AL110 - Algebra 1 - A.A. 2015/2016
Appello A (Gennaio 2016)

Matricola (O ALTRO IDENTIFICATIVO) → ▭

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

---

esercizio	1.1	1.2	1.3	1.4	2.1α	2.1β	2.2α	2.2β	2.2γ	3.1	3.2	3.3
punti max	5	2	8	4	6	8	4	4	5	4	8	4
valutazione												

LEGGERE ATTENTAMENTE LE AVVERTENZE

NON SFOGLIARE IL TESTO

PRIMA CHE VENGA DATO UFFICIAMENTE
INIZIO ALLA PROVA DAL DOCENTE

AVVERTENZE:

– *Utilizzare soltanto gli spazi bianchi di questo fascicolo per lo svolgimento degli esercizi:* **NON si accettano altri fogli**.

– *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.*

– *Fino a* **due punti (malus)** *potranno essere tolti agli elaborati scritti in modo confuso o difficilmente leggibile.*

– *Un* **bonus del 5% di punti ottenuti** *potrà essere assegnato a coloro che consegneranno l'elaborato entro la prima scadenza fissata dai docenti.*

⋆ ⋆ ⋆

ESERCIZIO 1. (1) Sia $(G, \cdot)$ un gruppo tale che l'inverso di ciascun suo elemento sia uguale all'elemento stesso (cioè, per ogni $x \in G$, $x^{-1} = x$). Mostrare che $(G, \cdot)$ è un gruppo abeliano. *(Motivare chiaramente ciascun passaggio della dimostrazione, argomentazioni confuse non verranno prese in esame!)*

(2) Verificare se $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)$, dove l'operazione di somma, $+$, è definita componente per componente, è un gruppo che verifica la condizione enunciata in (1).

(3) Sia $(G, \cdot)$ un gruppo tale che, presi $a, b \in G$, esiste un intero $n \geq 2$ con $(ab)^n = 1$. Dimostrare che $(ba)^n = 1$. *(Motivare chiaramente ciascun passaggio della dimostrazione, argomentazioni confuse non verranno prese in esame!)*

(4) Sia $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, +)$, dove l'operazione di somma, $+$, è definita componente per componente. Dopo aver osservato che $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, +)$ è un gruppo abeliano, determinare due elementi $(x, y), (u, v) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ in modo tale che

$$6 \cdot ((x, y) + (u, v)) = ([0]_2, [0]_3) \quad \text{e} \quad k \cdot ((x, y) + (u, v)) \neq ([0]_2, [0]_3) \text{ per } 1 \leq k \leq 5\,.$$

Osservare che, in questo caso, preso comunque un elemento $(a, b) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ accade che $6 \cdot (a, b) = ([0]_2, [0]_3)$, ma non necessariamente $k \cdot (a, b) \neq ([0]_2, [0]_3)$ per $1 \leq k \leq 5$, dando un controesempio.

ESERCIZIO 2. (1) Sia $(A, +, \cdot)$ un anello con unità (moltiplicativa) 1. Assumiamo che a, b siano elementi di A con le seguenti proprietà:

$$ab + ba = 1\,; \quad a^2b + ba^2 = a\,.$$

(α) Mostrare che $a^2b = aba = ba^2$ e $2aba = a$. *(Motivare chiaramente ciascun passaggio della dimostrazione, argomentazioni confuse non verranno prese in esame!)*

(β) Mostrare che $a^2b^2 = b^2a^2$ e che a è invertibile in A, determinandone esplicitamente il suo inverso (moltiplicativo). *(Motivare chiaramente ciascun passaggio della dimostrazione, argomentazioni confuse non verranno prese in esame!)*

(2) Sia $(A := \mathbb{Z} \times \mathbb{Q}, +, \cdot)$ l'anello prodotto diretto degli anelli $(\mathbb{Z}, +, \cdot)$ e $(\mathbb{Q}, +, \cdot)$.

(α) Stabilire se $\mathbb{Z} \times \{0\}$ o/e $\mathbb{Z} \times \mathbb{Z}$ sono ideali di A.

(β) Dato un ideale I di $(\mathbb{Z}, +, \cdot)$ e un ideale J di $(\mathbb{Q}, +, \cdot)$, stabilire se $I \times J$ è un ideale di A.

(γ) Determinare tutti gli ideali dell'anello A.

ESERCIZIO 3.

(1) Risolvere (se possibile) il seguente sistema di congruenze:

$$\begin{cases} X \equiv 2 \pmod{5} \\ X \equiv 5 \pmod{6} \\ X \equiv 5 \pmod{12} \end{cases}$$

determinando, in caso affermativo le soluzioni, x, con $0 \leq x \leq 59$.

(2) Siano $a, n \in \mathbb{Z}$, con $n \geq 2$ e $\text{MCD}(a, n) = 1$. Sia $\varphi(n)$ il valore della funzione di Euler, calcolata in n. Dimostrare che $a^{\varphi(n)} \equiv 1 \pmod{n}$. *(Motivare chiaramente ciascun passaggio della dimostrazione, argomentazioni confuse non verranno prese in esame!)*

(3) Calcolare $15^{15} \pmod{17}$ e determinare la soluzione della congruenza $15X \equiv 7 \pmod{17}$.

RIPETERE Matricola (o altro identificativo) $\rightarrow$ ______________________

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

esercizio	4.1	4.2	4.3	4.4	4.5	5.1	5.2	5.3	6.1	6.2	6.3
punti max	2	4	4	5	6	3	3	3	4	4	8
valutazione											

ESERCIZIO 4. Sia $\mathcal{X}$ l'insieme delle parti non vuote di $\mathbb{N}$, e sia $\preceq$ la relazione binaria su $\mathcal{X}$ definita ponendo

$$A \preceq B :\iff (A = B) \vee (\min(A) < \min(B)) \,, \quad \text{per } A, B \in \mathcal{X} \,,$$

dove, per ogni insieme $S \in \mathcal{X}$, $\min(S)$ denota il minimo di S, rispetto all'ordine usuale su $\mathbb{N}$.

(1) Si verifichi che $(\mathcal{X}, \preceq)$ è un insieme parzialmente ordinato, e si dica se esso è totalmente ordinato.

(2) Si trovino, laddove esistano, tutti gli elementi minimali di $(\mathcal{X}, \preceq)$.

(3) Si trovino, laddove esistano, tutti gli elementi massimali di $(\mathcal{X}, \preceq)$.

(4) Si trovi, laddove esista, una catena in $(\mathcal{X}, \preceq)$ (i.e., un sottoinsieme totalmente ordinato di $(\mathcal{X}, \preceq)$) priva di maggioranti in $(\mathcal{X}, \preceq)$.

(5) Per ogni $h \in \mathbb{N}$ si ponga $A_h := \{hn \mid n \in \mathbb{N}\}$, $B_h := \{n^2 + h + 1 \mid n \in \mathbb{N}\}$, $C_h := \{n^2 + 4n + 4 + h \mid n \in \mathbb{N}\}$.

Si consideri il sottoinsieme $\mathcal{Y} := \{A_h, B_h, C_h \mid h \in \mathbb{N}\}$ di $\mathcal{X}$.

Si determinino, se esistono, estremo superiore e inferiore di $\mathcal{Z} := \{A_h \mid h \in \mathbb{N}\}$ in $\mathcal{Y}$.

ESERCIZIO 5. Si consideri il polinomio

$$f := f(T) := 2T^4 - 2T^3 + 2T^2 - T - 1 \in \mathbb{Z}[T]\,.$$

(1) Si determini l'espansione di $f(T)$ come prodotto di fattori irriducibili nell'anello $\mathbb{Z}[T]$.

(2) Si determini l'espansione come prodotto di fattori irriducibili in $(\mathbb{Z}/3\mathbb{Z})[T]$ del polinomio $\overline{f}(T)$ ottenuto da f riducendo i coefficienti di f modulo 3.

(3) Si stabilisca se $[T-1]_{f(T)}$ (cioè, la classe del polinomio $T - 1 \in \mathbb{Z}[T]$ nell'anello quoziente $A := \mathbb{Z}[T]/(f(T))$) è un divisore dello zero dell'anello $A = \mathbb{Z}[T]/(f(T))$.

ESERCIZIO 6. Affrontare le seguenti questioni.

(1) Sia $\mathrm{GL}_2(\mathbb{R})$ il gruppo delle matrici invertibili 2×2 a entrate reali, rispetto al prodotto riga per colonna, e sia N il sottogruppo di $\mathrm{GL}_2(\mathbb{R})$ generato dalla matrice $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.
Si stabilisca, motivando la risposta, se N è un sottogruppo normale in $\mathrm{GL}_2(\mathbb{R})$.

(2) Sia n un numero naturale positivo. Si stabilisca se

$$7^{10n} - 5^{20n^2} + 8^{30n^3} - 4^{40!n^4}$$

è divisibile per 11 (spiegando il ragionamento seguìto).

(3) Il piccolo Epsilon "ϵ" e la sua amata Delta "δ_ϵ" hanno deciso che il loro cortile sarà popolato soltanto da *galline*, *oche* e *pulcini*.
Ogni *gallina* costa 5₿ (₿ = *bitcoin*), ogni *oca* costa 3₿. Inoltre, con 1₿ possono acquistare 3 *pulcini*.
Sapendo che i due innamorati ϵ e δ_ϵ acquistano 100 volatili spendendo 100 ₿ e che, per ragioni di propensione avìcola, decidono che il numero di oche deve essere il minimo possibile, si determini precisamente quanti volatili per ciascuna specie sono stati acquistati.

SOLUZIONE ESERCIZIO 1

(1) Osservare che $x^2 = 1$ per ogni $x \in G$. Quindi, presi comunque $a, b \in G$, $1 = (ab)^2 = (ab)(ab) = a(ba)b$. Moltiplicando a sinistra per a^{-1} e a destra per b^{-1}, abbiamo $a^{-1}b^{-1} = ba$. Dall'ipotesi si ha che $a^{-1}b^{-1} = ab$. Quindi, si ha la conclusione

(2) E' facile vedere che $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)$ è un gruppo. Inoltre, per ogni elemento $(x, y, z) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $(-x, -y, -z) = (x, y, z)$.

(3) Osservare che $1 = (ab)^n = (ab)(ab) \dots (ab) = a(ba)^{n-1}b$, dunque $(ba)^{-1} = a^{-1}b^{-1} = (ba)^{n-1}$. Moltiplicando per ba, si conclude che $(ba)^n = 1$.

(4) Prendere, ad esempio, $(x, y)) = ([1]_2, [0]_3)$ e $(u, v)) = ([0]_2, [1]_3)$.
Per la seconda parte, osservare poi che $6 \cdot (a, b) = (6 \cdot a, 6 \cdot b) = ([0]_2, [1]_3)$. Però, ad esempio $2 \cdot ([1]_2, [0]_3) = (2 \cdot [1]_2, 2 \cdot [0]_3) = ([0]_2, [1]_3)$.

SOLUZIONE ESERCIZIO 2

(1, α) $a^2b + ba^2 = a \cdot 1 = a(ab + ba)$, da cui $ba^2 = aba$. Similmente, $a^2b + ba^2 = 1 \cdot a = (ab + ba)a$, da cui $a^2b = aba$. Pertanto, $2aba = aba + aba = a^2b + ba^2 = a$.
(1, β) Notare che $ab = 1 - ba$ e quindi

$$a^2b^2 = (ab)^2 = (1 - ba)^2 = 1 - ba - ba + baba = 1 - 2ba + b^2a^2\,.$$

Inoltre, $b^2a^2 = b(ba^2) = b(a^2b) = (ba^2)b = (a^2b)b = a^2b^2$. Pertanto, $1 - 2ba = 0$ cioè $1 = (2b)a$.
Similmente $ba = 1 - ab$ e quindi

$$b^2a^2 = (ba)^2 = (1 - ab)^2 = 1 - ab - ab + abab = 1 - 2ab + a^2b^2\,.$$

Dunque, $1 = 2ab = ab + ab = a(2b)$.

(2) Si può dimostrare che H è un ideale di A se e soltanto se $H = I \times J$ dove I è un ideale di $\mathbb{Z}$ e J è un ideale di $\mathbb{Q}$. Precisamente, se $\mathrm{pr}_1 : A \to \mathbb{Z}$ e $\mathrm{pr}_2 : A \to \mathbb{Q}$ sono i due omomorfismi suriettivi di proiezione, allora $I = \mathrm{pr}_1^{-1}(H)$ e $J = \mathrm{pr}_2^{-1}(H)$. Pertanto, tutti e soli gli ideali di A sono del tipo $n\mathbb{Z} \times \{0\}$ e $n\mathbb{Z} \times \mathbb{Q}$, al variare comunque di $n \in \mathbb{Z}$.

SOLUZIONE ESERCIZIO 3

(1) $x \equiv 17 \pmod{60}$.
(2) Vedere gli appunti delle lezioni.
(3) $15^{15} \equiv (15^3)^5 \equiv 9^5 \equiv 8 \pmod{17}$. Poiché $15^{16} \equiv 1 \pmod{17}$, segue che 15^{15} è un inverso aritmetico di 15 (mod 17), allora la soluzione della congruenza è data da $x \equiv 8 \cdot 7 \equiv 5 \pmod{17}$.

SOLUZIONE ESERCIZIO 4.

(1) La verifica che $\preceq$ è un ordine parziale è di routine e viene pertanto lasciata al lettore. Inoltre è immediatamente visto che $(\mathcal{X}, \preceq)$ non è totalmente ordinato, in quanto, per esempio $\{0\}, \{0, 1\}$ sono elementi di $\mathcal{X}$ non comparabili.

(2) Sono precisamente tutti i sottoinsiemi di $\mathbb{N}$ contenenti 0.
(3) Non esistono elementi massimali in $(\mathcal{X}, \preceq)$. Infatti, per ogni $A \in \mathcal{X}$, detto $x := \min(A)$, si ha $A \prec \{x+1\}$.
(4) Poniamo $T_i := \{i\}$, per ogni $i \in \mathbb{N}$. Allora è immediatamente visto che $\{T_i \mid i \in \mathbb{N}\}$ è una catena in $(\mathcal{X}, \preceq)$.
(5) Per ogni $h \in \mathbb{N}$, si ha $\min(A_h) = 0$, $\min(B_h) = h+1$, $\min(C_h) = 4+h$. Allora l'estremo superiore di $\mathcal{Z}$ in $\mathcal{Y}$ è B_0. Invece è immediato verificare che l'estremo inferiore di $\mathcal{Z}$ in $\mathcal{Y}$ non esiste.

SOLUZIONE ESERCIZIO 5.

(1) I fattori irriducibili di $f(T)$ in $\mathbb{Z}[T]$ sono $T-1$ e $2T^3+2T+1$ (si noti che l'irriducibilità del secondo polinomio è conseguenza immediata del Teorema di Eisenstein).
(2) Si ha $\overline{f}(T) = \overline{2}(T+\overline{1})(T+\overline{2})(T^2+\overline{2}T+\overline{2})$.
(3) Per quanto visto in (1), $[T-1]_{f(T)}$ è un divisore dello zero nell'anello quoziente A.

SOLUZIONE ESERCIZIO 6.

(1) Si ponga $A := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Allora $N := \{A^n \mid n \in \mathbb{Z}\} = \{\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \mid n \in \mathbb{Z}\}$. Posto $B := \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R})$, si ha $B^{-1}AB = \begin{pmatrix} 2 & 1 \\ -1 & 0 \end{pmatrix} \notin N$. Pertanto N non è normale in $\mathrm{GL}_2(\mathbb{R})$.
(2) Per il Piccolo Teorema di Fermat, si ha $m^{10} \equiv 1 \pmod{11}$, per ogni intero m che non è divisibile per 11. In particolare i numeri $7^{10n}, 5^{20n^2}, 8^{30n^3}, 4^{40!n^4}$ sono congrui a 1 modulo 11. Quindi $7^{10n} - 5^{20n^2} + 8^{30n^3} - 4^{40!n^4} \equiv 0 \pmod{11}$. L'asserzione è così provata.
(3) Sia G il numero di galline comprate, O il numero di oche comprate, P il numero di pulcini comprati. Allora $5G+3O+\frac{1}{3}P = 100$, i.e., $15G+9O+P = 300$. Inoltre $G+O+P = 100$, i.e., $P = 100-G-O$. Dunque si ottiene $15G+9O+100-G-O = 300$. Equivalentemente $14G+8O = 200$. Dividendo per 2 si ha $7G+4O = 100$. Risolvendo l'equazione e richiedendo che il numero di oche acquistate sia il minimo possibile si ottiene una unica soluzione al problema, precisamente Epsilon e la sua amata Delta hanno acquistato 12 galline, 4 oche e 84 pulcini.