MATRICOLA: ..... A B C D$^{\geq 8}$: .....1 2 3 4$^{\geq 8}$: ..... VOTO: .....

COGNOME: ..... NOME: ..... **6** **F** **E**

Algebra 1 – Esame 30.04.15

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

A Sia X_0 un insieme non vuoto tale che se $x \in X_0$ allora $X_0 - \{x\}$ è non vuoto. Sia X_1 un insieme tale che: $\emptyset \in X_1$ e inoltre se $x \in X_1$ allora $x \cup \{x\} \in X_1$.

1. Per quale $i = 0, 1$ esiste sempre almeno una funzione iniettiva $f : \mathbb{N} \to X_i$? [1]

Sia $X_0 = \{0, 1\}$. È evidente che X_0 soddisfa le ipotesi, tuttavia non esiste alcuna funzione iniettiva di $\mathbb{N}$ in X_0. Invece X_1 è per ipotesi un insieme apoditico, dunque $X_1 \supseteq \mathbb{N}$ e l'inclusione $i : \mathbb{N} \to X_1$ è iniettiva.

2. Per quale $i = 0, 1$ l'insieme X_i può essere finito ? [$i = 0$] [1]

Per quanto osservato sopra, X_0 può essere finito, mentre X_1 no poiché contiene $\mathbb{N}$.

B Sia X un insieme non vuoto. Sia $x \in X$ (fissato) e sia $\varphi : X^X \to \mathcal{P}(X)$ tale che $\varphi(f) \stackrel{\text{def}}{=} f^{-1}(x)$.

1. È vero che esistono X e $x \in X$ tali che φ è surgettiva ? [sì] [2]

Sia $X = \{0, 1\}$ e $x = 1$. Allora $X^X = \{0 \to 0 \cdot 0 \to 1 \cdot 0 \to 0 \cdot 1 \to 1 \cdot 1 \to 0 \cdot 1 \to 0 \cdot 0 \to 1 \cdot 1 \to 1\}$, mentre $\mathcal{P}(X) = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}$: denotando gli elementi di X^X con $f_{01}, f_{10}, f_{00}, f_{11}$, si ha - - -

2. È vero che esistono X e $x \in X$ tali che φ è bigettiva ? [sì] [2]

- - - $\varphi(f_{01}) = \{1\}$, $\varphi(f_{10}) = \{0\}$, $\varphi(f_{00}) = \emptyset$, $\varphi(f_{11}) = \{0, 1\}$. dunque φ è biettiva in questo caso.

C Sia $M_2(\mathbb{Z})$ l'insieme delle matrici quadrate di ordine 2 con entrate nell'anello degli interi $\mathbb{Z}$. Sia $(M_2(\mathbb{Z}), +, 0)$ con $+$ somma di matrici.

1. È vero che definendo $A \bullet B = 0$ per ogni $A, B \in M_2(\mathbb{Z})$ si ha che $(M_2(\mathbb{Z}), +, \bullet, 0)$ è un anello commutativo senza identità ? [Sì] | 1 |

Ogni gruppo abeliano dotato di un prodotto sempre nullo, diventa in modo ovvio un anello (zero-anello) commutativo senza identità (a meno che non sia il gruppo banale -)

2. È vero che definendo $A \cdot B =$ prodotto righe per colonne per ogni $A, B \in M_2(\mathbb{Z})$ si ha che $(M_2(\mathbb{Z}), +, \cdot, 0)$ è un anello con identità senza zero divisori ? [NO] | 2 |

E' senz'altro un anello con identità, ma ad esempio $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ è un elemento nilpotente visto che $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

3. È vero che l'insieme $\left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in \mathbb{Z} \right\}$ è un sottoanello di $(M_2(\mathbb{Z}), +, \cdot, 0)$? [NO] | 1 |

Non contiene l'identità $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

4. È vero che l'insieme $\left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in \mathbb{Z} \right\}$ è un ideale di $(M_2(\mathbb{Z}), +, \bullet, 0)$? [Sì] | 2 |

E' un sottogruppo (infatti $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a-c & b-d \\ 0 & 0 \end{pmatrix}$ sta nell'insieme considerato), e ovviamente "assorbe i prodotti", visto che i prodotti sono tutti nulli.

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

1. Mostrare un esempio di $(M, \circ, 1)$ non commutativo M=[$Sym(3)$] | 2 |

Si considera l'insieme delle permutazioni sull'insieme $\{1,2,3\}$, cioè $\left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}$. Con la composizione di mappe è un gruppo, e si ha $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, ma $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

2. Se $(M, \circ, 1)$ soddisfa la legge di cancellazione allora è un gruppo ? [Sì] | 2 |

Sia $x \in M$, e sia $f : M \to M$ l'applicazione $y \mapsto xy$. Se $f(y_1) = f(y_2)$ allora $xy_1 = xy_2$, e la legge di cancellazione implica $y_1 = y_2$. Concludiamo che f è iniettiva, e poiché M è finito, f è anche suriettiva. Ma allora $\exists\, y \in M$ tale che $xy = 1$, dunque x ha inverso destro. Ciò è vero per ogni $x \in M$, dunque M è un gruppo.

1. Sia $\mathbb{Z}_5[x]$ l'anello dei polinomi a coefficienti sul campo $\mathbb{Z}_5$ e siano $f(x) = x^4 + x^3 + 3x^2 - 2x$ e $g(x) = x^2 + k$.

   (a) Per ogni $k \in \mathbb{Z}_5$ si ha che $g(x)$ è irriducibile ? [NO] | 2 |

Evidentemente $g(x)$ non è irriducibile se $k=0$.

   (b) Per ogni $k \in \mathbb{Z}_5$ si ha che M.C.D.$(f(x), g(x)) = 1$? [NO] | 1 |

Per $k=0$, entrambi i polinomi sono divisibili per x.

   (c) Per $k = 3$ si ha che $g(x)$ divide $f(x)$? [SI'] | 1 |

Si ha $x^4+x^3+3x^2-2x = (x^2+3)\cdot(x^2+x)$

2. Sia $\mathbb{Z}_n$ l'anello delle classi di resto modulo $n > 1$ e sia $G = \{(x, y) \mid x, y \in \mathbb{Z}_n\}$. Si consideri in G la seguente operazione $\star$

$$(a, b) \star (c, d) = (ad, bc)$$

   (a) $(G, \star)$ è un semigruppo ? [NO] | 1 |

L'operazione è interna ma NON associativa. Infatti:
$((1,1)\star(1,1))\star(1,0) = (1,1)\star(1,0) = (0,1)$, mentre
$(1,1)\star((1,1)\star(1,0)) = (1,1)\star(0,1) = (1,0)$ - (Assurdo)

   (b) $(G, \star)$ è commutativo ? [NO] | 1 |

Ad esempio $(1,0)\cdot(0,1) = (1,0)$, mentre $(0,1)(1,0) = (0,1)$.

   (c) $(G, \star)$ ammette elemento neutro ? [NO] | 1 |

Sia (e,f) elemento neutro; allora $(1,1)\star(e,f) = (1,1)$, da cui $(f,e) = (1,1)$, ossia $f = e = 1$. D'altra parte
$(1,1)\star(1,0) = (0,1)$

3. Sia $A = \mathbb{Z}[i]$.

(a) Trovare il massimo comune divisore (a, b) di $a = 3 + i$ e $b = 4 - i$ in A. [1] | 2 |

Infatti i due elementi hanno norme coprime (rispettivamente 10 e 17), dunque un divisore comune deve avere norma 1, ed è pertanto invertibile.

(b) Trovare almeno un primo di $\mathbb{Z}$ che non è primo in A. [2] | 2 |

Si ha $2 = (1+i)\cdot(1-i)$

4. Sia $\mathbb{Z}_p$ il campo delle classi di resti modulo p primo dispari. Sia $\phi : \mathbb{Z}_p \longrightarrow \mathbb{Z}_p$ l'applicazione definita ponendo $\phi(x) = 2x^p$ per $x \in \mathbb{Z}_p$

(a) È vero che per $p = 3$ è bigettiva ? [Sì] | 1 |

Si ha $\varphi(0)=0$, $\varphi(1)=-1$, $\varphi(-1)=1$

(b) È vero che ϕ è sempre bigettiva ? [Sì] | 2 |

Per ogni $x \in \mathbb{Z}_p$ si ha $x^p = x$, dunque $\varphi(x) = 2x$,
Concludiamo che $\varphi(x) = 2x \ \forall x \in \mathbb{Z}_p$,
e A essendo 2 invertibile in $\mathbb{Z}_p$ (con p dispari) segue che φ è biettiva.

(c) È vero che $\phi(x + y) = \phi(x) + \phi(y)$? [Sì] | 1 |

Per quanto osservato sopra, si ha $\varphi(x+y) = 2(x+y) =$
$= 2x+2y = \varphi(x) + \varphi(y)$.