Dimostrazioni di Matematica del Discreto Richieste all'esame

1) Elemento Neutro Unico
2) congruenza modulo n è una relazione di equivalenza in Z
3) Esistenza ed unicità del quoziente e del resto
4) $(R^n, +)$ è un gruppo abeliano
5) $(Mat_{n \times m} R^n, +)$ è un gruppo abeliano
6) 0 è soluzione del sistema $Ax = b \Leftrightarrow b = 0$
7) Sol(A|0) è un sottospazio vettoriale
8) se U è sottoinsieme di V e U è sottospazio vettoriale allora $0V \in U$
9) il sottoinsieme <V> è un sottospazio vettoriale
10) L'intersezione di due sottospazi vettoriali è un sottospazio vettoriale
11) L'unione di due sottospazi vettoriali non per forza è sottospazio vettoriale
12) Se $f : V \rightarrow W$ è un'applicazione lineare, allora $f(0V) = 0W$
13) Immagine e Ker sono sottospazi vettoriali
14) la matrice rappresentativa rispetto ad una base di autovettori è diagonale
15) V spazio vettoriale su K di dimensione n. ⇨ V isomorfo allo spazio vettoriale K^n

Elemento Neutro Unico [PDF 2 pag 11]

Teorema: *Se ★ è dotata di elemento neutro e, tale elemento è univocamente determinato (ossia un'operazione non può ammettere più di un elemento neutro).*

Dimostrazione:

Supponiamo che e1 e e2 siano elementi neutri. Si ha

$$e1 \star e2 = e1 \qquad e1 \star e2 = e2$$

(la prima uguaglianza vale perché e2 è un elemento neutro, la seconda perché e1 è un elemento neutro). Pertanto e1 = e2

congruenza modulo n è una relazione di equivalenza in Z [PDF 3 pag 17]

Teorema: *La congruenza modulo n è una relazione di equivalenza in Z.*

Dimostrazione:

1) **Prop. Riflessiva:**
   $a \sim a \pmod n \ \forall a \in Z$ infatti $a-a=0=0*n$ $(h=0)$
2) **Prop. Simmetrica:**
   $a \sim b \pmod n \Rightarrow \exists h \in Z$ tale che $a - b = h \cdot n$ allora $b - a = (-h) \cdot n$ e quindi $b \sim a \pmod n$.
3) **Prop. Transitiva:**

   $a \sim b \pmod n$ e $b \sim c \pmod n \Rightarrow$

   $\exists h1 \in Z$ tale che $a - b = h1 \cdot n$ e $\exists h2 \in Z$ tale che $b - c = h2 \cdot n$

   allora $a - c = a - b + b - c = h1n + h2n = (h1 + h2) \cdot n$ e quindi $a \sim c \pmod n$.

Esistenza ed unicità del quoziente e del resto [PDF 4 pag 8]

Teorema: *Siano a, b ∈Z con b ≠ 0. Allora* ***esistono e sono unici*** *q,r ∈Z tali che*

1) *a=b*1+r (q=quoziente e r=resto)*
2) *0 ≤ r < |b|*

Dimostrazione:

1) **Unicità:** Supponiamo che ci siano due valori possibili sia per il quoziente (q e q') sia per il resto (r e r'), e mostriamo che in realtà coincidono.

   a = b · q + r con 0 ≤ r < |b| ed anche

   a = b · q' + r' con 0 ≤ r' < |b|

   se sottraiamo membro a membro le due uguaglianze:

   0 = b · (q − q') + (r − r') → |b| · |q − q' | = |r − r' |, per le condizioni ho che |r − r' |<|b| e quindi per rendere vera questa uguaglianza, per forza |q − q' |<1. Essendo nei naturali so che q − q' devono essere lo stesso numero per essere <1 e quindi lo stesso vale per r.

   Essendo negli interi positivi (la positività è dettata dal modulo) allora il numero che va a moltiplicare B è per forza zero. A questo punto si ha |b|*0=r'-r e quindi ottengo che r=r'

2) **Esistenza:** per induzione su a fissato b
   - **base**: a=0 allora a = 0 = b*0 + 0, ovvero q ed r esistono e sono q=r=0
   - **Ipotesi induttiva**: considero a'<a e vedo che se a'<a allora esistono q' e r' tali che

     a'=bq'+r' (0 ≤ r' < |b|) e vogliamo usarla per dimostrare che esistono q ed r t.c:

     a=bq+r (0 ≤ r <|b|)

   - se a > 0 ma a < b allora q=0 e r=a
   - se a ≥ b allora a-b ≥ b e a-b < a. Dato che a' < a posso applicare l'ipotesi induttiva con a'=a-b, di conseguenza esistono q' ed r' con 0 ≤ r' < |b| tali che

     a-b = b*q' + r' ovvero a = b*(q' + 1)+r'

   - abbiamo trovato q ed r tali che a=bq + r e sono **q=q' + 1** ed **r=r'**
   - essendo induzione il teorema vale ∀a≥0

$(R^n , +)$ è un gruppo abeliano [PDF 6 pag. 6]

Teorema: *la coppia $(R^n +)$ è un gruppo abeliano, ovvero l'operazione + definite su R^n è associativa, commutativa, ammette elemento neutro ed ogni elemento ammette un inverso*

Dimostrazione:

1) **Prop. Associativa:** bisogna mostrare che $\forall \underline{x}, \underline{y}, \underline{z} \in \mathbf{R^n}$ si ha che $(\underline{x} + \underline{y}) + \underline{z} = \underline{x} + (\underline{y} + \underline{z})$. Per dimostrare basta prendere elementi generici, calcolare i due membri dell'uguaglianza e confrontarli.

2) **Esistenza Neutro:** bisogna mostrare che $\exists \underline{e} \in \mathbf{R}$ n tale che $\forall \underline{x} \in \mathbf{R^n}$ si ha $\underline{x} + \underline{e} = \underline{x} = \underline{e} + \underline{x}$. Per dimostrare basta prendere come elemento e il vettore $\underline{0}$

3) **Esistenza dell'inverso:** Devo mostrare che $\forall \underline{x} \in \mathbf{R^n} \ \exists \underline{y} \in \mathbf{R^n}$ tale che $\underline{x} + \underline{y} = \underline{e} = \underline{y} + \underline{x}$. Per dimostrare basta scegliere come $\underline{y}$ un vettore cui le componenti sono -xi

4) **Prop. Commutativa:** bisogna mostrare che $\forall \underline{x}, \underline{y} \in \mathbf{R^n}$ si ha che $(\underline{x} + \underline{y}) = (\underline{y} + \underline{x})$. si dimostra come la prop. associativa

$(Mat_{n\,x\,m}\, R^n , +)$ è un gruppo abeliano [PDF 6 pag. 18]

Teorema: *la coppia $(Mat_{n\,x\,m}\, R^n , +)$ è un gruppo abeliano, ovvero l'operazione + definite su $Mat_{n\,x\,m}\, R^n$ è associativa, commutativa, ammette elemento neutro ed ogni elemento ammette un inverso*

Dimostrazione Analoga a quella sopra.

0 è soluzione del sistema $Ax = b \Leftrightarrow b = 0$

Teorema: *0 è soluzione del sistema $Ax = b \Leftrightarrow b = 0$*

Dimostrazione:

se $\underline{b} = \underline{0}$, cioè se si considera un sistema omogeneo, allora $\underline{x} = \underline{0}$ è soluzione (perché infatti $A\underline{0} = \underline{0}$)

Se so che $\underline{0}$ è soluzione, allora so anche che $\underline{b} = A\underline{0} = \underline{0}$

Sol(A|$\underline{0}$) è un sottospazio vettoriale

Teorema: *l'insieme delle soluzioni di un sistema omogeneo sono sottospazio vettoriale*

Dimostrazione:

per rouche' capelli 2 si ha che se x1 e x2 sono soluzioni di Ax = $\underline{0}$ allora anche a$\underline{x1}$+b$\underline{x2}$ è una soluzione. Bisogna verificare le proprietà del STSP.

1) **Somma chiusa:** A(a$\underline{x1}$+b$\underline{x2}$) = Aa$\underline{x1}$ + Ab$\underline{x2}$. Imponiamo a = b = 1 e vediamo che
   A($\underline{x1}$+$\underline{x2}$) = A$\underline{x1}$ + A$\underline{x2}$ → A($\underline{x1}$+$\underline{x2}$) = $\underline{0}$ e A$\underline{x1}$ + A$\underline{x2}$ = $\underline{0}$ + $\underline{0}$ = $\underline{0}$

2) **Prodotto per scalare chiuso:** A(k$\underline{x1}$) = kA($\underline{x1}$). Imponiamo k = 1 e vediamo che A(x1)=A(x1) = $\underline{0}$ = $\underline{0}$

3) **Zero incluso:** Si sa che in un sistema omogeneo esiste la soluzione banale e quindi lo zero è incluso

se U è sottoinsieme di V e U è sottospazio vettoriale allora $\underline{0V}$ ∈ U [PDF 10 pag 24]

Teorema: *se U è sottoinsieme di V e U è sottospazio vettoriale allora $\underline{0V}$ ∈ U*

Dimostrazione:

Consideriamo U come sottoinsieme di V allora U è STSP di V se è chiuso rispetto alla somma e al prodotto per uno scalare.

Quindi se U è STSP allora ∀k ∈ K e ∀$\underline{u}$ ∈ U si ha che k$\underline{u}$ ∈ U.

Consideriamo k=0k e vediamo che **0k$\underline{u}$ = $\underline{0v}$** e quindi **$\underline{0v}$ ∈ U**

<V> è un sottospazio vettoriale

Teorema: *Sia V un K-spazio vettoriale e v ∈ V un vettore in V, tale che v ≠0 allora l'insieme*

***<$\underline{v}$> := {$\underline{w}$ ∈ V : ∃k ∈ K con $\underline{w}$ = k$\underline{v}$}** si chiama spazio generato da $\underline{v}$ ed è un sottospazio vettoriale*

Dimostrazione:

1) Considero due elementi $\underline{w1}$,$\underline{w2}$ ∈ <$\underline{v}$>. Allora esistono k1 e k2 tali che

   $\underline{w1}$= (k1) $\underline{v}$ e **$\underline{w2}$ = (k2) $\underline{v}$.**

   Considero la **somma** $\underline{w1}$+$\underline{w2}$ per verificare che sia un elemento di <v> e vediamo che

   $\underline{w1}$ + $\underline{w2}$ = **(k1 + k2) $\underline{v}$** e quindi anche $\underline{w1}$+$\underline{w2}$ è multiplo di $\underline{v}$ → **$\underline{w1}$ + $\underline{w2}$ ∈ <$\underline{v}$>**

1) Considero il prodotto per uno scalare e si vede che anche lui sarà un multiplo dell'elemento dello spazio generato da $\underline{v}$

L'intersezione di due sottospazi vettoriali è un sottospazio vettoriale

Teorema: Sia X uno spazio vettoriale. Siano U e V due sottospazi. Allora U ∩ V è sottospazio vettoriale.

Dimostrazione: Si verificano le proprietà dei sottospazi vettoriali

1) **Chiusura rispetto alla somma**
   Siano $\underline{x}$, $\underline{y} \in U \cap V$. In particolare se

   1) $\underline{\mathbf{x}} \in (U \cap V) \Rightarrow \underline{\mathbf{x}} \in U, \underline{\mathbf{x}} \in V$
   2) $\underline{\mathbf{y}} \in (U \cap V) \Rightarrow \underline{\mathbf{y}} \in U, \underline{\mathbf{y}} \in V$

   Di conseguenza

   1) $\underline{\mathbf{x}} + \underline{\mathbf{y}} \in U$
   2) $\underline{\mathbf{x}} + \underline{\mathbf{y}} \in V$

   Quindi $\underline{\mathbf{x}} + \underline{\mathbf{y}} \in (U \cap V)$

2) **Chiusura rispetto al prodotto per scalare**
   Se $\underline{x} \in (U \cap V)$, $k \in K$ allora:

   1) $\underline{x} \in U \Rightarrow k\underline{x} \in U$
   2) $\underline{x} \in V \Rightarrow k\underline{x} \in V$

   Quindi $\mathbf{k}\underline{\mathbf{x}} \in (U \cap V)$

   Lo zero non va dimostrato perché è ovvio che sia incluso. Inoltre la intersezione tra due insieme è un sottoinsieme dei due insiemi, quindi, come dimostrato prima, lo zero è incluso a prescindere.

L'unione di due sottospazi vettoriali non per forza è sottospazio vettoriale

Teorema: L'unione di due sottospazi vettoriali non per forza è sottospazio vettoriale

Dimostrazione: Si prenda come esempio il sottospazio di vettori R^3 con x1=0 unito con sottospazio vettoriale di R^3 con x3=0. Se uniamo esce il sottoinsieme con x1 = 0 o x3 = 0.

Se sommiamo (0,1,3) + (1,2,0) si ottiene (1,3,3) che non appartiene all'unione

Se f : V → W è un'applicazione lineare, allora f($\underline{0V}$) = $\underline{0W}$

Teorema: Se f : V → W è un'applicazione lineare, allora f($\underline{0V}$) = $\underline{0W}$

Dimostrazione:

Sia f una applicazione lineare. Allora $\forall \underline{\mathbf{v}} \in \mathbf{V}$ e per ogni $\mathbf{k} \in \mathbf{K}$ si ha $\mathbf{f(k\underline{v}) = k\, f(\underline{v})}$.

Se $k=0_k$ allora si ha $\mathbf{f(\underline{0}_V) = f(0_K * v1) = 0_K * f(\underline{v1}) = \underline{0}_W}$

Ker è Sottospazio vettoriale

Teorema: il sottoinsieme **ker(f) = {$\underline{v} \in V : f(\underline{v}) = \underline{0}_w\} \subset V$** è un sottospazio vettoriale di V.

Dimostrazione: Si verificano le proprietà dei STSP:

1) **Chiusura rispetto a somma**
   Siano $\underline{v1}$, $\underline{v2} \in$ ker(f), allora **f ($\underline{v1}$) = $\underline{0}_w$** e **f ($\underline{v2}$) = $\underline{0}_w$** quindi f ($\underline{v1}$ + $\underline{v2}$) = f($\underline{v1}$) + f($\underline{v2}$) = **0w + 0w → $\underline{v1}$ + $\underline{v2}$ ∈ ker(f)**

2) **Chiusura rispetto a prodotto scalare**
   Sia $\underline{v} \in$ ker(f) e k ∈ K allora f($\underline{v}$) = 0w e f (k $\underline{v}$) = k* f ($\underline{v}$) = **0w**. → **k$\underline{v}$ ∈ ker(f)**

Imm è Sottospazio vettoriale

Teorema: *il sottoinsieme **Im(f) = {$\underline{w} \in W : \exists \underline{v} \in V$ con f($\underline{v}$) = $\underline{w}$} ⊂ W** è un sottospazio vettoriale di V.*

Dimostrazione: Si verificano le proprietà dei STSP:

1) **Chiusura rispetto a somma**
   Siano $\underline{w1}$, $\underline{w2} \in$ Im(f), allora si sa che esistono $\underline{v1}$ e $\underline{v2}$ tali che **f($\underline{v1}$) = $\underline{w1}$** e **f($\underline{v2}$) = $\underline{w2}$**
   Consideriamo il vettore $\underline{v1}$+$\underline{v2}$ e la sua immagine f($\underline{v1}$+$\underline{v2}$) = f($\underline{v1}$) + f($\underline{v2}$) = **$\underline{w1}$ + $\underline{w2}$.**
   w1 + w2 sono immagine del vettore v1 + v2 e quindi **($\underline{w1}$ + $\underline{w2}$) ∈ Im(f)**

2) **Chiusura rispetto a prodotto scalare**
   sia k ∈ K e $\underline{w} \in$ Im(f) allora esiste $\underline{v}$ tale che f($\underline{v}$)=$\underline{w}$ Quindi **f(k v) =** k f(v) = **k $\underline{w}$**
   Deduciamo che k $\underline{w} \in$ Im(f) perché è l'immagine di un vettore specifico, che in questo caso è k $\underline{v}$

la matrice rappresentativa rispetto ad una base di auto vettori è diagonale

Teorema: *Sia f : V → V un'applicazione lineare e sia C un K-spazio vettoriale finitamente generato. La matrice $M_C(f)$ è diagonale se e solo se la base C è formata da auto vettori*

Dimostrazione:

si supponga che C={v1,…,vn} una base fatta di auto vettori. Questo significa che per ogni i, ∃ **ki ∈ K : f ($\underline{vi}$)=ki vi** quindi:

f ($\underline{v1}$) = k1$\underline{v1}$ = **k1$\underline{v1}$** + 0$\underline{v2}$ + … + 0$\underline{vn}$ ⇨
f ($\underline{v2}$) = k2$\underline{v2}$ = 01$\underline{v1}$ + **k2$\underline{v2}$** + … + 0$\underline{vn}$ ⇨ ⇨
f ($\underline{vn}$) = kn$\underline{vn}$ = 01$\underline{v1}$ + 0$\underline{v2}$ + … + **kn$\underline{vn}$** ⇨

$$\begin{bmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda_n \end{bmatrix}$$

V spazio vettoriale su K di dimensione n. ⇨ V isomorfo allo spazio vettoriale K^n

Teorema: *Sia V uno spazio vettoriale sul campo K di dimensione n. Allora V è isomorfo allo spazio vettoriale K^n*

Dimostrazione sia dim(V) = n e dim(K^n) = n allora sono isomorfi perché hanno la stessa dimensione.

1) **V isomorfo a W ⇨ dim(V) = dim(W)**
   Se V e K^n sono isomorfi per definizione esiste un'applicazione lineare biiettiva f: V → W.
   Se questa applicazione è biiettiva allora è iniettiva e suriettiva.
   Iniettiva ⇨ dim(ker(f)) = 0
   Suriettiva ⇨ dim(im(f)) = dim(W)
   Dal teorema di nullità più rango si sa che dim(V) = dim(ker (f)) + dim(Im(f)) = 0 + dim(W)

2) **dim(V) = dim(W) ⇨ V isomorfo a W**

   considero una base di V = {v1,…,vn} e una base di W = {w1,…,wn}
   Si è visto che se esiste un'applicazione lineare fra V e W allora essa è determinata dall'immagine dei vettori di una base.
   considero una applicazione lineare tale che f(vi) = wi Questa parte è totalmente determinata dal fatto che si da un'immagine dei vettori di base
   Questa applicazione definita è suriettiva (nell'immagine ci sono tutte le combinazioni lineari dei wi, che pero sono base di W, quindi nell'immagine ci sono tutti i vettori di W) e quindi **dim(Im(f)) = dim(W).**
   A questo punto per nullità più rango si ha che **dim(ker(f)) = 0** e quindi f è iniettiva e suriettiva.
   se una applicazione lineare è biiettiva allora è un isomorfismo e V si dice isomorfo a W