Università degli Studi Roma Tre
Corso di Laurea Triennale in Matematica, a.a. 2009/2010
AL110 - Algebra 1
Soluzioni dell'appello A
26 Gennaio 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 :

$$21 \mid 4^{n+1} + 5^{2n-1}$$

   (b) Siano i numeri s_n definiti da $s_1 = 1$ e $s_n = s_{n-1} + (3n-2)$ per $n \geqslant 2$.

      i. Utilizzando il principio di induzione, provare che per ogni numero naturale $n \geqslant 1$ si ha:

$$s_n = \frac{n(3n-1)}{2}$$

      ii. Provare che per ogni numero naturale $n \geqslant 2$ si ha:

$$s_n = \binom{n}{2} + n^2$$

Soluzione

(a) Base dell'induzione: per $n = 1$ si ha che $4^2 + 5 = 21$ e $21 \mid 21$.
Passo induttivo: sia $n \geq 1$ e supponiamo che $21 \mid 4^{n+1} + 5^{2n-1}$; proviamo che $21 \mid 4^{n+2} + 5^{2n+1}$.

$$\begin{aligned}4^{n+2}+5^{2n+1} =& 4\cdot 4^{n+1}+5^2\cdot 5^{2n-1}\\ =& 4\cdot 4^{n+1}+(21+4)\cdot 5^{2n-1}\\ =& 4\cdot 4^{n+1}+21\cdot 5^{2n-1}+4\cdot 5^{2n-1}\\ =& 21\cdot 5^{2n-1}+4\cdot(4^{n+1}+5^{2n-1})\end{aligned}$$

Poiché per l'ipotesi induttiva $21 \mid 4^{n+1}+5^{2n-1}$, si ha che $21 \mid 4^{n+2}+5^{2n+1}$.

(b) i. Base dell'induzione: per $n=2$ si ha che $s_2 = s_1 + (3\cdot 2-2) = 1+4=5$ e $\frac{2(3\cdot 2-1)}{2}=5$; pertanto $s_2=\frac{2(3\cdot 2-1)}{2}$.
Passo induttivo: sia $n \geq 2$ e supponiamo che $s_n = \frac{n(3n-1)}{2}$; proviamo che $s_{n+1}=\frac{(n+1)(3n+2)}{2}$.

$$\begin{aligned}s_{n+1} =& s_n+(3n+1)\\ =& \frac{n(3n-1)}{2}+(3n+1)\\ =& \frac{n(3n-1)+6n+2}{2}\\ =& \frac{3n^2+5n+2}{2}\\ =& \frac{(n+1)(3n+2)}{2}\end{aligned}$$

ii. Per ogni $n \geqslant 2$ si ha:
$\binom{n}{2}+n^2 = \frac{n!}{2!(n-2)!}+n^2 = \frac{n(n-1)}{n^2}+n^2 = \frac{3n^2-n}{2} = \frac{n(3n-1)}{2} = s_n$.

2. Sia data la seguente applicazione:

$$\begin{array}{rcl} f:\mathbb{R} & \longrightarrow & \mathbb{C} \\ x & \longmapsto & \cos(2\pi x)+i\sin(2\pi x)\end{array}$$

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

(b) Determinare l'immagine di f.

(c) Descrivere la relazione nucleo ρ_f.

(d) Descrivere le classi d'equivalenza $[x]_{\rho_f}$.

Soluzione

(a) L'applicazione f non è iniettiva: ad esempio $f(0)=1=f(1)$.

(b) Per ogni $x\in\mathbb{R}$ $f(x)$ è un numero complesso di modulo 1; se z è un numero complesso di modulo 1, allora $z=\cos\theta+i\sin\theta$ con $\theta\in\mathbb{R}$; allora $\frac{\theta}{2\pi}$ è un numero reale tale che $f(\frac{\theta}{2\pi})=\cos\theta+i\sin\theta=z$. In conclusione

$$\mathtt{Im}(f)=\{z\in\mathbb{C} \mid |z|=1\}$$

(c) Siano $x,\ x' \in \mathbb{R}$; si ha

$$x\rho_f x' \Leftrightarrow f(x) = f(x') \Leftrightarrow \cos(2\pi x)+i\sin(2\pi x) = \cos(2\pi x')+i\sin(2\pi x') \Leftrightarrow x-x' \in \mathbb{Z}$$

(d) $[x]_{\rho_f} = \{x' \in \mathbb{R} \mid x\rho_f x'\} = \{x' \in \mathbb{R} \mid x - x' \in \mathbb{Z}\} = \{x + h \mid h \in \mathbb{Z}\}$.

3. Sia $X = \{n \in \mathbb{N} \ \mid \ n \geqslant 5\}$. Nel prodotto cartesiano $X \times X$ si consideri la seguente relazione:

$$(a, b)\theta(c, d) :\Longleftrightarrow a \text{ divide } c \text{ in } \mathbb{N} \text{ e } b \leqslant d$$

con $a, b, c, d \in X$.

(a) Verificare che θ è una relazione d'ordine in $X \times X$.

(b) Stabilire se l'insieme ordinato $(X \times X, \theta)$ è ordinato totalmente.

(c) Determinare gli eventuali elementi minimali di $(X \times X, \theta)$.

(d) Determinare gli eventuali elementi massimali di $(X \times X, \theta)$.

(e) **(FAC.)** Si consideri il seguente sottoinsieme di $X \times X$:

$$A = \{(14, 6),\ (21, 20),\ (105, 10)\}$$

Stabilire se esiste l'estremo inferiore e l'estremo superiore di A in $(X \times X, \theta)$.

Soluzione

(a) θ è una relazione d'ordine in $X \times X$ poiché gode delle seguenti proprietà:

i. riflessiva: per ogni $(a, b) \in X \times X$ si ha che $(a, b)\theta(a, b)$ poiché a divide a e $b \leqslant b$;

ii. antisimmetrica: siano $(a, b), (c, d) \in X \times X$ tali che $(a, b)\theta(c, d)$ e $(c, d)\theta(a, b)$; allora a divide c e c divide a implica che $a = c$; $b \leqslant d$ e $d \leqslant b$ implica che $b = d$; pertanto $(a, b) = (c, d)$;

iii. transitiva: siano $(a, b),\ (c, d),\ (e, f) \in X \times X$ tali che $(a, b)\theta(c, d)$ e $(c, d)\theta(e, f)$; allora a divide c e c divide e implica che a divide e; $b \leqslant d$ e $d \leqslant f$ implica che $b \leqslant f$; pertanto $(a, b)\theta(e, f)$.

(b) L'insieme ordinato $(X \times X, \theta)$ non è ordinato totalmente; basta considerare gli elementi $(5, 5)$ e $(6, 6)$: si ha che $(5, 5)$ non è in relazione θ con $(6, 6)$ e $(6, 6)$ non è in relazione θ con $(5, 5)$.

(c) Un elemento (a, b) di $(X \times X, \theta)$ è minimale se $(c, d)\theta(a, b)$ implica che $(c, d) = (a, b)$. Sono pertanto elementi minimali tutti gli elementi del tipo $(p, 5)$ con p numero primo $\geqslant 5$ e gli elementi: $(6, 5),\ (9, 5)$ e $(8, 5)$.

(d) Un elemento (a, b) di $(X \times X, \theta)$ è massimale se $(a, b)\theta(c, d)$ implica che $(a, b) = (c, d)$. In $(X \times X, \theta)$ non esistono elementi massimali poiché per ogni $(a, b) \in (X \times X, \theta)$ si ha che $(a, b)\theta(2a, b + 1)$ con $(a, b) \neq (2a, b + 1)$.

(e) **(FAC.)** (a, b) è un minorante per A se e solo se a divide 14, 21 e 105 e $b \leqslant 6$ e quindi se e solo se a divide il MCD(14,21,105) = 7 e $b \leqslant 6$. Quindi l'insieme dei minoranti di A è costituito dagli elementi (7,5) e (7,6); per questo insieme (7,6) risulta essere il massimo e pertanto l'estremo inferiore di A in $(X \times X, \theta)$.

(a, b) è un maggiorante di A se e solo se a è un multiplo di 14, 21 e 105 e $b \geqslant 20$; quindi l'insieme dei maggioranti è costituito dagli elementi (a, b) tali che a è un multiplo di mcm(14,21,105) = 210 e $b \geqslant 20$. Questo insieme possiede il minimo dato da (210,20) che è pertanto l'estremo superiore di A in $(X \times X, \theta)$.

4. Trovare l'ordine del sottogruppo del gruppo dato generato dall'elemento assegnato:

(a) il sottogruppo di $\mathbb{Z}_{36}$ generato da $[4]_{36}$;

(b) il sottogruppo di $\mathcal{C}_9$ generato da $\cos\frac{8\pi}{9} + i\sin\frac{8\pi}{9}$

(c) il sottogruppo di S_9 generato da $(372) \circ (1987) \circ (56) \circ (6291)$;

(d) il sottogruppo del gruppo delle biiezioni di $\mathbb{R}^2$ in se stesso generato dalla biiezione f definita da $f((x, y)) = (-x, 3 + y)$, per ogni $(x, y) \in \mathbb{R}^2$;

(e) il sottogruppo del gruppo additivo delle matrici quadrate a coefficienti in $\mathbb{Z}_{12}$ generato da $\begin{pmatrix} [3]_{12} & [2]_{12} \\ [2]_{12} & [6]_{12} \end{pmatrix}$.

Soluzione

(a) Sappiamo che se g è un elemento di un gruppo G e $o(g) = n$, allora $o(g^k) = \frac{n}{\text{MCD}(n,k)}$. Poiché $\mathbb{Z}_{36}$ è un gruppo ciclico di ordine 36 generato da $[1]_{36}$ e $[4]_{36} = 4[1]_{36}$, si ha che $o([4]_{36}) = \frac{36}{\text{MCD}(36,4)} = 9$.

(b) $\mathcal{C}_9$ è il gruppo ciclico delle radici none dell'unità; le radici none dell'unità sono:

$$\omega_k = \cos\frac{2\pi k}{9} + i\sin\frac{2\pi k}{9}, \quad k = 0, 1, \cdots, 8$$

Sappiamo che ω_k è un generatore di $\mathcal{C}_9$ se e solo se $\text{MCD}(9, k) = 1$; poiché $\cos\frac{8\pi}{9} + i\sin\frac{8\pi}{9} = \omega_4$ e 4 e 9 sono primi tra loro, l'ordine di $\cos\frac{8\pi}{9} + i\sin\frac{8\pi}{9}$ è 9.

(c) La decomposizione in cicli disgiunti della permutazione data è $(15637)\circ(28)$; il suo ordine è dato dal minimo comune multiplo delle lunghezze dei suoi cicli disgiunti, cioè da $5 \cdot 2 = 10$.

(d) Essendo $f^2 = f \circ f$, si ha che $f^2((x,y)) = (x, 6+y)$; induttivamente si verifica facilmente che per ogni $n \in \mathbb{Z}$, $n \geqslant 1$ si ha che $f^n((x,y)) = ((-1)^n x, 3n+y)$; da ciò segue che f è aperiodico.

(e) Banalmente

$$12 \begin{pmatrix} [3]_{12} & [2]_{12} \\ [2]_{12} & [6]_{12} \end{pmatrix} = \begin{pmatrix} [0]_{12} & [0]_{12} \\ [0]_{12} & [0]_{12} \end{pmatrix}$$

Da ciò segue che l'ordine della matrice data divide 12; è immediato verificare che 12 è il più piccolo intero positivo k tale che $k \begin{pmatrix} [3]_{12} & [2]_{12} \\ [2]_{12} & [6]_{12} \end{pmatrix} = \begin{pmatrix} [0]_{12} & [0]_{12} \\ [0]_{12} & [0]_{12} \end{pmatrix}$; pertanto 12 è l'ordine della matrice assegnata.

5. Si consideri il seguente sottoinsieme del campo $\mathbb{Q}$ dei numeri razionali:

$$A = \left\{ \frac{a}{b} \in \mathbb{Q} \quad | \quad a,\ b \in \mathbb{Z} \ \text{ e } \ 7 \ \text{ non divide } \ b \right\}$$

(a) Verificare che A è un sottoanello di $\mathbb{Q}$.

(b) Stabilire se A è un dominio d'integritá.

(c) Stabilire se A è un campo.

(d) Caratterizzare gli elementi invertibili di A.

(e) Sia I l'insieme degli elementi non invertibili di A, cioè $I = A - U(A)$. Verificare che:

i. se $\frac{x}{y},\ \frac{z}{t} \in I$, allora $\frac{x}{y} - \frac{z}{t} \in I$;

ii. se $\frac{a}{b} \in A$, $\frac{x}{y} \in I$, allora $\frac{a}{b}\frac{x}{y} \in I$.

Soluzione

(a) Siano $\frac{a}{b},\ \frac{c}{d} \in A$; allora 7 non divide b e 7 non divide d. Essendo 7 un numero primo, 7 non divide bd. Da qui segue che $\frac{a}{b} - \frac{c}{d} = \frac{ad-bc}{bd} \in A$ e $\frac{a}{b}\frac{c}{d} = \frac{ac}{bd} \in A$. A risulta essere un sottoanello di $\mathbb{Q}$.

(b) A è un dominio d'integritá poiché è un sottoanello di un campo.

(c) A non è un campo poiché ha elementi non invertibili, ad esempio $\frac{7}{2} \in A$ e $\frac{2}{7} \notin A$.

(d) Sia $\frac{a}{b}$ un elemento non nullo di A; allora $a \neq 0$ e 7 non divide b; $\frac{a}{b}$ è invertibile in A se e solo se il suo inverso in $\mathbb{Q}$ appartiene ad A, cioè se e solo se $\frac{b}{a} \in A$, cioè se e solo se 7 non divide a.

(e) Per il punto precedente

$$I = \left\{ \frac{a}{b} \in \mathbb{Q} \mid a,\ b \in \mathbb{Z},\ \ 7 \ \text{ divide} \, a \ \text{ e } \ 7 \ \text{ non divide } \ b \right\}$$

i. Se$\frac{x}{y},\ \frac{z}{t} \in I$, allora 7 divide sia x che z e 7 non divide né y né t; allora $\frac{x}{y} - \frac{z}{t} = \frac{xt-yz}{yt}$ è tale che 7 divide $xt - yz$ e 7 non divide yt da cui $\frac{x}{y} - \frac{z}{t} \in I$.

ii. Sia $\frac{x}{y} \in I$, allora 7 divide x e 7 non divide y; sia $\frac{a}{b} \in A$, allora 7 non divide b.
$\frac{a}{b}\frac{x}{y} = \frac{ax}{by}$ è tale che 7 divide ax e 7 non divide by da cui $\frac{a}{b}\frac{x}{y} \in I$.

6. (a) Sia $f(X) = 10X^5 - 20X^4 + 20X^3 + 20X^2 - 40X + 40 \in \mathbb{Z}[X]$.

i. Verificare che $1 + i$ è radice di $f(X)$.

ii. Decomporre $f(X)$ in fattori irriducibili in $\mathbb{C}[X]$, $\mathbb{R}[X]$, $\mathbb{Q}[X]$ e $\mathbb{Z}[X]$.

(b) Decomporre il polinomio $X^4 + 1 \in \mathbb{Z}_3[X]$ in fattori irriducibili in $\mathbb{Z}_3[X]$.

(c) Utizzando il criterio di Eisenstein, dimostrare che il polinomio $f(X) = X^4 - X^3 + X^2 - X + 1 \in \mathbb{Z}[X]$ è irriducibile in $\mathbb{Z}[X]$.

Soluzione

(a) $f(X) = 10X^5 - 20X^4 + 20X^3 + 20X^2 - 40X + 40 = 10(X^5 - 2X^4 + 2X^3 + 2X^2 - 4X + 4)$

i. Si verifica facilmente che $(1 + i)^2 = 2i$, $(1 + i)^3 = -2 + 2i$, $(1+i)^4 = -4$ e $(1+i)^4 = -4-4i$; è immediato pertanto verificare che $f(1 + i) = 0$.

ii. Poiché $f(X) \in \mathbb{R}[X]$ e $1+i$ è una radice complessa di $f(X)$, si ha che anche $1-i$ è radice di $f(X)$ che ha pertanto tra i suoi fattori $(X - (1 + i))\,(X - (1 - i)) = X^2 - 2X + 2$; dividendo $f(X)$ per $X^2 - 2X + 2$, si ottiene

$$f(X) = 10(X^5-2X^4+2X^3+2X^2-4X+4) = 10(X^2-2X+2)(X^3+2)$$

$X^2 - 2X + 2$ ha due radici complesse (e coniugate): $1+i$ e $1-i$;
$X^3 + 2$ ha una radice reale $-\sqrt[3]{2}$, pertanto

$$\begin{aligned} X^3 + 2 =& (X + \sqrt[3]{2})(X^2 - \sqrt[3]{2}X + \sqrt[3]{4}) \\ =& (X + \sqrt[3]{2}) \left(X - \left(\frac{\sqrt[3]{2}}{2} + i\frac{\sqrt[3]{4}\sqrt{3}}{2} \right) \right) \left(X - \left(\frac{\sqrt[3]{2}}{2} - i\frac{\sqrt[3]{4}\sqrt{3}}{2} \right) \right) \end{aligned}$$

Allora la decomposizione del polinomio $f(X) = 10X^5 - 20X^4 + 20X^3 + 20X^2 - 40X + 40$ in fattori irriducibili in $\mathbb{C}[X]$ è:

$$10(X-1-i)(X-1+i)(X+\sqrt[3]{2}) \left(X - \left(\frac{\sqrt[3]{2}}{2} + i\frac{\sqrt[3]{4}\sqrt{3}}{2} \right) \right) \left(X - \left(\frac{\sqrt[3]{2}}{2} - i\frac{\sqrt[3]{4}\sqrt{3}}{2} \right) \right)$$

la decomposizione del polinomio $f(X) = 10X^5 - 20X^4 + 20X^3 + 20X^2 - 40X + 40$ in fattori irriducibili in $\mathbb{R}[X]$ è:

$$10(X^2 - 2X + 2)(X + \sqrt[3]{2})(X^2 - \sqrt[3]{2}X + \sqrt[3]{4});$$

la decomposizione del polinomio $f(X) = 10X^5 - 20X^4 + 20X^3 + 20X^2 - 40X + 40$ in fattori irriducibili in $\mathbb{Q}[X]$ è:

$$10(X^2 - 2X + 2)(X^3 + 2);$$

la decomposizione del polinomio $f(X) = 10X^5 - 20X^4 + 20X^3 + 20X^2 - 40X + 40$ in fattori irriducibili in $\mathbb{Z}[X]$ è:

$$2 \cdot 5(X^2 - 2X + 2)(X^3 + 2).$$

iii. E' immediato verificare che il polinomio $X^4 + 1 \in \mathbb{Z}_3[X]$ è privo di radici in $\mathbb{Z}_3$; $X^4 + 1$ 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 $b = b' = 2$, $a = 1$ e $a' = -1$. Pertanto la decomposizione di $X^4 + 1$ in fattori irriducibili in $\mathbb{Z}_3[X]$ è:

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

iv. E' immediato verificare che $f(X-1) = X^4 - 5X^3 + 10X^2 - 10X + 5$; 5 è un numero primo che divide il termine noto di $f(X-1)$ e tutti gli altri suoi coefficienti tranne quello direttore; inoltre 5 non divide il termine noto di $f(X-1)$; si può pertanto applicare il criterio di Eisenstein a $f(X-1)$; dalla irriducibilità di $f(X-1)$ segue la irriducibilità di $f(X)$.