Università degli Studi Roma Tre
Corso di Laurea Triennale in Matematica, a.a. 2009/2010
AL110 - Algebra 1
Soluzioni dell'appello B
9 Febbraio 2010

*Cognome*_____ *Nome*_____

*Numero di matricola*_____

Avvertenza: Svolgere ogni esercizio nello spazio assegnato, senza consegnare altri fogli e **giustificando tutte le affermazioni fatte**. Non è consentito l'uso di libri, appunti. E' consentito l'uso della calcolatrice.

1. (a) Utilizzando il principio di induzione si dimostri che per ogni numero naturale $n \geq 1$ si ha :

$$\frac{1}{2} + \frac{2}{2^2} + \frac{3}{2^3} + \cdots + \frac{n}{2^n} = 2 - \frac{n+2}{2^n}.$$

   (b) Si considerino i numeri C_n con $n \geqslant 1$ definiti induttivamente nel seguente modo:

$$C_1 = 1 \quad \text{e, per } n \geqslant 2, \quad C_n = \frac{2(2n-1)}{n+1} C_{n-1}$$

   Utilizzando il principio di induzione si dimostri che per ogni numero naturale $n \geq 1$ si ha :

$$C_n = \frac{(2n)!}{n!(n+1)!}$$

Soluzione

(a) Base dell'induzione: per $n = 1$ si ha che $2 - \frac{3}{2} = \frac{1}{2}$.
Passo induttivo: sia $n \geq 1$ e supponiamo che

$$\frac{1}{2} + \frac{2}{2^2} + \frac{3}{2^3} + \cdots + \frac{n}{2^n} = 2 - \frac{n+2}{2^n};$$

proviamo che

$$\frac{1}{2}+\frac{2}{2^2}+\frac{3}{2^3}+\cdots+\frac{n}{2^n}+\frac{n+1}{2^{n+1}}=2-\frac{n+3}{2^{n+1}}.$$

$$\begin{aligned}\frac{1}{2}+\frac{2}{2^2}+\frac{3}{2^3}+\cdots+\frac{n}{2^n}+\frac{n+1}{2^{n+1}} &= 2-\frac{n+2}{2^n}+\frac{n+1}{2^{n+1}}\\ &= 2-\frac{2n+4-n-1}{2^{n+1}}\\ &= 2-\frac{n+3}{2^{n+1}}\end{aligned}$$

(b) Base dell'induzione: per $n=1$ si ha che $\frac{(2)!}{1!(1+1)!}=1=C_1$.

Passo induttivo: sia $n\geq 1$ e supponiamo che $C_n=\frac{(2n)!}{n!(n+1)!}$; proviamo che $C_{n+1}=\frac{(2n+2)!}{(n+1)!(n+2)!}$.

$$\begin{aligned}C_{n+1} &= \frac{2(2n+1)}{n+2}C_n\\ &= \frac{2(2n+1)}{n+2}\frac{(2n)!}{n!(n+1)!}\\ &= \frac{2(2n+1)(2n)!}{(n+2)n!(n+1)!}\\ &= \frac{2(2n+1)(2n)!}{(n+2)n!(n+1)!}\end{aligned}$$

2. Sia $f:\mathbb{R}\longrightarrow\mathbb{R}$ l'applicazione definita da:

$$x\longmapsto\begin{cases}x^2+3 & \text{se } |x|<7\\ \cos x & \text{se } |x|\geqslant 7\end{cases}$$

(a) Stabilire se l'applicazione f è iniettiva.

(b) Descrivere $\mathtt{Im}(f)$.

(c) Sia ρ_f la relazione nucleo di f. Descrivere $[1]_{\rho_f}$ e $[7]_{\rho_f}$.

Soluzione

(a) f non è iniettiva poiché esistono elementi di $\mathbb{R}$ distinti x,x' tali che $f(x)=f(x')$, ad esempio $f(1)=4=f(-1)$.

(b) Se $|x|<7$, allora $f(x)\in[3,52)$; se $|x|\geqslant 7$, allora $f(x)\in[-1,1]$; pertanto $\mathtt{Im}(f)\subseteq[3,52)\cup[-1,1]$.
Inoltre per ogni $y\in[-1,1]$ esiste $x\in\mathbb{R}$ con $|x|\geqslant 7$ tale che $y=\cos x$; inoltre per ogni $z\in[3,52)$ si ha che $\sqrt{z-3}$ è un numero reale non negativo e minore di 7 tale che $f(\sqrt{z-3})=z$ In conclusione

$$\mathtt{Im}(f)=[-1,1]\cup[3,52)\,.$$

(c) $[1]_{\rho_f} = \{x \in \mathbb{R} \mid f(x) = f(1)\} = \{x \in \mathbb{R} \mid f(x) = 4\} = \{1, -1\}$;
$[7]_{\rho_f} = \{x \in \mathbb{R} \mid f(x) = f(7)\} = \{x \in \mathbb{R} \mid f(x) = \cos 7\} = \{\pm 7 + 2\pi k \mid k \in \mathbb{Z}\} - (-7,\ 7)$.

3. Dato un insieme X, si denoti con $\mathcal{P}^*(X)$ l'insieme delle sue parti privato dell'insieme vuoto.

   Si consideri su $\mathcal{P}^*(\mathbb{N}) \times \mathcal{P}^*(\mathbb{N})$ la seguente relazione:

   $$(A, B) \leq (C, D) :\Longleftrightarrow (A \subsetneq C) \text{ oppure } (A = C \text{ e } B \subseteq D).$$

   (a) Dimostrare che $\leq$ è una relazione d'ordine.

   (b) Stabilire se la relazione d'ordine $\leq$ è totale.

   (c) Calcolare gli eventuali elementi massimali, minimali, massimo e minimo.

   (d) Si consideri la seguente applicazione:

   $$\begin{array}{rcl} i : \mathcal{P}^*(\mathbb{N}) \times \mathcal{P}^*(\mathbb{N}) & \longrightarrow & \mathcal{P}(\mathbb{N} \times \mathbb{N}) \\ (A, B) & \longmapsto & \{(a, b) : a \in A, b \in B\}. \end{array}$$

   i. Dimostrare che i è iniettiva.

   ii. Dimostrare o confutare il seguente asserto:

   $$(A, B) \leq (C, D) \Longleftrightarrow i((A, B)) \subseteq i((C, D)), \forall A, B, C, D \in \mathcal{P}^*(\mathbb{N})$$

Soluzione

(a) $\leq$ gode delle seguenti proprietà:

i. riflessiva:
per ogni $(A, B) \in \mathcal{P}^*(\mathbb{N}) \times \mathcal{P}^*(\mathbb{N})$ si ha che

$$(A, B) \leq (A, B)$$

poiché $A = A$ e $B \subseteq B$;

ii. antisimmetrica:
siano $(A, B),\ (C, D) (\in \mathcal{P}^*(\mathbb{N}) \times \mathcal{P}^*(\mathbb{N})$ tali che $(A, B) \leq (C, D)$ e $(C, D) \leq (A, B)$; da $(A, B) \leq (C, D)$ segue che $A \subsetneq C$ oppure $A = C$ e $B \subseteq D$; se fosse $A \subsetneq C$, non potrebbe essere $(C, D) \leq (A, B)$; pertanto $A = C$ e $B \subseteq D$; da $(C, D) \leq (A, B)$ segue che $D \subseteq B$; in conclusione si ha che $(A, B) = (C, D)$.

iii. transitiva:
siano $(A, B),\ (C, D),\ (E, F) \in \mathcal{P}^*(\mathbb{N}) \times \mathcal{P}^*(\mathbb{N})$ tali che $(A, B) \leq (C, D)$ e $(C, D) \leq (E, F)$; da $(A, B) \leq (C, D)$ segue che $A \subsetneq C$ oppure $A = C$ e $B \subseteq D$; da $(C, D) \leq (E, F)$ segue che $C \subsetneq E$ oppure $C = E$ e $D \subseteq F$.

Sia $A \subsetneq C$; essendo in ogni caso $C \subseteq E$, si ha che $A \subsetneq E$, da cui $(A, B) \leq (E, F)$.
Sia $A = C$ e $B \subseteq D$; se $C \subsetneq E$, allora anche $A \subsetneq E$, da cui $(A, B) \leq (E, F)$; se $C = E$ e $D \subseteq F$, allora $A = E$ e $B \subseteq F$, da cui $(A, B) \leq (E, F)$.

(b) La relazione d'ordine $\leq$ non è totale: ad esempio, se $\mathbb{P}$ è l'insieme dei numeri naturali pari e $\mathbb{D}$ è l'insieme dei numeri naturali dispari, allora $(\mathbb{P}, \mathbb{D}) \nleq (\mathbb{D}, \mathbb{P})$ e $(\mathbb{D}, \mathbb{P}) \nleq (\mathbb{P}, \mathbb{D})$.

(c) $(\mathbb{N}, \mathbb{N}) \in \mathcal{P}^*(\mathbb{N}) \times \mathcal{P}^*(\mathbb{N})$ è tale che per ogni $(A, B) \in \mathcal{P}^*(\mathbb{N}) \times \mathcal{P}^*(\mathbb{N})$ si ha che $(A, B) \leq (\mathbb{N}, \mathbb{N})$; pertanto $(\mathbb{N}, \mathbb{N})$ è il massimo .

Siano $n, m \in \mathbb{N}$; allora $(\{n\}, \{m\})$ è un elemento minimale: sia $(A, B) \in \mathcal{P}^*(\mathbb{N}) \times \mathcal{P}^*(\mathbb{N})$ tale che $(A, B) \leq (\{n\}, \{m\})$; essendo $A \neq \emptyset$ e $B \neq \emptyset$, si ha che $(A, B) = (\{n\}, \{m\})$. E' immediato verificare che se A è un sottoinsieme di $\mathbb{N}$ con almeno due elementi, allora per ogni sottoinsieme di $\mathbb{N}$ non vuoto, (A, B) non è un elemento minimale; analogamente per B sottoinsieme di $\mathbb{N}$ con almeno due elementi. Si può pertanto concludere che gli unici elementi minimali di $(\mathcal{P}^*(\mathbb{N}) \times \mathcal{P}^*(\mathbb{N}), \leq)$ sono $(\{n\}, \{m\})$, con $n, m \in \mathbb{N}$. Essendoci infiniti elementi minimali, ovviamente non esiste minimo.

i. Siano $(A, B),\ (C, D) (\in \mathcal{P}^*(\mathbb{N}) \times \mathcal{P}^*(\mathbb{N})$ tali che $(A, B) \neq (C, D)$; allora $A \neq C$ oppure $B \neq D$;
se $A \neq C$, allora esiste $a \in A - C$ oppure esiste $c \in C - A$; siano b un elemento di B comunque scelto e d un elemento di D comunque scelto ; se esiste $a \in A - C$, allora $(a, b) \in i(A, B) - i(C, D)$; se esiste $c \in C - A$, allora $(c, d) \in i(C, D) - i(A, B)$.
Analogamente se $B \neq D$.

ii. Esistono sottoinsiemi $A,\ B,\ C,\ D$ non vuoti di $\mathbb{N}$ tali che $(A, B) \leq (C, D)$ e $i((A, B)) \nsubseteq i((C, D))$, ad esempio $A = \{1\}$, $B = \{3\}$, $C = \{1,\ 2\}$ e $D = \{7\}$; pertanto non è vero che

$$(A, B) \leq (C, D) \iff i((A, B)) \subseteq i((C, D)), \forall A, B, C, D \in \mathcal{P}^*(\mathbb{N})$$

è banalmente vero che $\forall A, B, C, D \in \mathcal{P}^*(\mathbb{N})$

$$i((A, B)) \subseteq i((C, D)) \Longrightarrow (A, B) \leq (C, D).$$

4. (a) Sia: $\sigma := (156) \circ (68) \circ (543) \circ (1374) \in S_8$.

i. Scrivere σ come prodotto di cicli disgiunti e determinarne l'ordine e la parità.

ii. Calcolare σ^2 e σ^4.

iii. Sia $\tau := (73) \circ (36) \in S_8$. Calcolare $\sigma \circ \tau$, $\tau^{-1} \circ \sigma^{-1}$.

(b) Sia $n \in \mathbb{N}_+$. Provare che se a è un numero naturale positivo tale che $\sqrt[n]{a}$ è un numero razionale, allora $\sqrt[n]{a}$ è un numero intero.

(c) **(FAC.)** Provare che se n è un numero naturale positivo $\geqslant 2$, allora $\sqrt[n]{n}$ è un numero irrazionale.

Soluzione

(a) i. La decomposizione di σ come prodotto di cicli disgiunti è:

$$\sigma = (168) \circ (37) \circ (45).$$

L'ordine di σ è dato dal $\mathrm{mcm}(3,2) = 6$; σ è pari in quanto prodotto di una permutazione pari e di due permutazioni dispari.

ii. $\sigma^2 = (168)^2 \circ (37)^2 \circ (45)^2 = (186)$ e $\sigma^4 = (168)$.

iii. $\tau = (367)$;
$\sigma \circ \tau = (1638) \circ (45)$;
$\tau^{-1} \circ \sigma^{-1} = (\sigma \circ \tau)^{-1} = (1836) \circ (45)$.

(b) Sia a un numero naturale positivo tale che $\sqrt[n]{a}$ è un numero razionale; allora esistono $b, c \in \mathbb{N}_+$ primi tra lora tali che $\sqrt[n]{a} = \frac{b}{c}$; da $c\sqrt[n]{a} = b$, elevando alla potenza $n-$esima, si ottiene $c^n a = b^n$; sappiamo che, essendo b e c primi tra loro, anche b^n e c^n sono primi tra loro; sia $1 = \lambda b^n + \mu c^n$ una loro identità di Bézout; allora $1 = \lambda c^n a + \mu c^n = c^n(\lambda a + \mu)$ da cui segue che $c = 1$; pertanto $\sqrt[n]{a}$ è un numero intero.

(c) **(FAC.)** Sia n è un numero naturale positivo $\geqslant 2$; se $\sqrt[n]{n}$ fosse un numero razionale, per il punto precedente $\sqrt[n]{n}$ sarebbe un numero naturale positivo m, cioè $\sqrt[n]{n} = m$; essendo $n \geqslant 2$, si avrebbe che $m \geqslant 2$; si avrebbe quindi che $n = m^n \geqslant 2^n$ e ciò contraddice il fatto che per ogni $t \in \mathbb{N}_+$ si ha che $2^t > t$ (dimostrarlo per induzione su t)

5. (a) Verificare che il gruppo moltiplicativo $(U(\mathbb{Z}_{15}), \cdot)$ non è ciclico.

(b) Verificare che il gruppo moltiplicativo $(U(\mathbb{Z}_{18}), \cdot)$ è ciclico.

(c) Si consideri l'anello commutativo unitario

$$\left(\mathbb{R}^{[0,1]} = \{f : [0,1] \longrightarrow \mathbb{R} \mid f \text{ applicazione}\}, +, \cdot\right)$$

con $+, \cdot$ definiti nel seguente modo:

$$(f+g)(x) = f(x) + g(x), \qquad (f \cdot g)(x) = f(x)g(x)$$

per ogni $x \in [0,1]$ e per ogni $f, g \in \mathbb{R}^{[0,1]}$.

Stabilire se questo anello è un dominio d'integrità e/o un campo.

Scrivere esplicitamente un elemento di $\mathbb{R}^{[0,1]}$ invertibile (e diverso dall'elemento neutro moltiplicativo).

Soluzione

(a) $U(\mathbb{Z}_{15}) = \{[a] \in \mathbb{Z}_{15} \mid a \text{ è primo con } 15\} =$
$= \{[1],\ [2],\ [4],\ [7],\ [8],\ [11],\ [13],\ [14]\}$.
$U(\mathbb{Z}_{15})$ ha $\varphi(15) = \varphi(3)\varphi(5) = 2 \cdot 4 = 8$ elementi.
L'ordine di [2] è 4: $[2]^2 = [4]$, $[2]^3 = [8]$ e $[2]^4 = [1]$; inoltre l'ordine di [4] e l'ordine di [8] sono divisori di 4.
L'ordine di [7] è 4: $[7]^2 = [4]$, $[7]^3 = [13]$ e $[7]^4 = [1]$; inoltre l'ordine di [13] è un divisore di 4.
L'ordine di [11] è 2 così come l'ordine di $[14] = [-1]$.
Poiché nessuno degli elementi di $(U(\mathbb{Z}_{15}), \cdot)$ ha ordine 8, $(U(\mathbb{Z}_{15}), \cdot)$ non è ciclico

(b) $U(\mathbb{Z}_{18}) = \{[a] \in \mathbb{Z}_{18} \mid a \text{ è primo con } 18\} =$
$= \{[1],\ [5],\ [7],\ [11],\ [13],\ [17]\}$.
$U(\mathbb{Z}_{18})$ ha $\varphi(18) = \varphi(2)\varphi(3^2) = 6$ elementi.
L'ordine di [5] è 6: $[5]^2 = [7]$, $[5]^3 = [17]$, $[5]^4 = [13]$, $[5]^5 = [11]$ e $[5]^6 = [1]$; pertanto $U(\mathbb{Z}_{18})$ è ciclico ed ha $\varphi(6) = \varphi(2)\varphi(3) = 2$ generatori; l'altro generatore è $[5]^5 = [11]$.

(c) $\mathbb{R}^{[0,1]}$ con l'addizione e la moltiplicazione definite puntualmente non è un dominio d'integrità; ad esempio siano φ l'applicazione da $[0,1]$ in $\mathbb{R}$ definita da

$$x \longmapsto \begin{cases} 0 & \text{se } 0 \leqslant x < \frac{1}{2} \\ x & \text{se } \frac{1}{2} \leqslant x \end{cases}$$

e ψ l'applicazione da $[0,1]$ in $\mathbb{R}$ definita da

$$x \longmapsto \begin{cases} x & \text{se } 0 \leqslant x < \frac{1}{2} \\ 0 & \text{se } \frac{1}{2} \leqslant x \end{cases}$$

Allora φ e ψ sono entrambe diverse dalla applicazione da $[0,1]$ in $\mathbb{R}$ identicamente nulla, cioè dallo zero di $\mathbb{R}^{[0,1]}$, ed il loro prodotto è lo zero di $\mathbb{R}^{[0,1]}$. Non essendo $\mathbb{R}^{[0,1]}$ un dominio d'integrità, esso non è neanche un campo.
Essendo l'elemento neutro moltiplicativo di $\mathbb{R}^{[0,1]}$ costituito dalla applicazione da $[0,1]$ in $\mathbb{R}$ identicamente uguale ad 1, un elemento f di $\mathbb{R}^{[0,1]}$ è invertibile se e solo se $f(x) \neq 0$ per ogni $x \in [0,1]$. Un elemento di $\mathbb{R}^{[0,1]}$ invertibile è l'applicazione da $[0,1]$ in $\mathbb{R}$ identicamente uguale a 2.

6. (a) Trovare il MCD e dare una identità di Bézout per i seguenti due polinomi di $\mathbb{Q}[X]$:

$$X^4 - X^3 + 4X^2 - X + 3 \text{ e } X^3 - 2X^2 + X - 2$$

(b) Decomporre il polinomio $f(X) = X^4 - X^2 - 2 \in \mathbb{Z}[X]$ in fattori irriducibili in $\mathbb{C}[X]$, $\mathbb{R}[X]$, $\mathbb{Q}[X]$ e $\mathbb{Z}[X]$.

(c) Decomporre i polinomi

$$g(X) = X^4 + 1 \in \mathbb{Z}_5[X] \text{ e } h(X) = X^3 + 3X^2 + 2X + 1 \in \mathbb{Z}_5[X]$$

in fattori irriducibili in $\mathbb{Z}_5[X]$.

Soluzione

(a) $X^4 - X^3 + 4X^2 - X + 3 = (X^3 - 2X^2 + X - 2)(X + 1) + 5X^2 + 5$
$X^3 - 2X^2 + X - 2 = (5X^2 + 5)(\frac{1}{5}X - \frac{2}{5})$
Pertanto il MCD$(X^4 - X^3 + 4X^2 - X + 3, X^3 - 2X^2 + X - 2) = X^2 + 1$ e una identità di Bézout è:

$$X^2 + 1 = \frac{1}{5}(X^4 - X^3 + 4X^2 - X + 3) - \frac{1}{5}(X^3 - 2X^2 + X - 2)(X + 1)$$

(b) Ponendo $Y = X^2$ si ha che $Y^2 - Y - 2 = (Y - 2)(Y + 1)$; allora $\pm\sqrt{2}$ sono le radici reali di $X^2 - 2$ e $\pm i$ sono le radici complesse di $X^2 + 1$.
Allora la decomposizione del polinomio $f(X) = X^4 - X^2 - 2$ in fattori irriducibili in $\mathbb{C}[X]$ è:

$$(X - i)(X + i)(X - \sqrt{2})(X + \sqrt{2});$$

la decomposizione del polinomio $f(X) = X^4 - X^2 - 2$ in fattori irriducibili in $\mathbb{R}[X]$ è:

$$(X^2 + 1)(X - \sqrt{2})(X + \sqrt{2})$$

la decomposizione del polinomio $f(X) = X^4 - X^2 - 2$ in fattori irriducibili in $\mathbb{Q}[X]$ è:

$$(X^2 + 1)(X^2 - 2)$$

la decomposizione del polinomio $f(X) = X^4 - X^2 - 2$ in fattori irriducibili in $\mathbb{Z}[X]$ è:

$$(X^2 + 1)(X^2 - 2).$$

(c) E' immediato verificare che il polinomio $g(X) = X^4 + 1 \in \mathbb{Z}_5[X]$ è privo di radici in $\mathbb{Z}_5$; $X^4 + 1$ potrebbe decomporsi nel prodotto di due polinomi di secondo grado; da $X^4 + 1 = (X^2 + aX + b)(X^2 + a'X + b')$ si ottiene che il sistema

$$\begin{cases} a + a' &= 0 \\ b + b' + aa' &= 0 \\ ab' + a'b &= 0 \\ bb' &= 1 \end{cases}$$

ammette come soluzione $b = 2$, $b' = 3$, $a = a' = 0$. Pertanto la decomposizione di $X^4 + 1$ in fattori irriducibili in $\mathbb{Z}_5[X]$ è:

$$X^4 + 1 = (X^2 + 2)(X^2 + 3).$$

$h(X) = X^3 + 3X^2 + 2X + 1 \in \mathbb{Z}_5[X]$ ha soltanto 2 come radice in $\mathbb{Z}_5[X]$; dividendo $h(X)$ per $X - 2$ si ottiene

$$h(X) = X^3 + 3X^2 + 2X + 1 = (X - 2)(X^2 + 2)$$

che risulta essere la decomposizione di $h(X)$ in fattori irriducibili poiché 2 non é radice di $(X^2 + 2)$.