

ESAME DI GEOMETRIA E ALGEBRA
INGEGNERIA INFORMATICA (PROF. ACCASCINA)
PROVA SCRITTA DEL 4 LUGLIO 2000
Tempo assegnato: 2 ore e 30 minuti

PRIMO ESERCIZIO [7 punti]

1. Dimostrare che, per ogni naturale n , ciascuna classe di congruenza modulo n è formata da un insieme numerabile di numeri interi.
2. Determinare esplicitamente un'applicazione biunivoca $f : \mathbb{N} \rightarrow [4]_5$.

SECONDO ESERCIZIO [8 punti]

Se H e K sono due sottogruppi di un gruppo (G, \cdot) si definisca il sottoinsieme HK formato da tutti gli elementi del tipo hk al variare di h in H e di k in K .

1. Si dimostri che se $HK = KH$ allora HK è un sottogruppo di G (si noti che affinché sia $HK = KH$ non è necessario che $hk = kh$ per ogni $h \in H$ e $k \in K$);
2. Si dimostri che se H è un sottogruppo normale di G allora $HK = KH$ (suggerimento: esprimere HK e KH come unione di laterali, rispettivamente destri e sinistri, di H).
3. Si dimostri che se H e K sono sottogruppi normali di G allora HK è un sottogruppo normale di G .

TERZO ESERCIZIO [8 punti]

Si consideri la matrice a coefficienti reali:

$$A := \begin{pmatrix} 2 & 2 & 3 & 0 & 0 & 0 \\ 0 & 0 & -2 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 2 & 3 \\ 0 & 0 & 0 & 0 & 0 & -2 \\ 0 & 0 & 0 & 0 & 0 & 2 \end{pmatrix}.$$

1. Si determinino una matrice di Jordan J e una matrice invertibile M tali che $J = M^{-1}AM$.
2. Si calcoli \sqrt{A} .
3. Si determini una funzione $f : \mathbb{R} \rightarrow \mathbb{R}$ tale che $f(A)$ non sia definita. (NB: $f(x)$ deve essere definito per ogni $x \in \mathbb{R}$).

QUARTO ESERCIZIO [7 punti]

Si determini se la classe $[228]_n$ è invertibile in (\mathbb{Z}_n, \cdot) nei casi $n = 14$, $n = 91$, $n = 229$, $n = 323$, $n = 2280$. Nei casi in cui è possibile calcolare esplicitamente $[228]_n^{-1}$ descrivendo in maniera dettagliata il procedimento seguito.

ESAME DI GEOMETRIA E ALGEBRA
INGEGNERIA INFORMATICA (PROF. ACCASCINA)
RISOLUZIONE DEL TEMA D'ESAME DEL 21 GIUGNO 2000

PRIMO ESERCIZIO

1. La classe di congruenza $[m]_n$ modulo n di un intero m è formata da tutti gli interi r tali che $r - m$ è multiplo di n . Dunque r è congruente a m modulo n se e solo se r si può scrivere come $m + nk$ per qualche k in \mathbb{Z} . Ma allora l'applicazione $g : \mathbb{Z} \rightarrow [m]_n$ definita da $g(k) := m + nk$ è biunivoca, e, pertanto $[m]_n$ ha la cardinalità di \mathbb{Z} ovvero la cardinalità del numerabile.
2. Al punto precedente abbiamo definito un'applicazione biunivoca $g : \mathbb{Z} \rightarrow [4]_5$ ponendo $g(k) := 4 + 5k$. Inoltre l'applicazione $h : \mathbb{N} \rightarrow \mathbb{Z}$ definita da:

$$h(n) := \begin{cases} \frac{n}{2} & \text{se } n \text{ è pari} \\ \frac{1-n}{2} & \text{se } n \text{ è dispari} \end{cases}$$

è un'applicazione biunivoca. Pertanto la composizione $g \circ h$ realizza una corrispondenza biunivoca tra \mathbb{N} e $[4]_5$.

SECONDO ESERCIZIO

1. Per dimostrare che HK è un sottogruppo di G , occorre verificare che HK è non vuoto, è chiuso rispetto al prodotto e contiene l'inverso di ciascun suo elemento.
 - (a) Chiaramente HK è non vuoto, perché sia H che K sono non vuoti.
 - (b) Siano g_1 e g_2 due elementi di HK : allora $g_1 = h_1k_1$ e $g_2 = h_2k_2$ con $h_1, h_2 \in H$ e $k_1, k_2 \in K$. Il prodotto g_1g_2 è, dunque, uguale a $h_1k_1h_2k_2$. Osserviamo che k_1h_2 è un elemento di KH : poiché $KH = HK$ esistono allora $h_3 \in H$ e $k_3 \in K$ tali che $k_1h_2 = h_3k_3$. In conclusione $g_1g_2 = (h_1h_3)(k_3k_2)$. Poiché $h_1h_3 \in H$ e $k_3k_2 \in K$ si ha allora che $g_1g_2 \in HK$ e, dunque, HK è chiuso rispetto al prodotto.
 - (c) Sia g un elemento di HK : allora $g = hk$ con $h \in H$ e $k \in K$. Pertanto $g^{-1} = k^{-1}h^{-1}$. Poiché $k^{-1} \in K$ e $h^{-1} \in H$ si ha che $g^{-1} \in KH$. Dal momento che $HK = KH$ si ha che $g^{-1} \in HK$.

In conclusione, se $HK = KH$, allora HK è un sottogruppo di G .

2. Per definizione di HK si ha che HK è l'unione dei laterali destri di H rappresentati da elementi di K , vale a dire:

$$HK = \bigcup_{k \in K} Hk.$$

Analogamente si ha:

$$KH = \bigcup_{k \in K} kH.$$

Poiché H è normale in G si ha che $Hg = gH$ per ogni $g \in G$. In particolare si ha che $Hk = kH$ per ogni $k \in K$. Ma allora $HK = KH$.

3. Se H e K sono normali sappiamo già dal punto 2 che $HK = KH$, e, dunque, dal punto 1 sappiamo che HK è un sottogruppo di G . Per verificare che HK è normale è sufficiente verificare che glg^{-1} appartiene a HK per ogni $g \in G$ e ogni $l \in HK$. Poiché $l \in HK$ esistono $h \in H$ e $k \in K$ tali che $l = hk$. Allora $glg^{-1} = ghkg^{-1} = (ghg^{-1})(gkg^{-1})$. Dal momento che H e K sono normali in G si ha che $ghg^{-1} \in H$ e $gkg^{-1} \in K$: pertanto $glg^{-1} \in HK$ come richiesto.

TERZO ESERCIZIO

1. La matrice A è una matrice a blocchi costituita da due blocchi uguali tra loro. Consideriamo allora la matrice:

$$A' := \begin{pmatrix} 2 & 2 & 3 \\ 0 & 0 & -2 \\ 0 & 0 & 2 \end{pmatrix},$$

e applichiamo a questa matrice il processo di Jordanizzazione. Poiché A' è una matrice triangolare (superiore) i suoi autovalori sono gli elementi lungo la diagonale principale contati con le opportune molteplicità. Dunque A' ha come autovalori 0 di molteplicità algebrica 1 e 2 di molteplicità algebrica 2. Possiamo innanzitutto determinare un autovettore $\mathbf{v}_1 = (x, y, z)$ per l'autovalore 0 risolvendo il sistema lineare:

$$(A' - 0 \cdot I)^t \mathbf{v}_1 = 0$$

ovvero

$$\begin{cases} 2x + 2y + 3z = 0 \\ - 2z = 0 \\ 2z = 0 \end{cases}$$

che, risolto, dà $x = -y$, $z = 0$. Possiamo dunque porre $\mathbf{v}_1 = (1, -1, 0)$.

Consideriamo ora l'altro autovalore 2: sia θ l'endomorfismo di \mathbb{R}^3 la cui matrice rispetto alla base canonica $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3\}$ di \mathbb{R}^3 sia A' , e sia $\theta_2 = \theta - 2I$. Determiniamo le immagini dei vettori della base canonica tramite le potenze successive di θ_2 (dobbiamo proseguire fino a che troviamo una potenza θ_2^i tale che $\dim \ker \theta_2^i = \text{ma}(2) = 2$, ovvero $\dim \text{Im } \theta_2^i = 1$):

$$\begin{array}{llll} \mathbf{e}_1 & \rightarrow & \mathbf{0} & \rightarrow & \mathbf{0} \\ \mathbf{e}_2 & \rightarrow & 2\mathbf{e}_1 - 2\mathbf{e}_2 & \rightarrow & -4\mathbf{e}_1 + 4\mathbf{e}_2 \\ \mathbf{e}_3 & \rightarrow & 3\mathbf{e}_1 - 2\mathbf{e}_2 & \rightarrow & -4\mathbf{e}_1 + 4\mathbf{e}_2 \end{array}$$

Si nota facilmente che $\dim \text{Im } \theta_2 = 2$ e $\dim \text{Im } \theta_2^2 = 1$ e dunque $\dim \ker \theta_2 = 1$ e $\dim \ker \theta_2^2 = 2$. Poiché $\text{mg}(2) = \dim \ker \theta_2 = 1$ avremo 1 blocco di Jordan relativo all'autovalore 2. Consideriamo allora la seguente successione dei nuclei (sulla prima riga della tabella abbiamo riportato le loro dimensioni) e le seguenti catene di autovettori generalizzati:

$$\begin{array}{ccccccc} 0 & < & 1 & < & 2 \\ \{\mathbf{0}\} & \subset & \ker \theta_2 & \subset & \ker \theta_2^2 \\ \mathbf{0} & \leftarrow & \mathbf{v}_2 & \leftarrow & \mathbf{v}_3 \end{array}$$

Occorre allora scegliere \mathbf{v}_3 in $\ker \theta_2^2 - \ker \theta_2$: ad esempio scegliamo $\mathbf{v}_3 = \mathbf{e}_2 - \mathbf{e}_3$. Determiniamo così $\mathbf{v}_2 = \theta_2(\mathbf{v}_3) = -\mathbf{e}_1$. Consideriamo ora la matrice:

$$M' := \begin{pmatrix} 1 & -1 & 0 \\ -1 & 0 & 1 \\ 0 & 0 & -1 \end{pmatrix}$$

le cui colonne sono, rispettivamente, le componenti dei vettori $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$ rispetto alla base canonica. Risulta allora $M'^{-1}A'M' = J'$, dove

$$J' := \begin{pmatrix} 0 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix}.$$

Allora se consideriamo le matrici

$$M := \begin{pmatrix} 1 & -1 & 0 & 0 & 0 & 0 \\ -1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & -1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & -1 \end{pmatrix}$$

e

$$J := \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 0 & 2 \end{pmatrix},$$

risulta $M^{-1}AM = J$.

- La matrice A ha come autovalori 0 di indice 1 e 2 di indice 2 (si ricorda che l'indice di un autovalore λ riferito a una matrice A è uguale alla dimensione del massimo blocco di Jordan relativo all'autovalore λ presente nella Jordanizzata di A). Allora, se consideriamo la funzione f che manda x in \sqrt{x} affinché sia definita $f(A)$ occorre e basta che la funzione f sia definita in 0 e 2 e che f sia derivabile in 2. Tale condizioni sono soddisfatte: infatti $f(0) = 0$, $f(2) = \sqrt{2}$, e $f'(2) = \frac{1}{2\sqrt{2}}$ (infatti $f'(x) = \frac{1}{2\sqrt{x}}$). Pertanto \sqrt{A} è definita. Possiamo calcolare \sqrt{A} in due modi diversi:

- Calcoliamo \sqrt{J} : questa si ottiene nel modo seguente

$$\begin{aligned} \sqrt{J} &= \begin{pmatrix} f(0) & 0 & 0 & 0 & 0 & 0 \\ 0 & f(2) & f'(2) & 0 & 0 & 0 \\ 0 & 0 & f(2) & 0 & 0 & 0 \\ 0 & 0 & 0 & f(0) & 0 & 0 \\ 0 & 0 & 0 & 0 & f(2) & f'(2) \\ 0 & 0 & 0 & 0 & 0 & f(2) \end{pmatrix} = \\ &= \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \sqrt{2} & \frac{1}{2\sqrt{2}} & 0 & 0 & 0 \\ 0 & 0 & \sqrt{2} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \sqrt{2} & \frac{1}{2\sqrt{2}} \\ 0 & 0 & 0 & 0 & 0 & \sqrt{2} \end{pmatrix}. \end{aligned}$$

Ora $\sqrt{A} = M\sqrt{J}M^{-1}$.

- Alternativamente determiniamo il polinomio minimo di A : considerato che l'autovalore 0 ha indice 1 e l'autovalore 2 ha indice 2, questo è $x(x-2)^2$. Esiste un polinomio $p(x)$ di grado minore di quello del polinomio minimo che coincide con f sullo spettro di A , ovvero $p(0) = f(0)$, $p(2) = f(2)$ e $p'(2) = f'(2)$. Se $p(x) = a + bx + cx^2$ (e, dunque, $p'(x) = b + 2cx$) ciò significa che $a = 0$, $a + 2b + 4c = \sqrt{2}$ e $b + 4c = \frac{1}{2\sqrt{2}}$, ovvero $a = 0$, $b = \frac{3}{4}\sqrt{2}$ e $c = -\frac{1}{8}\sqrt{2}$. Ma allora

$$\begin{aligned} \sqrt{A} = p(A) &= \frac{3}{4}\sqrt{2}A - \frac{1}{8}\sqrt{2}A^2 = \\ &= \begin{pmatrix} \sqrt{2} & \sqrt{2} & \frac{5}{4}\sqrt{2} & 0 & 0 & 0 \\ 0 & 0 & -\sqrt{2} & 0 & 0 & 0 \\ 0 & 0 & \sqrt{2} & 0 & 0 & 0 \\ 0 & 0 & 0 & \sqrt{2} & \sqrt{2} & \frac{5}{4}\sqrt{2} \\ 0 & 0 & 0 & 0 & 0 & -\sqrt{2} \\ 0 & 0 & 0 & 0 & 0 & \sqrt{2} \end{pmatrix}. \end{aligned}$$

QUARTO ESERCIZIO

Un elemento $[m]_n$ è invertibile in (\mathbb{Z}_n, \cdot) se e solo se m è primo con n . Verifichiamo questa condizione nei diversi casi:

1. 228 e 14 sono entrambi pari e non sono, quindi, primi fra loro, pertanto $[228]_{14}$ non è invertibile.
2. Per verificare se 228 e 91 sono primi fra loro possiamo usare l'algoritmo euclideo. Consideriamo allora le divisioni successive:

$$\begin{aligned} 228 &= 91 \cdot 2 + 46 \\ 91 &= 46 \cdot 1 + 45 \\ 46 &= 45 \cdot 1 + 1 \end{aligned}$$

Dal momento che abbiamo ottenuto un resto uguale a 1 sappiamo che 228 e 91 sono primi tra loro. Dunque $[228]_{91}$ è invertibile. Inoltre utilizzando le divisioni precedentemente effettuate possiamo scrivere la catena di uguaglianze:

$$\begin{aligned} 1 &= 46 - 45 \cdot 1 = 46 - (91 - 46 \cdot 1) \cdot 1 = 46 \cdot 2 - 91 \\ &= (228 - 91 \cdot 2) \cdot 2 - 91 = 228 \cdot 2 - 5 \cdot 91. \end{aligned}$$

Ma allora $228 \cdot 2 \equiv 1 \pmod{91}$, ovvero $[228]_{91}^{-1} = [2]_{91}$.

3. Osserviamo che $[228]_{229} = [-1]_{229}$. Poiché $[-1]_{229} [-1]_{229} = [1]_{229}$ si ha che $[228]_{229}$ è invertibile e la sua inversa è $[228]_{229}$.
4. Per verificare se 228 e 323 sono primi fra loro applichiamo l'algoritmo euclideo:

$$\begin{aligned} 323 &= 228 \cdot 1 + 95 \\ 228 &= 95 \cdot 2 + 38 \\ 95 &= 38 \cdot 2 + 19 \\ 38 &= 19 \cdot 2 \end{aligned}$$

Poiché l'ultimo resto non nullo è diverso da 1 si ha che 323 e 228 non sono primi fra loro (in particolare il loro massimo comun divisore è 19): dunque $[228]_{323}$ non è invertibile.

5. Poiché 2280 è un multiplo di 228 si ha che 228 e 2280 non sono primi fra loro: dunque $[228]_{2280}$ non è invertibile.