Matematica Discreta (I modulo)

Secondo appello, a.a. 1998/99

7 luglio 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 l'insieme delle soluzioni del sistema di congruenze:

$$\begin{cases} x \equiv 165 & \mod 164 \\ x \equiv 79 & \mod 75 \end{cases}$$

Esercizio 2 Si determini la soluzione dell'equazione ricorsiva lineare

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

con dati iniziali $x_0 = 2$ e $x_1 = 2$.

Esercizio 3 Sia $G = \{\alpha \in \mathbb{C} \mid \exists n \in \mathbb{N} - \{0\} : \alpha^n = 1\}$. Si provi che $(G, \cdot)$ è un gruppo.

Esercizio 4 Sia $(B, \vee, \wedge, ', 0, 1)$ un'algebra di Boole; un elemento $a \in B$ si dice un *atomo* se

$$a \neq 0 \quad \text{e} \quad a = b \vee c \Rightarrow b = a \text{ oppure } c = a. \tag{1}$$

1. Si provi che a è un atomo se e solo se

   $$a \neq 0 \quad \text{e} \quad b \leq a \Rightarrow b = 0 \text{ oppure } b = a. \tag{2}$$

   essendo $\leq$ l'ordinamento parziale indotto dalla struttura di algebra di Boole.

2. Si usi il punto precedente per provare che se B è un'algebra di Boole finita allora possiede atomi e se ne calcoli il numero in funzione del numero di elementi di B.

Esercizio 5 Si consideri l'insieme

$$A = \left\{ \begin{pmatrix} a & b \\ 4b & a \end{pmatrix} \middle| \, a, b \in \mathbb{Q} \right\}$$

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 dominio d'integrità.
4. A è un campo.

Soluzioni proposte

Soluzione dell'esercizio 1 Dato che $165 \equiv 1 \mod 164$ e $79 \equiv 4 \mod 75$ il sistema è equivalente a:

$$\begin{cases} x \equiv 1 & \mod 164 \\ x \equiv 4 & \mod 75 \end{cases}$$

Calcoliamo il massimo comun divisore tra 164 e 75 usando l'algoritmo di Euclide.

$$\begin{aligned} 164 &= 75 \cdot 2 + 14 \\ 75 &= 14 \cdot 5 + 5 \\ 14 &= 5 \cdot 2 + 4 \\ 5 &= 4 \cdot 1 + 1 \\ 4 &= 1 \cdot 4 \end{aligned}$$

quindi $(164, 75) = 1$ e quindi il sistema di congruenze ha soluzione (dato che $(164, 75) \mid 1 - 4$. Esprimiamo 1 come combinazione intera di 113 e 84.

$$\begin{array}{rclcrcl} & & & \quad & 164 &=& 164(1) + 75(0) \\ & & & & 75 &=& 164(0) + 75(1) \\ 14 &=& 164 - 75 \cdot 2 & & 14 &=& 164(1) + 75(-2) \\ 5 &=& 75 - 14 \cdot 5 & & 5 &=& 164(-5) + 75(11) \\ 4 &=& 14 - 5 \cdot 2 & & 4 &=& 164(11) + 75(-24) \\ 1 &=& 5 - 4 & & 1 &=& 164(-16) + 75(35) \end{array}$$

Quindi,

$$1 - 4 = -3 = -3(164(-16) + 75(35)) = 164 \cdot 48 + 75 \cdot (-105)$$

e per tanto

$$-7871 = 1 - 164 \cdot 48 = 4 + 75 \cdot (-105)$$

è una soluzione del sistema. Dato che il minimo comune multiplo tra 164 e 75 è dato da $[164, 75] = 164 \cdot 75/(164, 75) = 164 \cdot 75 = 12300$, l'insieme delle soluzioni del sistema è:

$$\{-7871 + k12300 \mid k \in \mathbb{Z}\} = \{4429 + k12300 \mid k \in \mathbb{Z}\}.$$

❏

Soluzione dell'esercizio 2 Il polinomio caratteristico è dato da $x^2 - 2x + 2$ le cui radici sono $1 + i$ e $1 - i$, quindi una base dello spazio delle soluzioni è data dalle due successioni $a_n = (1 + i)^n$ e $b_n = (1 - i)^n$, quindi la soluzione generale dell'equazione è data da:

$$x_n = A(1 + i)^n + B(1 - i)^n \quad A, B \in \mathbb{C}.$$

Imponendo le condizioni iniziali si ottiene il sistema

$$\begin{cases} 2 = x_0 = A + B \\ 2 = x_1 = A(1 + i) + B(1 - i) \end{cases}$$

risolvendo il quale si ottiene $A = B = 1$, e quindi la soluzione è:

$$x_n = (1 + i)^n + (1 - i)^n = \Re e((1 + i)^n) = \sqrt{2^n} \cos \frac{\pi n}{4}.$$

❏

Soluzione dell'esercizio 3 Siano $\alpha, \beta \in G$ quindi esistono $n, m \in \mathbb{N} - \{0\}$ tali che $\alpha^n = \beta^m = 1$. Ma allora

$$(\alpha\beta)^{nm} = \alpha^{nm}\beta^{nm} = (\alpha^n)^m(\beta^m)^n = 1^m 1^n = 1 \cdot 1 = 1$$

dato che $nm \in \mathbb{N} - \{0\}$, allora $\alpha\beta \in G$ e quindi G è chiuso rispetto al prodotto.

Evidentemente $1 \in G$, dato che $1^1 = 1$.

Se $\alpha \in G$ allora $\alpha^-1 \in G$. Infatti esiste $n \in \mathbb{N} - \{0\}$ tale che $\alpha^n = 1$, ma allora $(\alpha^{-1})^n = (\alpha^n)^{-1} = 1^{-1} = 1$.

Coò basta per concludere, dato che il prodotto di numeri complessi è associativo. ❏

Soluzione dell'esercizio 4 (1)⇒(2). Supponiamo che $b \leq a$, ossia, per definizione di ordinamento indotto, $b = a \wedge b$. Dato che $b \vee b' = 1$ si ha:

$$a = a \wedge 1 = a \wedge (b \vee b') = (a \wedge b) \vee (a \wedge b') = b \vee (a \wedge b')$$

ma allora, per (1) o $b = a$ oppure $(a \wedge b') = a$, ma da quest'ultima segue allora che

$$0 = a \wedge 0 = a \wedge (b' \wedge b) = (a \wedge b') \wedge b = a \wedge b = b$$

essendo l'ultima uguaglianza data da $b \leq a$. Ciò conclude la prova.

(2)⇒(1). Supponiamo che $a = b \vee c$, allora $b \leq a$ e quindi, per (2), si ha che o $b = a$ oppure $b = 0$ e quindi $a = 0 \vee c = c$.

Proviamo olra il secondo punto. Se B è un'algebra di Boole finita, allora, per il teorema di rappresentazione, è isomorfa all'algebra di Boole $\mathcal{P}(X)$ delle parti di un insieme finito X. Per il punto precedente, gli atomi sono allora i sottoinsiemi A di X che non contengono alcun sottoinsieme diverso da $\varnothing$ ossia sono i sottoinsiemi costituiti da un solo elemento, e quindi sono tanti quanti gli elementi di X. In definitiva se $|X|$ ha n elementi, $|B| = 2^n$ e quindi gli atomi di B sono $n = \log_2(|B|)$. ❏

Soluzione dell'esercizio 5 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 $M = \begin{pmatrix} a & b \\ 4b & a \end{pmatrix}$ allora

$$-M = -\begin{pmatrix} a & b \\ 4b & a \end{pmatrix} = \begin{pmatrix} -a & -b \\ -4b & -a \end{pmatrix} = \begin{pmatrix} -a & -b \\ 4(-b) & -a \end{pmatrix} \in A$$

Siano $M = \begin{pmatrix} a & b \\ 4b & a \end{pmatrix}$, $N = \begin{pmatrix} c & d \\ 4d & c \end{pmatrix} \in A$ allora

$$\begin{aligned} M + N &= \begin{pmatrix} a & b \\ 4b & a \end{pmatrix} + \begin{pmatrix} c & d \\ 4d & c \end{pmatrix} = \\ &= \begin{pmatrix} a+c & b+d \\ 4b+4d & a+c \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ 4(b+d) & a+c \end{pmatrix} \in A \end{aligned}$$

E anche

$$\begin{aligned} MN &= \begin{pmatrix} a & b \\ 4b & a \end{pmatrix}\begin{pmatrix} c & d \\ 4d & c \end{pmatrix} = \\ &= \begin{pmatrix} ac+4bd & ad+bc \\ 4bc+4ad & 4bd+ac \end{pmatrix} = \begin{pmatrix} ac+4bd & ad+bc \\ 4(ad+bc) & ac+4bd \end{pmatrix} \in A \end{aligned}$$

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 non è un dominio. Osserviamo infatti che

$$\begin{pmatrix} 2 & 1 \\ 4 & 2 \end{pmatrix}\begin{pmatrix} -2 & 1 \\ 4 & -2 \end{pmatrix} = \begin{pmatrix} -4+4 & 2-2 \\ -8+8 & -4+4 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

in particolare allora non è nemmeno un campo (si ricordi che ogni dominio è un campo). ❏