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

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

Algebra 1 – Esame 27.01.15

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

A Sia $f : X \to X$ una funzione iniettiva ma non surgettiva. Sia $Y_1 = \mathrm{Im} f$ e $Y_n = \mathrm{Im} f^n$ per $n \geq 2$ e dunque $Y_1 \supseteq Y_2 \cdots \supseteq Y_n \supseteq \cdots$

1. Mostrare che esiste $g : X \to X$ surgettiva non iniettiva tale che $g \circ f = id_X$. | 2 |

Fissato $\overline{x} \in X$, si definisca $g : X \to X$ come segue: se $x \in f(X)$, sia $g(x)$ l'unica preimmagine di x tramite f, mentre se $x \notin f(X)$, si pone $g(x) = \overline{x}$. Si ha $g \circ f = id_X$, e se g fosse iniettiva sarebbe biettiva e lo sarebbe f.

2. È vero che $Y_n \neq Y_{n+1}$ per ogni $n \in \mathbb{N}^+$? [Sì] | 2 |

Sia per assurdo m il minimo numero in $\mathbb{N}^+$ tale che $Y_{m-1} \supsetneq Y_m = Y_{m+1}$ e sia $y \in Y_{m-1} \setminus Y_m$. Si ha $f(y) \in Y_m = Y_{m+1}$, ma poiché $f : Y_m \to Y_{m+1}$ è biettiva, esiste un unico $y_0 \in Y_m$ tale che $f(y_0) = f(y)$. Poiché $y \notin Y_m$, è $y \neq y_0$, contro l'iniettività di f.

B Sia $\mathcal{P} = \{p \in \mathbb{Z} \mid p \text{ è primo}, p > 0\}$ e sia $\mathcal{S} = \{p^n \mid p \in \mathcal{P}, n \in \mathbb{N}, n \geq 1\}$. Si consideri la seguente relazione di equivalenza $\mathcal{R} \subset \mathcal{S} \times \mathcal{S}$ per cui $(x, y) \in \mathcal{R}$ se $\exists\, p \in \mathcal{P}$ tale che p divide sia x che y.

1. $p^n \mathcal{R} q^m \iff p = q$? [Sì] | 2 |

L'implicazione ($\Leftarrow$) è ovvia, dunque proviamo ($\Rightarrow$). Se $p^n \mathcal{R} q^m$ esiste $r \in \mathcal{P}$ tale che $r \mid p^n$ e $r \mid q^m$. Ma $r \mid p^n$ implica $r = p$, e $r \mid q^m$ implica $r = q$, dunque $p = q$.

2. L'insieme quoziente $\mathcal{S}/\mathcal{R}$ è numerabile ? [Sì] | 2 |

È evidente che ogni classe di equivalenza in $\mathcal{S}/\mathcal{R}$ contiene uno e un solo numero primo, dunque l'applicazione $\varphi : \mathcal{P} \to \mathcal{S}/\mathcal{R}$ tale che $p \mapsto [p]$ è biettiva, e $|\mathcal{S}/\mathcal{R}| = |\mathcal{P}|$. Ma $\mathcal{P}$ è un sottoinsieme infinito di $\mathbb{N}$, dunque è numerabile.

C Sia k un campo e sia $A = k[t]$ l'anello dei polinomi in una variabile. Consideriamo $M = k[t]/(t^n)$ con $n \in \mathbb{N}$ come A-modulo e come k-modulo.

1. Per quali $n \in \mathbb{N}$ si ha che M è un A-modulo libero ? Per tali n mostrare una base. | 2 |

Se M è A-libero, esiste una A-base $\mathcal{B}$ di M, e possiamo scegliere $[f(t)] \in \mathcal{B}$. Si ha $t^n \cdot [f(t)] = [t^n f(t)] = [0]$ con $t^n \in A \setminus \{0\}$, e questo è assurdo poiché abbiamo trovato una combinazione lineare degli elementi di $\mathcal{B}$, a coefficienti non tutti nulli, che dà $[0]$. Concludiamo che M non è A-libero per alcun valore di n.

2. Per quali $n \in \mathbb{N}$ si ha che M è un k-modulo libero ? Per tali n mostrare una base. | 2 |

Per ogni $n \in \mathbb{N} \setminus \{0\}$, si ha che M è K-libero con base $[1], [t], \dots, [t^{n-1}]$. Infatti, è ben noto che ogni classe di equivalenza in M contiene uno e un solo polinomio che sia nullo o di grado minore di n, e $[a_0 + a_1 t + \dots + a_{n-1} t^{n-1}] = \sum_{i=0}^{n-1} a_i \cdot [t^i]$. Inoltre, $\sum_{i=0}^{n-1} \beta_i [t^i] = [0] \Rightarrow [\beta_0 + \dots + \beta_{n-1} t^{n-1}] = [0] \Rightarrow$ $\Rightarrow \beta_0 + \dots + \beta_{n-1} t^{n-1} = 0 \Rightarrow \beta_i = 0 \ \forall i$.

D Supponiamo di avere una catena crescente $(a_1) \subseteq \cdots (a_n) \subseteq (a_{n+1}) \subseteq \cdots$ di ideali principali e propri in un dominio A.

1. È vero che se a_n è irriducibile allora $(a_n) = (a_{n+1}) = \cdots$? [Sì] | 2 |

Se $(a_n) \subseteq (a_{n+1})$, si ha $a_{n+1} \mid a_n$. L'irriducibilità di a_n forza dunque a_{n+1} ad essere o invertibile o associato ad a_n, ma nel primo caso avremmo la contraddizione $(a_{n+1}) = A$. Dunque a_{n+1} è associato ad a_n, e si ha $(a_{n+1}) = (a_n)$. Lo stesso argomento si applica ad $a_m \ \forall m > n$.

2. È vero che se l'unione $\cup(a_n) = (a)$ allora $\exists\, a_n$ tale che $(a_n) = (a_{n+1}) = \cdots$? [Sì] | 2 |

Se $\cup(a_n) = (a)$, in particolare $a \in \cup(a_n) \Rightarrow \exists\, n$ tale che $a \in (a_n) \Rightarrow (a) \subseteq (a_n)$; d'altra parte, ovviamente, $(a_n) \subseteq (a)$, dunque $(a_n) = (a)$. Ora, $\forall m > n$ si ha $(a) = (a_n) \subseteq (a_m) \subseteq (a)$, dunque $(a_m) = (a)$.

1. Sia $\mathbb{Z}_p[x]$ l'anello dei polinomi sul campo $\mathbb{Z}_p$ delle classi di resti modulo p (p primo) e siano $f(x) = x^3 - 3x^2 + 2$ e $g(x) = x^3 - 6x^2 + 11x - 6 \in \mathbb{Z}_p[x]$

(a) Per $p = 2$ si ha M.C.D.$(f(x), g(x)) = x + 1 \in \mathbb{Z}_2[x]$? [No] | 1 |

Per $p=2$ è $f(x) = x^3 + x^2 = x^2(x+1)$ e $g(x) = x^3 + x = x(x^2+1) = x(x+1)^2$, dunque $\text{mcd}(f(x), g(x)) = x(x+1)$.

(b) Per ogni p si ha che $f(x) - g(x) \in \mathbb{Z}_p[x]$ ha radici non-nulle $\in \mathbb{Z}_p$? [Sì] | 1 |

Si ha che 1 è radice di $f(x)$ e $g(x)$, dunque lo è anche della loro differenza.

(c) I polinomi $f(x)$ e $g(x) \in \mathbb{Z}_p[x]$ sono coprimi se $p \neq 2$? [No] | 2 |

Da quanto osservato sopra e dal Teorema di Ruffini, segue che $f(x)$ e $g(x)$ sono entrambi divisibili per $x-1$.

2. Sia $\mathbb{Q}$ il campo dei numeri razionali e sia $G = \{(x, y) \mid x, y \in \mathbb{Q},\ y \neq 0\}$. Si consideri in G la seguente operazione $\star$

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

(a) $(G, \star)$ è un semigruppo ? [Sì] | 2 |

L'operazione è ovviamente chiusa. Inoltre, per $(a,b), (c,d), (e,f) \in G$:
$((a,b) \star (c,d)) \star (e,f) = (a+bc, bd) \star (e,f) = (a+bc+(bd)e, (bd)f)$;
$(a,b) \star ((c,d) \star (e,f)) = (a,b) \star (c+de, df) = (a+b(c+de), b(df)) =$
$= (a+bc+b(de), b(df))$
e le espressioni coincidono.

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

Ad esempio $(1,2) \star (2,1) = (5,2)$, $(2,1) \star (1,2) = (3,2)$.

(c) $(G, \star)$ è un gruppo ? [Sì] | 1 |

L'elemento neutro è $(0,1)$, poiché $(a,b) \cdot (0,1) = (a+b\cdot 0, b\cdot 1) = (a,b)$ e $(0,1) \cdot (a,b) = (0+1\cdot a, 1\cdot b) = (a,b)$. Inoltre, $\forall (a,b) \in G$, l'elemento $(-\frac{a}{b}, \frac{1}{b})$ è l'inverso di (a,b).

3. Sia $A = \mathbb{Z}[\sqrt{-7}]$.

(a) Esiste un massimo comune divisore di $3 + i\sqrt{7}$ e 5 in A ? [Si'] | 2 |

I due elementi hanno norma rispettivamente 16 e 25, dunque hanno norme coprime. Se $d \mid 3+i\sqrt{7}$ e $d \mid 5$, si ha $N(d) \mid 16$ e $N(d) \mid 25$, dunque $N(d) = 1$, da cui $d = \pm 1$.
Concludiamo che $MCD(3+i\sqrt{7}, 5) = 1$.

(b) Esiste un massimo comune divisore di $i\sqrt{7}$ e -7 in A ? [Si'] | 2 |

Si ha che $i\sqrt{7}$ e' un divisore di -7 $(-7 = (i\sqrt{7})^2)$.
Dunque $MCD(i\sqrt{7}, -7) = i\sqrt{7}$

4. Sia $\mathbb{Z}_p$ il campo delle classi di resti modulo p (p primo). Sia $\phi : \mathbb{Z}_p \longrightarrow \mathbb{Z}_p$ l'applicazione definita ponendo $\phi(a) = a^5 + 2a$ per $a \in \mathbb{Z}_p$

(a) Esiste p tale che $\phi(a+b) = \phi(a) + \phi(b)$? [$p = 2$] | 2 |

Per $p \neq 2$ si ha $\varphi(a) = a^5$, che in $\mathbb{Z}_2$ e' l'identita'.
Dunque $\varphi(a+b) = a+b = \varphi(a) + \varphi(b)$.

(b) Esiste p tale che ϕ è bigettiva ? [$p = 2$] | 2 |

Vedi sopra.