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

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

Algebra 1 – Esame 17.07.14

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

A Sia $(G, +, 0_g)$ un gruppo abeliano, S un insieme non vuoto e X l'insieme delle funzioni da S a G.

1. Se G è infinito, X è infinito? [Sì] Se X è infinito, S è infinito ? [No] | 2 |

Sia $s \in S$, $\bar{g} \in G$, e $\{g_i\}_{i \in \mathbb{N}}$ un sottoinsieme numerabile di G. Definiamo $f_i \in X$ come segue: $f_i(x) = \begin{cases} g_i & \text{se } x = s \\ \bar{g} & \text{se } x \neq s \end{cases}$. Ovviamente $\{f_i\}_{i \in \mathbb{N}}$ è un sottoinsieme numerabile di X, dunque X è infinito. Se $S = \{0\}$ e $G = (\mathbb{Z}, +)$ - - -

2. Presi $f, g \in X$ definiamo $(f+g)(s) = f(s)+g(s)$. L'insieme $(X, +)$ è un monoide? [Sì] Un gruppo ? [Sì] | 2 |

L'operazione è ben definita, ed "eredita" l'associatività da $(G, +)$. Inoltre, la funzione $f(s) = 0 \ \forall s \in S$ è l'elemento neutro, mentre $g(s) := -f(s) \ \forall s \in S$ è l'inversa di $f \in X$.

B Sia $\mathbb{Q}^+$ l'insieme dei razionali positivi. Presi $q_1, q_2 \in \mathbb{Q}^+$ si consideri la relazione

$$q_1 \leq q_2 \text{ se } \frac{q_1}{q_2} \in \mathbb{N}.$$

1. È vero che $(\mathbb{Q}^+, \leq)$ è un insieme totalmente ordinato? [No] | 2 |

Ad esempio, gli elementi 2 e 3 non sono confrontabili.

2. Qual è un maggiorante per la coppia $(\frac{2}{3}, \frac{10}{7})$? [$\frac{1}{21}$] | 2 |

C Sia $\alpha : \mathbb{Z} \to \mathbb{Z}$ la funzione definita da:

$$\alpha(x) = \begin{cases} 3x & \text{se 2 divide } x \\ 2x & \text{se 2 non divide } x \end{cases}$$

1. Si dimostri che α non è né iniettiva né suriettiva. | 2 |

La funzione non e' iniettiva, poiché $\alpha(2) = \alpha(3)$
Inoltre, l'immagine di α contiene solo numeri pari.

2. Si mostri che $\alpha(\mathbb{Z}) = \{12t, 4t+2 | t \in \mathbb{Z}\}$ e che gli elementi che hanno piú di una controimmagine sono tutti e soli gli elementi della forma $4t+2$ con $t \equiv 1 \pmod 3$. | 2 |

Sia $x \in \mathbb{Z}$: se $x = 2k+1$, allora $\alpha(x) = 4k+2$. Se $x = 2h$ allora $\alpha(x) = 6h$ e, per h pari, $\alpha(x)$ e' del tipo $12t$ mentre per h dispari si vede che $\alpha(x)$ e' del tipo $4t+2$. Viceversa, $12t = \alpha(6t)$, e $4t+2 = \alpha(2t+1)$. Poi, $|\alpha^{-1}(\{z\})| > 1 \iff \exists\, h, k \in \mathbb{Z}$ con $3(2h) = z = 2(2k+1)$. La diofantea $6h = 4k+2$ ha soluzione $\{(1+2t, 1-3t) : t \in \mathbb{Z}\}$, dunque $z = 4k+2$ con $k = 1-3t$, ovvero $k \equiv_3 1$.

D Sia $\mathbb{Z}_p[x]$ l'anello dei polinomi in x sul campo $\mathbb{Z}_p$ delle classi di resto modulo p primo. Consideriamo i due ponimomi

$$a(x) = x^4 + x^3 + x + 1 \text{ e } b(x) = x^2 - 1.$$

1. Al variare di p si determini un $MCD(a(x), b(x)) = d(x)$. [$b(x)$ se $p = 2$, $x+1$ se $p \neq 2$] | 2 |

Eseguendo la divisione $a(x) : b(x)$, si vede che $a(x) = b(x)(x^2+x+1) + (2x+2)$. Dunque, se $p = 2$, $b(x)$ divide $a(x)$ e $d(x) = b(x)$. Se $p \neq 2$, la divisione $b(x) : x+1$ da' resto 0, dunque $d(x) = x+1$

2. Al variare di p si determinino due polinomi $h(x)$ e $k(x)$ tali che $d(x) = a(x)h(x) + b(x)k(x)$. [$h(x) =$ $k(x) =$] | 2 |

Se $p = 2$, basta porre $h(x) = 0$, $k(x) = 1$; se $p \neq 2$, si pone $h(x) = 1$, $k(x) = -(x^2+x+1)$ (e così si ottiene l'mcd $d(x) = 2x+2$).