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

Svolgere i seguenti esercizi,

giustificando pienamente tutte le risposte.

Sui fogli consegnati vanno indicati: **nome**, **cognome**, **matricola**, **gruppo di appartenenza**.

Non è necessario consegnare la traccia.

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

Esercizio 2

$f: (a,b) \in \mathbb{Z}\times\mathbb{Z} \to 30a+b \in \mathbb{Z}$

i) Non è iniettiva es.

$a=1 \quad b=0 \qquad 30\cdot 1 + b = 30$

$a=0 \quad b=30 \qquad 30\cdot 0 + b = 30$

È suriettiva. Basta porre $a=0$ e $b=$ qualsiasi $\mathbb{Z}$

ii) $(a,b) \in \mathbb{N}\times T \mid [f(a,b)_{45}]$ inv in $\mathbb{Z}_{45}$

$[f(a,b)]_{45} = [30a+b]_{45}$ è inv $\leftrightarrow$ $30a+b \equiv_{45} 1$ è vera

$\leftrightarrow$ $MCD(30a+b, 45) = 1$ poiché $45 = 3^2\cdot 5$

$30a+b$ non deve essere multiplo né di 3 né di 5

↳ Poiché 30 è diviso sia da 5 che da 3 e dunque anche $30a$ lo è sia tutto nel fatto che 3 e 5 non devono dividere b

$S = \{(a,b) \mid 3 \nmid DIV(30a+b) \wedge 5 \nmid DIV(30a+b)\} =$

$\{(0,61)(0,62)(0,64)(0,67)(0,68)\}$

iii) $\Rightarrow (0,61)$ minimo S

60 è escluso

inverso

$61 \cdot (31)$

$[f(0,61)]_{45} \leftrightarrow [61]_{45}$ $\quad 61x \equiv_{45} 1$

$61 = 45\cdot 1 + 16$

$45 = 16\cdot 2 + 13$

$16 = 13\cdot 1 + 3$

$13 = 3\cdot 4 + 1$

$1 = 13 + 3(-4)$

$3 = 16 + 13(-1)$

$13 = 45 + 16(-2)$

$16 = 61 + 45(-1)$

$1 = 13 + (16 + 13(-1))(-4)$

$13(5) + 16(-4)$

$1 = (45 + 16(-2))(5) + 16(-4)$

$45(5) + 16(-14)$

$45(5) + (61 + 45(-1))(-14)$

$45(-) + 61(-14) \equiv (31)$

31 è l'inverso di 61

Esercizio 3

$(R, +, \cdot)$ comm. unitario con $R = \mathbb{Z}_4 \times \mathbb{Z}_6$ = (00)(01)(02)(03)(04)(05)(10)(11)(12)(13)(14)(15)(20)(21)(22)(23)(24)(25)(30)(31)(32)(33)(34)(35)

$\mathbb{Z}_4$: 0,1,2,3 — $\mathbb{Z}_6$: 0,1,2,3,4,5

i) $|R| = 6 \cdot 4 = 24$

ii) Neutro ddi $+$

è commutativo quindi

$(\forall a, b \in R)(a * u = u * a = a)$

$a * u = a + u = a \iff u = (0,0)$

$u = (0,0)$

neutro ddi $\cdot$

$a * u = u * a = a$

$a \cdot u = a$

$u = (1,1)$

Invertibili

$\mathbb{Z}_6 = U(1,5)$

$\mathbb{Z}_4 = U(1,3)$

$\mathbb{Z}_4 \times \mathbb{Z}_6 = \{(1,1), (1,5), (3,1), (3,5)\}$

Div dello zero $= \{(1,2), (1,3), (1,4)\}$

SBAGLIATO!

Non è corretto fare il prodotto cartesiano

$(\forall a \setminus \{0\})(\exists b \setminus \{0\} \; a \cdot b = 0)$

$\mathbb{Z}_6 = \{2,3,4\}$ $\quad \mathbb{Z}_4 = \{2\}$

0 1 2 3 4 5 — 0 1 2 3

(Solo sul $*$)

$(x,y) \in Div_0(R) \iff \exists (w,z) \in \mathbb{Z}_4 \times \mathbb{Z}_6 \setminus \{\bar{0},\bar{0}\} \; ((xw, yz) = (\bar{0},\bar{0}))$

$\iff xw = \bar{0} \wedge yz = \bar{0} \iff$ { se $w = 0 \to z \neq 0 \to (y = \bar{0} \vee y \in Div_0(\mathbb{Z}_4))$; se $w \neq 0 \to z = 0 \to (x = \bar{0} \vee x \in Div_0(\mathbb{Z}_6))$ }

$\updownarrow$

$x \in Div_0(\mathbb{Z}_6) \vee y \in Div_0(\mathbb{Z}_4)$

Basta che uno dei due componenti della coppia sia un divisore dello zero

Es. $\{3\} \times Div_0(\mathbb{Z}_6) \Rightarrow$ esiste una coppia tale per cui $(1, Div_0(\mathbb{Z}_6))(x \cdot y) = (\bar{0},\bar{0})$

(non è un divisore dello zero in $\mathbb{Z}_4$)

Es. $(\bar{3},\bar{2}) \cdot (\bar{0},\bar{3}) = (\bar{0},\bar{0})$

↳ lo zero può APPARTENERE ALLA COPPIA UNA SOLA VOLTA, INFATTI $(0,3) \neq (0,0)$

Idempotenti

$a * a = a$

$\mathbb{Z}_4$: $0 \cdot 0 = 0$ ✓
$1 \cdot 1 = 1$ ✓
$2 \cdot 2 = 4 = 0$ ×
$3 \cdot 3 = 9$ ×

$\mathbb{Z}_6$: $0 \cdot 0 = 0$ ✓
$1 \cdot 1 = 1$ ✓
$3 \cdot 3 = 9 = 3$ ✓
$4 \cdot 4 = 16 = 4$ ✓
$5 \cdot 5 = 25$

$\mathbb{Z}_4 \times \mathbb{Z}_6 = \{(0,0), (0,2), (0,3), (0,4), (1,0), (1,1), (1,3), (1,4)\}$

iii) $x^2 - x \in \mathbb{R}([x]) \iff x^2 = x \iff x \cdot x = x$ sono gli idempotenti delle operazioni

iv) $m \cdot 1_R = 0_R$

$m \cdot (1,1) = (0,0)$

$(\mathbb{Z}_4, \mathbb{Z}_6) \cdot (1,1) = (0,0)$

0 1 2 3 4 5

$12 \cdot (1,1) = (0,0)$

mcm $(\mathbb{Z}_4\ \mathbb{Z}_6)$ deve essere comune a entrambi

v) No, in quanto non tutti gli elem sono invertibili

vi) $M = \mathbb{Z}_4 \times \{[0]_6, [3]_6\}$ — 0,6,12,18,24,30,36 — 3,9,15,21,27,33

$\mathbb{Z}_4 \times \{\bar{0},3\}$ → Sappiamo che un elemento di $\mathbb{Z}_4$ appartiene sempre => dobbiamo vedere solo se ogni elemento di $\{\bar{0},3\}$ appartiene, cioè

MOLTIPLICAZIONE:
$(0,0) = 0 \in \{0,3\}$
$(0,3) = 0 \in \{0,3\}$
$(3,3) = 9 = 6 \in \{\bar{0},3\}$

=> È chiuso rispetto a $\cdot$

ADDIZIONE:
$(0,0) = 0+0 = 0 \in \{\bar{0},3\}$
$(0,3) = 0+3 = 3 \in \{\bar{0},3\}$
$(3,3) = 3+3 = 6 = 0 \in \{\bar{0},3\}$

=> È chiuso rispetto a +

vii)

Il neutro di $\cdot$ $(1,1) \notin \mathbb{Z}_4 \times \{[0]_6, [3]_6\}$ => non ho neutro

=> semigruppo commutativo

Esercizio a.

$(\forall a,b \in \mathbb{N})(a \rho b \leftrightarrow b-a \in 2ak)$ con $k \in \mathbb{N}$

$b - a = 2ak$
$b = a(2k+1)$

Doveva esser vista così

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

$(b-a \in 2ak \wedge a-b \in 2ak \rightarrow a=b)$

Vero. Se prendessimo 2 numeri diversi, una delle due sottrazioni risulterebbe negativa e non apparterrebbe a $2a\mathbb{N}$

transitività: $(\forall a,b,c \in \mathbb{N})(a \rho b \wedge b \rho c \rightarrow a \rho c)$

$b-a \in 2ak \wedge c-b \in 2ak \rightarrow c-a \in 2ak)$

nego $(\exists a,b,c \in \mathbb{N})(a \rho b \wedge b \rho c \wedge \neg a \rho c)$

$(\exists a,b,c \in \mathbb{N})(b-a \in 2ak \wedge c-b \in 2ak \wedge c-a \notin 2ak$ → $\nexists c-a \mid c-a \notin 2ak$

$50-2 = 48 \in \{2 \cdot 2 \cdot 12\}$ $650-50 = 600 : 600 \in 2 \cdot 50$ $650-2 = 648 = 2 \cdot 2 \cdot 162$ ✓

i) $t = \{12\}$ $m \in \text{minor} \leftrightarrow (\forall x \in t)(m \rho x)$

$x - m \in 2a\mathbb{N}$

$12 - m \in 2a\mathbb{N}$

$2 \cdot 4 \cdot 1$

minor $\{12\} = \{4, 12\}$

0 ✗
1 ✗
2 ✗
3 ✗
4 ✓
5 ✗
6 ✗
⋮ ✗

ii) Facciamo prove con numeri semplici

$a \rho b \rightarrow b = a(2k+1) \rightarrow b = 0$ (→ mon)

$b \rho a \rightarrow 0 = a(2k+1) \rightarrow a = 0$ (→ minimale)

⟶ questa caratteristica ci dice che 0 è sia minimale che massimale

$1 \rho b \rightarrow b = 1(2k+1) \rightarrow b$ è dispari

$a \rho 1 \rightarrow 1 = a(2k+1) \rightarrow a = 1$

⟶ 1 è minimale, perché se c'è uno in relazione con 1 allora è 1 stesso

$2 \rho b \rightarrow b = 2(2k+1) \rightarrow b$ è dispari

$a \rho 2 \rightarrow 2 = a(2k+1) \rightarrow a = 2$

⟶ 2 è minimale

Continuando tale ragionamento notiamo che i minimali sono tutte le potenze di 2. Dunque

MINIMALI: $\{0, 1, 2, 4, 8, \dots 2^n\}$ MASSIMALE = $\{0\}$

iii) Poiché 0 è sia minimale che massimale è scollegato => non è un reticolo

iv) Sia $f: \mathbb{N} \to \mathbb{N}$ è crescente $\leftrightarrow (\forall a,b \in \mathbb{N})(a \mid b \to f(a) \mid f(b))$

$(\forall a,b \in \mathbb{N})(b-a \in 2ak \to a \mid b)$

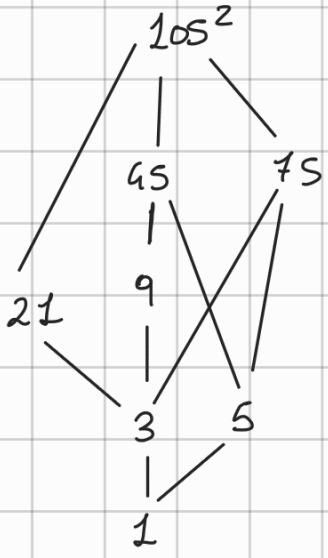
$(b = a(2k+1) \to a \mid b)$ ovvio

NON È UN ISOMORFISMO in quanto

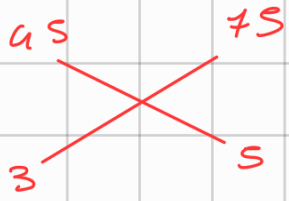
$2 \mid 4$, MA $4 \neq 2(2k+1)$

$4-2 \notin 2 \cdot 2 \cdot k$

v) $S = \{1, 3, 5, 9, 21, 45, 75, 105^2\}$



NON è un reticolo



~~∃~~ inf e sup tra 75 e 45

stessa cosa per 3 e 5

Esercizio 5

i) $0\rho 7 \quad 1\rho 4 \quad 2\rho 3 \quad 2\rho 4 \quad 2\rho 7 \quad 2\rho 2 \quad 3\rho 1 \to 5\rho 0$
$3\rho 4 \quad 3\rho 7 \quad 4\rho 7$

ii) $\{\{0,7,3,4,2,1,5\}\{6\}\}$ $\{\{0,7,3,4,2,1,5,6\}\}$ → queste sono le due partizioni

Esercizio 6

$f=(x^2-5)g \in \mathbb{Z}_{11}[x] \quad g = x^5+4x^2-x+7$

$g(1)=0$
$g(-1)=0$

$(x^2-5)\,x^5+4x^2-x+7$ 0 1 2 3 4 5

4 è radice

$(x-4)(x+4)$

$x^2+4x-4x-16$

x^2-16

x^2-5

$$\begin{array}{l|l} x^5+4x^2-x+7 & x-1 \\ \hline -x^5+x^4 & x^4+x^3+x^2+5x+4 \\ \hline = x^4+4x^2-x+7 & \\ -x^4+x^3 & \\ \hline = x^3+4x^2-x+7 & \\ -x^3+x^2 & \\ \hline = 5x^2-x+7 & \\ -5x^2+5x & \\ \hline = 4x+7 & \\ -4x+4 & \\ \hline = = & \end{array}$$

$(x^4+x^3+x^2+5x+4)(x+1)$

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

$$(x^3 + x + 4)(x+1)(x+1)$$

$$(x-4)(x+4)(x^3+x+4)(x+1)(x+1)$$

i) No, la scomp. è unica e ha solo 5 fattori

ii) $x^5 \equiv_{11} 1 \iff 2^5 = 32 \overset{\mathbb{Z}_{11}=10}{=}$

$3^5 = \mathbb{Z}_{11} = 2$

$4^5 = \mathbb{Z}_{11} = 1$ ✓

$$4(x-4)\ 4(x+4)\ 4(x^3+x+4)\ 4(x+1)\ 4(x+1)$$