PROVA SCRITTA DI ALGEBRA PER INFORMATICA, 17/2/2022 – CANALE M-Z, PROF. P. PAPI

Nome, Cognome, Numero di Matricola: ....

1. Non sono ammessi appunti, libri di testo, calcolatrici né l'uso del computer (al di fuori di exam.net)

2. Spiegare il procedimento ed i calcoli eseguiti, e **giustificare ogni risposta**. *La valutazione terrà conto della* **presentazione***: leggibilità, grammatica, sintassi, ordine, chiarezza, capacità di sintesi.*

3. Una risposta giusta con giustificazione sbagliata viene valutata ≤ 0.

4. Per gli esercizi da 1 a 4, riportare la risposta sintetica nella colonna centrale della tabella sottostante.

5. Il tempo a disposizione è due ore e mezzo.

6. **Per gli esami in presenza: consegnare i fogli da 1 a 12, ordinati secondo la numerazione naturale. Non scrivere sul retro dei fogli.**

7. **Per gli esami on-line**: assicurarsi di scannerizzare esclusivamente la bella copia, in formato verticale.

Esercizio	*Risposta sintetica*	*Valutazione*
1.a		
1.b		
2.a		
2.b		
2.c		
2.d		
3.a		
3.b		
3.c1		
3.c2		
3.d		
4.a		
4.b		
4.c		

Esercizio 1. *Si risolvano i seguenti sistemi di congruenze lineari*

a)

$$\begin{cases} x \equiv 1 \mod 4 \\ x \equiv 2 \mod 3 \\ x \equiv 3 \mod 5 \\ x \equiv 5 \mod 7 \end{cases}$$

b)

$$\begin{cases} x \equiv 3 \mod 10 \\ x \equiv 8 \mod 15 \\ x \equiv 5 \mod 84 \end{cases}$$

a) Poiché i moduli sono coprimi, il sistema ha soluzione unica mod $4 \cdot 3 \cdot 5 \cdot 7 = 420$

$x = 1 + 4k \qquad 1 + 4k \equiv 2 \mod 3 \qquad k \equiv 1 \mod 3$

$k = 1 + 3s \qquad x = 1 + 4(1 + 3s) = 5 + 12s$

$5 + 12s \equiv 3 \mod 5 \qquad 2s \equiv 3 \mod 5 \qquad s \equiv 9 \equiv 4 \mod 5$

$s = 4 + 5t \qquad x = 5 + 12(4 + 5t) = 53 + 60t$

$53 + 60t \equiv 5 \mod 7 \qquad 4 + 4t \equiv 5 \mod 7$

$4t \equiv 1 \mod 7 \qquad t \equiv 2 \mod 7 \qquad t = 2 + 7r$

$$x = 53 + 60(2 + 7r) = 173 + 420r$$

In definitiva $x \equiv 173 \mod 420$.

b) Usando il teorema cinese dei resti otteniamo

$$x \equiv 3 \mod 10 \iff \begin{cases} x \equiv 3 \equiv 1 \mod 2 \\ x \equiv 3 \mod 5 \end{cases}$$

$$x \equiv 8 \mod 15 \iff \begin{cases} x \equiv 8 \equiv 3 \mod 5 \\ x \equiv 8 \equiv 2 \mod 3 \end{cases}$$

$$x \equiv 5 \bmod 84 \iff \begin{cases} x \equiv 5 & \bmod 7 \\ x \equiv 5 \equiv 1 & \bmod 4 \\ x \equiv 5 \equiv 2 & \bmod 3 \end{cases}$$

Dunque il sistema è equivalente a quello dato nel punto a.

Esercizio 2. *Siano G, G' gruppi finiti e $f : G \to G'$ un omomorfismo di gruppi.*

a) *Definire l'ordine $o(g)$ di $g \in G$. Dimostrare che $o(f(g))$ divide $o(g)$, e che $o(g) = o(f(g))$ se f è un isomorfismo.*

b) *Calcolare il numero degli elementi di ordine 3 nel gruppo simmetrico S_6.*

c1) *Dimostrare che se $gg' = g'g$ allora $o(gg')$ divide $o(g)o(g')$.*

c2)* *Dimostrare che se $g, g' \in G, MCD(o(g), o(g')) = 1, gg' = g'g$ allora $o(gg') = o(g)o(g')$.*

d) *Dire se i seguenti gruppi sono isomorfi*

1. $\mathbb{Z}_2 \times \mathbb{Z}_4$ e $\mathbb{Z}_8$;
2. $\mathbb{Z}_3 \times \mathbb{Z}_5$ e $\mathbb{Z}_{15}$.

Il punto c2) è più impegnativo; può essere assunto per svolgere il punto d).

a) $o(g)$ è il minimo intero positivo n tale che $g^n = e$

Se $g^n = e$, allora $f(g^n) = f(g)^n = f(e) = e'$

da cui $o(f(g)) \mid o(g)$.

Applicando l'argomento a f^{-1} abbiamo che $o(f^{-1}(g')) \mid o(g')$ per ogni $g' \in G'$; posto $g = f^{-1}(g')$ otteniamo

$o(g) \mid o(f(g))$

b) In S_6 un elemento ha ordine 3 se e solo se ha struttura ciclica 31^3, 3^2.

Dette C_1, C_2 le rispettive classi di coniugio, si ha

$|C_1| = \binom{6}{3} \cdot 2 = 20 \cdot 2 = 40$

Infatti devo scegliere tre elementi su sei e ciascuno dà luogo a due tre cicli; e.g. $(1\,2\,3)$ $(1\,3\,2)$.

$|C_2| = \dfrac{\binom{6}{3} \cdot 2 \cdot 2}{2} = 40$

Infatti dev...

scegliere [illegible] 3-ciclo, i rimanenti elementi danno luogo a due 3-cicli; infine devo dividere per 2 perché cicli disgiunti commutano

c1) Sia $o(g)=n$, $o(g')=n'$; allora $(gg')^{nn'} = (g^n)^{n'}(g'^{n'})^n = e$

e pertanto $o(gg') \mid nn'$

c2) D'altra parte, se $(gg')^m = e$,

$$e = (gg')^{mn} = g'^{mn}$$

per cui $n' \mid mn$; poiché $(n', n) = 1$, $n \mid m$

similmente $n' \mid m$, quindi $nn' \mid m$ e $o(gg') = nn'$;

d) $\mathbb{Z}_2 \times \mathbb{Z}_4$ non ha elementi di ordine 8 (verifica diretta), per cui non è ciclico e quindi non è isomorfo a $\mathbb{Z}_8$.

Invece, per il punto c2),

$(1 \bmod 3, 1 \bmod 5) \in \mathbb{Z}_3 \times \mathbb{Z}_5$ ha ordine 15, per cui $\mathbb{Z}_3 \times \mathbb{Z}_5$ è isomorfo a $\mathbb{Z}_{15}$.

Esercizio 3. *Nello spazio vettoriale V dei polinomi a coefficienti complessi di grado minore o uguale a 3, si consideri il sottoinsieme*

$$U_k = \{p(z) \in V \mid p''(1) - 3p'(1) + 2p(-1) = k^2 + 4\}.$$

(Notazione: $p'(z) = \frac{d}{dz}p(z), p''(z) = \frac{d^2}{dz^2}p(z)$).

a) *Dimostrare che U_k è un sottospazio vettoriale di V per esattamente due valori $k_1, k_2 \in \mathbb{C}$. Verificare che per tali valori $U_{k_1} = U_{k_2}$. Poniamo $U := U_{k_1} = U_{k_2}$.*

b) *Determinare una base di U.*

c) *Completare una base di U a una base di V.*

d) *Determinare una base di V/U.*

a) Sia $p(z) = a_0 + a_1 z + a_2 z^2 + a_3 z^3$. La condizione che definisce U_k è

$$2a_2 + 6a_3 - 3(a_1 + 2a_2 + 3a_3) + 2(a_0 - a_1 + a_2 - a_3) = k^2 + 4$$

che è omogenea solo per $k^2+4=0$, ovvero per $k = \pm 2i$. Per tali valori

$$U_{2i} = U_{-2i} = U = \{a_0 + a_1 t + a_2 t^2 + a_3 t^3 \mid 2a_0 - 5a_1 - 2a_2 - 5a_3 = 0\}$$

è un sottospazio di V.

b) Una base per le soluzioni del sistema che definisce U è $\begin{pmatrix} 5 \\ 2 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 5 \\ 0 \\ 0 \\ 2 \end{pmatrix}$,

cui corrispondono i polinomi $5+2t$, $1+t^2$, $5+2t^3$

c) Una possibile complemento è dato dal polinomio costante 1

d) Abbiamo dimostrato che se $\{u'_1, \dots, u'_s\}$ è una base di un complemento U' di U in V (così $V = U \oplus U'$)

una base per V/U è data dalle classi $u'_1 + U, \dots, u'_s + U$.

Nel nostro caso $\dim V/U = 1$ e quindi una base può essere $\{1 + U\}$

Esercizio 4. *Si consideri l'operatore lineare $s_a : \mathbb{R}^4 \to \mathbb{R}^4$ definito da*

$$s_a(x) = x - 2\frac{a^t\,x}{x^t\,x}a$$

$a\,a$

ove $a = \begin{pmatrix}1\\1\\1\\1\end{pmatrix}$, $x = \begin{pmatrix}x_1\\x_2\\x_3\\x_4\end{pmatrix}$.

a) *Determinare la matrice A di s_a rispetto alla base standard di $\mathbb{R}^4$ presa come base di partenza e di arrivo. Verificare che A è una matrice ortogonale e dedurre che è invertibile.*

b) *Dimostrare che s_a è diagonalizzabile e trovare una base di autovettori.*

c) *Determinare a meno di isomorfismo il sottogruppo di $Aut(\mathbb{R}^4)$ generato da s_a.*

a) $$s_a\begin{pmatrix}x_1\\x_2\\x_3\\x_4\end{pmatrix} = \begin{pmatrix}x_1\\x_2\\x_3\\x_4\end{pmatrix} - 2\,\frac{x_1+x_2+x_3+x_4}{4}\begin{pmatrix}1\\1\\1\\1\end{pmatrix}$$

$$= \frac{1}{2}\begin{pmatrix} x_1 - x_2 - x_3 - x_4 \\ -x_1 + x_2 - x_3 - x_4 \\ -x_1 - x_2 + x_3 - x_4 \\ -x_1 - x_2 - x_3 + x_4 \end{pmatrix}$$

La matrice di s_a rispetto alla base standard è

$$A = \begin{pmatrix} \frac12 & -\frac12 & -\frac12 & -\frac12 \\ -\frac12 & \frac12 & -\frac12 & -\frac12 \\ -\frac12 & -\frac12 & \frac12 & -\frac12 \\ -\frac12 & -\frac12 & -\frac12 & \frac12 \end{pmatrix}$$

che è ortogonale, quindi invertibile, poiché $\det A = -1$

b) Dalla formula che definisce S_a si vede subito che se $x^t a = 0$ allora $S_a(x) = x$, pertanto l'autospazio di autovalore 1 ha equazione $x_1 + x_2 + x_3 + x_4 = 0$, e una possibile base è

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

Inoltre $S_a(a) = -a$, dunque a genera l'autospazio di autovalore -1.

c) Dal punto b è chiaro che $S_a^2 = Id$. Inoltre $S_a \neq Id$. Dunque

$$\langle S_a \rangle \cong \mathbb{Z}_2$$

Esercizio 5.

1. *Dare la definizione di dipendenza lineare per un insieme finito* $\{v_1, \ldots, v_n\}$ *di vettori in uno spazio vettoriale* V *su un campo* F*.*

2. *Dimostrare* $v_1, \ldots, v_n$ *che sono linearmente dipendenti se e solo se uno di essi è combinazione lineare degli altri.*

3. *Dimostrare che la seguente affermazione è in generale falsa: se* $v_1, \ldots, v_n$ *sono linearmente dipendenti allora* v_1 *è combinazione lineare di* $v_2, \ldots, v_n$*.*

1.2. Si vedano i testi consigliati

3. Controesempio: V spazio vettoriale non zero, $v_1 \neq 0$, $v_2 = \cdots = v_n = 0$