AL110 - Algebra 1 - A.A. 2014/2015
Appello C (Giugno 2015)

Matricola (O ALTRO IDENTIFICATIVO) $\rightarrow$ ☐

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

---

esercizio	1.1	1.2	1.3	1.4	2.1	2.2	2.3	2.4	2.5.1	2.5.2	3.1	3.2	3.3	3.4
punti max	2	1	2	3	1	2	5	3	1	3	4	4	2	3
valutazione														

esercizio	4.1	4.2	4.3	4.4	4.5	4.6	5.1	5.2	5.3	5.4	6.1	6.2	6.3
punti max	2	2	3	3	2	3	2	2	3	2	3	3	3
valutazione													
TOTALE $\rightarrow$										*"bonus"* $\rightarrow$			

AVVERTENZE: *Svolgere gli esercizi in modo conciso, ma esauriente, nello spazio assegnato.*
– *Fino a* **due punti ulteriori (bonus)** *potranno essere assegnati agli elaborati scritti in modo molto chiaro.*
– *La soluzione degli esercizi deve essere scritta negli appositi spazi bianchi di questo fascicoletto. Non debbono essere consegnati altri fogli.*

LEGGERE LE AVVERTENZE

NON SFOGLIARE IL TESTO
PRIMA CHE VENGA DATO UFFICIAMENTE
INIZIO ALLA PROVA DAL DOCENTE

ESERCIZIO 1.

(1) Sia dato un intero

$$a := a_m 10^m + a_{m-1}10^{m-1} + \ldots + a_2 10^2 + a_1 10 + a_0$$

scritto in forma decimale (con $0 \leq a_i \leq 9$). Dimostrare che:

$$9 \mid a \quad \Leftrightarrow \quad 9 \mid (a_m + a_{m-1} + \ldots + a_2 + a_1 + a_0)\,.$$

(2) Determinare il resto r, con $0 \leq r \leq 8$, della divisione di 111111111 per 9 spiegando il metodo seguito.

(3) Sia $\mathbf{2} := \{0, 1\}$ l'insieme composto da due elementi, sia $\mathbb{N}$ l'insieme dei numeri naturali e sia $\mathbb{N}^+$ l'insieme dei numeri naturali positivi.
Dimostrare che l'insieme:

$$\mathbf{2}^{\mathbb{N}} := \{f : \mathbb{N} \to \mathbf{2} \mid f \text{ è un'applicazione tra insiemi}\}$$

e l'insieme delle parti dell'insieme $\mathbb{N}$:

$$\boldsymbol{P}(\mathbb{N}) := \{S \mid S \subseteq \mathbb{N}\}$$

sono in corrispondenza biunivoca, descrivendo esplicitamente un'applicazione biunivoca tra i due insiemi.

(4) Stabilire se esiste una applicazione biunivoca dall'insieme $\mathbf{2}^{\mathbb{N}}$ all'insieme $\mathbf{2}^{\mathbb{N}^+}$ ($:= \{f : \mathbb{N}^+ \to \mathbf{2} \mid f \text{ è un'applicazione tra insiemi}\}$).
In caso affermativo descrivere esplicitamente una tale applicazione biunivoca.

ESERCIZIO 2.

(1) Definire la funzione $\varphi : \mathbb{N}^+ \to \mathbb{N}^+$ di Euler e calcolare $\varphi(15)$.

(2) Enunciare il Teorema di Euler, che estende il "Piccolo" Teorema di Fermat.

(3) Dare una dimostrazione del Teorema di Euler.

(4) Determinare il più piccolo intero positivo x , $1 \le x \le 14$, tale che:

$$7^{38} \equiv x \pmod{15}.$$

(5.1) Determinare per quali valori del parametro λ, con $0 \le \lambda \le 5$, il seguente sistema di congruenze è risolubile:

$$\begin{cases} 3X \equiv 2 \pmod{5} \\ 2X \equiv \lambda \pmod{6} \\ 4X \equiv 5 \pmod{11} \end{cases} .$$

(5.2) Per il più piccolo valore *positivo* di λ, con $1 \le \lambda \le 5$, per il quale il sistema (5.1) è risolubile, determinare le sue soluzioni.

ESERCIZIO 3.

(1) Dati due interi non nulli $a, b \in \mathbb{Z}$, e sia $d = \mathrm{MCD}(a, b) > 0$.
Dimostrare che esistono sempre due interi $\lambda, \mu \in \mathbb{Z}$ in modo tale che $d = a\lambda + b\mu$.

(2) Siano $\lambda, \mu \in \mathbb{Z}$ come in **(1)**. Dimostrare che necessariamente $\mathrm{MCD}(\lambda, \mu) = 1$.

(3) Se $a = 90$ e $b = 84$. Determinare, in questo caso, $d = \mathrm{MCD}(a, b)$ e due interi $\lambda, \mu \in \mathbb{Z}$ in modo tale che $d = a\lambda + b\mu$.
Mostrare esplicitamente che $\lambda, \mu \in \mathbb{Z}$ non sono univocamente determinati

(4) Stabilire se l'elemento 5 nell'anello degli interi di Gauss $\mathbb{Z}[i] := \{a + ib \mid a, b \in \mathbb{Z}\}$ è riducibile. In caso affermativo, determinare $\alpha, \beta \in \mathbb{Z}[i]$, non invertibili in $\mathbb{Z}[i]$, in modo tale che $\alpha \cdot \beta = 5$.

Ripetere Matricola (o altro identificativo) $\rightarrow$ ☐

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

ESERCIZIO 4. Si consideri il campo $\mathbb{F}_3 := (\mathbb{Z}/3\mathbb{Z}, +, \cdot)$. Si denotino semplicemente con $0,\ 1,\ 2$ gli elementi di $\mathbb{F}_3$. Sia

$$G := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{F}_3,\ ad - bc = 1 \right\}$$

e si dia per buono che G, munito dell'operazione di prodotto "riga per colonna", è un gruppo. Si ponga

$$A := \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \qquad B := \begin{pmatrix} 2 & 2 \\ 2 & 1 \end{pmatrix} \qquad C := \begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix}.$$

(1) Si calcoli l'ordine di ciascuno degli elementi $A, B, C \in G$.

(2) Si mostri che il seguente sottoinsieme di G:

$$H := \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{F}_3 \right\}$$

è un sottogruppo di G.

(3) Si dica se H è normale in G.

(4) Si dica se H è ciclico e, in caso di risposta affermativa, si trovi un generatore di H.

(5) Si mostri che $AX = XA$, per ogni $X \in G$.

(6) Si dica se il sottogruppo K di G generato da A è normale in G.

ESERCIZIO 5. Si considerino i seguenti sottoinsiemi:

$$
\begin{aligned}
A &:= \{f \in \mathbb{Q}[T] \mid f(n) \in \mathbb{Z}, \text{per ogni } n \in \mathbb{N}\}\,,\\
B &:= \{f \in \mathbb{Q}[T] \mid f(n) \in \mathbb{N}, \text{per ogni } n \in \mathbb{N}\}\,,\\
C &:= \{f \in \mathbb{Q}[T] \mid f(1) \in \,]0,1[\, \cap \mathbb{Q}\}\,,\\
D &:= \{f \in \mathbb{Q}[T] \mid f(1-i) = 0\}\,,\ \text{fissato } 1-i \in \mathbb{C}\,,
\end{aligned}
$$

dell'anello dei polinomi $\mathbb{Q}[T]$ a coefficienti razionali nell'indeterminata T.

(1) Si dica, per ciascuno degli insiemi assegnati, se questo è un sottoanello di $\mathbb{Q}[T]$.

(2) Si dica, per ciascuno degli insiemi assegnati, se questo è un ideale di $\mathbb{Q}[T]$.

(3) Si determini un polinomio $g(T) \in \mathbb{Q}[T]$ in modo che D sia precisamente l'insieme dei multipli di $g(T)$ in $\mathbb{Q}[T]$.

(4) Sia $g(T)$ come in **(3)**, si dica se l'anello quoziente $\mathbb{Q}[T]/(g(T))$ è un campo.

ESERCIZIO 6. Per ciascuna delle seguenti questioni si esibisca un argomento conciso ed esauriente.

(1) Si consideri la successione $\{x_n \mid n \in \mathbb{N}\}$ di numeri reali definita per ricorrenza ponendo

$$x_0 := 1, \qquad x_{n+1} := \sqrt{1+2x_n} \ \text{ per ogni } n \geq 0\,.$$

Utilizzando una delle forme del Principio di Induzione, si mostri che $x_n < 4$, per ogni $n \in \mathbb{N}$.

(2) Si determini struttura ciclica, ordine e segno della permutazione

$$\sigma := (1\ 5\ 3\ 4\ 6) \circ (4\ 5\ 2\ 6) \in \mathbb{S}_6$$

(3) Sia $\leq$ l'ordine usuale su $\mathbb{N}$. Sull'insieme $X := \mathbb{N} \cup \{\heartsuit\}$, con $\heartsuit \notin \mathbb{N}$, si consideri la relazione $\preceq_X$ definita ponendo

$$a \preceq_X b :\iff (a \leq b \text{ e } a, b \in \mathbb{N}) \text{ oppure } (a = b = \heartsuit)$$

e si dia per buono che $\preceq_X$ è un ordine parziale su X. Si trovino eventuali elementi massimali, minimali, massimo e minimo dell'insieme parzialmente ordinato $(X, \preceq_X)$.

SOLUZIONE ESERCIZIO 1.

(1) vedere gli appunti del corso.

(2) da (1) segue che $r = 0$.

(3) sussiste più generalmente per ogni insieme (vedere gli appunti del corso).

(4) basta osservare che $\varphi : \mathbb{N} \to \mathbb{N}^+$, $x \mapsto x+1$, è un'applicazione biunivoca che determina un'applicazione biunivoca $\varphi^\sharp : \mathbf{2}^{\mathbb{N}^+} \to \mathbf{2}^{\mathbb{N}}$, $\lambda \mapsto \lambda \circ \varphi$, per ogni $\lambda \in \mathbf{2}^{\mathbb{N}^+}$. I dettagli delle verifiche sono da sviluppare.

SOLUZIONE ESERCIZIO 2.

(1), (2) e (3) vedere gli appunti del corso; $\varphi(15) = \varphi(3)\varphi(5) = 2{\cdot}4 = 8$

(4) $x \equiv 7^2 \equiv 4 \pmod{15}$

(4.1) $2|\lambda$, cioè $\lambda = 0, 2, 4$

(4.2) Per $\lambda = 2$, la soluzione del sistema è $x \equiv 4 \pmod{165}$.

SOLUZIONE ESERCIZIO 3.

(3) $\mathrm{MCD}(90, 84) = 6$, $\lambda = 1$, $\mu = -1$.

(4) $5 = (2+i)(2-i)$.

SOLUZIONE ESERCIZIO 4.

(1) A ha ordine 2, B ha ordine 4, C ha ordine 6.

(2) Per ogni $a, b \in \mathbb{F}_3$ si ha
$$\begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & b\\ 0 & 1\end{pmatrix}^{-1} = \begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & -b\\ 0 & 1\end{pmatrix} = \begin{pmatrix}1 & a-b\\ 0 & 1\end{pmatrix} \in H.$$
Dunque, a norma di definizione, H è un sottogruppo di G.

(3) H non è normale in G perché $D := \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix} \in H$ ma
$$C^{-1}DC = \begin{pmatrix}1 & 0\\ 2 & 1\end{pmatrix} \notin H$$

(4) Una facile verifica mostra che H è ciclico generato dalla matrice D definita in **(3)**.

(5) Basta usare la definizione del prodotto riga per colonna.

(6) Per ogni matrice $X \in G$ si ha, in virtù di **(5)**, $X^{-1}AX = X^{-1}XA = IA = A \in K$. Ciò prova che K è normale in G.

SOLUZIONE ESERCIZIO 5.

(1) A, D sono sottoanelli di $\mathbb{Q}[T]$, B, C non lo sono. Si osservi, per esempio, che $T \in B$ ma $-T \notin B$. Inoltre $1/2 \in C$, ma $1/2 + 1/2 \notin C$. Le verifiche che A, D sono sottoanelli sono totalmente standard.

(2) Ovviamente B, C non sono ideali, non essendo sottoanelli. A non è un ideale di $\mathbb{Q}[T]$, perché $T \in A$ ma $T/2 \notin A$. Invece D è un ideale di A (anche in questo caso si tratta di una verifica di routine).

(3) Un polinomio a coefficienti razionali che si annulla in $1 - i$ deve necessariamente annullarsi anche in $1 + i$, per quanto visto a lezione. Il polinomio $g(T) := (T - (1 - i))(T - (1 + i))$ si annulla in $1 - i, 1 + i$ ed è a coefficienti razionali, essendo $g(T) = T^2 - 2T + 2$. Ovviamente tutti i polinomi multipli di g si annullano in $1 - i$. Viceversa, sia $f \in \mathbb{Q}[T]$ tale che $f(1 - i) = 0$. Per il Teorema di divisione con resto, esistono polinomi $q(T), a + bT \in \mathbb{Q}[T]$ tali che $f(T) = g(T)q(T) + a + bT$. Dal momento che f, g si annullano in $1 - i$, si ha facilmente $0 = a + b(1 - i)$, da cui segue subito $a = b = 0$. Ciò prova che $f(T) = q(T)g(T)$, i.e., $f(T)$, è multiplo di $g(T)$ in $\mathbb{Q}[T]$.

(4) L'anello quoziente è un campo, essendo g irriducibile in $\mathbb{Q}[T]$ (è un polinomio di secondo grado privo di radici reali).

SOLUZIONE ESERCIZIO 6.

(1) L'asserzione è palesemente vera per $n = 0$. Sia adesso $n \geq 0$ e si assuma che $x_n < 4$. Proviamo che $x_{n+1} < 4$. Si ha

$$x_{n+1} = \sqrt{1 + 2x_n} < \sqrt{1 + 2 \cdot 4} = 3 < 4.$$

Il Principio di Induzione basta quindi per concludere.

(2) Si ha $\sigma = (1\ 5\ 2) \circ (3\ 4)$. Dunque σ è dispari e ha ordine 6.

(3) X non ha massimo. Gli elementi $0, \heartsuit$ sono minimali (dunque X non ha minimo), $\heartsuit$ è anche massimale.