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

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

Algebra 1 – Esame 18.09.13

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

A Sia S un insieme e sia $\mathcal{P}(\mathcal{S})$ l'insieme delle parti di S. Denotiamo $A+B \stackrel{\text{def}}{=} (A \setminus B) \cup (B \setminus A)$ e $A \cdot B \stackrel{\text{def}}{=} A \cap B$ per $A, B \in \mathcal{P}(\mathcal{S})$

1. È vero che $+$ è commutativa ? [Sì] $A + A = \emptyset$? [Sì] | 2 |

   La commutatività segue immediatamente dal fatto che l'unione tra insiemi è commutativa. Inoltre, per ogni $A \in \mathcal{P}(\mathcal{S})$ si ha $A \setminus A = \emptyset$..

2. È vero che $(\mathcal{P}(\mathcal{S}), \cdot)$ è un monoide ? [Sì] È vero che è un gruppo ? [No] | 2 |

   L'intersezione tra insiemi è un'operazione associativa, ed S funziona da elemento neutro, dunque $\mathcal{P}(\mathcal{S})$ è un monoide. Non è però in generale un gruppo, poiché (ad esempio), qualora S sia non vuoto, non esiste alcun sottoinsieme di S che intersecato con $\emptyset$ dia l'elemento neutro S.

B Nell'anello $A = \mathbb{Z}[i] \stackrel{\text{def}}{=} \{x + iy \mid x, y \in \mathbb{Z}\}$ degli interi di Gauss sia $B \stackrel{\text{def}}{=} \{(a-b) + i(a+b) \mid a, b \in \mathbb{Z}\}$

1. B è un sottoanello di A ? [No] B è un anello? [Sì] | 2 |

   L'insieme B non contiene l'unità di A, poiché non esistono due interi a, b tali che $a - b = 1$ e $a + b = 0$. D'altra parte, B è un sottogruppo di $(A, +)$ perché è non vuoto ed evidentemente chiuso per somme ed opposti. Inoltre B è chiuso rispetto al prodotto:

   $$[(a-b) + i(a+b)] \cdot [(c-d) + i(c+d)] = (-2ad - 2bc) + i(2ac - 2bd).$$

   Si tratta dunque di trovare due interi x, y tali che $x - y = -2(ad+bc)$ e $x+y = 2(ac-bd)$. Tale sistema di equazioni ha soluzione $x = ac - ad - bc - bd$, $y = ac + ad + bc - bd$, come si vede facilmente. Ciò è sufficiente a garantire che B sia un anello.

2. Sia $\mathcal{R}$ la relazione su A così definita: $\alpha \mathcal{R} \beta$ se $\alpha - \beta \in B$. Mostrare che $\mathcal{R}$ è di equivalenza. La classe $[0]_{\mathcal{R}} = B$? [Sì] | 2 |

   La relazione in questione è precisamente quella che definisce la congruenza modulo B in $(A, +)$ (ovvero, la struttura di gruppo quoziente A/B), che ha senso in quanto $(A, +)$ è un gruppo abeliano e B è un suo sottogruppo. In tale congruenza, è ben noto che la classe di equivalenza di 0 coincide con B.

C Si consideri l'anello $M \stackrel{\text{def}}{=} \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mid a, b \in \mathbb{Z}_{10} \right\}$ rispetto alle usuali operazioni di somma di matrici e prodotto righe per colonne.

1. È vero che $(M, +, \cdot)$ possiede divisori dello zero ? [Sì] | 2 | |

   Si consideri ad esempio che si ha

   $$\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

2. Mostrare che il sottoinsieme $N \stackrel{\text{def}}{=} \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix} \right\}$ è un campo che non è un sottocampo di M. | 2 | |

   Si vede facilmente che la prima matrice funziona da zero e la seconda da unità, dunque si tratta di un campo con i soli elementi 0 *e* 1*. Non è tuttavia un sottoanello di* M *poiché non contiene l'unità di* M*.*

D Siano $a(x) = (x^2+x-2)(x^2-x-1)$ e $b(x) = x^4-2x^3-x^2-2x-1$ nell'anello $K[x]$ dei polinomi a coefficienti in un campo K.

1. Per $K = \mathbb{Q}$ trovare un M.C.D. di $a(x)$ e $b(x)$ M.C.D. = [1] | 2 | |

   Si osservi che $a(x) = (x+2)(x-1)(x^2-x-1)$*, ove quest'ultimo polinomio è irriducibile in* $\mathbb{Q}[x]$ *poiché le sue radici sono irrazionali. Ora, né* -2 *né* 1 *sono radici di* $b(x)$*, e* x^2-x-1 *non divide* $b(x)$*, come si verifica facilmente svolgendo la divisione tra polinomi.*

2. Per $K = \mathbb{Z}_p$ trovare i valori di p (primo) tali che $a(x)$ e $b(x)$ siano coprimi: $p =$ [un qualsiasi primo eccetto 2, 5, 31] | 2 | |

   I due polinomi sono coprimi se e solo se -2 *e* 1 *non sono radici di* $b(x)$ *e* x^2-x-1 *è coprimo con* $b(x)$*. ebbene,* $b(-2) = 31$*,* $b(1) = -5$*, e il resto della divisione di* $b(x)$ *per* x^2-x-1 *è* $-4x-2$*. è dunque evidente che se* $p \in \{2, 5, 31\}$ *allora* $a(x)$ *e* $b(x)$ *non sono coprimi. In caso contrario, tramite l'algoritmo delle divisioni successive, si vede che non soltanto* x^2-x-1 *non divide* $b(x)$*, ma esso risulta anche coprimo con* $b(x)$*.*