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

Appello A

Matricola (O ALTRO IDENTIFICATIVO) → [ ]

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

esercizio	1.1	1.2	1.3	2.1	2.2	2.3,a	2.3,b	3.1	3.2	3.3,a	3.3,b	3.3,c
punti max	1	3	2	5	1	1	1	1	5	1	2	2
punti assegnati												
totale												

esercizio	4.1	4.2	5.1	5.2	6.1	6.2	6.3	6.4	7.1	7.2	7.3,a	7.3,b	7.3,c
punti max	1	3	3	3	1	3	3	3	2	3	1	1	1
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. Sia R l'insieme delle matrici (ad entrate reali) del tipo seguente:

$$\begin{pmatrix} a & b\sqrt{7} \\ -b\sqrt{7} & a \end{pmatrix}, \qquad \text{con } a\,,\ b \in \mathbb{Z}\,.$$

(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:

$$\begin{pmatrix} x & (3y+x)\sqrt{7} \\ -(3y+x)\sqrt{7} & x \end{pmatrix}, \qquad \text{con } x\,,\ y \in \mathbb{Z}\,.$$

forma un sottoanello o/e un ideale di $(R, +, \cdot\,)$.

ESERCIZIO 2. **(1)** Sia $z = r(\cos(\theta) + i\sin(\theta))$ un numero complesso scritto in forma polare. Dimostrare che, per ogni $n \in \mathbb{Z}$ (e non soltanto per $n \in \mathbb{N}$), $z^n = r^n(\cos(n\theta) + i\sin(n\theta))$.

(2) Determinare esplicitamente tutte le radici quarte dell'unità, cioè tutti i numeri complessi $z \in \mathbb{C}$ tali che $z^4 = 1$.

(3) Siano dati i numeri complessi

$$u =: 3 + 2i \quad \text{e} \quad v := 5 - i.$$

(3, a) Determinare il numero complesso $z := x + iy$ in modo tale che $u = vz$.

(3, b) Determinare $a, b \in \mathbb{Q}$ in modo tale che $z^{-1} = a + ib$.

ESERCIZIO 3. **(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.

(3) Sia $\varphi : \mathbb{Z}[T] \to \mathbb{Q}$ l'applicazione dall'anello dei polinomi a coefficienti interi al campo dei numeri razionali definita da $\varphi(f(T)) := f(1/2)$, per ogni polinomio $f(T) \in \mathbb{Z}[T]$.

(3, a) Stabilire se φ è un omomorfismo di anelli.

(3, b) Descrivere $\mathrm{Im}(\varphi)$ (cioè, dare delle condizioni esplicite su $a, b \in \mathbb{Z}$ affinché la frazione $a/b \in \mathbb{Q}$ appartenga ad $\mathrm{Im}(\varphi)$).

(3, c) Descrivere la relazione di equivalenza nucleo $\mathrm{Ker}(\varphi)$ definita su $\mathbb{Z}[T]$ (cioè, stabilire quando due polinomi di $\mathbb{Z}[T]$ hanno la stessa immagine tramite φ). In particolare, determinare tutti i polinomi $g(T) \in \mathbb{Z}[T]$ tali che $\varphi(g(T)) = 0$.

ESERCIZIO 4. (1) Sia $f : X \to Y$ un'applicazione biiettiva tra insiemi non vuoti e sia A un altro insieme non vuoto. Stabilire se l'applicazione (associata ad f) definita nella maniera seguente:

$$\begin{array}{rcl} F : A^Y := \{g : Y \to A \mid g \text{ applicazione}\} & \to & A^X := \{h : X \to A \mid h \text{ applicazione}\} \\ g & \mapsto & g \circ f \end{array}$$

è un'applicazione iniettiva o/e suriettiva o/e biiettiva (dare una completa giustificazione teorica).

(2) Siano $A = \{0, 1\}$, $X := \{a, b\}$ e $Y := \{c, d\}$. Sia $f : X \to Y$, l'applicazione definita da $f(a) := d$ e $f(b) := c$. In questo caso, descrivere esplicitamente gli insiemi A^Y e A^X e l'applicazione $F : A^Y \to A^X$.

ESERCIZIO 5. (1) Determinare tutti i polinomi riducibili di grado 2 nell'anello dei polinomi $\frac{\mathbb{Z}}{3\mathbb{Z}}[T]$ (cioè, anello dei polinomi in una indeterminata a coefficienti nel campo $\frac{\mathbb{Z}}{3\mathbb{Z}}$ (i cui elementi –per semplicità– possono essere denotati $0, 1, 2$)).

(2) Decomporre il polinomio $T^4 - 25$ in fattori irriducibili in ciascuno dei seguenti anelli di polinomi: $\mathbb{Z}[T]$, $\mathbb{Q}[T]$, $\mathbb{R}[T]$, $\mathbb{C}[T]$, $\frac{\mathbb{Z}}{3\mathbb{Z}}[T]$.

Esercizio 6. Sia $(G, \cdot)$ un gruppo.

(1) Definire la nozione di sottogruppo normale $(N, \cdot)$ per il gruppo $(G, \cdot)$.

(2) Sia $(H, \cdot)$ un sottogruppo fissato di $(G, \cdot)$ e sia
$$N_H := \bigcap_{g \in G} g^{-1} H g\,.$$
Mostrare che $(N_H, \cdot)$ è un sottogruppo normale di $(G, \cdot)$.

(3) Fissato $\alpha \in G$. Mostrare o confutare (in funzione della scelta dell'elemento α) il fatto che l'insieme $A_\alpha := \{g^{-1}\alpha g \mid g \in G\}$ sia un sottogruppo di $(G, \cdot)$.

(4) Sia $\varphi : G \to G$ l'applicazione definita ponendo $\varphi(x) := x^{-1}$, per ogni $x \in G$. Dimostrare che φ è un omomorfismo di gruppi se, e soltanto se, G è un gruppo abeliano. Stabilire, in tal caso, se φ è un omomorfimo iniettivo e/o suriettivo e/o biiettivo.

ESERCIZIO 7. Si consideri l'applicazione $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ definita ponendo

$$f((a, b)) := (ab, a + b + ab)$$

(1) Determinare se f è iniettiva e/o suriettiva e/o biiettiva.
(2) Dimostrare che, per ogni $(x, y) \in \mathbb{N}\times\mathbb{N}$, il numero degli elementi $n_{(x,y)}$ della sua fibra è finito ed al più uguale a 2 (cioè, $\#(f^{-1}(\{(x, y)\}) =: n_{(x,y)} \leq 2)$.
(3) Determinare espicitamente, se esiste, un elemento $(x, y) \in \mathbb{N} \times \mathbb{N}$, con $0 \leq x, y \leq 10$, tale che
(3, a) $n_{(x,y)} = 0$;
(3, b) $n_{(x,y)} = 1$;
(3, c) $n_{(x,y)} = 2$.

SOLUZIONE ESERCIZIO 1. **(1)**, **(2)** Per ogni $a, b \in \mathbb{Z}$, poniamo

$$A_{a,b} := \begin{pmatrix} a & b\sqrt{7} \\ -b\sqrt{7} & a \end{pmatrix}$$

Dunque $R = \{A_{a,b} : a, b \in \mathbb{Z}\}$. È immediatamente visto che, per ogni $a, b, \alpha, \beta \in \mathbb{Z}$, si ha

$$A_{a,b} - A_{\alpha,\beta} = A_{a-\alpha,b-\beta} \qquad A_{a,b} \cdot A_{\alpha,\beta} = A_{a\alpha-7b\beta,a\beta+b\alpha} = A_{\alpha,\beta} \cdot A_{a,b}$$

Siccome $a-\alpha, b-\beta, a\alpha-7b\beta, a\beta+b\alpha \in \mathbb{Z}$, segue che R è un sottoanello commutativo di $M_2(\mathbb{R})$.

L'unità moltiplicativa di R è, ovviamente, $A_{1,0}$ (cheè anche l'unità moltiplicativa dentro $M_2(\mathbb{R})$).

Mostriamo che R è un dominio di integrità. Sia $A_{\alpha,\beta}$ un elemento non nullo di R, e siano $a, b \in \mathbb{Z}$ tali che $A_{a,b} \cdot A_{\alpha,\beta} = A_{a\alpha-7b\beta,a\beta+b\alpha} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

Dunque, a, b, α, β soddisfano le relazioni $a\alpha = 7b\beta$, $a\beta = -b\alpha$.

Dal momento che $(\alpha, \beta) \in \mathbb{Z} \times \mathbb{Z} \setminus \{(0, 0)\})$, supponiamo, dapprima che $\alpha \neq 0$ e, allo stesso tempo, $\beta \neq 0$. Moltiplicando la seconda uguaglianza per α e usando la prima, si ottiene

$$7b\beta^2 = a\alpha\beta = -b\alpha^2,$$

o, equivalentemente, $b(7\beta^2 + \alpha^2) = 0$. Poiché, ovviamente, $\mathbb{Z}$ è un dominio di integrità, segue $b = 0$. Dunque, si ottiene $a\alpha = a\beta = 0$ e, poiché anche $\beta \neq 0$, si ha $a = 0$, ovvero $A_{a,b} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

Supponiamo ora che $\alpha = 0$ ma $\beta \neq 0$. Dalle relazioni $0 = 7b\beta$ e $a\beta = 0$, ricaviamo che $a = 0 = b$.

Supponiamo ora che $\beta = 0$ ma $\alpha \neq 0$. Dalle relazioni $a\alpha = 0$ e $0 = -b\alpha$, si conclude ugualmente che $a = 0 = b$.

(3) La matrice $A_{1,1} := \begin{pmatrix} 1 & \sqrt{7} \\ -\sqrt{7} & 1 \end{pmatrix}$ è elemento di S (infatti, essa si ottiene per $x := 1, y := 0$). Si vede immediatamente che

$$(A_{1,1})^2 = \begin{pmatrix} -6 & 2\sqrt{7} \\ -2\sqrt{7} & -6 \end{pmatrix}$$

Siccome, per ogni $y \in \mathbb{Z}$, $-6 + 3y \neq 2$, segue subito che $(A_{1,1})^2 \notin S$. Ciò mostra che S non è chiuso rispetto al prodotto di matrici e, quindi, S non è un sottoanello di R (né, a maggior ragione, un ideale di R).

SOLUZIONE ESERCIZIO 2. **(1)**: vedere gli appunti del corso oppure uno dei libri consigliati.

(2) Le radici quarte dell'unità sono 1, -1, i e $-i$.

(3, a) $z = 1/2 + i \cdot 1/2$.

(3, b) $z^{-1} = 1 - i$.

SOLUZIONE ESERCIZIO 3. **(1)** e **(2)**: vedere gli appunti del corso oppure uno dei libri consigliati.

(3) L'applicazione φ è un omomorfismo di anelli, perché in generale, presi comunque $\alpha \in \mathbb{Q}$ ed $f, g \in \mathbb{Z}[T]$, si vede facilmente che:

$$(f + g)(\alpha) = f(\alpha) + g(\alpha)\,, \quad (f \cdot g)(\alpha) = f(\alpha) \cdot g(\alpha)\,,$$

in particolare, ciò vale per $\alpha = 1/2$.

(4) Si dimostra facilmente che $\mathrm{Im}(\varphi) = \{x/2^k \mid x \in \mathbb{Z}, k \geq 1\}$.

(5) Usando opportunamente la divisione con il resto (in $\mathbb{Z}[T]$) si vede che $\mathrm{Ker}(\varphi) = (2T-1)\mathbb{Z}[T]$.

SOLUZIONE ESERCIZIO 4. (1) F è un'applicazione biiettiva con applicazione inversa $F^{-1} : A^X \to A^Y$, così definita: $F^{-1}(h) := h \circ f^{-1}$, per ogni $h \in A^X$.

(2) Scriviamo gli elementi di A^X ed A^Y sotto forma matriciale:

$$A^Y = \left\{ \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} c & d \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} c & d \\ 1 & 1 \end{pmatrix} \right\}.$$

$$A^X = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} a & b \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} a & b \\ 1 & 1 \end{pmatrix} \right\}.$$

Allora, la biiezione cercata F da A^Y ad A^X è facilmente esplicitabile. Ad esempio:

$$F\left(\begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} \right) = \begin{pmatrix} a & b \\ 1 & 0 \end{pmatrix}.$$

SOLUZIONE ESERCIZIO 5. (1) Poniamo $\mathbb{F}_3 := \frac{\mathbb{Z}}{3\mathbb{Z}}$. Se $f(T) \in \mathbb{F}_3[T]$ è un polinomio riducibile di grado 2, allora esso ha radici in $\mathbb{F}_3$. Pertanto, stante il Teorema di Ruffini, si ha $f(T) = (T-\alpha)(T-\beta)$, per opportuni $\alpha, \beta \in \mathbb{F}_3$. Dunque, l'insieme dei polinomi riducibili in $\mathbb{F}_3$ e aventi grado 2 è

$$\mathfrak{R} := \{T^2, (T-1)^2 = T^2-2T+1, (T-2)^2 = T^2+2T+1, T(T-1), T(T-2), (T-1)(T-2) = T^2-1\}.$$

(2) Sia $f(T) := T^4 - 25$. In $A[T]$, la decomposizione di $f(T)$ in fattori irriducibili è

$$\begin{cases} (T^2-5)(T^2+5) & \text{se } A \in \{\mathbb{Z}, \mathbb{Q}\} \\ (T-\sqrt{5})(T+\sqrt{5})(T^2+5) & \text{se } A = \mathbb{R} \\ (T-\sqrt{5})(T+\sqrt{5})(T-i\sqrt{5})(T+i\sqrt{5}) & \text{se } A = \mathbb{C} \\ (T-1)(T+1)(T^2+1) & \text{se } A = \mathbb{F}_3 \end{cases}$$

Per ottenere la decomposizione in $\mathbb{F}_3[T]$, si osservi che $-25 \equiv -1 (\bmod 3)$, e pertanto

$$T^4 - 25 = T^4 - 1 = (T-1)(T+1)(T^2+1)$$

e poi si usi il fatto che T^2+1 è irriducibile in $\mathbb{F}_3[T]$), per il principio di identità dei polinomi, non avendo radici in $\mathbb{F}_3$.

ESERCIZIO 6. (1) "Dovrebbe" essere ben noto (altrimenti, si consultino le note del corso).

(2) Osserviamo preliminarmente che, se $\mathcal{S}$ è una collezione non vuota di sottogruppi di G, allora $K := \bigcap \boldsymbol{\mathcal{S}} := \bigcap\{S \mid S \in \boldsymbol{\mathcal{S}}\}$ è un sottogruppo di G. Infatti, siano $k_1, k_2 \in K$, e sia $S \in \mathcal{S}$. Poiché S è un sottogruppo di G e $K \subseteq S$, si deve avere $k_1 k_2^{-1} \in S$. Per l'arbitrarietà di S in $\boldsymbol{\mathcal{S}}$, segue $k_1 k_2^{-1} \in K$. Ciò prova che K è un sottogruppo di G.

Adesso, per mostrare che N_H è un sottogruppo di G, basterà verificare che, per ogni $g \in G$, l'insieme $H_g := g^{-1}Hg$ è un sottogruppo di G. Fissiamo elementi $x, y \in H_g$. Per definizione, esistono $h_1, h_2 \in H$ tali che $x = g^{-1}h_1 g$, $y = g^{-1}h_2 g$. Allora $xy^{-1} = g^{-1}h_1 g g^{-1} h_2^{-1} g = g^{-1}h_1 h_2^{-1} g$. Dunque, poiché $h_1 h_2^{-1} \in H$, si ha $xy^{-1} \in H_g$. Ciò prova che H_g è un sottogruppo di G.

Per mostrare che N_H è normale in G, fissiamo $\alpha \in N_H$ e $\gamma \in G$, e proviamo che $\gamma^{-1}\alpha\gamma \in H_g$, per ogni $g \in G$. Sia $g \in G$. Poiché $\alpha \in N_H$, allora –in particolare–

$\alpha \in H_{g\gamma^{-1}}$. Segue che esiste un elemento $h \in H$ tale che $\alpha = (g\gamma^{-1})^{-1}hg\gamma^{-1}$. Segue immediatamente $\gamma^{-1}\alpha\gamma = \gamma^{-1}(g\gamma^{-1})^{-1}hg\gamma^{-1}\gamma = g^{-1}hg \in H_g$, che è quanto si voleva provare.

(3) Se A_α fosse un sottogruppo, allora $1 \in A_\alpha$, dunque $g = \alpha g$, quindi per la legge di cancellazione $\alpha = 1$. In tal caso, $A_1 = \{1\}$ e questo è l'unico caso in cui A_α è un sottogruppo. Ad esempio per $G := \{1, -1\}$ (gruppo moltiplicativo) ed $\alpha := -1$, $A_{-1} = \{-1\}$ non è un sottogruppo di G.

(4) Siano $g, h \in G$. Per risolvere la prima parte dell'esercizio, sarà sufficiente verificare che $\varphi(gh) = \varphi(g)\varphi(h)$ se, e soltanto se, $gh = hg$. Infatti, si hanno le seguenti equivalenze logiche

$$\varphi(gh) = \varphi(g)\varphi(h) \Leftrightarrow (gh)^{-1} = g^{-1}h^{-1} \Leftrightarrow gh = ((gh)^{-1})^{-1} = (g^{-1}h^{-1})^{-1} = hg$$

Sia G abeliano (i.e., φ è un omomorfismo di gruppi), e sia $\mathtt{id}_G : G \longrightarrow G$ l'identità di G. Dal fatto che $\varphi \circ \varphi = \mathtt{id}_G$ segue immediatamente che φ è un automorfismo di G.

ESERCIZIO 7. (1) Dalla definizione di f si deduce che $f((a, b)) = f((b, a))$, per ogni $(a, b) \in \mathbb{N}\times\mathbb{N}$. Dunque, f non è iniettiva, essendo, per esempio, $f((1, 0)) = f((0, 1))$. Inoltre si osservi che, se $a, b, c \in \mathbb{N}$, allora $f((a, b)) = (1, c)$ se, e soltanto se, $a = b = 1$ e $c = 3$. Pertanto, f non è surgettiva (infatti, per esempio, $(1, 0) \notin f(\mathbb{N} \times \mathbb{N})$).

(2) Fissiamo $(x, y) \in \mathbb{N}\times\mathbb{N}$ e cerchiamo eventuali elementi $(a, b) \in \mathbb{N}\times\mathbb{N}$ tali che $f((a, b)) = (x, y)$. Ciò equivale a dire che valgono simultaneamente le uguaglianze seguenti

$$ab = x \qquad a + b + ab = y$$

Dunque $b = y - x - a$ e, sostituendo nella prima uguaglianza, si ottiene subito $a^2 + (x - y)a + x = 0$. In altri termini, a è un numero naturale che è radice del polinomio $f_{(x,y)}(T) := T^2 + (x - y)T + x$. Per concludere, basta tenere presente che $f_{(x,y)}(T)$ ha, al più, due radici.

(3, a) Come visto in **(1)**, $(1, 0) \notin f(\mathbb{N} \times \mathbb{N})$, i.e., $n_{(1,0)} = 0$.

(3, b) $n_{(0,0)} = 1$. Infatti, l'unica radice di $f_{(0,0)}(T) = T^2$ è 0. Segue immediatamente $a = b = 0$ e $f^{-1}(\{(0, 0)\} = \{(0, 0)\}$.

(3, c) Si ha $f((1, 0)) = f((0, 1)) = (0, 1)$. Dunque $n_{(0,1)} \geq 2$. D'altra parte, per quanto visto in **(2)**, $n_{(0,1)} \leq 2$. Ciò basta per concludere.