$\boxed{\Psi}$ Matricola: .... A $B^{\leq 6}$: ... C $D^{\geq 4}$: ... 1 2 3 $4^{\geq 8}$: ... Voto: ......

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

Algebra 1 – Esame 02.02.12

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

A Siano A e B due insiemi non vuoti disgiunti tali che esiste $f : A \to B$ iniettiva.

1. Se A è infinito allora B è infinito ? [Sì] $\boxed{1}\boxed{}$

   Per definizione, se esiste un'applicazione iniettiva di A in B, la cardinalità di A è minore o uguale a quella di B. Se B fosse finito ...

2. Esiste $C \subseteq B$ non vuoto tale che $|A| = |C|$? [Sì] $\boxed{1}\boxed{}$

   Basta scegliere $C = f(A)$ e quindi $f : A \to C$ bigettiva ...

B Sia $f : \mathbb{N} \to \mathbb{N}$ un'applicazione iniettiva e sia $f^n : \mathbb{N} \to \mathbb{N}$ la composta n-esima, $f^0 = id$, $f^1 = f$, $f^2 = f \circ f$, etc...

1. Mostrare che f^n è iniettiva per ogni $n \in \mathbb{N}$. $\boxed{2}\boxed{}$

   Come si verifica ovviamente, la composizione di due funzioni iniettive è iniettiva. L'affermazione può quindi essere provata per induzione: per $n = 1$ è vero per ipotesi, mentre, per $n \geq 2$, $f^n = f^{n-1} \circ f$ è composizione di due funzioni iniettive per ipotesi induttiva.

2. Se f^n è surgettiva per qualche $n > 1$ allora f^n è bigettiva per ogni $n \in \mathbb{N}$? $\boxed{2}\boxed{}$

   È noto che, qualora la composizione di due funzioni sia suriettiva, allora quella che viene applicata per seconda è suriettiva. Se f^n è suriettiva per un certo $n > 1$ allora, poiché $f^n = f \circ f^{n-1}$, anche f lo è. Concludiamo che f è bigettiva, dunque anche f^n lo è per ogni $n \in \mathbb{N}$.

C Sia $\mathbb{M}_2(\mathbb{Z}_n) = \{\text{matrici } 2\times 2 \text{ ad entrate in } \mathbb{Z}_n\}$ con $n \geq 3$. Sia $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathbb{M}_2(\mathbb{Z}_n)$ e sia $B \perp B' = A \cdot B + B' \cdot A$ per $B, B' \in \mathbb{M}_2(\mathbb{Z}_n)$.

1. Esiste $B \neq 0, I$ tale che $B \perp I = 0$? [Sì] | 2 | |

   Si tratta di trovare una soluzione, diversa da 0 e da I, dell'equazione $A \cdot B + A = 0$ ovvero $A \cdot (B + I) = 0$ e $B = -I$ è ovviamente una tale soluzione, in quanto per $n \geq 3$ si ha $-I \neq I$.
   (N.B. osserviamo inoltre che tale B è unica in quanto $\det A = 1$ è un elemento invertibile in $\mathbb{Z}_n$ per ogni $n \geq 3$, dunque A è una matrice invertibile: $A \cdot X = 0$ implica $X = 0$. In altre parole, essendo A invertibile non è zero-divisore in $\mathbb{M}_2(\mathbb{Z}_n)$.)

2. Esiste $B \neq 0, I$ tale che $B \perp 0 = 0 \perp B$? [Sì] | 2 | |

   In questo caso, dobbiamo risolvere l'equazione $A \cdot B + 0 \cdot A = A \cdot 0 + B \cdot A$, ovvero $A \cdot B = B \cdot A$ ovvero trovare una matrice che commuti con A. Una tale matrice è ovviamente $B = A$ ma anche la matrice $-I$ ha questa proprietà.

3. $(\mathbb{M}_2(\mathbb{Z}_n), \perp)$ è un semigruppo ? [No] | 2 | |

   Si ha $0 \perp (-I \perp I) = 0 \perp 0 = 0$, mentre $(0 \perp -I) \perp I = -A \perp I = -A^2 + A$. Siccome $A^2 \neq A$ l'ultima espressione non è 0.

D Sia (A, δ) dominio euclideo con norma $\delta : A \setminus \{0\} \to \mathbb{N}$. Sia $I \subset A$ un ideale $I \neq 0, A$.

1. È vero che $I = (\pi)$ tale che $\delta(\pi)$ è il minimo di $\{\delta(a) \mid a \in I \quad a \neq 0\}$? [Sì] | 2 | |

   Infatti, sia $x \in I \setminus \{0\}$, e consideriamo la divisione di x per π: esistono q, r in I tali che $x = \pi q + r$, con $r = 0$ oppure $\delta(r) < \delta(\pi)$. D'altra parte, $r = x - \pi q$ è differenza di elementi in I, dunque è a sua volta in I. Ma poiché $\delta(\pi)$ è minima tra le valutazioni degli elementi non nulli di I, non può che essere $r = 0$. Concludiamo che $x = \pi q$, dunque $x \in (\pi)$. Ciò vale per ogni $x \in I$, da cui $I \subseteq (\pi)$, dunque ovviamente $I = (\pi)$. (Si tratta di un argomento standard, svolto durante le lezioni e le esercitazioni.)

2. È vero che $\delta(a) > \delta(1)$ per ogni $a \in I \setminus \{0\}$? [Sì] | 1 | |

   È noto che, in un dominio euclideo, gli elementi invertibili sono tutti e soli quelli la cui valutazione coincide con $\delta(1)$. (N.B. la valutazione di ogni elemento non nullo è $\geq \delta(1)$.) Perciò, se esistesse $a \in I \setminus \{0\}$ con $\delta(a) = \delta(1)$, l'elemento a sarebbe invertibile, e I sarebbe tutto A, contro le ipotesi.

3. È vero che π è irriducibile ? [No] | 1 | |

   Sia ad esempio $A = \mathbb{Z}$ con l'usuale valutazione euclidea, e sia $I = (4)$. Evidentemente, $4 = 2 \cdot 2$ non è irriducibile.

1. Sia $f(X) \in \mathbb{Z}[X]$ il polinomio $f(X) = X^5 - 1$.

   (a) $\dfrac{f(X)}{X-1}$ ammette la radice 1 ? [No] $\boxed{2}\boxed{}$

   Basta eseguire la divisione di polinomi e si ottiene $X^4 + X^3 + X^2 + X + 1$. *Dunque il polinomio* $\frac{f(X)}{X-1}$ *non ammette* 1 *come radice.*

   (b) Sia $\mu_5 = \{\zeta \in \mathbb{C} \mid f(\zeta) = 0\}$. È vero che $\mu_5 \subset \mathbb{C}^*$ è un sottogruppo finito ? [Sì] $\boxed{2}\boxed{}$

   L'insieme μ_5 *è costituito da tutte e sole le radici quinte di* 1; *è ovviamente non vuoto, poiché contiene* 1. *Inoltre, se* $x, y \in \mu_5$, *si ha* $(xy^{-1})^5 = x^5 \cdot (y^5)^{-1} = 1 \cdot 1^{-1} = 1$, *dunque* $xy^{-1} \in \mu_5$. *Si tratta dunque di un sottogruppo, ovviamente finito in quanto i suoi elementi sono le radici di un polinomio di grado* 5 *(dunque sono al più* 5*).*

2. Sia $G = \mathbb{Q} \setminus \{-1\} \times \mathbb{Q} \setminus \{-1/2\}$ e sia $\star$ l'operazione così definita:

$$(x, y) \star (x', y') = (x + 2y' + 2xy', x'/2 + y + x'y)$$

   per $(x, y), (x', y') \in G$.

   (a) G è chiuso rispetto a $\star$? [Sì] $\boxed{1}\boxed{}$

   Infatti, supponiamo $x + 2y' + 2xy' = -1$: *si ha* $(1 + x)(1 + 2y') = 0$, *da cui* $x = -1$ *oppure* $y' = -1/2$. *Analogamente, supponendo* $x'/2 + y + x'y = -1/2$, *si ottiene* $x' = -1$ *oppure* $y = -1/2$. *Se* $(x, y), (x', y') \in G$, *nessuna delle quattro posibilità si verifica, pertanto anche* $(x, y) \star (x', y') \in G$.

   (b) $(G, \star)$ è un semigruppo ? [No] $\boxed{2}\boxed{}$

   Ad esempio, si ha $[(0, 0) \star (1, 0)] \star (0, 1) = (2, 1/2)$, *mentre* $(0, 0) \star [(1, 0) \star (0, 1)] = (0, 5/2)$.

3. Consideriamo la relazione di equivalenza in $\mathbb{Z}[\sqrt{-2}]$ definita da $a+b\sqrt{-2} \equiv c+d\sqrt{-2}$ se $a \equiv_3 c$ e $b \equiv_3 d$. Le classi di equivalenza costituiscono un anello che denotiamo

$$A = \{a + b\sqrt{-2} \mid a, b \in \mathbb{Z}_3\}$$

(a) Mostrare che A non è un campo. | 2 | |

Siccome $(1+\sqrt{-2})(1-\sqrt{-2}) = 3$ *che è zero in* A *si ha che l'anello* A *possiede zero-divisori.(N.B. Osserviamo che* A *è l'anello quoziente* $\mathbb{Z}[\sqrt{-2}]/(3)$*.)*

(b) È vero che $x = x^3$ per ogni $x \in A$? [Sì] | 2 | |

Si ha $(a+b\sqrt{-2})^3 = (a^3 - 6ab^2) + (3a^2b - 2b^3)\sqrt{-2}$. *D'altra parte, si ha* $a^3 - 6ab^2 \equiv_3 a^3 \equiv_3 a$, *inoltre* $3a^2b - 2b^3 \equiv_3 -2b^3 \equiv_3 b^3 \equiv_3 b$.

4. Sia $\phi_n : \mathbb{Z}_n \to \mathbb{Z}_n$ l'applicazione $\phi_n(x) = x^n + x^{n-1} + \cdots + x + 1$ con $x \in \mathbb{Z}_n$ e $n \geq 2$. È vero che per ogni $n \geq 2$:

(a) esiste x tale che $\phi_n(x) = x$? [Sì] | 2 | |

Per ogni $n \geq 2$ *si ha* $\phi_n(1) = n \cdot 1 + 1 = 0 + 1 = 1$.

(b) $\phi_n : \mathbb{Z}_n \to \mathbb{Z}_n$ non è surgettiva ? [Sì] | 2 | |

L'applicazione ϕ_n *non è iniettiva, visto che* $\phi_n(0) = 1 = \phi_n(1)$, *pertanto (trattandosi di un'applicazione di un insieme finito in sé) non è neanche surgettiva.*