$\odot$ MATRICOLA: .... A ... B ... C ... D ... VOTO$^{\geq 10}$: ......

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

Algebra 1 – Esame 20.09.12

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

A Sia S un insieme non vuoto e sia $Y \in \mathcal{P}(S)$. Sia $f : \mathcal{P}(S) \to \mathcal{P}(S)$ definita associando ad ogni $X \in \mathcal{P}(S)$ l'insieme $S - (X \cup Y) \in \mathcal{P}(S)$.

1. L'inversa f^{-1} esiste sempre ? 2

No. Per una qualunque scelta di S, si ponga $Y = X_1 = S$ e $X_2 = \emptyset$. Si verifica immediatamente che $f(X_1) = \emptyset = f(X_2)$, dunque f non è in generale iniettiva.

2. Esiste Y tale che l'applicazione f^n è invertibile per ogni $n \in \mathbb{N}$? 2

Sì. Se si sceglie $Y = \emptyset$, l'applicazione f è quella che ad ogni elemento in $\mathcal{P}(S)$ associa il suo complementare in S. Tale applicazione è ovviamente invertibile (la sua inversa è lei stessa) e coincide con tutte le sue potenze dispari, mentre le sue potenze pari sono l'identità.

B 1. Mostrare per induzione che 2

$$\begin{bmatrix} 1 & -2 & 5 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & -2n & 2n^2+3n \\ 0 & 1 & -2n \\ 0 & 0 & 1 \end{bmatrix}$$

Per $n = 0$ entrambi i membri sono la matrice identica, dunque la proposizione è vera. Facciamo dunque il passo induttivo e, supponendo la proposizione vera per il numero naturale n, proviamola vera per $n+1$. Si ha

$$\begin{bmatrix} 1 & -2 & 5 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{bmatrix}^{n+1} = \begin{bmatrix} 1 & -2 & 5 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{bmatrix}^n \cdot \begin{bmatrix} 1 & -2 & 5 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{bmatrix} =$$

$$= \begin{bmatrix} 1 & -2n & 2n^2+3n \\ 0 & 1 & -2n \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & -2 & 5 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & -2(n+1) & 2(n+1)^2+3(n+1) \\ 0 & 1 & -2(n+1) \\ 0 & 0 & 1 \end{bmatrix},$$

come si voleva.

2. Mostrare per induzione che $3^{2n} \equiv_8 1$ 2

Per $n = 0$ la proposizione è ovviamente vera. Supponiamola dunque vera per il numero naturale n, e proviamola vera per $n+1$. Si ha

$$3^{2(n+1)} \equiv_8 3^{2n} \cdot 3^2 \equiv_8 3^{2n} \cdot 1 \equiv_8 1,$$

come si voleva.

C Siano $a, b \in \mathbb{Q}$. Sia $g_{a,b} : \mathbb{Q} \to \mathbb{Q}$ $x \mapsto ax + b$ e G=$\{g_{a,b} \ \mid a, b \in \mathbb{Q}, a \neq 0\}$

1. Mostrare che $(G, \circ)$ è un gruppo rispetto al prodotto $\circ$ di applicazioni. | 2 | |

   Sappiamo che l'insieme S di tutte le applicazionii biettive di $\mathbb{Q}$ in sé, dotato dell'operazione di composizione, è un gruppo. Ogni elemento di G sta in S (infatti ogni $g_{a,b} \in G$ è invertibile, e $(g_{a,b})^{-1} = g_{a^{-1},-a^{-1}b}$; si noti che quest'ultima applicazione esiste poiché esiste a^{-1} in $\mathbb{Q}$), e si tratta dunque di far vedere che G è un sottogruppo di S. Ovviamente G è non vuoto (contiene l'identità, che è $g_{1,0}$), inoltre, per $g_{a,b}$ e $g_{c,d}$ in G, si ha

   $$g_{a,b}(g_{c,d})^{-1} = g_{c^{-1},-c^{-1}d} \circ g_{a,b} = g_{ac^{-1},c^{-1}(b-d)}.$$

   Quest'ultima applicazione è in G, visto che $ac^{-1} \in \mathbb{Q} \setminus \{0\}$, e la dimostrazione è conclusa.

2. Se $g_{a,b} \neq e$ allora $g_{a,b}^n \neq e$ per ogni $n \in \mathbb{N}$ dove e è l'elemento neutro di G ? | 2 | |

   No. Si consideri ad esempio $g = g_{-1,0}$; si vede immediatamente che $g^2 = e$, e naturalmente $g \neq e$.

D Sia $\mathbb{Z}_3[x]$ l'anello dei polinomi a coefficienti nel campo $\mathbb{Z}_3$ delle classi di resti modulo 3 e siano $f_k(x) = x^2 + kx + 1 \in \mathbb{Z}_3[x]$

1. per quali valori di $k \in \mathbb{Z}_3$ il polinomio $f_k(x)$ è irriducibile ? | 2 | |

   Essendo $f_k(x)$ un polinomio di grado 2 a coefficienti nel campo $\mathbb{Z}_3$, esso è irriducibile precisamente se non ha radici in $\mathbb{Z}_3$. Gli interi k per cui non ci sono radici sono, come si vede facilmente, tutti e soli i multipli di 3.

2. per quali valori di $k \in \mathbb{Z}_3$ il polinomio $f_k(x)$ è primo con $g(x) = x^3 - 1$? | 2 | |

   Si ha che $f_0(x)$ è irriducibile e non divide $g(x) = (x-1)^3$. Inoltre, $f_1(x) = (x-1)^2$ divide $g(x)$, mentre $f_{-1}(x) = (x+1)^2$ non ha fattori comuni con $g(x)$. Concludiamo dunque che $f_k(x)$ e $g(x)$ sono coprimi per $k \in \{0, -1\}$.