Algebra. Laurea in Informatica a.a. 2023-2024

Canale 1. Proff. Paolo Piazza e Gabriele Viaggi

Esame scritto del 9/1/2024. Compito A.

Tempo a disposizione: 2 ore e 30 minuti.

Nome e Cognome: ____________________

email istituzionale: ____________________

Esercizio	Punti totali	Punteggio
1	7	
2	6	
3	6	
4	6	
5	8	
Totale	33	

ATTENZIONE:

- Utilizzare il retro della pagina se necessario.
- I compiti disordinati o poco leggibili non saranno neanche corretti.
- Spiegare il procedimento ed i calcoli eseguiti, e **giustificare ogni risposta**. La valutazione terrà conto della presentazione: leggibilità, grammatica, sintassi, ordine, chiarezza, rigore matematico, capacità di sintesi.
- Una risposta giusta con giustificazione sbagliata viene valutata ≤ 0.
- Scrivete le risposte negli appositi riquadri quando presenti.
- I fogli di brutta non saranno accettati; consegnare **esclusivamente** questi fogli.
- Tutti i dispositivi elettronici (smartphones, tablets, PC, etc, etc) devono essere spenti ed in borsa.
- Non sono ammessi libri o appunti ad eccezione di un formulario di una pagina A4 fronte retro (max 35 righe a facciata, no dimostrazioni).

Esercizio 1.

(1) In un anello unitario $(A, +, \cdot)$ definire l'insieme degli elementi invertibili $\mathcal{U}(A)$ e spiegare, *giustificando i passaggi*, qual è la sua struttura algebrica rispetto alla moltiplicazione.

(2) Siano $(G, \cdot)$ e $(H, \star)$ due gruppi, con elementi neutri 1_G e 1_H.
(2.1). Come si definisce il nucleo di un omomorfismo $\psi : G \to H$ e che cosa ha a che fare con l'iniettività di ψ ?
(2.2) Il nucleo di un omomorfismo ψ è un sottogruppo ? Il nucleo di un omomorfismo ψ è un sottogruppo normale ?
Spiegare in dettaglio.

(3) Dare la definizione di indipendenza lineare di k vettori $\{\underline{v}_1, \dots, \underline{v}_k\}$ in uno spazio vettoriale V.

(4) Sia $T : V \to V$ un'applicazione lineare. Cosa possiamo dire su autovettori associati ad autovalori distinti ?
(4.1) Enunciare il risultato.
(4.2) Dimostrarlo.

Soluzione.
(1) $\mathcal{U}(A) := \{a \in A \,|\, \exists a' \in A \quad \text{tale che} \quad a \cdot a' = 1 = a' \cdot a\}$. $\mathcal{U}(A)$ contiene ovviamente l'unità moltiplicativa di A ed è chiuso rispetto al prodotto in A perché se $a, b \in \mathcal{U}(A)$ con inversi a' e b' allora $a \cdot b$ ha inverso $b' \cdot a'$ e quindi è in $\mathcal{U}(A)$. Per definizione ogni elemento in $\mathcal{U}(A)$ ha un inverso. Infine, il prodotto è associativo perché indotto da A. Ne segue che $\mathcal{U}(A)$ è un gruppo rispetto a $\cdot$.
(2) [PC] p. 246 e p. 257.
(3) [A-dF] definizione 4.6
(4) [A-dF] Prop. 13.6.

Esercizio 2. Si trovino tutte le soluzioni intere del sistema di equazioni congruenziali

$$\begin{cases} x \equiv 13^{190} & \mod 35 \\ 4x \equiv 8 & \mod 6 \end{cases}$$

Soluzione. Applicando il teorema cinema dei resti nella seconda formulazione alla prima equazione ($35 = 5 \cdot 7$, $\mathrm{MCD}(5, 7) = 1$) e semplificando la seconda equazione, il sistema risulta equivalente al seguente:

$$\begin{cases} x \equiv 13^{190} & \mod 5 \\ x \equiv 13^{190} & \mod 7 \\ 2x \equiv 4 & \mod 3. \end{cases}$$

La prima equazione si può semplificare nel seguente modo:

$$\begin{array}{llll} x \equiv & 3^{190} & \mod 5 & (\text{essendo } 13 \equiv 3 \mod 5) \\ x \equiv & 3^{\varphi(5)\cdot 47+2} & \mod 5 & (\text{essendo } \varphi(5) = 4) \\ x \equiv & 3^2 & \mod 5 & (\text{per il teorema di Eulero-Fermat}) \\ x \equiv & 4 & \mod 5 & (\text{essendo } 3^2 \equiv 4 \mod 5) \end{array}$$

La seconda equazione, osservando che $13 \equiv -1 \mod 7$, equivale a $x \equiv (-1)^{190} \mod 7$ e cioè a

$$x \equiv 1 \mod 7$$

Infine la terza equazione, essendo $2 \cdot 2 \equiv 1 \mod 3$ ed essendo $8 \equiv 2 \mod 3$, si può riscrivere, moltiplicando per 2, come

$$x \equiv 2 \mod 3$$

Il sistema da risolvere è in conclusione

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

Una soluzione dell'ultimo sistema (che è un sistema cinese in forma standard) è 29, quindi l'insieme delle soluzioni è

$$S = \{29 + 105z \,|\, z \in \mathbb{Z}\}$$

dove $105 = 3 \cdot 5 \cdot 7$.

Esercizio 3. Sia G un gruppo e $H \leq G$ un suo sottogruppo. Verificare che

(1) per ogni fissato $g \in G$ l'insieme $H^g := \{g^{-1}hg \,|\, h \in H\}$ è un sottogruppo di G.
(2) H è **isomorfo** a H^g. (Suggerimento: l'applicazione $H \ni h \to g^{-1}hg \in H^g$ può risultare utile).

Soluzione.
Utilizzeremo la seguente notazione: $h^g := g^{-1}hg$.
Sia $g \in G$. L'insieme H^g è non vuoto poichè $1_G^g = 1_G \in H^g$.
Siano ora $h_1^g, h_2^g \in H^g$. Allora

$$(h_1^g)(h_2^g)^{-1} = g^{-1}h_1g(g^{-1}h_2g)^{-1} = g^{-1}h_1gg^{-1}h_2^{-1}g = g^{-1}h_1h_2^{-1}g = (h_1h_2^{-1})^g,$$

che è in H^g in quanto $h_1h_2^{-1} \in H$. Per la caratterizzazione dei sottogruppi di un gruppo si ha che $H^g \leq G$.
Consideriamo l'applicazione

$$\phi_g : H \longrightarrow H^g, \qquad h \longmapsto g^{-1}hg.$$

È facile vedere che ϕ_g è biettiva. Siano ora $h_1, h_2 \in H$. Si ha

$$\phi_g(h_1h_2) = g^{-1}h_1h_2g = (g^{-1}h_1g)(g^{-1}h_2g) = \phi_g(h_1)\phi_g(h_2).$$

Pertanto ϕ_g è un omomorfismo, quindi un isomorfismo di gruppi.

Esercizio 4.
4.1 Consideriamo il gruppo simmetrico S_3.

(1) Quali sono i possibili ordini dei sottogruppi di S_3 e perché ?
(2) Elencare i 4 sottogruppi non-banali di S_3. Disegnare il diagramma di Hasse (o reticolo) dei sottogruppi di S_3.
(3) Spiegare se esistono sottogruppi ciclici in S_3 ed in caso affermativo esplicitarli.
(4) Spiegare se esistono sottogruppi normali in S_3; in caso affermativo esplicitarli e spiegare perché sono normali.

4.2 Determinare la parità in S_9 di $\sigma := (2345) \circ (35) \circ (479) \circ (218)$. (Attenzione, questa *non* è una decomposizione in cicli disgiunti).
Calcolare σ^{-1}.

Soluzione.
Per (1) vedere [PC] p. 225. Gli ordini sono $1, 2, 3, 6$ per il Teorema di Lagrange. I 4 sottogruppi non-banali sono tutti ciclici. L'unico sottogruppo di ordine 3 è normale perché ha indice 2 oppure si verifica "a mano". Vedere pagina 239 e 240 in [PC].
(2) È facile vedere che la decomposizione in cicli disgiunti di σ è: $\sigma = (1832) \circ (4795)$
Ne segue che σ è pari.
$\sigma^{-1} = (1238)(4597)$.
Esercizio 5. Sia $u \in \mathbb{R}$ e sia $A(u)$ la matrice

$$A(u) := \begin{vmatrix} 1 & u/2 & 1/2 \\ 0 & 2 & 0 \\ 2 & u & 1 \end{vmatrix}$$

Sia $T_u : \mathbb{R}^3 \to \mathbb{R}^3$ l'applicazione lineare definita da $A(u)$: $T_u := L_{A(u)}$.
5.1. Determinare il polinomio caratteristico di T_u e gli autovalori di T_u.
5.2 Verificare che T_0 è diagonalizzabile e determinare una base di autovettori.
5.3. Studiare la diagonalizzabilità di T_u al variare di $u \in \mathbb{R}$.

Soluzione: Il polinomio caratteristico di A_u è $(2-\lambda)(\lambda^2 - 2\lambda)$ che ha radici $\lambda_1 = 2$ con molteplicità algebrica 2 e $\lambda_2 = 0$ con molteplicità algebrica 1. Notiamo che il polinomio caratteristico non dipende da u.
Si ha

$$A(0) = \begin{vmatrix} 1 & 0 & 1/2 \\ 0 & 2 & 0 \\ 2 & 0 & 1 \end{vmatrix}$$

L'autospazio V_0 di $A(0)$ è il nucleo di $A(0)$, che è $\{\underline{x}\,|A(0)\underline{x} = \underline{0}\}$; lo riscriviamo come le soluzioni del sistema

$$\begin{cases} x_1 + \frac{x_3}{2} = 0 \\ x_2 = 0 \\ 2x_1 + x_3 = 0 \end{cases}$$

Si ha (facile) $V_0 = \mathbb{R}(1, 0, -2)$. Passiamo a $V_2 = \mathrm{Ker}(A(0) - 2I_3)$; quindi V_2 è il nucleo di

$$A(0) - 2I_3 = \begin{vmatrix} -1 & 0 & 1/2 \\ 0 & 0 & 0 \\ 2 & 0 & -1 \end{vmatrix}$$

Ne segue che

$$V_2 = \{\underline{x}\,|2x_1 - x_3 = 0\}$$

che ha base, ad esempio, $\{(1, 0, 2), (0, 1, 0)\}$. Conclusione: i tre vettori

$$\{(1, 0, -2), (1, 0, 2), (0, 1, 0)\}$$

sono una base di autovettori per T_0. In particolare T_0 è diagonalizzabile.
Passiamo allo studio della diagonalizzabilità di T_u al variare di u. Per l'autovalore λ_2 sappiamo che la molteplicità algebrica è necessariamente uguale a quella geometrica (perché $1 \leq m_g(\lambda_2)$; $m_g(\lambda_2) \leq m_a(\lambda_2) = 1$ e quindi $m_g(\lambda_2) = m_a(\lambda_2) = 1$). Possiamo quindi concentrarci sull'autovalore $\lambda_1 = 2$. L'autospazio relativo all'autovalore

$\lambda_1 = 2$ è dato da $\mathrm{Ker}(A_u - 2I_3)$. Ma

$$A_u - 2I_3 = \begin{vmatrix} -1 & u/2 & 1/2 \\ 0 & 0 & 0 \\ 2 & u & -1 \end{vmatrix}$$

La dimensione dell'autospazio V_2 è quindi uguale a $3 - r_u$ con r_u uguale al rango di questa matrice. Questa dimensione è quindi uguale a 2, che è la molteplicità algebrica dell'autovalore, se e solo se r_u è uguale a 1. Tuttavia, è semplice verificare che $r_u = 1$ se e solo se $u = 0$. Quindi, la molteplicità algebrica di ogni autovalore è uguale alla sua molteplicità geometrica se e solo se $u = 0$. La conclusione è che T_u è diagonalizzabile se e solo se $u = 0$.