AL1 - Algebra 1: fondamenti - A.A. 2003/2004

APPELLO B

Matricola (O ALTRO IDENTIFICATIVO) $\rightarrow$ ____________________

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

---

esercizio	1	2		3		4		5		6	7		
punti max	4	2	3	3	2	5	3	4	3	4	5	5	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. Utilizzando il Principio di Induzione, provare che, per ogni $n \geq 0$, la seguente espressione:

$$3 \cdot 1 + 3 \cdot 3 + 3 \cdot 5 + \ldots + 3 \cdot (2n-1) + 3 \cdot (2n+1)$$

è uguale ad una soltanto tra le seguenti:

(a) $3 + 9n^2$;
(b) $\frac{3n(n+1)}{2}$;
(c) $3(n+1)^2$;
(d) $(n+1)n^3$.

ESERCIZIO 2. (1) Negare la seguente proposizione: *"Ogni uomo possiede una casa in cui abita".*

[Suggerimento: dal punto di vista logico la proposizione precedente si può schematizzare in modo equivalente nella forma: *"Per ogni uomo esiste una casa di sua proprietà in cui abita".*]

(2) Date le proposizioni $\boldsymbol{P}$, $\boldsymbol{Q}$, $\boldsymbol{R}$, scrivere la tabella di verità della proposizione:

$$(\neg \boldsymbol{P} \wedge (\boldsymbol{Q} \vee \boldsymbol{P})) \wedge \boldsymbol{R}\,.$$

ESERCIZIO 3. Siano $a := 67375$ e $b := 504$. Utilizzando l'Algoritmo Euclideo delle divisioni successive calcolare:

(1) $d \in \mathbb{N},\ d = \mathrm{MCD}(a, b)$;
(2) $\alpha,\ \beta \in \mathbb{Z}$, in modo tale che:

$$d = \alpha \cdot a + \beta \cdot b \qquad \text{[Identità di Bézout].}$$

ESERCIZIO 4. (1) Dare le definizioni di sottogruppo e sottogruppo normale di un gruppo $(G,\ \cdot)$ e dimostrare che un sottogruppo H di $(G,\ \cdot)$ è normale se e soltanto se, per ogni $x \in G$, $x^{-1}Hx = H$.

(2) Dati due gruppi $(G,\ \cdot)$ e $(G',\ \cdot)$, dimostrare che il nucleo di un omomorfismo $f : G \rightarrow G'$ è sempre un sottogruppo normale di $(G',\ \cdot)$.

ESERCIZIO 5. Sia $(K, +, \cdot) := (\frac{\mathbb{Z}}{3\mathbb{Z}}, +, \cdot)$ il campo delle classi resto $\pmod 3$. In $K \times K$ si definiscano due operazioni nella maniera seguente:

$$(a, b) + (c, d) := (a + c, b + d)\,,$$
$$(a, b) \odot (c, d) := (ac + bd, ad + bc)\,.$$

(1) Dimostrare che $(K \times K, +, \odot)$ è un anello commutativo unitario.

(2) Stabilire se $(K \times K, +, \odot)$ possiede divisori dello zero.

ESERCIZIO 6. Determinare $\pmod{770}$ tutte le eventuali soluzioni del sistema di congruenze:

$$\begin{cases} 3X \equiv 9 \pmod{10} \\ 4X \equiv 3 \pmod{11} \\ -2X \equiv 6 \pmod 7\ . \end{cases}$$

ESERCIZIO 7. Sia dato il seguente polinomio

$$f(X) := (X^2 + 5)(X^4 + 3X^3 - 3X^2 - 7X + 6) \in \mathbb{Z}[X]\ (\subset \mathbb{Q}[X]).$$

(1) Utilizzando il teorema di Ruffini, determinare tutte le radici intere di $f(X)$ (cioè, determinare tutti gli elementi $\alpha \in \mathbb{Z}$ tali che $f(\alpha) = 0$).

(2) Dimostrare che, in $\mathbb{Q}[X]$,

(a) un polinomio non costante di grado 2 è irriducibile se e soltanto se non possiede radici in $\mathbb{Q}$;

(b) un polinomio non costante di grado 1 è sempre irriducibile in $\mathbb{Q}$.

(3) Scrivere esplicitamente la fattorizzazione del polinomio $f(X)$ come prodotto di polinomi irriducibili di $\mathbb{Q}[X]$.

SOLUZIONI

ESERCIZIO 1. La risposta esatta è la (c): le altre uguaglianze sono false ad esempio per $n = 0$ o/e $n = 1$ o/e $n = 2$. Passo induttivo:

$$\begin{aligned} 3\cdot 1 + 3\cdot 3 + 3\cdot 5 + \ldots + 3\cdot(2n-1) + 3\cdot(2n+1) = 3\cdot(n+1)^2 \;\Rightarrow \\ \Rightarrow\; 3\cdot 1 + 3\cdot 3 + 3\cdot 5 + \ldots + 3\cdot(2n-1) + 3\cdot(2n+1) + 3\cdot(2n+3) = \\ = 3\cdot(n+1)^2 + 3\cdot(2n+3)\,. \end{aligned}$$

E' subito visto che $3\cdot(n+1)^2 + 3\cdot(2n+3) = 3\cdot(n+2)^2$

ESERCIZIO 2. (1) *Esiste un uomo che non possiede la casa in cui abita.*
(2) La tabella della verità è la seguente:

$\boldsymbol{P}$	$\boldsymbol{Q}$	$\boldsymbol{R}$	$\neg\boldsymbol{P}$	$(\boldsymbol{Q}\vee\boldsymbol{P})$	$\neg\boldsymbol{P}\wedge(\boldsymbol{Q}\vee\boldsymbol{P})$	$(\neg\boldsymbol{P}\wedge(\boldsymbol{Q}\vee\boldsymbol{P}))\wedge\boldsymbol{R}$
v	v	v	f	v	f	f
v	v	f	f	v	f	f
v	f	v	f	v	f	f
v	f	f	f	v	f	f
f	v	v	v	v	v	v
f	v	f	v	v	v	f
f	f	v	v	f	f	f
f	f	f	v	f	f	f

ESERCIZIO 3.
(1) $\mathrm{MCD}(67375,\ 504) = 7\,.$
(2) $7 = 67375\cdot 25 + 504\cdot(-3342)\,.$

ESERCIZIO 4. Esercizio di tipo "teorico", completamente svolto negli appunti del corso e nel libro consigliato.

ESERCIZIO 5. (1) E' un anello, perché si vede immediatamente che rispetto alle operazioni assegnate è chiuso. Inoltre,

• $(K\times K, +)$ è un gruppo abeliano (perché prodotto diretto di gruppi abeliani, essendo l'operazione "+" definita componente per componente);

• Vale la proprietà associativa rispetto a "$\odot$":

$$((a,b)\odot(c,d))\odot(e,f) = (ace+bde+adf+bcf,\, acf+bdf+ade+bce) = (a,b)\odot((c,d)\odot(e,f))\ .$$

• Valgono le proprietà distributive (le verifiche avrebbero dovuto essere esplicitate), cioè:

$$\begin{array}{l} ((a,b)+(c,d))\odot(e,f) = ((a,b)\odot(e,f)) + ((c,d)\odot(e,f)) \\ (e,f)\odot((a,b)+(c,d)) = ((e,f)\odot(a,b)) + ((e,f)\odot(c,d)) \end{array}\ .$$

— Inoltre, è un anello unitario con unità uguale a $(1,0)$ (le verifiche avrebbero dovuto essere esplicitate). Precisamente, si può verificare che:

$$(a,b)\odot(x,y) = (a,b) \quad\Rightarrow\quad (x,y) = (1,0)\,.$$

— Infine, è un anello commutativo (essenzialmente perché $(K, +,\ \cdot)$ è un anello commutativo):

$$(a,b)\odot(c,d) = (ac+bd, ad+bc) = (ca+db, da+cb) = (c,d)\odot(a,b)\,.$$

(2) Non possiede divisori dello zero [N.B. si può dimostrare che è addirittura un campo]. Infatti,

$$(a, b) \odot (c, d) = (ac + bd, ad + bc) = (0, 0)\,,$$

determina il seguente sistema:

$$\begin{cases} ac + bd &= 0 \\ ad + bc &= 0 \end{cases}$$

il quale in K non è difficile vedere che non ammette soluzioni diverse da $(a, b) = (0, 0)$ oppure da $(c, d) = (0, 0)$. Infatti, supponiamo che $(a, b) \neq (0, 0)$. Se $a = 0$ e $b \neq 0$ (oppure se $a \neq 0$ e $b = 0$) allora è subito visto che $c = d = 0$. Simmetricamente, se $c = 0$ e $d \neq 0$ (oppure se $c \neq 0$ e $d = 0$) allora è subito visto che $a = b = 0$. Supponiamo quindi che $a \neq 0$ e $b \neq 0$ e che $d \neq 0$ e $c \neq 0$. Dovremmo avere che $ab^{-1} = -dc^{-1}$ e, contemporaneamente, che $ab^{-1} = -cd^{-1}$, dunque $c^2 + d^2 = 0$ (tutte queste uguaglianze sono in K), pertanto ciò implica che $(c, d) = (0, 0)$.
[N.B. Se $(a, b) \neq (0, 0)$ allora $a^2 - b^2 \neq 0$ in K, perciò $(a^2 - b^2)^{-1} \in K$, e dunque: $(a, b) \odot (c, d) = (ac+bd, ad+bc) = (1, 0) \;\Leftrightarrow\; (c, d) = \left(a(a^2 - b^2)^{-1}, -b(a^2 - b^2)^{-1}\right)$.]

ESERCIZIO 6. La soluzione del sistema è data da $x \equiv 53 \pmod{770}$.

ESERCIZIO 7. (1) Il Teorema di Ruffini si basa sul fatto che:

$$f(\alpha) = 0 \quad \Leftrightarrow \quad (X - \alpha) \mid f(X)\,,$$

e da questo si vede che:

$$f(\alpha) = 0\,,\; \alpha \in \mathbb{Z} \quad \Rightarrow \quad \alpha \text{ divide il termine noto di } f(X)\,.$$

Pertanto α può appartenere soltanto all'insieme $\{\pm 1,\ \pm 2,\ \pm 3,\ \pm 6\}$. A verifiche fatte, si vede che le radici intere di $f(X)$ sono date da $\alpha = 1, -2, -3$.

(2) Esercizio di tipo "teorico", completamente svolto nel libro consigliato [FG].

(3) Da (1) e (2) si ricava abbastanza agevolmente che:

$$f(X) = (X^2 + 5) \cdot (X - 1)^2 \cdot (X + 2) \cdot (X + 3)\,.$$