⊙ Matricola: ..... A ... B ... C ... D ... Voto$^{\geq 10}$: .....

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

Algebra 1 – Esame 29.06.11

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

A Sia S un insieme e per $A \subseteq S$ sottoinsieme sia $C_S(A)$ il complementare in S. Siano X e Y due sottoinsiemi di S e sia $X - Y$ l'insieme differenza.

1. È vero che $X - Y = X \cap C_S(Y)$? [Sì] | 2 |

L'insieme $X - Y$ è costituito dagli elementi di X (dunque di S) che non stanno in Y, dunque dagli elementi di X che stanno in $C_S(Y)$.

2. È vero che $C_S\ (X - Y) = C_S(X) \cup Y$? [Sì] | 2 |

Si ha $C_S(X-Y) = C_S(X \cap C_S(Y)) =$ (per le leggi di De Morgan) $= C_S(X) \cup C_S(C_S(Y)) = C_S(X) \cup Y$.

B Sia $(A, +, \cdot)$ un anello UFD (o fattoriale).

1. Se $a, b \in A$ sono primi fra loro anche $a + b$ e ab sono primi fra loro ? [Sì] | 2 |

Sia p un elemento primo di A che divide $a + b$ ed ab. Poiché p è primo e divide ab, possiamo supporre che divida a, dunque $a = pk$ per un opportuno $k \in A$. D'altra parte, $p \mid a + b$ significa $a + b = ph$, da cui $pk + b = ph$ e quindi $b = p(h - k)$. Concludiamo che p divide anche b, dunque abbiamo provato che se ab e $a + b$ non sono coprimi, allora neanche a e b lo sono, il che equivale a ciò che si voleva.

2. Se $d = \text{M.C.D.}(a, b)$ allora esiste $m \in A$ tale che $md = ab$ e $m = \text{m.c.m.}(a, b)$? [Sì] | 2 |

Consideriamo le decomposizioni (uniche a meno dell'ordine dei fattori e a meno di associature) di a e b in fattori irriducibili: sia $a = u \cdot p_1^{a_1} \cdot p_2^{a_2} \cdots p_h^{a_h}$ e $b = v \cdot q_1^{b_1} \cdot q_2^{b_2} \cdots q_k^{b_k}$ con u e v invertibili in A e $p_1, ..., p_h$, $q_1, ..., q_k$ irriducibili in A. Modulo un riordino dei fattori, possiamo supporre che per un opportuno intero non negativo t sia $p_i = q_i$ per ogni $i \leq t$, mentre $\{p_{t+1}, ..., p_h\} \cap \{q_{t+1}, ..., q_k\} = \emptyset$. Poniamo inoltre $\mu_i = \min\{a_i, b_i\}$ e $m_i = \max\{a_i, b_i\}$ per ogni $i \leq t$. È facile verificare che, posto $d = p_1^{\mu_1} \cdots p_t^{\mu_t}$ e $m = p_1^{m_1} \cdots p_t^{m_t} \cdot p_{t+1}^{a_{t+1}} \cdots p_h^{a_h} \cdot q_{t+1}^{b_{t+1}} \cdots q_k^{b_k}$, si ha che d è un massimo comun divisore ed m un minimo comune multiplo di a e b tali che $md = ab$.

C Sia G il sottoinsieme di $M_3(\mathbb{Z}_3)$ delle matrici della forma

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \text{ con } a, b, c \in \mathbb{Z}_3$$

1. Qual è la cardinalità dell'insieme G ? [3^3] | 2 | |

   Questo è infatti il numero di scelte per la terna (ordinata) di elementi (a, b, c).

2. Rispetto al prodotto righe per colonne G è un gruppo ? [Sì] | 2 | |

   Basta provare che G *è un sottogruppo del gruppo delle matrici invertibili* 3×3 *a coefficienti in* $\mathbb{Z}_3$. *Infatti, la matrice identica è ovviamente in* G, *la chiusura per prodotti è una ovvia verifica, e ogni elemento* $\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$ *in* G *ha inverso* $\begin{bmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{bmatrix}$ *in* G.

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 $f_k(x) = x^3 + kx + 1 \in \mathbb{Z}_3[x]$

1. Per quali valori di $k \in \mathbb{Z}_3$ il polinomio $f_k(x)$ ammette radici in $\mathbb{Z}_3$? [0 e 1] | 2 | |

   Per $k = 0$ *si ha la radice* 2, *per* $k = 1$ *si ha la radice* 1, *mentre per* $k = 2$ *il polinomio non ammette radici.*

2. Per quali valori di $k \in \mathbb{Z}_3$ il polinomio $f_k(x)$ è primo con $g(x) = x^2 + 1$? [Tutti] . | 2 | |

   Osserviamo che $x^2 + 1$ *non ha radici in* $\mathbb{Z}_3$, *pertanto è irriducibile in* $\mathbb{Z}_3[x]$. *Se non fosse coprimo con* $f_k(x)$, *dovrebbe dunque dividerlo. Ma il resto della divisione di* $f_k(x)$ *per* $x^2 + 1$ *è* $(k-1)x + 1$, *che non è* 0 *per alcun valore di* k.