AL1 - Algebra 1: fondamenti - A.A. 2002/2003

Valutazione "in itinere" - II Prova

MATRICOLA (O ALTRO IDENTIFICATIVO): .....

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

esercizio	1	2	3	4	5	6	7	8	9
punti max	(2, 2)	(5, 8)	(5, 8)	(4, 2, 3)	(3, 4, 5)	(4, 3, 3)	(4, 2)	(4, 4)	(2, 5)
punti assegnati									
totale									

AVVERTENZE : *Svolgere gli esercizi in modo conciso, ma esauriente, nello spazio assegnato. Fino a* **2** punti ulteriori *potranno essere assegnati agli elaborati scritti in modo molto chiaro.*

ESERCIZIO 1. (1) Determinare tutte le eventuali soluzioni della congruenza:

$$14X \equiv 21 \pmod{35}\,.$$

(2) Utilizzando il "metodo di sostituzione", determinare tutte le eventuali soluzioni del sistema:

$$\begin{cases} X \equiv 5 \pmod{11} \\ X \equiv 2 \pmod{13} \end{cases}.$$

ESERCIZIO 2. **(1)** Enunciare il teorema fondamentale di decomposizione di un'applicazione qualunque come prodotto operatorio di un'applicazione suriettiva, un'applicazione biiettiva ed un'applicazione iniettiva.

(2) Dimostrare l'enunciato precedente.

ESERCIZIO 3. **(1)** Dati $a, b, n \in \mathbb{Z}$ con $n \geq 2$ ed a e b non entrambi nulli, dimostrare che:

$$a \equiv b \pmod{n} \;\Rightarrow\; \mathrm{MCD}(a, n) = \mathrm{MCD}(b, n)\,.$$

Dare un controesempio per mostrare che l'implicazione inversa non è valida.

(2) Sia a un intero tale che:

$$a^3 \equiv a \pmod{5} \quad \text{e} \quad a^5 \equiv a \pmod{3}\,.$$

Utilizzando opportunamente il "Piccolo" Teorema di Fermat, dimostrare che vale una tra le seguenti affermazioni:

(a) $a^{3\cdot 5} \equiv a \pmod{5^3}$.
(b) $a^{3\cdot 5} \equiv a \pmod{3^5}$.
(c) $a^{3\cdot 5} \equiv a \pmod{3 \cdot 5}$.

ESERCIZIO 4. **(1)** Mostrare che l'insieme prodotto cartesiano $G := \mathbb{Q} \times \mathbb{Q}^*$ (dove $\mathbb{Q}^* := \mathbb{Q} \setminus \{0\}$) con l'operazione $\star$ definita nella maniera seguente:

$$(a, b) \star (x, y) := (a + bx, by) \quad \forall\, (a, b)\,,\ (x, y) \in \mathbb{Q} \times \mathbb{Q}^*\,,$$

forma un gruppo.

(2) Stabilire se $(G, \star)$ è un gruppo abeliano.

(3) Sia $H := \mathbb{Z} \times \mathbb{Z}^*$ (dove $\mathbb{Z}^* := \mathbb{Z} \setminus \{0\}$). Stabilire se H forma un sottogruppo di $(G, \star)$.

ESERCIZIO 5. Siano date le seguenti permutazioni:

$$\sigma := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 5 & 2 & 7 & 6 & 1 \end{pmatrix}, \quad \tau := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 3 & 2 & 5 & 6 & 7 & 1 \end{pmatrix} \in \boldsymbol{S}_7 .$$

(1) Scrivere σ e τ come prodotto di cicli disgiunti.
(2) Determinare l'ordine di σ e di τ.
(3) Calcolare $\tau^{-1}\sigma\tau$ e determinarne l'ordine.

ESERCIZIO 6. Sia R l'insieme delle matrici del tipo seguente:

$$\begin{pmatrix} a & b\sqrt{5} \\ -b\sqrt{5} & a \end{pmatrix}, \qquad \text{con } a\,,\ b \in \mathbb{Z}\,.$$

(1) Mostrare che $(R,+,\cdot\,)$ è un sottoanello dell'anello delle matrici $(\boldsymbol{M}_{2,2}(\mathbb{R}),+,\cdot\,)$.

(2) Stabilire se $(R,+,\cdot\,)$ è commutativo, se è unitario e se possiede divisori dello zero.

(3) Stabilire se il sottoinsieme S di R formato dalle matrici della forma seguente:

$$\begin{pmatrix} x & (3y+x)\sqrt{5} \\ -(3y+x)\sqrt{5} & x \end{pmatrix}, \qquad \text{con } x\,,\ y \in \mathbb{Z}\,.$$

forma un ideale di $(R,+,\cdot\,)$.

ESERCIZIO 7. Dati due polinomi

$$f(T) := 6 + 31T + 13T^2 - 20T^3 + 4T^4\,, \qquad g(T) := 9 - 12T + 3T^2$$

in $\mathbb{Q}[T]$, utilizzando l'algoritmo euclideo delle divisioni successive:

(1) Determinare il polinomio monico $d(T) := \mathrm{MCD}(f(T), g(T)) \in \mathbb{Q}[T]$.

(2) Determinare un'espressione del tipo $d(T) = a(T)f(T) + b(T)g(T)$ (cioè determinare due polinomi $a(T), b(T) \in \mathbb{Q}[T]$) [identità di Bézout].

ESERCIZIO 8. **(1)** Determinare tutti i polinomi irriducibili di grado 3 nell'anello dei polinomi $\frac{\mathbb{Z}}{2\mathbb{Z}}[T]$ [cioè, nell'anello dei polinomi in una indeterminata a coefficienti nel campo $\frac{\mathbb{Z}}{2\mathbb{Z}}$ che –per semplicità– può essere identificato con il campo $(\{0,1\},+,\cdot)$].

(2) Decomporre il polinomio T^4-9 in fattori irriducibili in ciascuno dei seguenti anelli: $\mathbb{Z}[T]$, $\mathbb{Q}[T]$, $\mathbb{R}[T]$, $\mathbb{C}[T]$.

ESERCIZIO 9 (Complementi). (1) Il presidente di una popolare squadra di calcio X, tale Benvoluto Dallalega, in vista del "derby" con l'altra squadra Y della città intende utilizzare al massimo la capienza del proprio stadio, che possiede una infinità numerabile di posti a sedere. Avendo ricevuto richiesta di assistere alla partita da parte della infinità numerabile dei sostenitori della propria squadra X e da parte della infinità numerabile dei tifosi della squadra Y ed, inoltre, la richiesta di biglietti omaggio da parte di un numero contabile di autorità politiche locali, potrà soddisfare tutte le richieste ? [Giustificare la risposta, utilizzando la teoria della cardinalità.]

(2) Stabilire (motivando la risposta) se l'insieme dei polinomi in una indeterminata a coefficienti nei numeri razionali, $\mathbb{Q}[T]$, ha cardinalità del numerabile oppure del continuo.

SOLUZIONI

Soluzione Esercizio 1. (1) $x \equiv 4, 9, 14, 19, 24, 29, 34 \pmod{35}$.
(2) $x \equiv 93 \pmod{11 \cdot 13 = 143}$.

Soluzione Esercizio 3. **(1)** Essendo $a = b + kn$, per qualche $k \in \mathbb{Z}$, è chiaro che i divisori comuni di a ed n sono anche divisori di b ed i divisori comuni di b ed n sono anche divisori di a. Pertanto, i divisori comuni di a ed n sono gli stessi dei divisori comuni di b ed n.

Per verificare che il viceversa non vale, basta prendere, ad esempio $a = 3, b = 5, n = 4$. Allora $\mathrm{MCD}(3,4) = \mathrm{MCD}(5,4) = 1$, però $3 \not\equiv 5 \pmod 4$.

(2) (c) $(a^3)^5 \equiv a^5 \equiv a \pmod 5$, $(a^5)^3 \equiv a^3 \equiv a \pmod 3$. Essendo $\mathrm{MCD}(5,3) = 1$, allora $(a^3)^5 \equiv a \pmod{3 \cdot 5}$.

Si noti che **(a)** e **(b)** non sussistono ad esempio se $a = 4$. Infatti $a \equiv -1 \pmod 5$, quindi $a^3 \equiv a \pmod 5$ ed inoltre $a \equiv 1 \pmod 3$, quindi $a^5 \equiv a \pmod 3$. Però, $4^{15} \equiv 154 \pmod{3^5}$ e $4^{15} \equiv 74 \pmod{5^3}$.

Soluzione Esercizio 4. **(1)** $(0,1)$ è l'elemento neutro (rispetto all'operazione $\star$); l'inverso (rispetto all'operazione $\star$) di (a,b) è l'elemento $(\frac{-a}{b}, \frac{1}{b})$; infine, si verifica facilmente (con un calcolo diretto) che vale la proprietà associativa.

(2) Non è un gruppo abeliano, perchè $a + bx \neq x + ay$. Ad esempio:

$$(1,0) \star (1,1) = (1,0) \neq (2,0) = (1+1,0) = (1,1) \star (1,0)\,.$$

(3) H non è un sottogruppo di $(G, \star)$, perché ad esempio l'inverso di $(1,2) \in H$ è l'elemento $(\frac{-1}{2}, \frac{1}{2}) \in G \setminus H$.

Soluzione Esercizio 5.
(1) $\sigma = (1357)(24)(6)\,, \quad \tau = (14567)(23)\,.$
(2) $\mathrm{Ord}(\sigma) = 4\,, \quad \mathrm{Ord}(\tau) = 10\,.$
(3)

$$\tau^{-1}\sigma\tau := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 6 & 5 & 2 & 3 & 1 & 7 \end{pmatrix} = (1426)(35)\,.$$

$\mathrm{Ord}(\tau^{-1}\sigma\tau) = 4\,.$

Soluzione Esercizio 6.
(1) Siano date due matrici in R:

$$A := \begin{pmatrix} a & b\sqrt{5} \\ -b\sqrt{5} & a \end{pmatrix}\,, \quad A' := \begin{pmatrix} a' & b'\sqrt{5} \\ -b'\sqrt{5} & a' \end{pmatrix}\,.$$

Allora:

$$A - A' = \begin{pmatrix} a-a' & (b-b')\sqrt{5} \\ -(b-b')\sqrt{5} & a-a' \end{pmatrix} \in R\,,$$
$$AA' = \begin{pmatrix} aa' - 5bb' & (ab' + a'b)\sqrt{5} \\ -(ab' + a'b)\sqrt{5} & aa' - 5bb' \end{pmatrix} \in R\,.$$

(2) R è un anello unitario con la stessa unità di $(\boldsymbol{M}_{2,2}(\mathbb{R}), +, \cdot\,)$:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0\sqrt{5} \\ 0\sqrt{5} & 1 \end{pmatrix}\,.$$

R è un anello commutativo, perché:

$$AA' = \begin{pmatrix} aa' - 5bb' & (ab' + a'b)\sqrt{5} \\ -(ab' + a'b)\sqrt{5} & aa' - 5bb' \end{pmatrix} = \begin{pmatrix} a'a - 5b'b & (a'b + ab')\sqrt{5} \\ -(a'b + ab')\sqrt{5} & a'a - 5b'b \end{pmatrix} = A'A\,.$$

R è un anello privo di divisori dello zero. Infatti, altrimenti, dovrebbe accadere che:

$$aa' - 5bb' = 0 \qquad ab' + a'b = 0\,.$$

A calcoli fatti si dovrebbe quindi avere che $a^2 - 5b^2 = 0$, e ciò è impossibile perché $\sqrt{5} \neq \frac{a}{b}$, presi comunque $a, b \in \mathbb{Z}$, con $b \neq 0$.

(3) Sia

$$X := \begin{pmatrix} x & (3y+x)\sqrt{5} \\ -(3y+x)\sqrt{5} & x \end{pmatrix} \in S\,,$$

allora:

$$AX = \begin{pmatrix} ax - 15by - 5bx & (3ay + (a+b)x)\sqrt{5} \\ -(3ay + (a+b)x)\sqrt{5} & ax - 15by - 5bx \end{pmatrix} = \begin{pmatrix} x' & (3y' + x')\sqrt{5} \\ -(3y' + x')\sqrt{5} & x \end{pmatrix} \in S\,,$$

dove:

$$x' := ax - 15by - 5bx\,, \quad 3ay + (a+b)x = 3y' + x'\,,$$

quindi:

$$x' := ax - 15by - 5bx\,, \quad y' = \frac{3ay + (a+b)x - (ax - 15by - 5bx)}{3} = \frac{3ay + 6bx + 15by}{3} \in \mathbb{Z}.$$

Abbiamo già dimostrato che R è un anello commutativo, pertanto $XA = AX \in S$.

Soluzione Esercizio 7. (1)

$$\begin{array}{ll} f(T) = & g(T)q_1(T) + r_1(T)\,, \quad \text{dove } q_1(T) := -5 - \frac{4}{3}T + \frac{4}{3}T^2\,, \quad r_1(T) := 51 - 17T\,, \\ g(T) = & r_1(T)q_2(T) + 0\,, \quad \text{dove } q_2(T) := \frac{3}{17} - \frac{3}{17}T \end{array}$$

Pertanto, il polinomio monico $3 - T = \frac{1}{17}r_1(T)$ è il $\mathrm{MCD}(f(T), g(T))$.

(2) $\frac{1}{17}r_1(T) = \frac{1}{17}f(T) - \frac{1}{17}q_1(T)g(T)\,,$ quindi:

$$a(T) := \frac{1}{17}\,, \quad b(T) := \frac{1}{17}(5 + \frac{4}{3}T - \frac{4}{3}T^2)\,.$$

Soluzione Esercizio 8. (1) I polinomi di grado 3 in $\frac{\mathbb{Z}}{2\mathbb{Z}}[T]$ sono i seguenti:

$$\begin{array}{l} T^3 + T^2 + T + 1\,, \\ T^3 + T + 1\,, \\ T^3 + T^2 + 1\,, \\ T^3 + T^2 + T\,, \\ T^3 + 1\,, \\ T^3 + T^2\,, \\ T^3 + T\,, \\ T^3\,. \end{array}$$

Tra questi, gli unici polinomi che non hanno radici in $\frac{\mathbb{Z}}{2\mathbb{Z}}$ (e, quindi, sono irriducibili in $\frac{\mathbb{Z}}{2\mathbb{Z}}[T]$) sono:

$$\begin{array}{l} T^3 + T + 1\,, \\ T^3 + T^2 + 1\,. \end{array}$$

(2)

$$\begin{array}{ll} T^4 - 9 & = (T^2+3)(T^2-3) \in \mathbb{Z}[T]\,, \\ T^4 - 9 & = (T^2+3)(T^2-3) \in \mathbb{Q}[T]\,, \\ T^4 - 9 & = (T^2+3)(T-\sqrt{3})(T+\sqrt{3}) \in \mathbb{R}[T]\,, \\ T^4 - 9 & = (T - i\sqrt{3})(T + i\sqrt{3})(T-\sqrt{3})(T+\sqrt{3}) \in \mathbb{C}[T]\,. \end{array}$$

Soluzione Esercizio 9. (1) Basta applicare il Teorema di Cantor per dedurre che l'unione di tre insiemi, di cui due numerabili ed uno contabile, è ancora un insieme numerabile.

(2) Si noti che $\mathbb{Q}[T] = \cup_{n\geq 0}\ \boldsymbol{P}^n\ \cup\ \{0\}$, dove $\boldsymbol{P}^n$:= l'insieme dei polinomi di grado esattamente uguale ad n a coefficienti in $\mathbb{Q}$. Dal momento che esiste una applicazione biunivoca canonica

$$\begin{array}{ccc} \boldsymbol{P}^n & \longrightarrow & \mathbb{Q}^* \times \underbrace{\mathbb{Q} \times \ldots \times \mathbb{Q}}_{n}, \\ a_n T^n + a_{n-1}T^{n-1} + \ldots + a_1 T^1 + a_0 & \mapsto & (a_n, a_{n-1}, \ldots, a_1, a_0) \end{array}$$

e che $\mathbb{Q}^* \times \mathbb{Q} \times \ldots \times \mathbb{Q}$ è un insieme numerabile (prodotto cartesiano di un numero finito di insiemi numerabili), allora $\boldsymbol{P}^n$ e, quindi, $\cup_{n\geq 0}\boldsymbol{P}^n$ (Teorema di Cantor) è ancora un insieme numerabile.