ℵ	Matricola:	$\mathbf{A}^{\geq 2}$:...	$\mathbf{B}^{\geq 3}$:...	$\mathbf{C}^{\geq 2}$:...	$\mathbf{D}^{\geq 3}$:...	Voto: .....

Cognome: ..... Nome: .....

Algebra 1 – Esame 05.02.14

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

A Sia X un insieme infinito.

1. È vero che esiste $f : X \to X$ surgettiva non iniettiva ? [Sì] | 2 |

Poiché X è infinito, per definizione esiste un'applicazione $g : X \to X$ iniettiva e non surgettiva. Sappiamo allora che esiste $f : X \to X$ tale che $f \circ g = \mathrm{id}_X$ (un'inversa sinistra di g). Poiché id_X è surgettiva, anche f lo è; inoltre f non può essere iniettiva, altrimenti sarebbe invertibile e la sua (unica) inversa destra g sarebbe anch'essa invertibile, mentre era stata scelta non surgettiva.

2. È vero che esiste $\mathcal{P}(\mathbb{N}) \to X$ iniettiva ? [No] | 2 |

Sia ad esempio $X = \mathbb{N}$; utilizzando l'argomento precedente, si vede che se esistesse una applicazione iniettiva di $\mathcal{P}(\mathbb{N})$ in $\mathbb{N}$, ne esisterebbe una surgettiva di $\mathbb{N}$ in $\mathcal{P}(\mathbb{N})$, contro il Teorema di Cantor.

3. È vero che $\mathcal{P}(X)$ non è numerabile ? [Sì] | 3 |

Poiché X è infinito, esiste un'applicazione iniettiva di $\mathbb{N}$ in X, dunque anche di $\mathcal{P}(\mathbb{N})$ in $\mathcal{P}(X)$, e infine (come sopra) ne esiste una surgettiva di $\mathcal{P}(X)$ in $\mathcal{P}(\mathbb{N})$ (sia essa f). Se $\mathcal{P}(X)$ fosse numerabile, esisterebbe una biezione $g : \mathbb{N} \to \mathcal{P}(X)$, e dunque $f \circ g$ sarebbe un'applicazione surgettiva di $\mathbb{N}$ in $\mathcal{P}(\mathbb{N})$, ancora in contrasto col Teorema di Cantor.

B Sia $G = \{(a, s) \mid a \in \mathbb{Q} \ \& \ s \in \mathbb{Z}\}$. Per $k \in \mathbb{Q}^{\neq 0}$ si consideri in G la seguente operazione

$$(a, s) \star_k (b, t) = (a + k^s b, s + t)$$

1. Mostrare che $(G, \star_k)$ è un gruppo. | 3 | |

L'operazione è senz'altro interna. Verifichiamo che sia associativa:

$$[(a, s) \star_k (b, t)] \star_k (c, u) = (a + k^s b, s + t) \star_k (c, u) = ((a + k^s b) + k^{s+t} c, (s + t) + u),$$

mentre

$$(a, s) \star_k [(b, t) \star_k (c, u)] = (a, s) \star_k (b + k^t c, t + u) = (a + k^s (b + k^t c), s + (t + u)),$$

e le due espressioni coincidono per le proprietà aritmetiche di $\mathbb{Z}$ e $\mathbb{Q}$. Si verifica poi facilmente che $(0, 0)$ funziona da elemento neutro, e che ogni elemento (a, s) ha inverso $(-ak^{-s}, -s) \in G$.

2. Per quali valori di k si ha che $(G, \star_k)$ è commutativo ? $[k = 1]$ | 2 | |

L'operazione $\star_k$ è commutativa se e solo se vale $a + k^s b = b + k^t a$ per ogni scelta di $a, b \in \mathbb{Q}$ e $s, t \in \mathbb{Z}$. In particolare, scegliendo $a = t = 1$ e $b = 0$, si ottiene $k = 1$. viceversa, è ovvio che per $k = 1$ l'operazione $\star_k$ risulti commutativa.

3. Per quali valori di k l'insieme $\{(3s, t) \mid s, t \in \mathbb{Z}\}$ è un sottogruppo di $(G, \star_k)$? $[k = \pm 1]$ | 3 | |

Condizione necessaria affinché l'insieme considerato sia un sottogruppo è che $(0, \pm 2) \star_k (3, 0)$ appartenga a tale insieme. D'altra parte $(0, \pm 2) \star_k (3, 0) = (3k^{\pm 2}, \pm 2)$, e se questo elemento appartiene al nostro insieme allora deve essere $3k^{\pm 2} \in \mathbb{Z}$. Se ciò avviene si ha $k \in \mathbb{Z}$ (da $3k^2 \in \mathbb{Z}$; perché?..) e $k = \pm 1$ (da $3k^{-2} \in \mathbb{Z}$). Viceversa, se $k = \pm 1$, si ha $(3s, t) \star_k (3u, v) = (3(s \pm u), t + v)$ dunque il nostro insieme è chiuso rispetto all'operazione; inoltre esso è chiuso anche per inversione, visto che $(3s, t)^{-1} = (\pm 3s, -t)$.

C Sia $A[X]$ anello dei polinomi a coefficienti in A dominio. Sia $p(X) = X^n - a^n$ per $n \in \mathbb{N}^+$ e $a \in A^{\neq 0}$. Sia $I = (p(X))$ l'ideale principale generato da $p(X)$ in $A[X]$. Mostrare che

1. se $A[X]/I$ è un dominio allora $n = 1$ | 3 | |

   Sia $n > 1$. Per il Teorema di Ruffini, il polinomio $p(X)$ è divisibile (propriamente) per $X - a$, ovvero esiste un polinomio $q(X)$ (di grado $n - 1$) tale che $p(X) = (X - a) \cdot q(X)$. Da ciò segue che $(I + (X - a)) \cdot (I + q(X)) = I + 0$, con entrambi i fattori diversi dallo zero di $A[X]/I$, dunque $A[X]/I$ ha zero-divisori.

2. se $A[X]/I$ è un campo allora A è un campo | 2 | |

   Se $A[X]/I$ è un campo, per il punto precedente si ha $n = 1$. Consideriamo ora l'applicazione $v_a : A[X] \to A$ che ad ogni $p(X) \in A[X]$ associa $p(a)$. È noto che si tratta di un omomorfismo suriettivo di anelli e, per il teorema di Ruffini, il suo nucleo è esattamente I. Dal Teorema di Isomorfismo deduciamo che $A[X]/I$ è isomorfo (come anello) ad A, dunque ovviamente anche A è un campo.

3. se A è ordinato allora $p(X)$ ha al più a come radice positiva ovvero se $a^n = b^n$ con $a, b \in A^+$ allora $a = b$. | 3 | |

   Se è $a > b$, allora per ogni $n \in \mathbb{N}^+$ si ha $a^n > b^n$ (infatti, per $n = 1$ questo è ovviamente vero, mentre, supponendo che ciò valga per n e tenendo conto che $a, b^n \in A^+$, si ha $a^{n+1} = a^n \cdot a > b^n \cdot a > b^n \cdot b = b^{n+1}$). Analogamente, $a < b$ implica $a^n < b^n$ per ogni $n \in \mathbb{N}^+$. Concludiamo che $a \neq b$ implica $a^n \neq b^n$ (si ricordi che l'ordinamento di A è totale), da cui segue ciò che si voleva.

D Sia $S : \begin{cases} x \equiv_3 1 \\ x \equiv_5 2 \\ x \equiv_7 0 \end{cases}$

1. È vero che esiste una unica soluzione $x \in \mathbb{Z}$ di S tale che $0 < x < 105$? [Sì] | 3 | |

   Questo segue dal Teorema Cinese del Resto.

2. È vero che se x e y sono soluzioni di S allora $x \equiv_{105} y$? [Sì] | 2 | |

   È una diversa formulazione della domanda precedente (nella parte riguardante l'unicità).

3. È vero che non esiste x primo in $\mathbb{Z}$ e soluzione di S ? [No] | 2 | |

   È chiaro che l'unica soluzione del sistema tra 0 *e* 104 *è in effetti* 7.