CORSO DI LAUREA TRIENNALE IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II E III)
22 APRILE 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. (i) Enunciare il teorema fondamentale sulle relazioni di equivalenza e le partizioni.
Posto $T = \{13, 24, 202, 1104, 110211\}$,

(ii) determinare il numero delle partizioni di T aventi ordine (cardinalità) 2.

(iii) Se α è la relazione di equivalenza definita in T da: per ogni $a, b \in T$,

$$a\ \alpha\ b \longleftrightarrow \text{la somma delle cifre di } a^{(\ddagger)} \text{ è uguale alla somma delle cifre di } b,$$

descrivere esplicitamente le classi di equivalenza di α e l'insieme quoziente T/α.

Esercizio 2. Si consideri l'applicazione $f\colon (a, b) \in \mathbb{N} \times \mathbb{N}^* \longmapsto a^b \in \mathbb{N}$.

(i) Determinare $\overrightarrow{f}(\mathbb{N} \times \mathbb{N}^*)$, $\overrightarrow{f}(\varnothing)$, $\overleftarrow{f}(\varnothing)$ $\overleftarrow{f}(\{1\})$, $\overleftarrow{f}(\{5\})$.

(ii) Verificare se f è iniettiva, suriettiva, biettiva.

(iii) Dare le definizione di reticolo (come insieme ordinato).

Si consideri la relazione d'ordine τ definita in $\mathbb{N} \times \mathbb{N}^*$ da: $\forall a, c \in \mathbb{N}\ \forall b, d \in \mathbb{N}^*$

$$(a, b)\ \tau\ (c, d) \longleftrightarrow \big((a, b) = (c, d) \vee f((a, b)) \text{ è un divisore proprio di } f((c, d))\big).$$

(iv) Determinare in $(\mathbb{N} \times \mathbb{N}^*, \tau)$ eventuali minimo, massimo, elementi minimali, elementi massimali e verificare se $(\mathbb{N} \times \mathbb{N}^*, \tau)$ è o meno un reticolo.

Sia $M = \{(4, 1), (2, 2), (2, 3), (6, 2), (4, 2), (12, 2)\}$.

(v) Disegnare un diagramma di Hasse di (M, τ).

(vi) Stabilire se (M, τ) è un reticolo. Se lo è decidere se è distributivo, complementato, booleano. Se non lo è determinare una coppia $(a, b) \in M$ tale che $(M \smallsetminus \{(a, b)\}, \tau)$ sia un reticolo e decidere se questo è distributivo, complementato, booleano.

Esercizio 3. Sia $*$ l'operazione binaria definita in $\mathbb{Z}_6$ ponendo, per ogni $a, b \in \mathbb{Z}_6$, $a * b = \bar{3}a + \bar{4}b$.

(i) Dopo aver dato la definizione di semigruppo, verificare che $(\mathbb{Z}_6, *)$ è un semigruppo.

(ii) $(\mathbb{Z}_6, *)$ è un monoide? È commutativo?

(iii) Verificare che, in $(\mathbb{Z}_6, *)$, $\{\bar{0}, \bar{3}\}$ è una parte stabile (cioè chiusa).

Esercizio 4. Sia ρ la relazione binaria in $\mathbb{Z}$ definita da: per ogni $a, b \in \mathbb{Z}$, $a\ \rho\ b \leftrightarrow a + b$ è dispari.

(i) Verificare che $(\mathbb{Z}, \rho)$ definisce un grafo.

(ii) Determinare un sottoinsieme S di $\mathbb{Z}$ tale che $|S| = 5$ e (S, ρ) definisca un albero.

Esercizio 5. Vero o falso (e perché)?

(i) In $\mathbb{Z}_{13}[x]$, un polinomio f ammette $\bar{3}$ e $\bar{5}$ come radici se e solo se f è multiplo di $x^2 - \bar{8}x + \bar{2}$.

(ii) Il polinomio $x^2 - \bar{8}x + \bar{2} \in \mathbb{Z}_{13}[x]$ è irriducibile in $\mathbb{Z}_{13}[x]$.

(iii) Il polinomio $x^2 - \bar{8}x + \bar{2} \in \mathbb{Z}_3[x]$ è irriducibile in $\mathbb{Z}_3[x]$.

(iv) Per ogni primo p, il polinomio $x^2 - \bar{8}x + \bar{2} \in \mathbb{Z}_p[x]$ è irriducibile in $\mathbb{Z}_p[x]$.

(v) Per ogni primo p, il polinomio $x^2 - \bar{8}x + \bar{2} \in \mathbb{Z}_p[x]$ è riducibile in $\mathbb{Z}_p[x]$.

(vi) Il polinomi $g = \bar{3}x^2 - \overline{11}x + \bar{6}$ e $\ell = \bar{7}x^2 + \bar{9}x - \overline{12}$ sono associati in $\mathbb{Z}_{13}[x]$ (utilizzare un'opportuna equazione congruenziale per verificarlo).

Esercizio 6. Se φ, θ e δ sono variabili proposizionali, stabilire se una, entrambe o nessuna delle seguenti è una tautologia:

(i) $\big(\varphi \wedge \neg(\neg\theta \vee \neg\delta)\big) \longleftrightarrow (\varphi \wedge \theta \wedge \delta)$;

(ii) $\big(\varphi \wedge \neg(\neg\theta \vee \neg\delta)\big) \longleftrightarrow (\varphi \wedge (\theta \vee \delta))$.

$^{(\ddagger)}$le cifre sono intese in base 10. In modo esplicito: la 'somma delle cifre' di a è $\sum_{i=0}^{h} c_i$, dove $a = \sum_{i=0}^{h} c_i 10^i$ per un opportuno $h \in \mathbb{N}$ e numeri naturali $c_0, c_1, \ldots, c_h$ minori di 10.

Schema risposte 22/4/2024

- Compilare il file riassuntivo e consegnarlo insieme allo svolgimento completo del compito.
- Verranno valutati solo i compiti consegnati nei tempi previsti e completi di tutte e due le parti.

cognome e nome: Ponte Montone Simone matricola: N86004297

1. (i): SIA A UN INSIEME, ~~$\exists f: E(A) \to$~~ $\exists f: \sim E(A) \mapsto A/\sim$ ($P(A)/A$) BIETTIVA

(ii): 15

(iii): FOGLIO ALLEGATO, PAGINA 1

2. (i): FOGLIO ALLEGATO, PAGINA 2

(ii): SOLO SURIETTIVA, SPIEGAZIONE A PAGINA 2

(iii): PAGINA 2

(iv): PAGINA 3

(v): PAGINA 3

(vi): PAGINA 3

3. (i): SI, SPIEGAZIONE PAG 4

(ii): NON MONOIDE (PAG 6), NON COMMUTATIVO (PAG 4)

(iii): SI, PAGINA 4

4. (i): PAGINA 5

(ii): PAGINA 5

5. (i): SI PER RUFFINI GENERALIZZATO

iii) (ii): SI PERCHÉ UN POLINOMIO IN UN CAMPO $\mathbb{Z}_3$ DI GRADO 2 O 3 È IRRIDUCIBILE $\iff$ NON HA RADICI

ii) (iii): NO PERCHÉ AMMETTE RADICI $\bar{3}$ E $\bar{5}$

(iv): NON VALE PER OGNI PRIMO, VEDI RISPOSTE PRECEDENTI

(v): NON VALE PER OGNI PRIMO, VEDI RISPOSTE PRECEDENTI

(vi): FOGLIO 7

6. (i): SI, PROCEDIMENTO SU FOGLIO A PAG 6

(ii): SI, PROCEDIMENTO SU FOGLIO A PAG 6

ESERCIZIO 1

i) SIA $A \neq \emptyset$, $\exists f : \sim \in EQ(A) \longmapsto A/_\sim \in PART(A)$, f BIETTIVA

ii) $T = \{13, 24, 202, 1104, 110211\}$

$\cancel{PART(T) = \{\{13, 24, 202\}, \{1104, 110211\}\}}$

iii) $\kappa : \forall a, b \in T$

$a \kappa b \iff$ SOMMA CIFRE a = SOMMA CIFRE b

SIA g LA FUNZIONE CHE ASSOCIA AD x ~~IL NUMERO DELLE~~ LA SOMMA DELLE CIFRE DI x

$g(13) = 4$
$g(24) = 6$
$g(202) = 4$
$g(1104) = 6$
$g(110211) = 6$

$T/_\kappa = \{\underbrace{\{13, 202\}}_{r}, \underbrace{\{24, 1104, 110211\}}_{l}\}$

r e l SONO LE CLASSI DI EQUIV.

$r = \{13, 202\}$, $l = \{24, 1104, 110211\}$

ESERCIZIO 2

$f : (a,b) \in \mathbb{N}\times\mathbb{N}^* \longmapsto a^b \in \mathbb{N}$

i) $\overrightarrow{f}(\mathbb{N}\times\mathbb{N}^*) = \mathbb{N}$, PRESI $a \in \mathbb{N}$, $b \in \mathbb{N}^*$, SIA $a = n$, $b = 1$ $\forall n \in \mathbb{N} \longrightarrow n^1 = n$, QUINDI IL CODOMINIO È TOTALMENTE COPERTO

- $\overrightarrow{f}(\emptyset) = \emptyset$,
- $\overleftarrow{f}(\emptyset) = \emptyset$ PERCHÉ OGNI ELEMENTO HA IMMAGINE
- $\overleftarrow{f}(\{1\})$ CIOÈ TUTTE LE COPPIE CHE HANNO 1 COME IMMAGINE, CIOÈ L'INSIEME $\{(1,1)\}$ $\cancel{\cup\{(n,0) \mid n \in \mathbb{N}\}}$
- $\overleftarrow{f}(\{5\}) = \{(5,1)\}$

ii) NON INIETTIVA, $f(5,2) = 25 = f(25,1)$

SURIETTIVA, VEDERE PUNTO i

NON BIETTIVA PERCHÉ NON INIETTIVA

iii) SIA (A,ρ) UN INSIEME ORDINATO, CIOÈ CON $A \neq \emptyset$ E ρ REL. D'ORDINE, (A,ρ) È UN RETICOLO SE

$(\forall a,b \in A)(\exists \inf\{a,b\} \wedge \exists \sup\{a,b\})$

T DEF. IN $\mathbb{N} \times \mathbb{N}^*$, $\forall a, c \in \mathbb{N}, \forall b, d \in \mathbb{N}^*$

$$(a,b)\, T\, (c,d) \iff (a,b) = (c,d) \vee f(a,b) \mid f((c,d))$$

iv) IL MINIMO E UNICO MINIMALE È (1,1), PERCHÉ DIVISORE DI OGNI NATURALE

I MASSIMALI SONO TUTTE LE COPPIE $(0,n) \mid n \in \mathbb{N}^*$, PERCHÉ 0 È MULTIPLO DI TUTTI I NATURALI

NON ESISTE MAX

È UN RETICOLO

$M = \{\overset{a}{(4,1)}, \overset{b}{(2,2)}, \overset{c}{(2,3)}, \overset{d}{(6,2)}, \overset{e}{(4,2)}, \overset{f}{(12,2)}\}$

$f((4,1)) = 4^1 = 4 \cdot a$

$f(2,2) = 2^2 = 4 \cdot b$

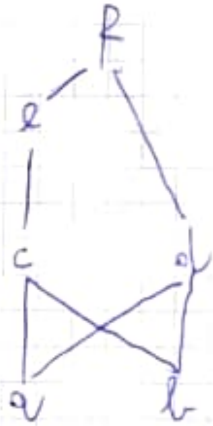
$f((2,3)) = 2^3 = 8 \cdot c$

$f((6,2)) = 6^2 = 36 \quad d$

$f((4,2)) = 4^2 = 16 \cdot e$

$f((12,2)) = 144 \quad f$

v)



vi) NON È UN RETICOLO PERCHÉ $\nexists \inf\{c, d\}$

$M \setminus \{(4,1)\}$ È UN RETICOLO PERCHÉ OGNI EL AMMETTE INF E SUP

NON È DISTRIBUTIVO PERCHÉ È UN PENTAGONALE

~~NON PUÒ ESSERE~~ È COMPLEMENTATO PERCHÉ OGNI EL. HA COMPLEMENTO

4, 144 | 16, 8 | 36, 16 OPPURE 36, 8, I COMPLEMENTI NON DEVONO ESSERE UNICI PERCHÉ NON DISTRIBUTIVO.

NON BOOLEANO PER QUANTO VISTO PRIMA

4

$*: \mathbb{Z}_6$, $\forall a, b \in \mathbb{Z}_6$, $a * b = \bar{3}a + \bar{4}b$

i) UN SEMIGRUPPO È UNA STRUTTURA CON UN'OPERAZIONE ASSOCIATIVA

$(\mathbb{Z}_6, *)$ $*$ ASSOCIATIVA $\Leftrightarrow$

$\forall a, b, c \in \mathbb{Z}_6$ ~~$a * b * c$~~

$$(a * b) * c = a * (b * c)$$
$$(3a + 4b) * c = a * (3b + 4c)$$
$$3(3a + 4b) + 4c = 3a + 4(3b + 4c)$$
$$9a + 12b + 4c = 3a + 12b + 16c \text{ OVVERO}$$
$$3a + 0b + 4c = 3a + 0b + 4c$$

ASSOCIATIVA

ii) MONOIDE $\Leftrightarrow$ AMMETTE NEUTRO SX E DX

PROVO PRIMA COMMUTATIVITÀ

$$a * b = b * a \Leftrightarrow 3a + 4b = 3b + 4a$$

SIANO $a = 1$, $b = 2$

$$3(1) + 4(2) = 3(2) + 4(1)$$
$$3 + 8 = 6 + 4$$
$$11 = 10 \quad \text{NO}$$

~~NEUTRO SX È $\bar{2}$ PERCHÉ $\bar{3} \cdot \bar{2} = 0$~~

~~NEUTRO DX NON È 2 PERCHÉ $4 \cdot 2 = 8 = \bar{2}$~~

~~QUINDI $(\mathbb{Z}_6, *)$ NON È UN MONOIDE~~

iii) IN $(\mathbb{Z}_6, *)$, $\{\bar{0}, \bar{3}\}$ È STABILE?

$0 * 0 = \bar{0}$ V

$0 * 3 = 0 + 12 = 12 = \bar{0}$

$3 * 0 = 9 = \bar{3}$ V

$3 * 3 = 9 + 12 = 21 = 3$ V

ESERCIZIO 4

$P: \forall a,b \in \mathbb{Z},\ a P b \iff a+b$ È DISPARI

i) P DEFINISCE UN GRAFO $\iff$ È ANTIRIFLESSIVA E SIMMETRICA

ANTIRIFLESSIVA PERCHÉ OGNI NUMERO + SÈ STESSO DÀ UN PARI COME RISULTATO

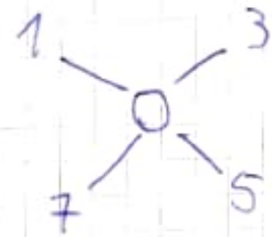
RIFLESSIVA PER COMMUTATIVITÀ DI +

ii) $|S|=5$ E (S,P) ALBERO

ALBERO $\iff$ FORESTA CONNESSA

QUINDI GRAFO CONNESSO SENZA CIRCUITI

$S=\{0,1,3,5,7\}$



ESERCIZIO 5

i) IN $\mathbb{Z}_{13}[x]$ UN POLINOMIO f AMMETTE $\bar{3}$ E $\bar{5}$ RADICI SE E SOLO SE f È MULTIPLO DI $x^2-8x+2 \iff x^2+5x+2$

~~NO, x^2+5x~~ SI, PER ~~RUFFI~~ RUFFINI GENERALIZZATO

$f=(x-3)(x-5) = x^2+5x+2$

iii) ~~DUE POLINOMI SONO ASSOCIATI IN UN CAMPO~~

~~SE~~, SIA f UN POLINOMIO, I SUOI ASSOCIATI (IN UN CAMPO) SONO L'INSIEME $\{uf \mid u \in U(\mathbb{Z}_{13})\}$

$f \wedge \neg(\neg\theta \vee \neg\delta) \Leftrightarrow f \wedge \theta \wedge \delta$

$f \wedge \theta \wedge \delta \Leftrightarrow f \wedge \theta \wedge \delta$

$f \wedge \neg(\neg\theta \vee \neg\delta) \Leftrightarrow (f \wedge (\theta \vee \delta))$

$f \wedge (\neg\neg\theta \vee \neg\neg\delta) \Leftrightarrow f \wedge (\theta \vee \delta)$

ESERCIZIO 3. ...)

NON COMMUTATIVA, VEDI PAG 4

NEUTRO DX

$a * y = a \Leftrightarrow 3a + 4y = a$

~~$4a = 2y$~~ ~~MA 2 NON È CANC. IN Z_6 PERCHÉ DIV. DELLO 0~~

$2a = 2b$

MA 2 NON È CANCELLABILE IN Z_6 PERCHÉ DIV. DELLO 0

NEUTRO SX

$x * b = b \Leftrightarrow 3x + 4y = y \Leftrightarrow$

$3x = y - 4y$

$3x = -5y$

$3x = 1$ CIOÈ SE $3x \equiv_6 1$ HA SOL,

$MCD(3,6) = 3$, $3 \nmid 1 \Rightarrow$ NO SOL $\Rightarrow$

$\nexists$ NEUTRO DX

[illegible]

$3x^2+2x+6 \equiv_{13} 7x^2+9x+1$

$3x^2-7x^2+2x-9x \equiv_{13} 1-6$

$-4x^2-7x \equiv_{13} -7$

$9x^2+6x \equiv_{13} 6$ HA SOL $\Leftrightarrow$ $\cancel{9x^2+6x}$ MCD$(9x^2+6x, 13)$

HA SOL, MA 13 È PRIMO QUINDI MCD È $1 \Rightarrow \exists$ SOL

~~DUE POLINOMI SONO ASSOCIATI IN UN CAMPO~~

GLI ASSOCIATI DI g IN $\mathbb{Z}_{13}$ CAMPO SONO I POLINOMI DEL ~~TIPO~~ $\{ux \mid u \in \mathbb{Z}_{13} \setminus \{\bar{0}\}\}$

U IN QUESTO CASO È 11 PERCHÉ

$3x \equiv_{13} 7$

$13 = 3 \cdot 4 + 1 \mid 1 = 13 + 3[-4] \cdot 7 = \overline{11}$

$6x \equiv_{13} 1$

$13 = 6 \cdot 2 + 1 \mid 1 = 13 + 6[-2] \cdot$ $\overline{11}$

$2x \equiv_{13} 9$

$13 = 2 \cdot 6 + 1 \mid 1 = 13 + 2[-6] \cdot 9 = \overline{11}$