⊕ Matricola: ..... A B C D$^{\geq 8}$: .....1 2 3 4$^{\geq 8}$: ..... Voto: .....

Nome: ..... Cognome: .....

**Algebra 1 – Esame 03.05.11**

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

**A** Sia $X$ un insieme non vuoto e sia $Y \subset X$.

1. Per ogni $Y \neq X$ mostrare che esiste $f : X \to X$ applicazione tale che $f(X) \cap Y = \emptyset$. | 2 |

   *Si scelga $\bar{x} \in X \setminus Y$. Basta definire $f : X \to X$ tale che $f(x) = \bar{x}$ per ogni $x \in X$.*

2. Esiste $Y$ e una tale $f : X \to X$ bigettiva per cui $f(X) \cap Y = \emptyset$ ? [Sì] | 1 |

   *Si ponga $Y = \emptyset$ e $f = \mathrm{Id}_X$.*

**B** Sia $n \in \mathbb{N}$.

1. Mostrare che $\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & n & \frac{n(n+1)}{2} \\ 0 & 1 & n \\ 0 & 0 & 1 \end{pmatrix}$

   *Procediamo per induzione su $n$. Per $n = 0$ l'uguaglianza è ovviamente verificata. Supponiamo dunque che, fissato $n \geq 1$, l'uguaglianza sia vera per $n - 1$. Si ha*

$$\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}^{n-1} \cdot \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n-1 & \frac{(n-1)n}{2} \\ 0 & 1 & n-1 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & 1+(n-1) & 1+(n-1)+\frac{(n-1)n}{2} \\ 0 & 1 & 1+(n-1) \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n & \frac{n(n+1)}{2} \\ 0 & 1 & n \\ 0 & 0 & 1 \end{pmatrix},$$

   *ed il passo induttivo è completato.* | 2 |

2. È vero che $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ ? [Sì] | 1 |

*Procediamo ancora per induzione. Per $n = 0$ l'uguaglianza è ovviamente vera. Fissato $n \geq 1$, supponiamola vera per $n - 1$. Si ha*

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{n-1} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n-1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & 1+(n-1) \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}.$$

**C** Sia $A$ un anello commutativo con identità e sia $a \in A$.

1. È vero che se $a \neq 0, 1$ è tale che $a^3 = 0$ allora $1 - a$ è invertibile ? [Sì] | 2 | |

   *Si ha* $1 - a^3 = (1 - a)(1 + a + a^2)$. *Poiché* $a^3 = 0$, *diventa* $(1 - a)(1 + a + a^2) = 1$, *dunque* $1 - a$ *ha inverso* $1 + a + a^2$.

2. È vero che se $a \neq 0, 1$ è tale che $a^3 = 1$ allora $1 - a$ è zero divisore ? [No] | 2 | |

   *Sia* $a$ *la classe di resto di* 2 *in* $\mathbb{Z}_7$*: si ha* $a^3 = 1$, *ma* $1 - a \neq 0$ *e dunque* $1 - a$ *è invertibile. Ciò esclude che sia uno zero divisore.*

3. Esiste $A$ tale che $(a + 1)^3 = a^3 + 1$ per ogni $a \in A$ ? [Sì] | 1 | |
   *Si consideri* $A = (\mathbb{Z}_3, +, \cdot)$.

**D** Supponiamo di avere una struttura di monoide $(M, \circ, 1)$ su un insieme <u>infinito</u> $M$.

1. Mostrare un esempio di $(M, \circ, 1)$ che non soddisfa la legge di cancellazione. | 2 | |

   *Sia* $(M, \circ, 1) = (M_2(\mathbb{Z}), \cdot, I)$. *Si ha*

   $$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},$$

   *ma* $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix}$.

2. Se $(M, \circ, 1)$ soddisfa la legge di cancellazione allora è un gruppo ? [No] | 2 | |

   *Si consideri ad esempio* $(\mathbb{Z} \setminus \{0\}, \cdot, 1)$.

1. Sia $\mathbb{Z}_p[x]$ l'anello dei polinomi a coefficienti in $\mathbb{Z}_p$ campo delle classi di resti modulo $p$ (numero primo). Sia $f(x) = x^3 + x^2 + x + k$ per $k \in \mathbb{Z}_p$.

   (a) per quali $k \in \mathbb{Z}_p$ il polinomio $f(x)$ è divisibile per $g(x) = x^2 + 1$ ? $[k = [1]]$ | 2 | |

   *Il resto della divisione di $f(x)$ per $g(x)$ è $k - 1$.*

   (b) posto $p = 3$ per quali valori di $k \in \mathbb{Z}_3$ il polinomio $f(x)$ è irriducibile ? $[k = [2]]$ | 1 | |

   *Poiché $f(x)$ ha grado 3, esso è irriducibile se e solo se non ha radici. È routine verificare che, per $k = [0]$ e per $k = [1]$, $f(x)$ ha radici (rispettivamente $[0]$ e $[2]$ -in ogni caso sappiamo che, per $k = [1]$, $f(x)$ ha un divisore proprio), mentre per $k = [2]$ non ne ha.*

   (c) il polinomio $f(x)$ coincide con il polinomio $x^2 + 2x + k$ in $\mathbb{Z}_3[x]$ ? [No] | 1 | |

   *Due polinomi di grado diverso non sono mai uguali. Ciò è evidente se si pensa ai polinomi come sequenze di coefficienti.*

2. Sia $\mathbb{Q}$ l'insieme dei numeri razionali, sia $k \in \mathbb{Q}$ fissato e si consideri in $\mathbb{Q}$ la seguente legge di composizione $a * b = a + b + kab$ per ogni $a, b \in \mathbb{Q}$

   (a) Per quali valori di $k$ $(\mathbb{Q}, *)$ è un semigruppo ? [Tutti] | 1 | |

   *Proviamo la proprietà associativa. Siano $a, b, c \in \mathbb{Q}$:*

   $$(a * b) * c = a + b + kab + c + kac + kbc + k^2abc = a * (b * c).$$

   (b) Per quali valori di $k$ $(\mathbb{Q}, *)$ è commutativo ? [Tutti] | 1 | |

   *È evidente che, scambiando i ruoli di $a$ e $b$ nella definizione dell'operazione $*$, non cambia il risultato.*

   (c) Per quali valori di $k$ $(\mathbb{Q}, *)$ è un gruppo ? $[k = 0]$ | 2 | |

   *Si verifica facilmente che 0 funziona da elemento neutro per l'operazione $*$ qualunque sia il valore di $k$. Se $k \neq 0$ però, l'elemento $-1/k$ non ha inverso. D'altra parte, per $k = 0$ l'operazione $*$ è l'ordinaria somma in $\mathbb{Q}$.*

3. Sia $\mathbb{Q}^+$ l'insieme dei numeri razionali positivi e si consideri la relazione $\leq$ definita in $\mathbb{Q}^+$ ponendo $a \leq b$ se $\dfrac{a}{b}$ è intero.

   (a) $(\mathbb{Q}^+, \leq)$ è un insieme ordinato ? [Sì] | 2 |

   *La proprietà riflessive è verificata, visto che per ogni $a \in \mathbb{Q}^+$ si ha $\frac{a}{a} = 1 \in \mathbb{Z}$. Siano $a, b$ in $\mathbb{Q}^+$ tali che $a \leq b$ e $b \leq a$: si ha $\frac{a}{b} \in \mathbb{Z}$ e $\frac{b}{a} \in \mathbb{Z}$, dunque $\frac{a}{b}$ è un intero positivo con inverso intero, e ciò significa $\frac{a}{b} = 1$. Segue che $a = b$, e la proprietà antisimmetrica è verificata. Infine, se $a \leq b$ e $b \leq c$, si ha $\frac{a}{b}, \frac{b}{c} \in \mathbb{Z}$, dunque $\frac{a}{c} = \frac{a}{b} \cdot \frac{b}{c} \in \mathbb{Z}$, il che prova la transitività.*

   (b) Si determinino $\mathrm{Inf}\{\frac{4}{9}, \frac{10}{21}\} = [\frac{20}{3}]$ $\mathrm{Sup}\{\frac{4}{9}, \frac{10}{21}\} = [\frac{2}{63}]$ | 2 |

   *Determiniamo l'insieme dei minoranti di $\frac{4}{9}$. Per $x, y \in \mathbb{Z}$ coprimi, se $\frac{x}{y} \leq \frac{4}{9}$, si ha $\frac{x}{y} \cdot \frac{9}{4} \in \mathbb{Z}$, da cui $4y \mid 9x$, da cui ancora $4 \mid x$ e $y \mid 9$. Analogamente, un minorante $\frac{x}{y}$ di $\frac{10}{21}$ è tale che $10 \mid x$ e $y \mid 21$ (sempre supponendo la frazione $\frac{x}{y}$ ridotta ai minimi termini). Concludiamo che i minoranti comuni $\frac{x}{y}$ per i due elementi sono tali che $20 \mid x$ e $y \mid 3$. Ora è facile vedere che $\frac{20}{3}$ è effettivamente il più grande dei minoranti.*
   *La seconda parte dell'esercizio è del tutto analoga.*

4. Sia $A = \mathbb{Z}[\sqrt{-8}]$.

   (a) È vero che 7 è primo ? [Sì] | 1 |

   *Supponiamo che 7 divida $(a + ib\sqrt{8}) \cdot (c + id\sqrt{8})$. Allora la norma di 7 (che è 49) divide $N(a + ib\sqrt{8}) \cdot N(c + id\sqrt{8}) = (a^2 + 8b^2) \cdot (c^2 + 8d^2)$. In particolare si ha $0 \equiv_7 (a^2 + 8b^2) \cdot (c^2 + 8d^2) \equiv_7 (a^2 + b^2) \cdot (c^2 + d^2)$. Ma allora 7 divide $(a^2 + b^2) \cdot (c^2 + d^2)$ in $\mathbb{Z}$, e poiché 7 è un primo di $\mathbb{Z}$, possiamo supporre che 7 sia un divisore di $a^2 + b^2$, ovvero $a^2 + b^2 \equiv_7 0$. D'altra parte i quadrati in $\mathbb{Z}_7$ sono le classi di resto di 0, 1, 2 e 4, e l'unico caso in cui la somma di due di essi dà la classe di 0 è per $a \equiv_7 b \equiv_7 0$. Concludiamo che $a$ e $b$ sono divisibili per 7 in $\mathbb{Z}$, dunque $a + ib\sqrt{8}$ è divisibile per 7 in $A$.*

   (b) È vero che $A$ è euclideo ? [No]

   *In effetti $A$ non è neppure un U.F.D., visto che si ha $3 \cdot 3 = 9 = (1 + i\sqrt{8}) \cdot (1 - i\sqrt{8})$ e 3 non è certamente associato a $1 + i\sqrt{8}$ né a $1 - i\sqrt{8}$.* | 2 |

   (c) È vero che $A$ è un dominio ? [Sì] | 1 |

   *Infatti è un sottoanello del campo complesso.*