MATRICOLA: ..... $\mathbf{A}^{\geq 3}$:... $\mathbf{B}^{\geq 3}$:... $\mathbf{C}^{\geq 3}$:... $\mathbf{D}^{\geq 3}$:... VOTO: .....

COGNOME: ..... NOME: .....

Algebra 1 – II Prova Intermedia/Esame 17.12.13

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

A Sia $X = S^S$ l'insieme delle funzioni $f : S \to S$ per S finito di cardinalità $|S| = n \in \mathbb{N}^+$.

1. Mostrare che X è finito. | 2 |

   Si osserva che $X \subseteq \mathcal{P}(S \times S)$ è costituito dai sottoinsiemi di $S \times S$ che sono grafici di $f : S \to S$. Siccome $\mathcal{P}(S \times S)$ è finito anche X è finito (ed è facile vedere che $|X| = |S|^{|S|} = n^n$).

2. È vero che $n! \leq |X| \leq 2^{n^2}$ per ogni $n \in \mathbb{N}^+$? [Sì] | 3 |

   Osserviamo che $n!$ è il numero delle funzioni iniettive *(quindi bigettive) di S in S mentre $|S \times S| = n^2$ e $|\mathcal{P}(S \times S)| = 2^{n^2}$. È quindi chiaro che sia vero quanto affermato. (Si potrebbe anche osservare che $2^{n^2} = (2^n)^n$ è il numero di tutte le funzioni di S nel suo insieme delle parti $\mathcal{P}(S)$ e poi sfruttare il Teorema di Cantor $|S| < |\mathcal{P}(S)|$).*

3. È vero che $|X| \neq 2^{n^2}$ per ogni $n \in \mathbb{N}^+$? [Sì] | 3 |

   Ciò è ovvio se si tiene conto di quanto detto in precedenza: infatti $\emptyset \in \mathcal{P}(S \times S)$ ma $\emptyset \notin X$ se $S \neq \emptyset$. Si può anche argomentare così: se fosse $n^n = 2^{n^2} = (2^n)^n$ si ottiene $n = 2^n$, il che è assurdo per il Teorema di Cantor.

B Si consideri il polinomio $p(X) = X^3 + X + 1$.

1. $p(X)$ è irriducibile in $\mathbb{Z}_2[X]$? [Sì] | 2 | |

   L'anello $\mathbb{Z}_2[X]$ è un anello di polinomi a coefficienti in un campo, e $p(X)$ è un polinomio di grado 3. Pertanto $p(X)$ è irriducibile in $\mathbb{Z}_2[X]$ se e solo se non ha radici in $\mathbb{Z}_2$. È evidente che né 0 né 1 risultano radici di $p(X)$.

2. $p(X) + X^2$ è riducibile in $\mathbb{Z}_2[X]$? [Sì] | 2 | |

   Per quanto osservato sopra, $p(X) + X^2$ è riducibile poiché $1 \in \mathbb{Z}_2$ è una sua radice.

3. $\mathbb{Z}_2[X]/(p(X))$ è un campo finito ? [Sì] | 3 | |

   È noto che l'anello $\mathbb{Z}_2[X]/(p(X))$ risulta un campo se e solo se $p(X)$ è irriducibile, e $p(X)$ lo è. È inoltre noto che ogni classe di equivalenza di polinomi in $\mathbb{Z}_2[X]/(p(X))$ può essere rappresentata mediante un polinomio di grado pari a $\deg(p(X)) - 1$, pertanto $\mathbb{Z}_2[X]/(p(X))$ ha 2^3 elementi.

C Sia A l'insieme delle matrici $\begin{pmatrix} a+2b & b \\ -b & a \end{pmatrix}$ al variare di $a, b \in \mathbb{Z}_5$. Mostrare che:

1. A è un sottoanello dell'anello delle matrici $M_2(\mathbb{Z}_5)$ | 2 |

   Verifichiamo che A sia un sottogruppo di $(M_2(\mathbb{Z}_5), +)$: evidentemente A è non vuoto (contiene ad esempio la matrice nulla), inoltre, per $\begin{pmatrix} a+2b & b \\ -b & a \end{pmatrix}$, $\begin{pmatrix} c+2d & d \\ -d & c \end{pmatrix}$ in A, si ha

$$\begin{pmatrix} a+2b & b \\ -b & a \end{pmatrix} - \begin{pmatrix} c+2d & d \\ -d & c \end{pmatrix} = \begin{pmatrix} (a-c)+2(b-d) & b-d \\ -b+d & a-c \end{pmatrix} \in A.$$

   Proviamo ora la chiusura rispetto al prodotto righe per colonne:

$$\begin{pmatrix} a+2b & b \\ -b & a \end{pmatrix} \cdot \begin{pmatrix} c+2d & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac+2bc+2ad+3bd & ad+2bd+bc \\ -bc-2bd-ad & -bd+ac \end{pmatrix}.$$

   Poiché $ac - bd + 2(ad + 2bd + bc) = ac + 2bc + 2ad + 3bd$, quest'ultima matrice è in A.

2. il gruppo moltiplicativo A^* degli elementi invertibili è finito | 2 |

   Ovvio, visto che lo è A (infatti $|A| = 5^2$)

3. $|A^*| = 20$ | 3 |

   La matrice $\begin{pmatrix} a+2b & b \\ -b & a \end{pmatrix}$ è invertibile in $M_2(\mathbb{Z}_5)$ se e solo se il suo determinante $a^2 + 2b + b^2 = (a+b)^2$ è diverso da 0. Osserviamo però che, qualora $\begin{pmatrix} a+2b & b \\ -b & a \end{pmatrix}$ sia invertibile in $M_2(\mathbb{Z}_5)$, la sua inversa è $(a+b)^{-2} \cdot \begin{pmatrix} a & -b \\ b & a+2b \end{pmatrix}$, che è ancora in A; dunque $\begin{pmatrix} a+2b & b \\ -b & a \end{pmatrix}$ è invertibile in A se e solo se $(a+b)^2 \neq 0$. Ovviamente $(a+b)^2 = 0$ se e solo se $a = -b$, dunque saranno 5 gli elementi non invertibili in A, e $|A^*| = 20$.

D Si consideri $A = \mathbb{Z}[\sqrt{-3}]$ sottoanello di $\mathbb{C}$.

1. È vero che $\mathrm{char}(A) = 0$? [Sì] | 2 | |

   La caratteristica di un anello (dotato di unità) è il più piccolo intero positivo n per cui si abbia $n \cdot 1 = 0$, qualora esso esista; altrimenti la carateristica è per definizione 0. L'anello A è un sottoanello di $\mathbb{C}$, pertanto è ovviamente un anello di caratteristica 0.

2. È vero che 2 è primo in A ? [No] | 3 | |

   Si ha che 2 è un divisore in A di $4 = (1 + i\sqrt{3}) \cdot (1 - i\sqrt{3})$, ma ovviamente non divide alcuno dei due fattori.

3. È vero che A è un U.F.D. ? [No] | 3 | |

   Se A fosse un U.F.D., ogni suo elemento irriducibile sarebbe anche primo. Si è osservato che 2 non è primo in A, tuttavia esso è un elemento irriducibile. Infatti non è invertibile (gli invertibili in A hanno norma 1, dunque sono soltanto 1 e -1) e, avendo norma 4, almeno uno dei (due) fattori di una sua decomposizione deve avere norma 1 o 2. Ma in A non esistono elementi di norma 2, poiché l'equazione $a^2 + 3b^2 = 2$ non ha alcuna soluzione in $\mathbb{Z} \times \mathbb{Z}$, dunque uno dei due fattori ha norma 1 ed è pertanto invertibile.