim \ker T = \dim V -$ il numero dei pivot, quindi $\dim \operatorname{Im} T$ coincide con il numero dei pivot. Concetto di rango di un'applicazione lineare e di una matrice. Il rango di una matrice è la dimensione del sottospazio vettoriale generato dalle sue colonne.

Precisazione: le colonne di una matrice corrispondenti alla posizione dei pivot al termine dell'eliminazione di Gauss sono una base del sottospazio vettoriale generato dalle colonne. Applicazione di questo fatto in un esercizio.

28. Martedì 4 dicembre 2018

Iniettività, suriettività, invertibilità di un'applicazione lineare in termini del suo rango. Teorema di Rouché-Capelli. Nuova interpretazione del rango di una matrice: le manipolazioni dell'eliminazione di Gauss non modificano il sottospazio vettoriale generato dalle righe di una matrice, e le righe non nulle al termine dell'eliminazione di Gauss sono linearmente indipendenti. Pertanto, il rango di una matrice coincide con la dimensione del sottospazio vettoriale generato dalle sue righe. Il teorema di struttura per la controimmagine di un elemento attraverso un'applicazione lineare. Applicazioni del teorema di struttura: un sistema lineare omogeneo ha per soluzioni un sottospazio vettoriale; un sistema lineare non omogeneo, quando ha soluzioni, descrive un insieme parallelo al sottospazio vettoriale delle soluzioni del sistema omogeneo associato; equazioni differenziali lineari a coefficienti costanti; primitiva di una funzione.

29. Mercoledì 5 dicembre 2018

Calcolo dell'inversa di una matrice invertibile per mezzo dell'eliminazione di Gauss. Possibili usi della matrice inversa: risoluzione di un sistema lineare di n equazioni in n incognite nel quale la matrice dei coefficienti è invertibile. Coordinate in una base: definizione, calcolo e matrice di cambiamento di coordinate.

Il determinante di matrici 2×2 come area di parallelogrammi. Proprietà di normalizzazione, alternanza e multilinearità: queste proprietà permettono il calcolo del determinante. Comportamento del determinante rispetto alle manipolazioni dell'eliminazione di Gauss. Il determinante di una matrice quadrata è non nullo se e solo se le righe (colonne) della matrice sono linearmente indipendenti. Un esempio di calcolo di determinante di una matrice 3×3.

30. Venerdì 7 dicembre 2018

Unicità della funzione determinante. Esistenza: espressione esplicita che calcola il determinante di una matrice per mezzo di una somma sulle permutazioni. Casi $n = 1, 2, 3$. Il determinante di una matrice coincide con quello della sua trasposta; pertanto, la funzione determinante è alternante e separatamente lineare anche nelle colonne della matrice argomento.

Formule di Cramer. Formula di Binet (senza dimostrazione). Una matrice quadrata ha le righe (colonne) linearmente indipendenti se e solo se il suo determinante è $\neq 0$. Sviluppo di Laplace lungo righe e colonne (senza dimostrazione). Determinante di matrici diagonali e triangolari.

31. Martedì 11 dicembre 2018

Calcolo del rango per mezzo del determinante. Teorema degli orlati. Calcolo delle equazioni cartesiane di sottospazi di $\mathbb{R}^n$ dei quali siano dati generatori.

Matrice associata ad un'applicazione lineare una volta fatta una scelta di una base in partenza e di una in arrivo. Come si associa la matrice? Come si usa la matrice? Questa costruzione generalizza la matrice associata ad un'applicazione $\mathbb{R}^m \to \mathbb{R}^n$.

Il concetto di diagonalizzazione. Se la matrice associata ad un'applicazione lineare $T : V \to V$ rispetto ad una base di V, utilizzata sia in partenza che in arrivo, è diagonale, allora ogni elemento della base è mandato da T in un suo multiplo. Esempi di operatori diagonalizzabili su $\mathbb{R}^2$.

32. Venerdì 14 dicembre 2018

Diagonalizzabilità: autovalori, autospazi, autovettori, polinomio e equazione caratteristica. Molteplicità algebrica e geometrica di autovalori. La molteplicità geometrica di un autovalore è sempre $\leq$ della corrispondente molteplicità algebrica.

Se $T : V \to V$ è un endomorfismo di uno spazio vettoriale V di dimensione finita, e la somma delle molteplicità geometriche degli autovalori di T è inferiore a $\dim V$, allora non possono esistere basi di V che diagonalizzino T.

33. Martedì 18 dicembre 2018

Riassunto generale sulla diagonalizzazione. Un lemma tecnico: se la somma di vettori presi da k autospazi distinti è il vettore nullo, allora ciascuno dei k addendi è il vettore nullo (in termini tecnici che non abbiamo definito: la somma di autospazi è diretta).

Se la somma delle molteplicità geometriche degli autovalori di $T : V \to V$ coincide con $\dim V$, allora T è diagonalizzabile. Vari esempi.

34. Mercoledì 19 dicembre 2018

Calcolo della potenza di una matrice diagonalizzabile. Page-rank.

Il corso, da GOMP, è di 84 ore: verranno svolte, pertanto, 32 lezioni da due ore e mezzo e 2 lezioni da due ore. Da calendario accademico, abbiamo 39 giorni di lezione; di conseguenza, salteranno cinque lezioni.

Dipartimento di Matematica, Università degli studi di Roma – "La Sapienza"
E-mail address: `dandrea@mat.uniroma1.it`