AL1 - Algebra 1: fondamenti - A.A. 2002/2003

Appello B

MATRICOLA (O ALTRO IDENTIFICATIVO): .....

COGNOME: ..... **NOME:** .....

esercizio	1	2	3	4	5	6	7
punti max	3	(2,2,2)	(5, 4)	(4, 8)	5	(3, 3)	((4,2), 3)
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 $n \geq 1$, la seguente espressione:

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

è uguale ad una soltanto tra le seguenti:

(a) $(2n)! - 1$;

(b) $(n+1)! - 1$;

(c) $(n+1)! - n$.

ESERCIZIO 2. Dati due numeri interi $a,\ b \in \mathbb{Z}$, si consideri l'applicazione:

$$f_{a,b} : \mathbb{Z} \to \mathbb{Z}\,, \quad x \mapsto ax + b\,.$$

(a) Determinare condizioni necessarie e sufficienti su $a,\ b$ in modo tale che $f_{a,b}$ risulti iniettiva.

(b) Determinare condizioni necessarie e sufficienti su $a,\ b$ in modo tale che $f_{a,b}$ risulti suriettiva.

(c) Nei casi in cui $f_{a,b}$ risulti essere biiettiva, descrivere esplicitamente l'applicazione inversa $(f_{a,b})^{-1} : \mathbb{Z} \to \mathbb{Z}$.

ESERCIZIO 3. (1) Sia $\mathbb{R}^{>} := \{x \in \mathbb{R} \mid x \gneq 0\}$. Dimostrare che i gruppi $(\mathbb{R}, +)$ e $(\mathbb{R}^{>}, \cdot\,)$ sono tra loro isomorfi, definendo esplicitamente un isomorfismo tra tali gruppi.

(2) Stabilire se i gruppi $\left(\frac{\mathbb{Z}}{8\mathbb{Z}}, +\right)$ e $\left(\boldsymbol{U}\left(\frac{\mathbb{Z}}{15\mathbb{Z}}\right), \cdot\,\right)$ sono oppure non sono tra loro isomorfi (si ricordi che $\boldsymbol{U}\left(\frac{\mathbb{Z}}{15\mathbb{Z}}\right) := \{k + 15\mathbb{Z} \mid \mathrm{MCD}(k, 15) = 1\,,\ \ 1 \leq k \leq 15\}$).

ESERCIZIO 4. (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. Dimostrare che:

$$4 \mid a \quad \Leftrightarrow \quad 4 \mid (a_1 10 + a_0)\,.$$

(2) Enunciare e dimostrare il "Piccolo" Teorema di Fermat.

ESERCIZIO 5. Determinare tutte le eventuali soluzioni del sistema di congruenze:

$$\begin{cases} X \equiv 2 \pmod 7 \\ X \equiv 1 \pmod 5 \\ X \equiv 4 \pmod 9 \end{cases} .$$

ESERCIZIO 6. Sia $A := \mathbb{Z} \times \mathbb{R}$ l'anello prodotto diretto degli anelli $(\mathbb{Z}, +, \cdot\,)$ e $(\mathbb{R}, +, \cdot\,)$.

(1) Stabilire se $(A, +, \cdot\,)$ è un anello unitario, se è commutativo, se possiede di divisori dello zero, se è un campo.

(2) Sia $B := \{(3x, y) \mid x \in \mathbb{Z}\,,\ y \in \mathbb{Q}\} \subseteq A$. Stabilire se B è un sottoanello di $(A, +, \cdot\,)$, se B è un ideale di $(A, +, \cdot\,)$.

ESERCIZIO 7. **(1)** Dati due polinomi $f(T) := 18 + 6T - 15T^2 + 2T^3$ e $g(T) := 21 - 17T + 2T^2$ in $\mathbb{Q}[T]$, utilizzando l'algoritmo euclideo delle divisioni successive:

(a) determinare il polinomio monico $d(T) := \mathrm{MCD}(f(T), g(T)) \in \mathbb{Q}[T]$;

(b) determinare un'espressione del tipo $d(T) = a(T)f(T) + b(T)g(T)$ (cioè determinare due polinomi $a(T), b(T) \in \mathbb{Q}[T]$) [identità di Bézout].

(2) Decomporre il polinomio $T^4 - T^2 - 2$ in fattori irriducibili in ciascuno dei seguenti due anelli: $\mathbb{Q}[T]$, $\mathbb{C}[T]$.

SOLUZIONI

ESERCIZIO 1. La risposta esatta è (b): le altre uguaglianze non false ad esempio per $n = 2$.

Base dell'induzione (b) vale per $n = 1$.

Ipotesi induttiva:

$$1 \cdot 1! + 2 \cdot 2! + 3 \cdot 3! + \ldots + (n-1) \cdot (n-1)! + n \cdot n! = (n+1)! - 1 \, .$$

Quindi:

$$\begin{aligned} &[1 \cdot 1! + 2 \cdot 2! + 3 \cdot 3! + \ldots + (n-1) \cdot (n-1)! + n \cdot n!] + (n+1) \cdot (n+1)! = \\ &= [(n+1)! - 1] + (n+1) \cdot (n+1)! = (n+1)! + (n+1) \cdot (n+1)! - 1 = \\ &= (n+1)!(1 + n + 1) - 1 = (n+2)! - 1 \, . \end{aligned}$$

ESERCIZIO 2. **(a)** Risposta: $a \neq 0$. Siano $x, \ x' \in \mathbb{Z}$, con $x \neq x'$, allora:

$$f_{a,b}(x) \neq f_{a,b}(x') \ \Leftrightarrow \ ax + b \neq ax' + b \ \Leftrightarrow \ a \neq 0 \, .$$

(b) Risposta: $a = \pm 1$. Un qualunque $y \in \mathbb{Z}$ è tale che esiste $x \in \mathbb{Z}$ con $y = ax + b = f_{a,b}(x)$ se e soltanto se $a = \pm 1$ (in tal caso $x = \pm(y - b)$).

(c) Per $a = 1$, $(f_{1,b})^{-1} = f_{1,-b}$. Per $a = -1$, $(f_{-1,b})^{-1} = f_{-1,b}$.

ESERCIZIO 3. **(1)** L'applicazione:

$$\log : \mathbb{R}^{>} \to \mathbb{R} \, , \quad x \mapsto \log(x) \, ,$$

è un omomorfismo biiettivo di gruppi tra $(\mathbb{R}^{>}, \cdot)$ e $(\mathbb{R}, +)$, con applicazione inversa (che è anch'essa un omomorfismo di gruppi) data da:

$$\exp : \mathbb{R} \to \mathbb{R}^{>} \, , \quad x \mapsto e^x \, .$$

(2) $\boldsymbol{U}(\frac{\mathbb{Z}}{15\mathbb{Z}}) = \{\overline{1}, \ \overline{2}, \ \overline{4}, \overline{7}, \ \overline{8}, \ \overline{11}, \ \overline{13}, \ \overline{14}\}$ (dove $\overline{k} := k + 15\mathbb{Z}$). Notare che:

$\overline{1}$ ha ordine (moltiplicativo) uguale ad 1 ;
$\overline{2}$ ha ordine (moltiplicativo) uguale ad 4 ;
$\overline{4}$ ha ordine (moltiplicativo) uguale ad 2 ;
$\overline{7}$ ha ordine (moltiplicativo) uguale ad 4 ;
$\overline{8}$ ha ordine (moltiplicativo) uguale ad 4 ;
$\overline{11}$ ha ordine (moltiplicativo) uguale ad 2 ;
$\overline{13}$ ha ordine (moltiplicativo) uguale ad 4 ;
$\overline{14}$ ha ordine (moltiplicativo) uguale ad 2 .

Pertanto $\left(\boldsymbol{U}(\frac{\mathbb{Z}}{15\mathbb{Z}}), \cdot\right)$ è un gruppo abeliano (moltiplicativo) di ordine 8 che *non* è ciclico. Dunque, non può esistere nessun isomorfismo tra $\left(\frac{\mathbb{Z}}{8\mathbb{Z}}, +\right)$ e $\left(\boldsymbol{U}(\frac{\mathbb{Z}}{15\mathbb{Z}}), \cdot\right)$, perché $\left(\frac{\mathbb{Z}}{8\mathbb{Z}}, +\right)$ è un gruppo abeliano (additivo) ciclico. (Notare che un omomorfismo di gruppi "conserva" l'ordine degli elementi.)

ESERCIZIO 4. Esercizio di tipo "teorico", completamente svolto nel libro consigliato [FG].

ESERCIZIO 5. (Teorema Cinese dei Resti) Soluzione: $x \equiv 121 \pmod{7 \cdot 5 \cdot 9 = 315}$.

ESERCIZIO 6. **(1)**

$(A, +, \cdot)$ è un anello unitario, con unità uguale a $(1, 1)$.

$(A, +, \cdot)$ è un anello commutativo, perché $(\mathbb{Z}, +, \cdot)$ e $(\mathbb{R}, +, \cdot)$ sono anelli commutativi e l'operazione di prodotto in $(A, +, \cdot)$ viene effettuata componente per componente (definizione di prodotto diretto di anelli).

$(A,+,\cdot\,)$ possiede divisori dello zero:

$$(n,0)\cdot(0,r)=(0,0)\,,\quad \forall n\in\mathbb{Z}\,,\,\forall r\in\mathbb{R}\,.$$

$(A,+,\cdot\,)$ non può essere un campo, dal momento che possiede divisori dello zero.

(2) $B:=\{(3x,y)\mid x\in\mathbb{Z},\ y\in\mathbb{Q}\}$ è un sottoanello di A, perché $(\forall(3x,y)\,,\,(3x',y')\in B)$:

$$(3x,y)-(3x',y')=(3(x-x'),y-y')\in B\,,\quad (3x,y)\cdot(3x',y')=(3(3xx'),yy')\in B\,.$$

Non è un ideale, perché ad esempio:

$$(3x,y)\cdot(1,\sqrt{2})\notin B\,,\quad \forall(3x,y)\in B\,,\quad \text{preso}\quad (1,\sqrt{2})\in A\,.$$

ESERCIZIO 7. (1) L'algoritmo euclideo delle divisioni successive è il seguente:

$$\begin{aligned}18+6T-15T^2+2T^3&=\ (21-17T+2T^2)\cdot(1+T)+(-3+2T)\,,\\ 21-17T+2T^2&=\ (-3+2T)\cdot(-7+T)+0\,.\end{aligned}$$

(a) Quindi il polinomio *monico* $d(T)=\mathrm{MCD}(f(T),g(T))$ è dato da $\frac{-3}{2}+T$.

(b) Infine:

$$\frac{-3}{2}+T=\frac{1}{2}((-3+2T))=\frac{1}{2}\cdot(18+6T-15T^2+2T^3)-\frac{1}{2}(1+T)\cdot(21-17T+2T^2)\,.$$

(2) Le fattorizzazioni in polinomi irriducibili sono le seguenti:

$$\begin{aligned}T^4-T^2-2&=(T^2-2)\cdot(T^2+1)\ \ \text{in}\ \mathbb{Q}[T]\,;\\ T^4-T^2-2&=(T-\sqrt{2})\cdot(T+\sqrt{2})\cdot(T-i)\cdot(T+i)\ \ \text{in}\ \mathbb{C}[T]\,.\end{aligned}$$