
AL110 - Algebra 1 - A.A. 2010/2011

Appello C - Giugno 2011

Matricola (O ALTRO IDENTIFICATIVO) →

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

esercizio	1.1	1.2	1.3	1.4	2	3.1	3.2	4.1	4.2	4.3	4.4	4.5
punti max	2	2	2	3	4	2	5	2	2	2	2	3
punti assegnati												
totale												

esercizio	5.1	5.2	5.3	5.4	5.5	5.6	6.1	6.2	6.3	7.1	7.2.1	7.2.2
punti max	8	5	4	2	3	4	3	8	2	4	3	6
punti assegnati												
totale												

AVVERTENZE : Svolgere gli esercizi in modo conciso, ma esauriente, nello spazio assegnato nel presente fascicolo. Non verranno accettati altri fogli aggiuntivi.

– Fino a “**due punti**” **ulteriori (bonus)** potranno essere assegnati agli elaborati scritti in modo molto chiaro.

– Fino a “ – **due punti**” (**malus**) potranno essere tolti agli elaborati scritti con calligrafia difficilmente leggibile.

ESERCIZIO 1. Siano $\mathbb{Z}$ l’anello degli interi relativi e $\mathbb{Q}$ il campo dei numeri razionali.

Dotiamo $\mathbb{Z} \times \mathbb{Q}$ della struttura naturale di anello (detto prodotto diretto) le cui operazioni sono definite componente per componente, cioè:

$$(a, b) + (a', b') := (a + a', b + b'), \quad (a, b) \cdot (a', b') := (aa', bb'), \quad \forall a, a' \in \mathbb{Z}, \forall b, b' \in \mathbb{Q}.$$

- (1) Determinare se $(\mathbb{Z} \times \mathbb{Q}, +, \cdot)$ è un anello commutativo o/e unitario.
- (2) Determinare se $(\mathbb{Z} \times \mathbb{Q}, +, \cdot)$ è un dominio o/e un campo.
- (3) Stabilire se, dato I un ideale di $\mathbb{Z}$, allora $I \times \{0\}$ o/e $I \times \mathbb{Q}$ è un ideale di $(\mathbb{Z} \times \mathbb{Q}, +, \cdot)$.
- (4) Sia I un ideale di $\mathbb{Z}$, verificare che l’applicazione $\varphi : \mathbb{Z} \times \mathbb{Q} \rightarrow (\mathbb{Z}/I) \times \mathbb{Q}$ definita ponendo

$$\varphi((a, b)) := (a + I, b), \quad \text{dove } a + I := \{a + i \mid i \in I\},$$

è un omomorfismo suriettivo di anelli. Determinare, poi, esplicitamente $\text{Ker}(\varphi)$.

ESERCIZIO 2. Determinare tutte le eventuali soluzioni del sistema di congruenze seguente, descrivendo brevemente il metodo utilizzato:

$$\begin{cases} 5X \equiv 2 \pmod{7} \\ 4X \equiv 1 \pmod{9} \\ -3X \equiv 4 \pmod{11} \end{cases} .$$

ESERCIZIO 3. Sia $f : \mathbb{Q} \setminus \{2\} \rightarrow \mathbb{Q}$ l'applicazione definita ponendo

$$f(x) := \frac{3x+1}{x-2} \quad \text{per ogni } x \in \mathbb{Q} \setminus \{2\}.$$

- (1) Stabilire se l'applicazione f è iniettiva e/o suriettiva o/e biiettiva.
- (2) Determinare tutte e sole le estensioni $\widehat{f} : \mathbb{Q} \longrightarrow \mathbb{Q}$ di f (cioè, tutte le applicazioni $\widehat{f}$ tali che $\widehat{f}|_{\mathbb{Q} \setminus \{2\}}$ coincide con f) che siano biiettive.

ESERCIZIO 4. Nel gruppo $(\mathcal{S}_4, \circ)$ delle biiezioni di $\{1, 2, 3, 4\}$ si considerino gli elementi:

$$\varphi := \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \quad \psi := \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}$$

Si ponga $G := \{\text{id}, \varphi, \psi, \varphi \circ \psi\}$ (dove id è la biiezione identità di $\{1, 2, 3, 4\}$).

- (1) Calcolare l'ordine di φ e di ψ , cioè, il più piccolo intero positivo n [rispettivamente, m] tale che $\varphi^n = \text{id}$ [rispettivamente, $\psi^m = \text{id}$].
- (2) Dimostrare che la composizione $\circ$ è una operazione su G (cioè, mostrare che presi *comunque* due elementi $\alpha, \beta \in G$, allora $\alpha \circ \beta \in G$; potrebbe essere utile calcolare esplicitamente $\psi \circ \varphi$).
- (3) Dedurre che $(G, \circ)$ è un sottogruppo di $(\mathcal{S}_4, \circ)$.
- (4) Stabilire se $(G, \circ)$ è un sottogruppo normale in $(\mathcal{S}_4, \circ)$.
- (5) Definire esplicitamente, se esiste, un isomorfismo gruppale tra $(G, \circ)$ e il gruppo additivo $((\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}), +)$ (quest'ultimo è il prodotto diretto del gruppo $(\mathbb{Z}/2\mathbb{Z}), +$ con sé stesso) .

ESERCIZIO 5. Sia T un'indeterminata su $\mathbb{Z}$.

- (1) Siano $f(T), g(T) \in \mathbb{Z}[T]$ con $g(T) \neq 0$. Assumendo che $g(T)$ è un polinomio monico, dimostrare che esistono, e sono univocamente determinati, due polinomi $q(T)$ e $r(T)$ in $\mathbb{Z}[T]$ in modo tale che $f(T) = q(T)g(T) + r(T)$, con $r(T) = 0$ oppure $\deg(r(T)) < \deg(g(T))$.
- (2) Mostrare con un esempio che (1) non vale in generale se $g(T)$ non è un polinomio monico.
- (3) Calcolare il MCD dei seguenti polinomi, spiegando il metodo utilizzato: $a(T) = -48 + 46T + 13T^2 - 9T^3 + T^4$, and $b(T) := -10 - 3T + T^2$.
- (4) Sia $f(T) \in \mathbb{Z}[T]$. Dimostrare che esistono, e sono univocamente determinati, due polinomi $q_f(T)$ e $r_f(T) := a_f + b_f T$ di $\mathbb{Z}[T]$ in modo tale che

$$f(T) = q_f(T)(T^2 - 2T + 1) + r_f(T).$$

- (5) Siano $a', b', a'', b'' \in \mathbb{Z}$. Dopo aver calcolato esplicitamente il polinomio prodotto:

$$\varphi(T) := (a'T + b')(a'' + b''T)$$

determinare esplicitamente (in funzione di a', b', a'', b'') il resto della divisione del polinomio $\varphi(T)$ per $T^2 - 2T + 1$.

- (6) Siano $f(T)$ e $g(T)$ due polinomi in $\mathbb{Z}[T]$ e siano $r_f(T) := a_f T + b_f$ e $r_g(T) := a_g T + b_g \in \mathbb{Z}[T]$ come in (1). Utilizzando (5), determinare il resto della divisione del polinomio prodotto $f(T)g(T)$ per $T^2 - 2T + 1$, in funzione di a_f, b_f, a_g, b_g .

ESERCIZIO 6.

- (1) Enunciare il “piccolo” teorema di Fermat e la sua generalizzazione detta teorema di Euler-Fermat.
- (2) Dimostrare il “piccolo” teorema di Fermat.
- (3) Determinare un intero a , con $0 \leq a \leq 100$ in modo tale che $501^{500} \equiv a \pmod{101}$.

ESERCIZIO 7. Si risolva, ricorrendo, eventualmente, a una delle formulazioni equivalenti del Principio di Induzione, ciascuna delle seguenti questioni.

- (1) È vero che, per ogni $n \in \mathbb{N}$, il numero $3^{n+2} + 4^{2n+1}$ è divisibile per 13?
 (2) Sia $M_2(\mathbb{Z})$ l'insieme delle matrici 2×2 a entrate in $\mathbb{Z}$, e sia $\cdot$ l'operazione di prodotto riga per colonna su $M_2(\mathbb{Z})$. Per ogni matrice $X := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in$

$$M_2(\mathbb{Z}) \text{ e ogni } m \in \mathbb{Z}, \text{ si ponga } m \star X := \begin{pmatrix} ma & mb \\ mc & md \end{pmatrix}.$$

Sia $I := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ la matrice identità di $M_2(\mathbb{Z})$ e sia $A := \begin{pmatrix} 1 & 0 \\ 2 & 3 \end{pmatrix} \in M_2(\mathbb{Z})$.

- (2.1) Dimostrare (calcolandoli esplicitamente) che esistono $\alpha, \beta \in \mathbb{Z}$, in modo tale che:

$$A^2 = \alpha \star A + \beta \star I.$$

- (2.2) Dimostrare che, per ogni intero $n \geq 2$, esistono $\alpha_n, \beta_n \in \mathbb{Z}$ in modo tale che

$$A^n = \alpha_n \star A + \beta_n \star I.$$

[Suggerimento: utilizzare (senza dimostrare) che prese comunque $X, Y \in M_2(\mathbb{Z})$, sussiste la seguente identità: $Y \cdot (m \star X) = m \star (Y \cdot X)$.]