Compito di MD
4 Giugno 2014

Cognome e nome: ....

Numero di matricola: .... Corso e Aula: ....

<u>IMPORTANTE:</u> Non si possono consultare libri e appunti. Non si possono usare calcolatrici, computer o altri dispositivi elettronici. Non saranno valutate risposte prive di motivazioni, o con motivazioni non chiare. Non si può scrivere con il lapis.

Esercizio 1. Sia $\mathbb{N}_{10} = \{1, 2, ..., 10\}$.
Quante sono le funzioni $f : \mathbb{N}_{10} \to \mathbb{N}_{10}$ tali che $MCD(f(x), 10) = MCD(x, 10)$ per ogni $x \in \mathbb{N}_{10}$?

Soluzione: Osserviamo che per gli x nell'intervallo considerato si ha:
$MCD(x, 10) = 1 \iff x \in \{1, 3, 7, 9\}$ (primo gruppo)
$MCD(x, 10) = 2 \iff x \in \{2, 4, 6, 8\}$ (secondo gruppo)
$MCD(x, 10) = 5 \iff x = 5$ (terzo gruppo)
$MCD(x, 10) = 10 \iff x = 10$ (quarto gruppo).
Poiché $MCD(f(x), 10) = MCD(x, 10)$ la f deve mandare i numeri di ciasun gruppo all'interno dello stesso gruppo. Ad esempio siccome $MCD(f(1), 10) = MCD(1, 10) = 1$ dobbiamo avere $f(1) \in \{1, 3, 7, 9\}$. Abbiamo quindi 4 possibili modi di definire $f(1)$ (ciascuna scelta corrisponde ad una f diversa). Analogamente dobbiamo avere $f(2) \in \{2, 4, 6, 8\}$ e ci sono quindi 4 possibili modi di definire $f(2)$. In generale abbiamo 4 possibilità per definire $f(x)$ in ciascuno degli altri casi eccetto quando $x = 5$ o $x = 10$. In questi ultimi due casi abbiamo una sola possibilità: $f(5)$ deve essere 5 e $f(10)$ deve essere 10. Il numero delle funzioni è pari al prodotto, al variare di x, del numero dei possibili modi di definire $f(x)$. Siccome ci sono 8 casi con 4 scelte e 2 casi con 1 scelta il risultato è 4^8. $\square$

Cognome e nome: ....

Numero di matricola: .... Corso e Aula: ....

Esercizio 2. Trovare tutte le soluzioni intere del seguente sistema di congruenze:

$$\begin{cases} 4x \equiv 11 \bmod (21) \\ x^2 \equiv 1 \bmod (15) \end{cases}$$

Soluzione: Con semplici calcoli si vede che la prima congruenza equivale a

$$x \equiv 8 \bmod (21).$$

(Infatti moltiplicando per 5 la congruenza $4x \equiv 11 \bmod (21)$ si ottiene $-x \equiv 55 \equiv 13 \bmod (21)$, ovvero $x \equiv -13 \equiv 8 \bmod (21)$.)

Per quanto riguarda la seconda congruenza, visto che il modulo è piccolo, possiamo anche risolverla per "forza bruta" sostituendo al posto di x tutti i possibili valori tra 0 e 14. Si trova che le uniche soluzioni in questo intervallo sono $1, 4, 11, 14$ e le altre si ottengono aggiungendo multipli di 15. In altre parole $x^2 \equiv 1 \bmod 15$ equivale alla disgiunzione dei seguenti quattro casi:

$$\begin{gathered} x \equiv 1 \bmod 15 \\ x \equiv 4 \bmod 15 \\ x \equiv 11 \bmod 15 \\ x \equiv 14 \bmod 15. \end{gathered}$$

Allo stesso risultato si poteva arrivare osservando che $x^2 \equiv 1 \bmod (15)$ se e solo se $(x-1)(x+1)$ è multiplo sia di 3 che di 5. Visto che $(x-1)(x+1)$ è multiplo di 3 e solo se lo è uno dei due fattori e analogamente per 5, riotteniamo gli stessi quattro casi, nello stesso ordine, come soluzioni dei sistemi

$$\begin{cases} x \equiv 1 \ (5) \\ x \equiv 1 \ (3) \end{cases}, \begin{cases} x \equiv -1 \ (5) \\ x \equiv 1 \ (3) \end{cases}, \begin{cases} x \equiv 1 \ (5) \\ x \equiv -1 \ (3) \end{cases}, \begin{cases} x \equiv -1 \ (5) \\ x \equiv -1 \ (3) \end{cases}$$

Per finire dobbiamo mettere a sistema la prima e la seconda congruenza. La prima congruenza, che avevamo già ridotto alla forma $x \equiv 8 \bmod 21$, equivale a

$$\begin{cases} x \equiv 8 \equiv -1 \bmod (3) \\ x \equiv 8 \equiv 1 \bmod (7) \end{cases}$$

che dobbiamo ora mettere a sistema con ciascuno dei quattro sistemi precedenti e prendere la disgiunzione dei casi. Essendo $x \equiv -1 \bmod 3$, dei quattro casi precedenti vanno scartati quelli con $x \equiv 1 \bmod 3$. Rimangono dunque i seguenti due casi

$$\begin{cases} x \equiv 1 \bmod (7) \\ x \equiv 1 \bmod (5) \\ x \equiv -1 \bmod (3) \end{cases} \qquad \text{oppure} \qquad \begin{cases} x \equiv 1 \bmod (7) \\ x \equiv -1 \bmod (5) \\ x \equiv -1 \bmod (3) \end{cases}$$

che possiamo semplificare in

$$\begin{cases} x \equiv 1 \bmod (35) \\ x \equiv -1 \bmod (3) \end{cases} \qquad \text{oppure} \qquad \begin{cases} x \equiv 1 \bmod (7) \\ x \equiv -1 \bmod (15) \end{cases}$$

Risolvendo i due sistemi con gli usuali metodi otteniamo rispettivamente

$$x \equiv 71 \bmod 105 \quad \text{oppure} \quad x \equiv 29 \bmod 105$$

Le soluzioni del sistema iniziale sono dunque gli x della forma $71 + s105$ o della forma $29 + t105$.

$\square$

Cognome e nome: ....

Numero di matricola: .... Corso e Aula: ....

Esercizio 3. Sia V il sottospazio di $\mathbb{R}[x]_{\leq 5}$ definito da

$$V := \{p(x) \in \mathbb{R}[x]_{\leq 5} \mid p(1) = p(-1) = 0\}.$$

a) Determinare una base di V su $\mathbb{R}$.
b) Dire, motivando bene la risposta, se esistono applicazioni lineari iniettive o applicazioni lineari surgettive da V nello spazio delle matrici simmetriche 2×2 con coefficienti in $\mathbb{R}$.

Soluzione: Le matrici 2×2 simmetriche sono quelle della forma

$$\begin{pmatrix} a & b \\ b & c \end{pmatrix}$$

Esse formano uno spazio vettoriale W di dimensione 3 con base data dalle tre matrici simmetriche

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

Per sapere se esistono applicazioni lineari iniettive o surgettive da V a W occorre confrontare le loro dimensioni. Infatti in generale esistono sempre applicazioni lineari iniettive da uno spazio ad un altro di dimensione maggiore o uguale (basta mandare una base del primo iniettivamente in un insieme di vettori indipendenti nel secondo), e applicazioni lineari surgettive da uno spazio ad un altro di dimensione minore o uguale (basta mandare una base del primo surgettivamente in una base del secondo). Questa casistica è inoltre completa, ovvero fornisce gli unici casi di esistenza di applicazioni lineari iniettive o surgettive.

Resta dunque da calcolare la dimensione di V. La condizione $p(1) = p(-1) = 0$ equivale a dire che $p(x)$ ha come fattori $(x-1)$ ed $(x+1)$, ovvero $p(x)$ si scrive nella forma $p(x) = (x-1)(x+1)q(x)$ dove $q(x) = ax^3 + bx^2 + cx + d$ è un polinomio di grado ≤ 3. Lo spazio di tali polinomi ha dimensione 4 con base data dai quattro polinomi $x^3, x^2, x, 1$. Ne segue che anche V ha dimensione 4 con base data dai quattro polinomi
$(x-1)(x+1)x^3$, $(x-1)(x+1)x^2$, $(x-1)(x+1)x$, $(x-1)(x+1)$.

Essendo la dimensione di V strettamente maggiore di quella di W, esiste un'applicazione lineare surgettiva da V a W, ma non una iniettiva. $\square$

Cognome e nome: ....

Numero di matricola: .... Corso e Aula: ....

Esercizio 4. a) Si consideri l'endomorfismo $A : \mathbb{C}^2 \to \mathbb{C}^2$ a cui nella base standard è associata la matrice

$$\begin{pmatrix} 1 & -2 \\ 2 & 1 \end{pmatrix}$$

Trovare gli autovettori di A e dire se A è diagonalizzabile.
b) Si consideri l'endomorfismo $B : \mathbb{R}^2 \to \mathbb{R}^2$ a cui nella base standard è associata la matrice

$$\begin{pmatrix} 1 & b \\ b & 1 \end{pmatrix}$$

i) Per quali valori di $b \in \mathbb{R}$ l'endomorfismo è diagonalizzabile ?
ii) Sia k un intero positivo. Si trovino, in funzione di k e del parametro b, gli autovalori dell'endomorfismo B^k.

Soluzione: a) Un breve calcolo mostra che il polinomio caratteristico $p_A(t)$ è $t^2 - 2t + 5$, le cui radici sono $1 + 2\imath$ e $1 - 2\imath$. Questi sono dunque i due autovalori dell'endomorfismo A. Sono distinti, dunque A è diagonalizzabile. Gli autovettori relativi all'autovalore $1 + 2\imath$ sono i vettori del nucleo di $A - (1 + 2\imath)I$ (eccetto il vettore O). Tale nucleo è di dimensione 1 ed è generato dal vettore $(\imath, 1)$. Gli autovettori relativi all'autovalore $1 - 2\imath$ sono i vettori del nucleo di $A - (1 - 2\imath)I$ (eccetto il vettore O). Tale nucleo è di dimensione 1 ed è generato dal vettore $(\imath, -1)$.

b) Il polinomio caratteristico di B risulta uguale a $t^2 - 2t + 1 - b^2$, le cui radici sono $1+b$ e $1-b$. Gli autovalori di B sono dunque $1+b$ e $1-b$. Si osserva subito che per $b \neq 0$ tali autovalori sono distinti e si conclude che in tal caso B è diagonalizzabile. Nel caso in cui $b = 0$ per decidere se B è diagonalizzabile potremmo calcolare la molteplicità geometrica dell'unico autovalore presente, ovvero 1. Però una considerazione ci permette di concludere in maniera ancora più immediata. Per $b = 0$ l'applicazione B è l' identità, dunque è diagonalizabile, anzi, qualunque base si scelga la matrice associata è la matrice diagonale

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Dunque B risulta diagonalizzabile per ogni valore di b. Per quel che riguarda l'ultima domanda, per calcolare B^k conviene scegliere una base in cui B è rappresentata da una matrice diagonale. In tale base troveremo sulla diagonale i due autovalori $1+b$ e $1-b$. Si osserva subito allora che gli autovalori di B^k sono $(1+b)^k$ e $(1-b)^k$. $\square$