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

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

Algebra 1 – Esame 27.02.15

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. Sia $S \overset{\text{def}}{=} \mathcal{P}(X \times X)$ ordinato per inclusione e $Y \in S$ (fissato).

1. È vero che esiste $\hat{Y} \overset{\text{def}}{=} \min\{R \supseteq Y \mid R \in S$ è relazione di equivalenza su $X\}$? [Sì] | 2 | |

Sia $\{R_i\}_{i\in I}$ una famiglia non vuota di relazioni di equivalenza su X. Posto $\hat{R} = \cap R_i$, si ha che $\hat{R}$ è una relazione di equivalenza: 1) $\forall x \in X$ e $\forall i \in I$, $(x,x) \in R_i \Rightarrow (x,x) \in \hat{R}$; 2) $(x,y) \in \hat{R} \Rightarrow (x,y) \in R_i \ \forall i$, dunque $(y,x) \in R_i \ \forall i \Rightarrow (y,x) \in \hat{R}$; 3) $(x,y),(y,z) \in \hat{R} \Rightarrow (x,y),(y,z) \in R_i \ \forall i \Rightarrow$ $\Rightarrow (x,z) \in R_i \ \forall i \Rightarrow (x,z) \in \hat{R}$. Allora $\hat{Y}$ è l'intersezione di tutte le rel. di eq. su X contenenti Y.

2. Se $Y \overset{\text{def}}{=} \{(x,x) \in X \times X \mid x \in X\} \in S$ è vero che $\hat{Y} = Y$? [sì] (Descrivere la relazione di equivalenza in questo caso) | 2 | |

In questo caso, Y è esso stesso una relazione di equivalenza su X (è l'uguaglianza). Dunque è chiaro che $\bigcap_{\substack{R \text{ rel. d'eq su } X \\ R \supseteq Y}} R$ coincide con Y.

B Sia $\lambda : \mathbb{Z} \to \mathbb{Z}$ la funzione così definita: $\lambda(a) \overset{\text{def}}{=} 5a - 4$ per numeri interi $a \in \mathbb{Z}$. Si denotino con $\lambda^1 \overset{\text{def}}{=} \lambda$, $\lambda^2 \overset{\text{def}}{=} \lambda\lambda$, ... le funzioni che si ottengono componendo λ con se stessa.

1. Per $n \geq 1$ si ha che $\lambda^n(a) = 5^n a - 5^n + 1$? [Sì] | 2 | |

Proviamo l'uguaglianza per induzione su n. Per $n=1$, si ha $\lambda^1(a) = 5^1 a - 5^1 + 1 = 5a - 4$, ed è vero. Supponiamo vero per $n \geq 1$ e proviamolo per $n+1$: $\lambda^{n+1}(a) = \lambda(\lambda^n(a)) = \lambda(5^n a - 5^n + 1) =$ $= 5 \cdot (5^n a - 5^n + 1) - 4 = 5^{n+1} a - 5^{n+1} + 5 - 4 = 5^{n+1} a - 5^{n+1} + 1$, come si voleva.

2. Per $m \geq 0$ si ha che $\lambda^{m+1}(a) = 5^{m+1}a - 5^m - 3$? [No] | 2 | |

Per $m=1$, si ha $\lambda^2(a) = 25a - 24$ (con la formula del punto precedente), mentre $5^{m+1}a - 5^m - 3 = 25a - 8$. Le due espressioni sono evidentemente diverse, ad esempio, per $a = 0$.

C Sia $\mathbb{R}[x]$ l'anello dei polinomi sul campo $\mathbb{R}$, che possiamo vedere come anello o come $\mathbb{R}$-modulo rispetto alle ordinarie operazioni di somma di polinomi e di prodotto per un elemento di $\mathbb{R}$. Consideriamo il sottoinsieme M di $\mathbb{R}[x]$ dei polinomi che si annullano per $x = 0$ e $x = 1$.

1. M è un sottogruppo di $(\mathbb{R}[x], +)$? [sì] | 1 | |

Supponiamo $f, g \in M$. Evidentemente si ha $(f-g)(0) = f(0) - g(0) = 0$, e $(f-g)(1) = f(1) - g(1) = 0$. Dunque $f - g \in M$.

2. M è un ideale dell'anello $\mathbb{R}[x]$? [sì] | 1 | |

Abbiamo già provato che è un sottogruppo. Sia allora $f \in M$, e sia $g \in \mathbb{R}[x]$. Si ha $(gf)(0) = g(0) \cdot f(0) = g(0) \cdot 0 = 0$, e analogamente $(gf)(1) = g(1) \cdot f(1) = g(1) \cdot 0 = 0$, dunque $gf \in M$.

3. M è un sottomodulo di $\mathbb{R}[x]$ come $\mathbb{R}$-modulo? [sì] | 1 | |

Abbiamo osservato che M è un sottogruppo di $(\mathbb{R}[x], +)$; inoltre se $r \in \mathbb{R}$ e $f \in M$, si ha $rf \in M$ (tra l'altro, è un caso particolare di quanto visto al punto precedente).

D In $\mathbb{Z}_6$ si consideri la legge

$$[a]_6 * [b]_6 = [a + 3b]_6 \quad \forall [a]_6, [b]_6 \in \mathbb{Z}_6.$$

Dire se le seguenti affermazioni sono vere o false.

1. $*$ è un'operazione su $\mathbb{Z}_6$. [V] | 1 | |

Poiché le ordinarie operazioni di somma e prodotto in $\mathbb{Z}$ "passano" a $\mathbb{Z}_6$, si ha $[a] * [b] = [a] + 3[b]$, e si tratta senz'altro di un'operazione.

2. $*$ è associativa. [V] | 1 | |

Siano $x, y, z \in \mathbb{Z}_6$. Si ha $(x * y) * z = (x + 3y) * z = (x + 3y) + 3z$. D'altra parte, $x * (y * z) = x * (y + 3z) = x + 3(y + 3z) = x + 3y + 9z = x + 3y + 3z$, dunque le due espressioni coincidono.

3. $*$ è commutativa. [F] | 1 | |

$1 * 2 = 1$; $2 * 1 = -1$

4. $*$ ammette elemento neutro. [F] | 1 | |

Se e fosse elemento neutro, sarebbe $e * 0 = 0$, ma anche $e * 1 = 1$. La prima uguaglianza implica $e = 0$, la seconda $e = -2$ ..

5. $(\mathbb{Z}_6, *)$ è un gruppo. [F] | 1 | |

Per il punto precedente, $(\mathbb{Z}_6, *)$ non è neanche un monoide.

1. In $\mathbb{Z}_p[x]$ (p primo) si consideri l'ideale $I = (x^3 - x^2 + x + 5, x^3 + x)$. Si determinino i valori di p per cui:

   (a) I è un ideale proprio. [2, 3, 5] $\boxed{2}\ \boxed{}$

Si ha $x^3 - x^2 + x + 5 = (x^3 + x) + \underbrace{(-x^2 + 5)}_{\text{resto}}$, e $x^3 + x = (-x^2 + 5)(-x) + \underbrace{6x}_{\text{resto}}$

Se $p \in \{2, 3\}$, si ha allora $I = (x^2 - 5) \subsetneq \mathbb{Z}_p[x]$. Altrimenti: $x^2 - 5 = (6x)(6^{-1}x) - 5$, e per $p = 5$ è $I = (x) \subsetneq \mathbb{Z}_p[x]$. In tutti gli altri casi, i due polinomi sono coprimi e $I = \mathbb{Z}_p[x]$.

   (b) I è un ideale primo. [3, 5] $\boxed{2}\ \boxed{}$

Poiché gli ideali primi sono innanzitutto propri, per $p \notin \{2, 3, 5\}$ I non è primo. Per $p = 2$ è $I = (x^2 + 1)$ e $x^2 + 1 = (x + 1)^2$ non è irriducibile, dunque I non è primo. Per $p = 3$, $I = (x^2 + 1)$ e $x^2 + 1$ non ha radici in $\mathbb{Z}_3$, dunque è irriducibile $\Rightarrow$ I è primo. Per $p = 5$, $I = (x)$

   (c) I è un ideale massimale. [3, 5] e x è ovviamente irriducibile. $\boxed{1}\ \boxed{}$

In $\mathbb{Z}_p[x]$, con p primo, gli ideali primi sono anche massimali (e viceversa).

2. Nel gruppo additivo $(\mathbb{C}, +)$ si definisca una relazione ponendo

$$a + ib \leq c + id \quad \text{se } b < d \text{ oppure } b = d \text{ e } a \leq c.$$

   (a) $(\mathbb{C}, \leq)$ è totalmente ordinato ? [Sì] $\boxed{2}\ \boxed{}$

Considerando $\mathbb{C}$ come $\mathbb{R} \times \mathbb{R}$ e ponendo su ciascuna copia di $\mathbb{R}$ l'ordinamento standard (che è totale), la relazione che stiamo studiando è l'ordinamento lessicografico. Dunque è un ordinamento, ed è totale perché lo è quello standard su $\mathbb{R}$.

   (b) $(\mathbb{C}, \leq)$ è un gruppo ordinato ? [Sì] $\boxed{1}\ \boxed{}$

Sia $a + ib \leq c + id$, dunque, $b < d$ oppure $b = d$ e $a \leq c$. Si ha, $\forall\, e + if \in \mathbb{C}$, $(a + ib) + (e + if) \leq (c + id) + (e + if)$; infatti, se $b < d$, allora $b + f < d + f$, mentre se $b = d$ e $a \leq c$, vale $b + f = d + f$ e $a + e \leq c + e$.

3. Sia $A = \mathbb{Z}[\sqrt{-2}]$.

(a) È vero che $A^* = \{\pm 1\}$? [Sì] $\boxed{2}$

Sia $x = a + ib\sqrt{2} \in A^*$. Allora x divide 1, dunque la sua norma a^2+2b^2 divide $N(1)=1$. Ciò implica $b=0$ e $a^2=1$.

(b) Esiste un massimo comune divisore di $i\sqrt{2}$ e -2 in A ? [Sì] $\boxed{2}$

Si ha $-2 = (i\sqrt{2})^2$, dunque $MCD(i\sqrt{2}, -2) = i\sqrt{2}$.
(In ogni caso, A è un dominio euclideo...)

4. Sia $\mathbb{Z}_p$ il campo delle classi di resti modulo p (p primo). Sia $\phi : \mathbb{Z}[x] \longrightarrow \mathbb{Z}_p[x]$ la funzione definita ponendo

$$\phi(a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0) = \bar{a}_n x^n + \bar{a}_{n-1}x^{n-1} + \cdots + \bar{a}_0$$

dove $\bar{a}_i \in \mathbb{Z}_p$ sono le classi di $a_i \in \mathbb{Z}$ modulo p.

(a) È vero che ϕ è un omomorfismo di anelli ? [Sì] $\boxed{2}$

Siano $f, g \in \mathbb{Z}[x]$. Dobbiamo provare:
1) $\varphi(f+g) = \varphi(f) + \varphi(g)$; 2) $\varphi(fg) = \varphi(f)\cdot\varphi(g)$; 3) $\varphi(1) = [1]$
Si tratta di tre verifiche del tutto banali.

(b) Esiste p tale che ϕ è un isomorfismo ? [No] $\boxed{2}$

Il polinomio costante p è sempre nel nucleo di φ, dunque φ non è mai iniettivo.