CORSO DI LAUREA TRIENNALE IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II E III)
16 MARZO 2024

Svolgere i seguenti esercizi,

$\longrightarrow$ $\boxed{\textbf{\textit{giustificando pienamente tutte le risposte.}}}$ $\longleftarrow$

Sui fogli consegnati vanno indicati: **nome**, **cognome**, **matricola**, **gruppo di appartenenza**.
Non è necessario consegnare la traccia.

Esercizio 1. La forma proposizionale $\big((p \Rightarrow r) \iff (s \vee \neg q)\big) \implies \big((s \wedge q) \Rightarrow (s \vee q)\big)$ è una tautologia?

Esercizio 2. Sia $f\colon (a,b) \in \mathbb{Z} \times \mathbb{Z} \mapsto 30a + b \in \mathbb{Z}$.

- (i) f è iniettiva? È suriettiva?
- (ii) Posto $T = \{n \in \mathbb{N} \mid 60 \leq n \leq 70\}$, determinare l'insieme S delle coppie in $(a,b) \in \mathbb{N} \times T$ tali che l'elemento $[f(a,b)]_{45}$ sia invertibile in $\mathbb{Z}_{45}$.
- (iii) Scelto $(a,b) \in S$ in modo che $a+b$ abbia il minimo valore possibile, si calcoli l'inverso di $[f(a,b)]_{45}$ in $\mathbb{Z}_{45}$.

Esercizio 3. Nel prodotto cartesiano $\mathbb{Z}_4 \times \mathbb{Z}_6$ si considerino le operazioni di addizione e moltiplicazione usuali componente per componente. Rispetto a tali operazioni, che indichiamo ancora con $+$ e $\cdot$, $R := \mathbb{Z}_4 \times \mathbb{Z}_6$ risulta essere un anello commutativo unitario. Determinare:

- (i) $|R|$;
- (ii) lo zero 0_R, l'unità 1_R, gli elementi invertibili, i divisori dello zero e gli elementi idempotenti di R;
- (iii) le radici in R del polinomio $x^2 - x \in R[x]$;
- (iv) la caratteristica di R (cioè il minimo $n \in \mathbb{N}^*$ tale che $n1_R = 0_R$).
- (v) R è un dominio di integrità?
- (vi) La parte $M = \mathbb{Z}_4 \times \{[0]_6, [3]_6\}$, è chiusa rispetto alle operazioni di addizione e moltiplicazione in R? Nel caso lo sia, che tipo di struttura risulta essere $(M, +, \cdot)$?
- (vii) Se M è chiusa rispetto a $\cdot$, (a) $(M, \cdot)$ ha elemento neutro? (b) Che tipo di struttura è $(M, \cdot)$?

Esercizio 4. Sia ρ la relazione binaria definita in $\mathbb{N}$ da: $\forall a, b \in \mathbb{N}$ $(a \ \rho \ b \iff b - a \in 2a\mathbb{N})$. (Qui, come altrove, $2a\mathbb{N} = \{2ak \mid k \in \mathbb{N}\}$). Decidere se ρ è una relazione d'ordine. Se lo è:

- (i) determinare i minoranti di $\{12\}$ in $(\mathbb{N}, \rho)$;
- (ii) determinare gli elementi minimali, massimali, minimo, massimo in $(\mathbb{N}, \rho)$;
- (iii) decidere se $(\mathbb{N}, \rho)$ è un reticolo;
- (iv) decidere se l'applicazione identica di $\mathbb{N}$ è crescente da $(\mathbb{N}, \rho)$ a $(\mathbb{N}, |)$ e se è un isomorfismo tra questi due insiemi ordinati;
- (v) posto $S = \{1, 3, 5, 9, 21, 45, 75, 105^2\}$, disegnare un diagramma di Hasse di (S, ρ) e stabilire se (S, ρ) è un reticolo, un reticolo distributivo, un reticolo complementato.

Esercizio 5. Dare la definizione di relazione binaria.

- (i) Sia $a = \{n \in \mathbb{N} \mid n \leq 7\}$. Determinare tutte le relazioni di equivalenza ρ in a tali che $0 \ \rho \ 7$, $(1,4)$ appartenga al grafico di ρ, $\{3,4,7\} \subseteq [2]_\rho$ e $3 \ \rho \ 1 \Rightarrow 5 \ \rho \ 0$.
- (ii) Presentare, se possibile, due distinte partizioni p_1 e p_2 di a tali che $p_1 = a/{\sim_1}$ e $p_2 = a/{\sim_2}$ per due delle relazioni di equivalenza, $\sim_1$ e $\sim_2$, trovate al punto (i).

Esercizio 6. Sia $f = (x^2 - \bar{5})g \in \mathbb{Z}_{11}[x]$, dove $g = x^5 + \bar{4}x^2 - x + \bar{7}$. Dopo aver calcolato $g(\bar{1})$ e $g(-\bar{1})$, dando per noto che non esistono numeri interi n tali che $n^3 + n \equiv_{11} 7$, scrivere f come prodotto di polinomi irriducibili in $\mathbb{Z}_{11}[x]$.

- (i) È possibile scrivere f come prodotto di sei polinomi (in $\mathbb{Z}_{11}[x]$) non costanti?
- (ii) È possibile scrivere f come prodotto di polinomi irriducibili (in $\mathbb{Z}_{11}[x]$) non monici tutti con lo stesso coefficiente direttore?

Es 1

$(s \wedge q) \Rightarrow (s \vee q)$

s	$\wedge$	q	$\vee$
V	V	V	V
V	F	F	V
F	F	V	V
F	F	F	F

Poiché B è sempre vera $A \Rightarrow B$ è una tautologia

Es 2

$a * b = 30a + b$

i) INIETTIVA: NO

$\forall x, y \in \mathbb{Z} \, (f(x) = f(y) \Rightarrow x = y)$

$0 * 31 = 31 \qquad 1 * 1 = 31$

SURRIETTIVA: SI

$\forall y \in \mathbb{Z} \, (\exists x \in \mathbb{Z} \, (y = f(x))$ Vero perché: $\forall y \in \mathbb{Z} \, (0 * y = y)$

ii) $T = \{ n \in \mathbb{N} \mid 60 \leq n \leq 70 \}$

$$f = (x^2 - 5)(x^5 + 4x^2 - x + 7)$$

$$\cancel{1} + 4 - \cancel{1} + 7 = \overline{11} = \bar{0}$$

$$-\cancel{1} + 4 + \cancel{1} + 7 = \overline{11} = \bar{0}$$

$$(x+4)\cdot(x-4)\left(x^4 + x^3 + x^2 + 5x + 4\right)(x-1)$$

$$\begin{array}{l|l}
x^5 + 0x^4 + 0x^3 + 4x^2 - x + 7 & x - 1 \\ \hline
-x^5 + x^4 & x^4 + x^3 + x^2 + 5x + 4 \\ \hline
// \quad + x^4 + 0x^3 + 4x^2 - x + 7 & \\
\quad - x^4 + x^3 & \\ \hline
\quad // \quad + x^3 + 4x^2 - x + 7 & \\
\quad\quad - x^3 + x^2 & \\ \hline
\quad\quad // \quad + 5x^2 - x + 7 & \\
\quad\quad\quad - 5x^2 + 5x + 7 & \\ \hline
\quad\quad\quad // \quad + 4x + 7 & \\
\quad\quad\quad\quad - 4x + 4 & \\ \hline
\quad\quad\quad\quad // \quad \overline{11} &
\end{array}$$

$$\begin{array}{l|l}
x^4 + x^3 + x^2 + 5x + 4 & x + 1 \\ \hline
-x^4 - x^3 & x^3 + x + 4 \\ \hline
// \quad // \quad + x^2 + 5x + 4 & \\
\quad - x^2 - x & \\ \hline
\quad // \quad 4x + 4 & \\
\quad\quad - 4x - 4 & \\ \hline
\quad\quad // \quad // &
\end{array}$$

$$(x+4)\cdot(x-4)\left(x^3 + x + 4\right)(x+1)(x-1)$$

NO, massimo 5.

$$5x \equiv_{11} 1 \qquad x = 9$$

$$11 = 5 \cdot 2 + 1 \qquad 1 = 11 \cdot 5(-2)$$

$$(9x+3)(9x-3)(9x^3+9x+3)(9x+9)(9x-9)$$

Es 3

$(R, +, \cdot)$ anello commutativo unitario

$R = \mathbb{Z}_4 \times \mathbb{Z}_6$

- $(R, +)$: GA
- $(R, \cdot)$: Monoide commutativo
- $\cdot$ è distributiva

i) $|R| = |\mathbb{Z}_4| \cdot |\mathbb{Z}_6| = 4 \cdot 6 = 24$

ii) 0_R : Elemento Neutro $(R, +)$: $(\bar{0}_4, \bar{0}_6)$

$(x, y) + (a, b) = (x, y)$

$x + a = x \Rightarrow a = \bar{0}$

$y + b = y \Rightarrow b = \bar{0}$

1_R . Elemento Neutro $(R, \cdot)$ $(\bar{1}_4, \bar{1}_6)$

$(x, y) \cdot (a, b) = (x, y)$

Invertibili

Es 4

$\rho: \forall a,b \in \mathbb{N} (a \rho b \iff b-a \in 2a\mathbb{N})$

ρ è d'ordine:

Antisimmetrica:

$\forall a,b \in \mathbb{N} (a\rho b \wedge b \rho a \iff a=b)$

$b-a \in 2a\mathbb{N} \wedge a-b \in 2a\mathbb{N} \iff a=b$

se prendiamo $a=3$ e $b=3$

$0 \in 6\mathbb{N} \wedge 0 \in 6\mathbb{N} \iff 3=3$ ✓

mentre se prendiamo $a=3$ e $b=15$

$15-3 \in 6\mathbb{N} \wedge 3-15 \in 6\mathbb{N} \iff 3=15$

$12 \in 6\mathbb{N} \wedge -12 \in 6\mathbb{N} \iff 3=15$

$3 \rho 15$, ma $15 \rho 3$ non è vero

Transitiva:

$a \rho b$ e $b \rho c \Rightarrow a \rho c$

$a \rho b \iff b-a \in 2a\mathbb{N} \iff \exists k \in \mathbb{N} (b-a = 2ak) \iff \exists k \in \mathbb{N} (b = a(2k+1))$

min e max 0

$a \rho 3a$

minimali sono le potenze di 2 $\{2^n \mid n \in \mathbb{N}\} \cup \{0\}$