

$\mathbb{N}$  MATRICOLA: .....  $A^{\geq 2}$ :...  $B^{\geq 3}$ :...  $C^{\geq 2}$ :...  $D^{\geq 3}$ :... VOTO: .....

COGNOME: ..... NOME: .....

### Algebra 1 – Esame 30.01.13

Rispondere alle domande su questo foglio usando gli appositi spazi e giustificando brevemente ma esaurientemente tutte le risposte.

A Sia  $2^X$  l'insieme delle funzioni  $f : X \rightarrow 2$  da un insieme  $X$  verso  $2 = \{0, 1\}$ .

1. È vero che per ogni  $f, g \in 2^X$  tale che  $g^{-1}(1) = f^{-1}(1)$  si ha  $g = f$ ? [Sì]

2

*Si ha  $f^{-1}(0) = X \setminus f^{-1}(1) = X \setminus g^{-1}(1) = g^{-1}(0)$ . Allora, sia  $x \in X$ ; se  $f(x) = i$  (con  $i \in 2$ ), si ha  $x \in f^{-1}(i) = g^{-1}(i)$ , da cui  $g(x) = i = f(x)$ . Concludiamo che  $f = g$ .*

2. È vero che non esiste  $X \rightarrow 2^X$  iniettiva? [No]

2

*È noto che l'insieme  $2^X$  può essere identificato in modo canonico con l'insieme delle parti  $\mathcal{P}(X)$ ; basta allora osservare che l'applicazione  $f : X \rightarrow 2^X$  definita da  $f(x) = \{x\}$  per ogni  $x \in X$  è iniettiva.*

3. È vero che non esiste  $X \rightarrow 2^X$  surgettiva? [Sì]

3

*Per il Teorema di Cantor, la cardinalità di  $2^X$  (i.e., di  $\mathcal{P}(X)$ ) è strettamente maggiore della cardinalità di  $X$ . Pertanto non esiste un'applicazione surgettiva di  $X$  in  $2^X$ .*

**B** Sia  $m > 1$  un intero. Sia  $\mathbb{Z}_m$  l'insieme delle classi  $[x]_m$  per  $x \in \mathbb{Z}$  e sia

$$[x]_m * [y]_m = [xy + x + y]_m$$

1. È vero che  $(\mathbb{Z}_m, *)$  è sempre un semigruppò ?

3	
---	--

*Sì. Infatti l'operazione  $*$  è evidentemente interna; dobbiamo verificarne l'associatività. Si ha*

$$([x]_m * [y]_m) * [z]_m = [xy + x + y]_m * [z]_m = [(xy + x + y)z + xy + x + y + z]_m,$$

*mentre*

$$[x]_m * ([y]_m * [z]_m) = [x]_m * [yz + y + z]_m = [x(yz + y + z) + x + yz + y + z]_m.$$

*Per le proprietà delle operazioni in  $\mathbb{Z}_m$ , le due espressioni coincidono.*

2. Per quali  $m > 1$  si ha che  $(\mathbb{Z}_m, *)$  è commutativo ? [Tutti]

2	
---	--

*Si ha  $[x]_m * [y]_m = [xy + x + y]_m$ , e  $[y]_m * [x]_m = [yx + y + x]_m$ . È evidente che le due espressioni coincidono, per ogni intero  $m > 1$  e per ogni  $x, y \in \mathbb{Z}$ .*

3. Per quali  $m > 1$  si ha che  $(\mathbb{Z}_m, *)$  è un gruppo ? [Nessuno]

3	
---	--

*Si vede facilmente che  $[0]_m$  funziona da elemento neutro per l'operazione  $*$  in  $\mathbb{Z}_m$ . D'altra parte,  $[-1]_m$  risulta non invertibile; infatti, se  $y \in \mathbb{Z}$  fosse tale che  $[-1]_m * [y]_m = [0]_m$ , si avrebbe  $[-y - 1 + y]_m = [0]_m$ , ovvero  $[-1]_m = [0]_m$ , il che è falso per ogni intero  $m > 1$ .*

C Sia  $\mathbb{Z}_3[X]$  anello dei polinomi a coefficienti in  $\mathbb{Z}_3$ . Sia  $p(X) = X^4 + X^3 + X^2 - 1$  e sia  $I = (p(X))$  l'ideale principale generato da  $p(X)$  in  $\mathbb{Z}_3[X]$ . Denotiamo  $A = \mathbb{Z}_3[X]/I$  l'anello quoziente.

1. Mostrare che  $A$  non è un dominio. 3

*Osserviamo che  $p(X) = X^3(X+1) + (X-1)(X+1) = (X^3+X-1)(X+1)$ . Allora si ha  $(I+X+1) \cdot (I+X^3+X-1) = I+p(x) = I+0$ . Poiché ovviamente  $I+X+1$  e  $I+X^3+X-1$  sono entrambi non nulli, essi sono zero-divisori.*

2. Trovare i nilpotenti di  $A$ . 2

*Osserviamo che  $p(X) = (X^3+X-1)(X+1) = (X^2-X-1)(X+1)^2$ , con  $X^2-X-1$ ,  $X+1$  entrambi irriducibili in  $\mathbb{Z}_3[X]$  (che, ricordiamo, è un U.F.D.). Un elemento  $I+f(x) \in A$  è nilpotente se esiste  $n \in \mathbb{N}$  tale che  $p(x)$  divida  $f(x)^n$ ; ciò implica che  $(X^2-X-1)(X+1)$  sia un divisore di  $f(x)^n$  e, poiché i due fattori sono entrambi primi in  $\mathbb{Z}_3[X]$ , questo implica a sua volta che  $(X^2-X-1)(X+1)$  sia un divisore di  $f(x)$ . Viceversa, si ha  $[(X^2-X-1)(X+1)]^2 = p(X)(X^2-X-1)$ , dunque, per ogni  $f(X)$  multiplo di  $(X^2-X-1)(X+1)$ , si ha  $I+f(x)^2 = I+0$ . Concludiamo che gli elementi nilpotenti di  $A$  sono esattamente quelli appartenenti all'ideale generato da  $I+(X^2-X-1)(X+1)$ .*

3. Mostrare che  $X^2+1$  diventa invertibile in  $A$  e trovarne l'inverso. 3

*Ricordando che  $\mathbb{Z}_3[X]$  è un dominio euclideo, possiamo applicare l'algoritmo delle divisioni successive, dividendo prima  $X^4+X^3+X^2-1$  per  $X^2+1$  (si ottiene resto  $-X-1$ ), e poi  $X^2+1$  per  $-X-1$  (resto  $-1$ ). Così facendo, si ricava che  $X^4+X^3+X^2-1$  e  $X^2+1$  sono coprimi, dunque esistono  $h(x), k(x) \in \mathbb{Z}_3[X]$  tali che  $1 = h(X)(X^4+X^3+X^2-1) + k(X)(X^2+1)$  e dunque  $(I+X^2+1)(I+k(x)) = I+1$ . Questo prova che  $X^2+1$  è invertibile modulo  $I$ . Il suo inverso  $I+k(X)$  si trova ripercorrendo "all'indietro" le divisioni successive: si ottiene  $(X^4+X^3+X^2-1)(-X+1) + (X^2+1)(X^3-X-1) = 1$ , dunque  $k(x) = X^3-X-1$ .*

D Si consideri l'anello  $A = \mathbb{Z}[\sqrt{-3}]$ .

1. È vero che  $A^* = \{\pm 1\}$  ? [Sì]

3	
---	--

*Se  $x \in A^*$ , allora  $x$  divide 1 in  $A$  e dunque la norma  $\nu(x)$  di  $x$  divide  $\nu(1) = 1$  in  $\mathbb{Z}$ . D'altra parte si ha  $\nu(a + b\sqrt{-3}) = a^2 + 3b^2$ , ed è evidente che  $a^2 + 3b^2$  divide 1 in  $\mathbb{Z}$  se e solo se  $a \in \{1, -1\}$  e  $b = 0$ .*

2. È vero che  $A$  è U.F.D. ? [No]

2	
---	--

*Osserviamo che  $2 \cdot 2 = 4 = (1 + \sqrt{-3}) \cdot (1 - \sqrt{-3})$ , con  $2$ ,  $1 + \sqrt{-3}$  e  $1 - \sqrt{-3}$  irriducibili in  $A$ : infatti si tratta di elementi di norma 4 e, non esistendo elementi di norma 2 in  $A$ , una fattorizzazione di  $x \in \{2, 1 + \sqrt{-3}, 1 - \sqrt{-3}\}$  contiene un fattore di norma 4 ed uno di norma 1 (dunque invertibile). Poiché 2 non divide  $1 + \sqrt{-3}$ , le due fattorizzazioni in irriducibili di  $4 \in A$  sono diverse.*

3. È vero che  $\sqrt{-3}$  è primo in  $A$  ? [Sì]

3	
---	--

*Supponiamo che  $\sqrt{-3}$  divida un prodotto  $x \cdot y$ , con  $x, y$  in  $A$ . Allora  $3 = \nu(\sqrt{-3})$  divide  $\nu(x) \cdot \nu(y)$  in  $\mathbb{Z}$ ; essendo 3 un primo di  $\mathbb{Z}$ , possiamo supporre che 3 divida la norma di  $x = a + b\sqrt{-3}$ . Si ottiene dunque  $a^2 + 3b^2 \equiv_3 0$ , da cui  $a = 3k$  per un opportuno  $k \in \mathbb{Z}$ . Concludiamo che  $x = a + b\sqrt{-3} = 3k + b\sqrt{-3} = \sqrt{-3} \cdot (b - \sqrt{-3}k)$ , dunque  $\sqrt{-3}$  divide  $x$ .*