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

Matricola (O ALTRO IDENTIFICATIVO) $\rightarrow$ ☐

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

---

esercizio	1.1	1.2	1.3	1.4	1.5	2.1	2.2	2.3	3.1.1	3.1.2	3.2	3.3
punti max	2	6	4	2	2	3	3	5	2	2	3	2
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)** 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) Siano α, β due interi fissati. Si consideri l'applicazione:

$$\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}\,, \quad x \mapsto \alpha + \beta x\,,$$

e si ponga per induzione $\varphi^n := \varphi \circ \varphi^{n-1}$, per ogni $n \geq 2$ (dove, ovviamente, $\varphi^1 := \varphi$).

Provare per induzione su $n \geq 1$ che vale almeno una delle seguenti formule:

(3a) $\varphi^n(x) = \alpha(\beta^n + 1) - \alpha\beta + \beta^n x\,;$

(3b) $\varphi^n(x) = \alpha(\beta^n - 1) + \beta^n x\,;$

(3c) $\varphi^n(x) = \alpha\frac{(\beta^n - 1)}{(\beta - 1)} + \beta^n x\,;$

(3d) $\varphi^n(x) = \alpha + \alpha\beta + \alpha\beta^2 + \beta^n x\,.$

(4) Stabilire eventuali condizioni sugli interi α e β in modo tale che l'applicazione $\varphi^n : \mathbb{Z} \longrightarrow \mathbb{Z}$, sia iniettiva o/e suriettiva o/e biiettiva, per ogni $n \geq 1$.

(5) Fissati $\alpha = 2$ e $\beta = 3$, determinare esplicitamente l'insieme:

$$(\varphi^2)^{-1}(\{16, 17, 18\})\,.$$

ESERCIZIO 2. 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 $0 \leq a_i \leq 9$).

(1) Dimostrare che:

$$3 \mid a \quad \Leftrightarrow \quad 3 \mid (a_m + a_{m-1} + \ldots + a_2 + a_1 + a_0)\,.$$

(2) Dimostrare che:

$$5 \mid a \quad \Leftrightarrow \quad 5 \mid a_0\,.$$

(3) Determinare una caratterizzazione per la condizione

$$15 \mid a\,,$$

utilizzando soltanto proprietà di divisibilità relativamente ai coefficienti

$$a_m, a_{m-1}, \ldots, a_2, a_1, a_0\,.$$

ESERCIZIO 3.

(1) Sia $f : (G_1, \cdot\ ) \to (G_2, \cdot\ )$ un omomorfismo di gruppi e sia H un sottogruppo di $(G_2, \cdot\ )$.

(1.1) Dimostrare che $f^{-1}(H) := \{x \in G_1 \mid f(x) \in H\}$ è un sottogruppo di $(G_1, \cdot\ )$.

(1.2) Se H è un sottogruppo normale di $(G_2, \cdot\ )$ stabilire se $f^{-1}(H)$ è un sottogruppo normale di $(G_1, \cdot\ )$.

(2) Sia $g : (\mathbb{C}, +) \to (\mathbb{R}, +)$ definita da $g(x + iy) := x$. Stabilire se g è un omomorfismo di gruppi.
Descrivere esplicitamente $g^{-1}(\mathbb{Q})$ e stabilire se $g^{-1}(\mathbb{Q})$ è un sottogruppo di $(\mathbb{C}, +)$.

(3) Sia $\mathbb{C}^\star := \mathbb{C} \setminus \{0\}$, $\mathbb{R}^\star := \mathbb{R} \setminus \{0\}$ e sia $h : (\mathbb{C}^\star, \cdot\ ) \to (\mathbb{R}^\star, \cdot\ )$ definita da $h(x + iy) := x$. Stabilire se h è un omomorfismo di gruppi.

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

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

esercizio	4.1	4.2	4.3.1	4.3.2	4.3.3	4.4	5.1	5.2	5.3	5.4	5.5	6.1	6.2	6.3	6.4
punti max	3	5	1	1	3	2	3	2	3	3	4	3	3	3	5
valutazione															

ESERCIZIO 4.

(1) Sia $\mathbb{N}^+ := \mathbb{N} \setminus \{0\}$. Definire la funzione di Eulero $\boldsymbol{\varphi} : \mathbb{N}^+ \to \mathbb{N}^+$ e dimostrare che, per $n > 1$,

$$\boldsymbol{\varphi}(n) = n - 1 \iff n \text{ è un numero primo}\,.$$

(2) Sia p un numero primo e $k \in \mathbb{N}^+$. Stabilire se vale la seguente uguaglianza:

$$\boldsymbol{\varphi}(p^k) = p^k \left(1 - \frac{1}{p}\right)\,.$$

In caso affermativo, darne una dimostrazione.

(3) Sia $0 \leq \lambda \leq 11$. Si consideri il seguente sistema di congruenze :

$$\begin{cases} 5X \equiv 2 \pmod{7} \\ 6X \equiv \lambda \pmod{12} \\ 7X \equiv 5 \pmod{11}\,. \end{cases}$$

- **(3.1)** Utilizzando la funzione $\boldsymbol{\varphi}$ di Eulero, determinare l'inverso aritmetico di $5 \pmod{7}$ e di $7 \pmod{11}$.
- **(3.2)** Determinare per quali valori del parametro λ, con $0 \leq \lambda \leq 11$, il precedente sistema di congruenze è risolubile.
- **(3.3)** Per ciascun valore del parametro di λ, con $0 \leq \lambda \leq 11$, per il quale il sistema di congruenze è risolubile, determinare le sue soluzioni.

(4) Determinare il più piccolo intero h , $0 \leq h \leq 153$, tale che:

$$9^{122} \equiv h \pmod{154}\,.$$

ESERCIZIO 5. Si consideri il polinomio $f(T) := T^3 - 4 \in \mathbb{Q}[T]$.

(1) Si stabilisca se $f(T)$ è irriducibile in $\mathbb{Q}[T]$.

(2) Si stabilisca se l'anello quoziente $A := \mathbb{Q}[T]/(f(T))$ è un dominio e/o è un campo.

(3) Dato un polinomio $g(T) \in \mathbb{Q}[T]$, si denoti $[g(T)]_f$ la classe di equivalenza di $g(T)$ nell'anello quoziente $A := \mathbb{Q}[T]/(f(T))$.
Si determini un polinomio $h(T)$ di grado al più 2 tale che $[T^7]_f = [h(T)]_f$.

(4) Si stabilisca se $[T^7]_f$ è invertibile in A e, in caso di risposta affermativa, si trovi esplicitamente il suo inverso.

(5) Si definisca un omomorfismo di anelli $\varphi : \mathbb{Q}[T] \longrightarrow \mathbb{R}$ in modo che

$$\mathrm{Ker}(\varphi) = \{f(T)g(T) \mid g(T) \in \mathbb{Q}[T]\}$$

ESERCIZIO 6. Il candidato risolva le seguenti questioni, esibendo un argomento conciso ed esauriente.

(1) Si stabilisca per ciascuno dei sottoinsiemi $S := \{f \in \mathbb{Z}[T] \mid f(1) \text{ è dispari}\}$, $S' := \{f \in \mathbb{Z}[T] \mid f(1) \text{ è pari}\}$ se esso è è un sottoanello e/o un ideale dell'anello $\mathbb{Z}[T]$.

(2) Si munisca l'insieme $\mathbb{N}^+ := \mathbb{N} \setminus \{0\}$ dell'ordine parziale $\leq$ di divisibilità (i.e., $n \leq m :\iff n$ divide m) e $\mathbb{N}^+ \times \mathbb{N}^+$ dell'ordine lessicografico indotto da $\leq$.

Si trovino gli elementi massimali e minimali del sottoinsieme

$$\mathcal{H} := \{(2,1), (1,2), (1,4), (2,4), (1,1), (2,3)\} \text{ di } \mathbb{N}^+ \times \mathbb{N}^+ .$$

(1) Si determini l'espansione del polinomio $f(T) := 6T^4+6T^2+6$ come prodotto di irriducibili di $\mathbb{Z}[T]$.

(2) Si enunci l'Assioma della Scelta e da esso si deduca -dandone esplicitamente una dimostrazione- la seguente proposizione:

Dati due insiemi non vuoti A, B, le seguenti condizioni sono equivalenti:

(3) *Esiste una funzione iniettiva $A \longrightarrow B$.*

(4) *Esiste una funzione surgettiva $B \longrightarrow A$.*

SOLUZIONE ESERCIZIO 1.

Per (1) e (2) vedere gli appunti delle lezioni.

La formula esatta è la (3c), che si dimostra agevolmente per induzione.

(4) φ^n è iniettiva per ogni n se e soltanto se $\beta \neq 0$.

φ^n è suriettiva per ogni n se e soltanto se φ^n è biiettiva per ogni n se e soltanto se $\beta \in \{1, -1\}$.

(5) $(\varphi^2)^{-1}(\{16, 17, 18\}) = (\varphi^2)^{-1}(\{17\}) = \{1\}$.

SOLUZIONE ESERCIZIO 2.

Per (1) e (2) vedere gli appunti delle lezioni.

(3) $15 \mid a$ se e soltanto se $(3 \mid a \quad e \quad 5 \mid a)$. Quindi, si conclude applicando (1) e (2).

SOLUZIONE ESERCIZIO 3.

(1.1) Se $x, y \in f^{-1}(H)$, allora $xy^{-1} \in f^{-1}(H)$. Infatti, $f(xy^{-1}) = f(x)(f(y))^{-1} \in H$, perché $f(x), f(y) \in H$ ed H è un sottogruppo diG_2.

(1.2) Se $a \in G_1$ ed $x \in f^{-1}(H)$, allora $axa^{-1} \in f^{-1}(H)$. Infatti, $f(axa^{-1}) = f(a)f(x)(f(a))^{-1} \in H$, perché $f(x) \in H$ ed H è un sottogruppo normale di G_2.

(2) Le risposte sono entrambe positive e facili da giustificare; notare che $g^{-1}(\mathbb{Q}) = \mathbb{Q} + i\mathbb{R} := \{a + iy \mid a \in \mathbb{Q}, y \in \mathbb{R}\}$ $(\subset \mathbb{C})$).

(3) Le risposta è negativa (cioè, h non conserva il prodotto) ed è facile da giustificare.

SOLUZIONE ESERCIZIO 4.

Per (1) e (2) vedere gli appunti delle lezioni ed osservare che se n non è primo allora esiste $1 < d < n-1$ tale che $d \mid n$ e quindi $\boldsymbol{\varphi}(n) \lneq n - 1$.

(3.1) 3 (mod 7); 8 (mod 11).

(3.2) $\lambda = 0, 6$.

(3.3) Per $\lambda = 0$: 62 (mod 154). Per $\lambda = 6$: 139 (mod 154).

(4) $h = 81$.

SOLUZIONE ESERCIZIO 5.

(1) Essendo $f(T)$ di terzo grado a coefficienti in un campo, cioè, il campo $\mathbb{Q}$ dei numeri razionali, basta far vedere che f non ha radici razionali. Le eventuali radici razionali di $f(T)$ sono $\pm 1, \pm 2, \pm 4$, ma è immediatamente visto che nessuno di tali numeri è radice di $f(T)$. Pertanto, $f(T)$ è irriducibile in $\mathbb{Q}[T]$.

(2) Per quanto visto a lezione e in (1), A è un campo (e quindi, in particolare, è un dominio).

(3) Si ha, per definizione $[T^3]_f = [4]_f$. Quindi

$$[T^7]_f = ([T^3]_f)^2 [T]_f = [16 \cdot T]_f$$

(4) $[T^7]_f$ è invertibile in A e il suo inverso è $\left[\frac{1}{64}T^2\right]_f$.

(5) Un tale omomorfismo è quello definito ponendo $\varphi(q(T)) := q(\sqrt[3]{4})$, per ogni $q(T) \in \mathbb{Q}[T]$.

SOLUZIONE ESERCIZIO 6.

(1) S non è un sottogruppo additivo di $\mathbb{Z}[T]$, perché $1 \in S$, ma $2 = 1 + 1 \notin S$. *A fortiori* S non è un sottoanello, né un ideale di $\mathbb{Z}[T]$.
Si dimostra molto facilmente che S' è sia un sottoanello che un ideale di $\mathbb{Z}[T]$, cioè, se $f, g \in S'$ allora $f - g$ e $f \cdot g$ sono in S' ed anche, per ogni $h \in \mathbb{Z}[T]$, $f \cdot h \in S'$.

(2) $(1, 1)$ è minimo di $\mathcal{H}$. Gli elementi massimali di $\mathcal{H}$ sono $(2, 4), (2, 3)$.

(3) $f(T) = 2 \cdot 3(T^2 + T + 1)(T^2 - T + 1)$. Gli ultimi due polinomi che appaiono nella fattorizzazione sono irriducibili in $\mathbb{Z}[T]$ perché primitivi, di secondo grado e privi di radici intere.

(4) Si vedano gli appunti delle esercitazioni o/e delle lezioni.