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

Svolgere i seguenti esercizi,

⟶ $\boxed{\textit{giustificando pienamente tutte le risposte.}}$ ⟵

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

Esercizio 1. Scrivere una negazione della formula $\exists y\Big(\forall x\big((\varphi(x)\wedge\psi(y))\to(\psi(y)\to\theta(x))\big)\Big)$ in cui non appaia il connettivo di implicazione (qui φ, ψ e θ sono predicati unari).

Esercizio 2. Dare una definizione di partizione di un insieme ed enunciare il teorema fondamentale su partizioni e relazioni d'equivalenza. Fornire una partizione di $\mathbb{Z}$ di cardinalità 2^{10}.

Esercizio 3. Determinare i numeri naturali n tali che $2^n < n!$. (Suggerimento: può essere utile fare uso del principio di induzione). Per quali insiemi finiti a si ha $|\mathcal{P}(a)| < |\operatorname{Sym}(a)|$?

Esercizio 4. Si consideri l'operazione $*\colon (a,b)\in\mathbb{Z}_{10}\times\mathbb{Z}_{10}\mapsto \bar{6}a+b\in\mathbb{Z}_{10}$.

(*i*) Decidere se $*$ è associativa, se è commutativa, se $(\mathbb{Z}_{10},*)$ ha elementi neutri a sinistra o a destra e, nel caso la domanda abbia senso, quali suoi elementi sono simmetrizzabili. Che tipo di struttura algebrica è $(\mathbb{Z}_{10},*)$?

(*ii*) Siano $P=\{\bar{2}a \mid a\in\mathbb{Z}_{10}\}$ e $D=\mathbb{Z}_{10}\setminus P$. Per ciascuno di P e D decidere se è una parte chiusa rispetto a $*$ e, nel caso, rispondere, per la corrispondente struttura indotta, alle stesse domande poste al punto precedente per $(\mathbb{Z}_{10},*)$.

Esercizio 5.

(*i*) Stabilire quali tra $[2027]_{2024}$, $[1024]_{2024}$, $[-2]_{2024}$ e $[10001!]_{2024}$ sono invertibili in $\mathbb{Z}_{2024}$ e quali sono divisori dello zero.

(*ii*) Calcolare, utilizzando l'algoritmo euclideo, il massimo comun divisore positivo tra 209 e 165 e trovare quindi tutte le soluzioni delle equazioni congruenziali $209x\equiv_{165}14$ e $165x\equiv_{209}44$.

Esercizio 6. Siano F l'insieme delle parti finite non vuote di $\mathbb{N}$ e f l'applicazione $x\in F\mapsto \min x+\max x\in\mathbb{N}$.

(*i*) Spiegare perché f è ben definita come applicazione;

(*ii*) determinare $\overleftarrow{f}(\{2\})$ e $|\overleftarrow{f}(\{2\})|$;

(*iii*) f è iniettiva, suriettiva, biettiva?

(*iv*) Detto σ il nucleo di equivalenza di f, determinare $[\{2\}]_\sigma$.

Sia ora τ la relazione d'ordine in F definita da:

$$\forall x,y\in F\ \big(x\ \tau\ y \iff (x=y\vee f(x)\text{ è un divisore proprio di }f(y))\big).$$

(*v*) Determinare in (F,τ) eventuali elementi minimali, massimali, minimo, massimo. (F,τ) è un reticolo?

(*vi*) Posto $M=\big\{\{1\},\{2\},\{2,3,4\},\{1,3,5,7\},\{5,6,7\},\{9\},\{10,11,15,60,62\}\big\}$, disegnare un diagramma di Hasse di (M,τ), verificare se questo è un reticolo e, nel caso, se è distributivo, complementato, booleano.

(*vii*) Determinare in (M,τ) una catena massimale C ed un sottoreticolo booleano massimale B.

Esercizio 7. Per ogni primo positivo p, si consideri il polinomio $f_p=(\bar{4}x^3+x^2-\bar{2}x-\bar{4})(x+\bar{1})\in\mathbb{Z}_p[x]$.

(*i*) Determinare l'insieme X dei primi p tali che il resto della divisione tra f_p e $x-\bar{2}$ sia $\bar{0}$.

(*ii*) Posto $p=\max X$, decomporre f_p in prodotto di polinomi irriducibili in $\mathbb{Z}_p[x]$.

(*iii*) f_p ha un divisore irriducibile monico di grado 2? In caso di risposta affermativa, dire quanti ne ha ed esibirne almeno uno.

1) $\forall y \, (\exists x \, (f(x) \wedge \varphi(y)) \wedge (\psi(y) \wedge \neg \theta(x)))$

2) DATO A INSIEME FINITO, UNA PARTIZIONE B DI A È:

- $\forall x \in B, \; x \neq \emptyset$
- $\forall x, y \in B, \; x \neq y \Rightarrow x \cap y = \emptyset$
- $\bigcup B = A$

3) $n \geq 4$

CASO BASE $2^n < n!$

$$16 = 2^4 < 4! = 24$$

PASSO INDUTTIVO

$$2^{n+1} < (n+1)! \qquad 2^n < n!$$

$$2^n \cdot 2 < (n+1) \cdot n! \qquad (n+1) > 2 \quad \checkmark$$

PER QUALI INSIEMI a SI HA $|P(a)| < Sym(a)$?

4) i)

ASSOCIATIVA

NON COMMUTATIVA

NEUTRO SX $\bar{0}$ E $\bar{5}$

NEUTRO DX NON ESISTE

NEUTRO NON ESISTE

NON ESISTONO SIMMETR.

SEMIGRUPPO

ii) ENTRAMBE PARTI CHIUSE

$\star$ ASSOCIATIVA (EREDITATA)

$\star$ COMMUTATIVA IN ENTRAMBE

SIMMETRIZZABILI

$(P, \star)$	$(D, \star)$
OGNI EL. SIMMETRIZZABILE $(P, \star)$ GRUPPO ABELIANO	

$\bar{2}a \star \bar{2}b = \bar{0}$

$\bar{2}a + \bar{2}b = \bar{0}$

$\bar{2}a = -\bar{2}b$

5) i) $[2027]_{2024} = \overline{3}_{2024}$ COPRIMI $\not\Rightarrow$ 2027 INVERT

1024 DIVISIBILE DA 2

$10001! \equiv_{2024} 0$

DIVISORI DELLO 0 : 1024, -2, 10001!

ii) $-2 \cdot \overline{1012} = \overline{2024} = \overline{0}$

$MCD(209, 165) = \pm 11$

$209x \equiv_{165} 14$

$11 \nmid 14$ NO SOLUZIONE

$\overline{165}\, x \equiv_{209} \overline{44}$ DIVIDO PER 11

$\overline{15}\, x \equiv_{19} \overline{4} \iff x \equiv_{19} 18$

6) R BEN DEFINITA

- OGNI PARTE DI $\mathbb{N}$ NON VUOTA AMMETTE min, PERCHÉ $\mathbb{N}$ BEN ORDINATO

- OGNI PARTE FINITA DI $\mathbb{N}$ AMMETTE MAX ESSENDO PER DEF. LIMITATA
- $\mathbb{N}$ SUP ILLIMIT. QUINDI $\min X$ + $\max X \in \mathbb{N}$

ii) $\overleftarrow{f}(\{2\}) = \{\{1\}, \{0, 2\}, \{0, 1, 2\}\}$

$|\overleftarrow{f}(\{2\})| = 3$

iii) NON INIETTIVA MA SURIETTIVA

iv) NUCLEO DI EQUIV | $[\{2\}]_\sigma$

$[\{2\}]_\sigma = \{x \in F \mid f(x) = 4\} =$

$\min \neq 3$, $\max \leq 4$

$\{\{0, 4\}, \{0, 1, 4\}, \{0, 2, 4\} \dots \{1, \dots, 3\}, \{2\}, etc\}$

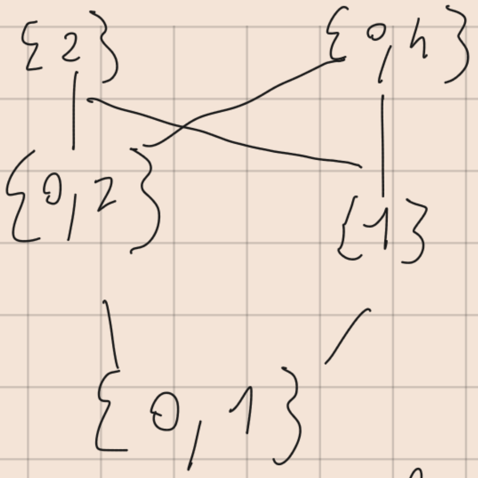
v) RIFLESSIVA PER $x = y$

$\min = \{0, 1\}$ MINIMALE, $\max = \{0\}$ MASSIMALE

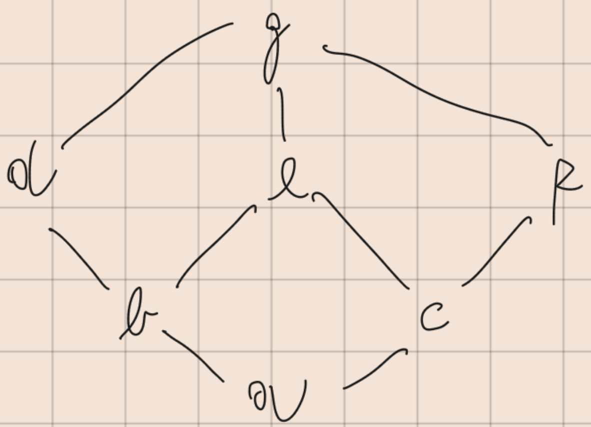
UNICI

NON È UN RETICOLO

PRENDO $\{2\}$ E $\{0, 4\}$ NON CONFRONTABILI TRA LORO



vi) $\{ \overset{a\;2}{\{1\}}, \overset{b\;4}{\{2\}}, \overset{c\;6}{\{2,3,4\}}, \overset{d\;8}{\{1,3,5,7\}}, \overset{e\;12}{\{5,6,7\}}, \overset{f\;18}{\{9\}}, \overset{g}{\underset{72}{\{9,11,15,60,62\}}} \}$



SUP E INF A 2 A 2 SI

DISTRIBUTIVO? NON PUÒ ESSERLO (e NON HA COMPL.)

$\Rightarrow$ NON BOOLEANO

7)

i) $x = \{2, 3, 7\}$ rotto $84 = 2 \cdot 2 \cdot 3 \cdot 7$

METODO SEMPLICE CON RUFFINI

ALTRIMENTI CON DIVISIONE LUNGA

ii) $p = 7$

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

iii) DIV IRRID. DI GRADO 2?

NO, SONO DI GRADO 1