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

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

Algebra 1 – Prova Intermedia: II Esonero 19.12.12

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

A Sia X un insieme finito non vuoto.

1. È vero che $|X| \neq |X \times X|$? [No] | 2 |

   È noto che, dato un insieme finito X, si ha $|X \times X| = |X|^2$. Dunque un qualsiasi insieme di cardinalità 1 è un controesempio all'asserto.

2. È vero che $\mathcal{P}(X \times X) = \mathcal{P}(X) \times \mathcal{P}(X)$? [No]

   È noto che, dato un insieme finito X, si ha $|\mathcal{P}(X)| = 2^{|X|}$. Dunque, in generale, vale $|\mathcal{P}(X \times X)| = 2^{|X|^2}$, mentre $|\mathcal{P}(X) \times \mathcal{P}(X)| = |\mathcal{P}(X)|^2 = 2^{2|X|}$. Come si vede ad esempio con un insieme X di cardinalità 1, gli insiemi $\mathcal{P}(X \times X)$ e $\mathcal{P}(X) \times \mathcal{P}(X)$ non hanno la stessa cardinalità, e non sono pertanto uguali.

| 2 |

3. Se esiste $f : X \to X \times X$ surgettiva allora $|X| = |X \times X|$? [Sì]

   Sia $y \in X$ fissato. È evidente che l'applicazione $g : X \to X \times X$ definita da $g(x) = (x, y)$ per ogni $x \in X$ risulta un'applicazione iniettiva, pertanto $|X| \leq |X \times X|$. (D'altra parte, $|X| \leq |X|^2 = |X \times X|$...) Se esiste un'applicazione f come nell'enunciato, si ha $|X \times X| \leq |X|$, da cui segue l'uguaglianza. | 3 |

B Si consideri il polinomio $p(X) = 7X^3 - 2X + 1$.

1. Mostrare che $p(X)$ non ha radici in $\mathbb{Q}$. | 3 | |

Siano a e $b \neq 0$ interi coprimi, tali che a/b sia radice di $p(X)$. Come mostrato a lezione (e come si vede facilmente), questa condizione implica $a \mid 1$ e $b \mid 7$, dunque $a/b \in \{\pm 1, \pm 1/7\}$. Basta verificare che nessun elemento di quest'ultimo insieme è effettivamente una radice di $p(X)$.

2. $p(X)$ è irriducibile in $\mathbb{R}[X]$? [No] | 3 | |

Se z è radice di $p(X)$ in $\mathbb{C}$, anche il complesso coniugato $\bar{z}$ di z lo è in quanto i coefficienti di $p(X)$ sono reali. Infatti $p(z) = 0$ implica $0 = \bar{0} = \overline{p(z)} = p(\bar{z})$. Concludiamo che il coniugio induce una permutazione delle radici complesse di $p(X)$ (preservandone la molteplicità) e, poiché $p(X)$ ha grado 3 (dispari) ed ha dunque tre radici in $\mathbb{C}$, una di queste deve essere lasciata invariata dal coniugio, i.e., deve essere reale. Notare che per il "Teorema Fondamentale dell'Algebra" *ogni polinomio (non costante) a coefficienti complessi si spezza nel prodotto di polinomi di primo grado in $\mathbb{C}[X]$.*

3. $p(X)$ è irriducibile in $\mathbb{Z}_6[X]$? [No] | 2 | |

Il polinomio $p(X)$ è senz'altro non invertibile, poiché di grado positivo e con coefficiente principale invertibile (dunque non uno zero-divisore). Inoltre si verifica immediatamente che $1 \in \mathbb{Z}_6$ è una radice di $p(X)$, pertanto il Teorema di Ruffini dà la fattorizzazione $p(X) = (X-1)(X^2 + X - 1)$. Poiché ciascuno dei due fattori ha coefficiente principale 1 (dunque invertibile, dunque non uno zero-divisore), nessuno di tali fattori può essere invertibile in $\mathbb{Z}_6[X]$, dunque la fattorizzazione è propria e $p(X)$ non è irriducibile.

C Sia $\phi : \mathbb{Z}_p \longrightarrow \mathbb{Z}_p$ la funzione definita ponendo

$$\phi(x) = (x+1)^p + x^{p-1} + 1$$

per $x \in \mathbb{Z}_p$ dove $\mathbb{Z}_p$ è il campo delle classi di resti modulo p primo.

1. Per quali p si ha che ϕ è invertibile ? [Nessuno] | 3 |

Ricordiamo che, per il "Piccolo Teorema di Fermat" *si ha $y^p = y$ per ogni $y \in \mathbb{Z}_p$, e $y^{p-1} = 1$ per ogni $y \in \mathbb{Z}_p \setminus \{0\}$. Se dunque $x \neq 0$, vale $\phi(x) = x + 3$, mentre $\phi(0) = 2$. Si vede allora che $\phi(-1) = 2 = \phi(0)$, da cui segue che ϕ non è iniettiva, e ciò indipendentemente dalla scelta di p. Concludiamo che ϕ non è invertibile per alcun primo p.*

2. Per quali p si ha $\phi(x+y) = \phi(x) + \phi(y)$? $[p = 2]$ | 3 |

Se vale l'uguaglianza dell'enunciato, si ha in particolare $2 = \phi(0) = \phi(0+0) = \phi(0) + \phi(0) = 2 + 2$, da cui $2 = 0$. Ciò implica che p sia un divisore di 2, dunque $p = 2$. In effetti, si verifica immediatamente che per $p = 2$ vale $\phi(x) = 0$ per ogni $x \in \mathbb{Z}_2$, dunque in questo caso l'uguaglianza è verificata.

3. Per quali p si ha che ϕ^p è invertibile ? [Nessuno] | 2 |

Per ogni p vale $\phi^{p-1} \circ \phi = \phi^p = \phi \circ \phi^{p-1}$. Se ϕ^p è invertibile, allora è iniettiva, dunque lo è $\phi^{p-1} \circ \phi$, dunque lo è ϕ. D'altra parte, se ϕ^p è invertibile, allora è suriettiva, dunque lo è $\phi \circ \phi^{p-1}$, dunque lo è ϕ. Concludiamo che l'invertibilità di ϕ^p implica l'invertibilità di ϕ, cosa che non sussiste per alcun valore di p.

D Si consideri $\mathbb{Z}[i]$ l'anello degli interi di Gauss. Sia $(1+2i)$ l'ideale principale generato da $1+2i$. Sia

$$A = \mathbb{Z}[i]/(1+2i)$$

l'anello quoziente.

1. È vero che $\mathrm{char}(A) = 0$? [No] | 3 | |

Si ha $5 \cdot ((1+2i)+1) = (1+2i)+5 = (1+2i)+0$ *(infatti* 5 *è divisibile per* $1+2i$*, essendo il prodotto di* $1+2i$ *per il suo complesso coniugato). Dunque* A *non ha caratteristica zero.*

2. È vero che A è finito ? [Sì] | 3 | |

Abbiamo osservato che $5 \in (1+2i)$*. Per ogni* a*,* b *in* $\mathbb{Z}$ *dunque, effettuando la divisione con resto per* 5*, si ottiene* $(1+2i)+a+ib = (1+2i)+5q_a+r_a+5q_bi+r_bi = (1+2i)+r_a+r_bi$*, dove* r_a *ed* r_b *sono interi compresi tra* 0 *e* 4*. Si vede dunque che abbiamo al più* 25 *possibilità per un elemento dell'anello* A*.*
Altrimenti, considerando l'omomorfismo caratteristico $\mathbb{Z} \to A$ *si vede che* $\mathbb{Z}_5 \cong A$*. Infatti, osserviamo che* $2i+1 = 0$ *in* A *e inoltre* $i^2+1 = 0$ *da cui segue che* $i = 2$ *in* A*. Se ne deduce dunque che* $\mathbb{Z} \to A$ *surgettivo con nucleo* (5)*.*

3. È vero che A è un campo ? [Sì] | 2 | |

Essendo A *un anello commutativo con unità finito, esso è un campo se e solo se è privo di zero-divisori. Osserviamo che* $1+2i$ *è un elemento primo in* $\mathbb{Z}[i]$ *in quanto la sua norma è* 5 *(un primo di* $\mathbb{Z}$*). Allora, se* $((1+2i)+x) \cdot ((1+2i)+y) = (1+2i)+0$ *(con* $x, y \in \mathbb{Z}[i]$*), si ha* $1+2i \mid xy$*, da cui* $1+2i \mid x$ *oppure* $1+2i \mid y$*. In ogni caso, uno dei due fattori deve essere* $(1+2i)+0$*, dunque non esistono fattorizzazioni di* 0 *mediante due elementi entrambi non nulli.*
Si può anche argomentare mediante l'omorfismo caratteristico oppure che l'applicazione $\phi : \mathbb{Z}[i] \to \mathbb{Z}_5$ *definita da*

$$f(a+ib) = [a-3b]_5$$

risulta un'omomorfismo suriettivo di anelli, il cui nucleo è $(1+2i)$*. Il teorema di omomorfismo garantisce allora che* A *è isomorfo (come anello) a* $\mathbb{Z}_5$*, ed è pertanto un campo.*