Matematica Discreta (I modulo)

Primo appello, a.a. 1998/99

7 giugno 1999

Da svolgersi in tre ore, senza l'ausilio di appunti e/o libri.
Si ricorda che, anche se non esplicitamente richiesto nei testi, tutte le risposte alle domande devono essere adeguatamente *motivate* con dimostrazioni o confutazioni.

Esercizio 1 Si determini la soluzione dell'equazione ricorsiva lineare

$$x_{n+3} = x_{n+2} - x_{n+1} + x_n$$

con dati iniziali $x_0 = 0$, $x_1 = 1$, $x_2 = 2$.

Esercizio 2 Sia G un gruppo si definisca

$$Z(G) = \{g \in G \mid hg = gh \ \forall h \in G\}.$$

1. Si provi che $Z(G)$ è un sottogruppo di G.
2. Si dica, motivando la risposta, se $Z(G)$ è normale.
3. Si determini $Z(S_3)$.

Esercizio 3 Siano X un insieme e $x \in X$ un suo elemento. Si ponga

$$L = \{A \in \mathcal{P}(X) \mid x \in A\}.$$

Si dica, motivando la risposta, se

1. L, con le operazioni di $\cup$ e $\cap$ (unione e intersezione) è un reticolo.
2. $(L, \cup, \cap)$ è un sottoreticolo di $(\mathcal{P}(X), \cup, \cap)$.
3. $(L, \cup, \cap)$ è un'algebra di Boole.

Esercizio 4 Si consideri l'insieme

$$A = \left\{ \begin{pmatrix} a & b \\ 3b & a \end{pmatrix} \;\middle|\; a, b \in \mathbb{Q} \right\}$$

Si dica, motivando la risposta, se con le operazioni di somma e prodotto di matrici

1. A è un anello.
2. A è commutativo.
3. A è un campo.

Si provi che esiste un morfismo surgettivo $\varphi : \mathbb{Q}[x] \to A$ tale che

$$\varphi(a) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \ \forall a \in \mathbb{Q}, \qquad \varphi(x) = \begin{pmatrix} 0 & 1 \\ 3 & 0 \end{pmatrix}.$$

Si usi questo fatto per provare che $A \cong \mathbb{Q}[x]/_{(x^2 - 3)}$

Esercizio 5 Si provi che l'insieme dei numeri naturali le cui cifre (nella usuale scrittura decimale) sono tutte diverse è finito e se ne determini il numero di elementi.

Soluzioni proposte

Soluzione dell'esercizio 1 Il polinomio caratteristico dell'equazione è $P(x) = x^3 - x^2 + x - 1 = (x-1)(x^2+1)$ che ha tre radici distinte: 1, i e $-i$. Quindi una base dello spazio delle soluzioni dell'equazione ricorsiva è datta dalle tre successioni:

$$a_n = 1^n = 1, \quad b_n = i^n, \quad c_n = (-i)^n.$$

Quindi la soluzione generale dell'equazione è:

$$x_n = A + Bi^n + C(-i)^n \qquad A, B, C \in \mathbb{R}.$$

Imponendo le condizioni iniziali si ottiene il sistema lineare:

$$\begin{cases} 0 = x_0 = A + B + C \\ 1 = x_1 = A + iB - iC \\ 2 = x_2 = A - B - C \end{cases}$$

risolvendo il quale si ottiene:

$$A = 1, \quad B = -\frac{1}{2}, \quad C = -\frac{1}{2}.$$

Pertanto la soluzione del problema è la successione

$$x_n = 1 - i^n \frac{1 + (-1)^n}{2}.$$

❑

Soluzione dell'esercizio 2 $1 \in Z(G)$. Infatti $1h = h = h1$ per ogni $h \in G$.

$g_1, g_2 \in Z(G) \Rightarrow g_1 g_2 \in Z(G)$. Infatti, dato $h \in G$ si ha

$$\begin{aligned} g_1 g_2 h &= g_1 h g_2 && \text{poiché } g_2 \in Z(G) \\ &= h g_1 g_2 && \text{poiché } g_1 \in Z(G) \end{aligned}$$

e quindi, per l'arbitrarietà di h, $g_1 g_2 \in Z(G)$.

$g \in Z(G) \Rightarrow g^{-1} \in Z(G)$. Infatti, se $h \in G$ allora, dato che $g \in Z(G)$ si ha che $gh = hg$, ma allora, moltiplicando a sinistra e destra per g^{-1} entrambi i membri si ottiene $hg^{-1} = g^{-1}h$. Per l'arbitrarietà di $h \in G$ si conclude.

$Z(G)$ è normale. Proviamo che per ogni $x \in G$, $g \in Z(G)$ si ha che $x^{-1}gx \in Z(G)$. Infatti $x^{-1}gx = x^{-1}xg = 1g = g \in G$.

$Z(S_3) = \langle 1 \rangle$.

$$\left.\begin{aligned} (1\ 2)(2\ 3) &= (1\ 2\ 3) \\ (2\ 3)(1\ 2) &= (1\ 3\ 2) \end{aligned}\right\} \Rightarrow (1\ 2), (2\ 3) \notin Z(G)$$

$$\left.\begin{aligned} (1\ 3)(1\ 2\ 3) &= (1\ 2) \\ (1\ 2\ 3)(1\ 3) &= (2\ 3) \end{aligned}\right\} \Rightarrow (1\ 3), (1\ 2\ 3) \notin Z(G)$$

inoltre, dato che $(1\ 2\ 3) = (1\ 3\ 2)^{-1}$ allora anche $(1\ 3\ 2) \notin Z(G)$ (se ci stesse ci starebbe anche il suo inverso. Quindi l'unica permutazione di S_3 che appartiene a $Z(S_3)$ è l'identità. ❑

Soluzione dell'esercizio 3 Proviamo che L è un sottoreticolo di $\mathcal{P}(X)$. Basta provare che dati $A, B \in L$ allora $A \cup b$ e $A \cap B \in L$.

$$A, B \in L \Rightarrow x \in A, x \in B \Rightarrow \Big\langle \begin{array}{l} x \in A \cup B \Rightarrow A \cup B \in L \\ x \in A \cap B \Rightarrow A \cap B \in L \end{array}$$

Essendo un sottoreticolo di $(\mathcal{P}(X), \cup, \cap)$, L è in particolare un reticolo con le operazioni $\cup, \cap$.

$(L, \cup, \cap)$ è un'algebra di Boole. Dato che le operazioni di reticolo sono $\cup$ e $\cap$ allora la relazione d'ordine è l'inclusione $(\subseteq)$ ed evidentemente $\{x\}$ e X sono rispettivamente il minimo ed il massimo di L (se $A \in L$ allora $x \in L \subseteq X$ ossia $\{x\} \subseteq A \subseteq X$). Quindi il reticolo è limitato. Che sia distributivo segue dal fatto che le operazioni $\cup$ e $\cap$ sono distributive. Proviamo che ogni elemento ha un complemento. Se $A \in L$ consideriamo $A' = (x \setminus A) \cup \{x\}$. Allora chiaramente $x \in A'$ ed inoltre:

$$\begin{array}{l} A \cup A' = A \cup (X \setminus A) \cup \{x\} = X \cup \{x\} = X \\ A \cap A' = A \cap ((X \setminus A) \cup \{x\}) = (A \cap (X \setminus A)) \cup (A \cap \{x\}) = \varnothing \cup \{x\} = \{x\} \end{array}$$

dove la penultima uguaglianza segue dal fatto che $x \in A$. Dunque A' è un complemento per A e quindi il reticolo è anche complementato. $\square$

Soluzione dell'esercizio 4 Proviamo che A è un sottoanello dell'anello delle matrici. Evidentemente $0 \in A$ (si ottiene ponendo $a = b = 0$) resta da provare che se che se $M, N \in A$ allora $M + N \in A$, $MN \in A$, $-M \in A$. Cominciamo dall'ultima sia $M = \begin{pmatrix} a & b \\ 3b & a \end{pmatrix}$ allora

$$-M = -\begin{pmatrix} a & b \\ 3b & a \end{pmatrix} = \begin{pmatrix} -a & -b \\ -3b & -a \end{pmatrix} = \begin{pmatrix} -a & -b \\ 3(-b) & -a \end{pmatrix} \in A$$

Siano $M = \begin{pmatrix} a & b \\ 3b & a \end{pmatrix}$, $N = \begin{pmatrix} c & d \\ 3d & c \end{pmatrix} \in A$ allora

$$\begin{aligned} M + N &= \begin{pmatrix} a & b \\ 3b & a \end{pmatrix} + \begin{pmatrix} c & d \\ 3d & c \end{pmatrix} = \\ &= \begin{pmatrix} a+c & b+d \\ 3b+3d & a+c \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ 3(b+d) & a+c \end{pmatrix} \in A \end{aligned}$$

E anche

$$\begin{aligned} MN &= \begin{pmatrix} a & b \\ 3b & a \end{pmatrix} \begin{pmatrix} c & d \\ 3d & c \end{pmatrix} = \\ &= \begin{pmatrix} ac+3bd & ad+bc \\ 3bc+3ad & 3bd+ac \end{pmatrix} = \begin{pmatrix} ac+3bd & ad+bc \\ 3(ad+bc) & ac+3bd \end{pmatrix} \in A \end{aligned}$$

A è commutativo. Si osservi infatti che l'espressione per MN che abbiamo trovato sopra, resta invariata se si scambiano a con c e b con d ossia $MN = NM$.

A è un campo. Osserviamo innanzitutto che la matrice $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in A$ (si ottiene ponendo $a = 1$ e $b = 0$), quindi A è un anello unitario.

Una matrice è invertibile se e solo se il suo determinante è diverso da 0, ma se $M = \begin{pmatrix} a & b \\ 3b & a \end{pmatrix} \in A$ allora $\det M = a^2 - 3b^2$ e quindi $\det M = 0$ se e solo se $a^2 - 3b^2 = 0$ e quindi o $b = 0$ e $a = 0$ (ossia $M = 0$) oppure $|a/b| = \sqrt{3}$. Dato che $a, b \in \mathbb{Q}$ allora $|a/b| \in \mathbb{Q}$ mentree $\sqrt{3} \notin \mathbb{Q}$ e quindi l'ultima eventualità non si può verificare. In altre parole se $m \in A$ e $M \neq 0$ allora M è invertibile. Un semplice calcolo mostra che in questo caso

$$M^{-1} = \begin{pmatrix} \frac{a}{a^2-3b^2} & -\frac{b}{a^2-3b^2} \\ -\frac{3b}{a^2-3b^2} & \frac{a}{a^2-3b^2} \end{pmatrix} = \begin{pmatrix} \frac{a}{a^2-3b^2} & -\frac{b}{a^2-3b^2} \\ 3(-\frac{b}{a^2-3b^2}) & \frac{a}{a^2-3b^2} \end{pmatrix} \in A$$

quindi A è un campo.

Consideriam o l'applicazione $\psi : \mathbb{Q} \to A$ definita da $\psi(a) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$. È immediato verificare che ψ è un morfismo di anelli con identità, quindi per la proprietà universale dell'anello dei polinomi, esiste un unico morfismo $\varphi : \mathbb{Q}[x] \to A$ tale che

$$\begin{array}{ll} \varphi(a) = \psi(a) & \forall a \in \mathbb{Q} \\ \varphi(x) = \begin{pmatrix} 0 & 1 \\ 3 & 0 \end{pmatrix} & \end{array}$$

osserviamo inoltre che se $M = \begin{pmatrix} a & b \\ 3b & a \end{pmatrix}$ con $a, b \in \mathbb{Q}$ allora

$$\begin{aligned} \varphi(a+bx) &= \varphi(a) + \varphi(b)\varphi(x) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} + \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 3 & 0 \end{pmatrix} = \\ &= \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} + \begin{pmatrix} 0 & b \\ 3b & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ 3b & a \end{pmatrix} = M \end{aligned}$$

quindi φ è surgettivo.

Proviamo che $\ker \varphi = (x^2 - 3)$. Osserviamo innanzitutto che $x^2 - 3 \in \ker \varphi$, infatti

$$\begin{aligned} \varphi(x^2 - 3) &= \varphi(x)^2 - \varphi(3) = \begin{pmatrix} 0 & 1 \\ 3 & 0 \end{pmatrix}^2 - \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix} \\ &= \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix} - \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \end{aligned}$$

e quindi $(x^2 - 3) \subseteq \ker \varphi$.

Viceversa, sia $f \in \ker \varphi$, effettuando la divisione euclidea di f per $x^2 - 3$ si determinano $q, r \in \mathbb{Q}[x]$ tali che $f = (x^2-3)q + r$ con $\deg r < 2$, ossia $r = a + bx$. Ma allora

$$\begin{aligned} 0 &= \varphi(f) = \varphi((x^2 - 3)q + r) = \varphi(x^2 - 3)\varphi(q) + \varphi(r) = \\ &= 0\varphi(q) + \varphi(r) = \varphi(r) = \varphi(a + bx) = \begin{pmatrix} a & b \\ 3b & a \end{pmatrix} \end{aligned}$$

e quindi $a = b = 0$, ossia $(x^2 - 3) \mid f$ e quindi $f \in (x^2 - r)$.

Ma allora per il primo teorema di omomorfismo

$$A \cong \mathbb{Q}[x]/_{\ker \varphi} = \mathbb{Q}[x]/_{(x^2 - 3)}.$$

❏

Soluzione dell'esercizio 5 Indichiamo con A l'insieme in questione. Osserviamo che, per il "lemma dei cassetti", se un numero n ha un espansione decimale con più di 10 cifre allora almeno due cifre sono uguali, quindi l'insieme A è contenuto nell'insieme B dei numeri con espansione di al più 10 cifre, e quest'ultimo è finito in quanto $B = \{n \in \mathbb{N} \mid n \leq 9999999999\}$ ha 10^{10} elementi.

Per ogni $i = 1, 2, \ldots, 10$ indichiamo con A_i l'insieme dei numeri diversi da 0 costituiti da i cifre distinte. Chiaramente $A = \{0\} \cup \bigcup_{i=1}^{10} A_i$ e $A_i \cap A_j = \varnothing$ se $i \neq j$, $\{)\} \cap A_i = \varnothing$ per ogni i e quindi

$$|A| = 1 + \sum_{i=1}^{10} |A_i|.$$

Calcoliamo $|A_i|$ per ogni i. Se $n \in A_i$ è diverso da 0, allora la sua prima cifra può essere un arbitrario numero $1, \ldots, 9$ (lo 0 non può essere la cifra iniziale) e quindi per la sua scelta si hanno 9 possibilità. Fissata la prima cifra, le restanti $i - 1$ possono essere scelte tra le rimanenti 9 cifre in modo che siano a due a due diverse, ossia in modo che l'applicazione che ad ognuno degli $i - 1$ "posti vuoti" associa una di queste 9 cifre sia iniettiva. Quindi fatta la prima scelta si hanno $9!/(9 - i + 1)!$ scelte possibili: tante quante le applicazioni iniettive da un insieme di $i - 1$ elementi in uno di 9 elementi. In definitiva

$$|A_i| = \frac{9 \cdot 9!}{(9 - i + 1)!} \quad \forall i = 1, \ldots, 10$$

e quindi

$$|A| = 1 + \sum_{i=1}^{10} \frac{9 \cdot 9!}{(9 - i + 1)!} = 1 + 9 \cdot 9! \sum_{i=1}^{10} \frac{1}{(9 - i + 1)!} = 1 + 9 \cdot 9! \sum_{j=0}^{9} \frac{1}{j!}.$$

❏