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

Svolgere i seguenti esercizi,

$\longrightarrow$ ***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. (*i*) È vero che vale la proprietà distributiva dell'intersezione rispetto alla differenza simmetrica? Se sì, dimostrarlo; se no, fornire un controesempio.

(*ii*) È vero che vale la proprietà distributiva dell'unione rispetto alla differenza simmetrica? Se sì, dimostrarlo; se no, fornire un controesempio.

(*iii*) Sia S un insieme e sia definita la seguente operazione binaria interna su $\mathcal{P}(S)$

$$\overline{\Delta} : (a,b) \in \mathcal{P}(S) \times \mathcal{P}(S) \mapsto (a \cap b) \cup \big((S \smallsetminus a) \cap (S \smallsetminus b)\big) \in \mathcal{P}(S).$$

Dare la definizione di anello booleano e stabilire se la terna $(\mathcal{P}(S), \overline{\Delta}, \cup)$ è o meno un anello booleano.

(*iv*) $(\mathcal{P}(S), \cap, \Delta)$ è un anello booleano? Se sì, a partire da questo, costruire un'algebra di Boole dopo averne dato la definizione.

Esercizio 2. Sia $T = \mathbb{N} \smallsetminus \{0,1\}$ e si consideri l'applicazione $f\colon T \to \mathbb{N}$ che ad ogni $a \in T$ associa il massimo degli esponenti nella decomposizione di a come prodotto di primi distinti, cioè il numero $f(a)$ così definito: scritto a come $\prod_{i=1}^{t} p_i^{\alpha_i}$, dove $t \in \mathbb{N}^{\#} = \mathbb{N} \smallsetminus \{0\}$, $p_1, p_2, \dots, p_t$ sono interi primi positivi a due a due distinti e $\alpha_i \in \mathbb{N}^{\#}$ per ogni $i \in \{1, 2, \dots, t\}$, poniamo $f(a) = \max\{\alpha_1, \alpha_2, \dots, \alpha_t\}$.

(*i*) Determinare $\overleftarrow{f}(\{0\})$, $\overleftarrow{f}(\{3\})$, $\overrightarrow{f}(\{3\})$;

(*ii*) f è iniettiva? f è suriettiva? f è biettiva?

Si consideri la relazione d'ordine σ definita in T da:

$$\forall a, b \in T\ \big(a\ \sigma\ b \iff (a = b \vee f(a) < f(b))\big).$$

(*iii*) Determinare eventuali minimo, massimo, elementi minimali e massimali in (T, σ);

(*iv*) determinare, se esistono, minoranti ed estremo inferiore in (T, σ) di ciascuno degli insiemi $R = \{8\}$, $S = \{54\}$ e $U = \{8, 54\}$;

(*v*) posto $L = \{12, 16, 18, 70, 243, 10000\}$, disegnare il diagramma di Hasse di (L, σ) e decidere se (L, σ) e $(L \smallsetminus \{12\}, \sigma)$ sono o non sono reticoli.

Esercizio 3. In $\mathbb{Z}_{10}$, si consideri l'operazione binaria $*$ definita da: $\forall a, b \in \mathbb{Z}_{10}\ (a * b = \bar{5}ab + a + b)$. Dando per noto che $(\mathbb{Z}_{10}, *)$ è un semigruppo commutativo,

(*i*) $(\mathbb{Z}_{10}, *)$ ha elemento neutro?

(*ii*) Determinare, se ne esistono, tutti gli elementi b di $\mathbb{Z}_{10}$ tali che $\bar{3} * b = \bar{5}$.

(*iii*) Determinare gli elementi idempotenti in $(\mathbb{Z}_{10}, *)$.

Esercizio 4. Dopo aver calcolato i quadrati degli elementi di $\mathbb{Z}_{11}$,

(*i*) determinare gli insiemi $A = \{a \in \mathbb{Z}_{11} \mid x^2 - a$ è irriducibile in $\mathbb{Z}_{11}[x]\}$ e
$B = \{b \in \mathbb{Z}_{11} \mid x^2 - b$ è riducibile in $\mathbb{Z}_{11}[x]\}$;

(*ii*) determinare le coppie di elementi $a, b \in \mathbb{Z}_{11}$ tali che, in $\mathbb{Z}_{11}[x]$, il polinomio $g_{a,b} = (x^2 - a)(x^2 - b)$ …
- (a) … sia irriducibile;
- (b) … sia riducibile;
- (c) … sia il prodotto di un polinomio di primo grado per uno di terzo grado;
- (d) … sia il prodotto di quattro polinomi di primo grado.

(*iii*) decomporre il polinomio $x^4 - \bar{7}x^2 - \bar{1}$ nel prodotto di polinomi irriducibili in $\mathbb{Z}_{11}[x]$.

Esercizio 5. Sia E l'insieme delle relazioni di equivalenza in $\mathbb{N}$. Vero o falso (e, come sempre, perché?):

(*i*) $\forall \alpha \in E\big(\forall n \in \mathbb{N}\,(\exists c \in (\mathbb{N}/\alpha)(n \in c))\big)$.

(*ii*) $\forall \alpha \in E\big(\forall c \in (\mathbb{N}/\alpha)\,(\exists n \in \mathbb{N}(n \in c))\big)$.

(*iii*) $\forall \alpha \in E\big(\forall n \in \mathbb{N}\,(\exists! c \in (\mathbb{N}/\alpha)(n \in c))\big)$.

(*iv*) $\forall \alpha \in E\big(\forall c \in (\mathbb{N}/\alpha)\,(\exists! n \in \mathbb{N}(n \in c))\big)$.

(*v*) $\forall \alpha, \beta \in E\big(\exists c \in (\mathbb{N}/\alpha)\,((\exists d \in (\mathbb{N}/\beta)\,(c \cap d \neq \varnothing))\big)$.

1) Bisogna dimostrare con insiemi e non con Venn

$a \cup (b \Delta c) \neq (a \cup b) \Delta (a \cup c)$ $\quad a = \{1\}, b = \{2\}, c = \{3\}$

ed 1 è presente solo a sx

iii) $a \bar{\Delta} b = (a \cap b) \cup ((S \setminus a) \cap (S \setminus b))$ $\quad (P(S), \bar{\Delta}, \cup)$

$f : x \in P(S) \mapsto S \setminus x \in P(S)$

è un isomorfismo tra $(P(S), \bar{\Delta}, \cup)$ e $(P(S), \Delta, \cap)$

$f(a \bar{\Delta} b) = S \setminus ((a \cap b) \cup ((S \setminus a) \cap (S \setminus b))) =$

$= S \setminus (a \cap b) \cap (S \setminus ((S \setminus a) \cap (S \setminus b))) = a \Delta b$

2) $\overleftarrow{f}(\{0\}) = \emptyset$

$\overleftarrow{f}(\{3\}) =$ tutti i numeri che hanno una pot di 3 tipo 24, 8

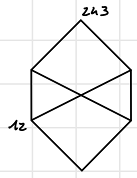
$\overrightarrow{f}(\{3\}) = \{1\}$

$\forall a, b \in T \ (a \,\sigma\, b \iff a = b \vee \underline{f(a) < f(b)})$

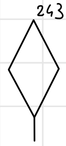
$\rightarrow$ Prodotti di primi distinti (es. 6)

$\{8\}$ è un minorante di se stesso, idem con $\{54\}$

$\{54, 8\}$ minoranti sono tutti quelli con esponenti ≥ 2



senza 12:



$\bar{p} = \max_{p \in P} (p \mid n) \quad f(n) < f(\bar{p} n)$

non è un reticolo

3) $a * b = \bar{5}ab + a + b$ $\qquad \mathbb{Z}_{10}$

E.N $= 0$

$\bar{3} * b = \bar{5} : \bar{5}b + \bar{3} + b \iff \bar{6}b \equiv_{10} \bar{2} \iff 3b \equiv_5 1 \iff b \equiv_5 2$

quindi $\bar{2}$ e $\bar{7}$

$a = a * a = \bar{5}a^2 + \bar{2}a \iff \bar{5}a^2 + a = \bar{0} \iff a(\bar{5}a + 1) = \bar{0}$

deve essere un multiplo di 5, quindi 5 o 0

non possono essere multipli di 5, per forza devono essere multipli di 2

4) I quadrati di $\mathbb{Z}_{11}$: $\{0, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{9}\} = B$

A $x^2 - a$ irriducibile
B $x^2 - b$ riducibile

$A = \mathbb{Z}_{11} \setminus B$

$g_{a,b} = (x^2 - a)(x^2 - b)$ non ha solo divisori banali, quindi sempre riducibile

c: $1 \cdot 3$ $\quad a \in B \vee b \in B$

d: $\quad a \in B \wedge b \in B$

5) i) $\forall \alpha \in E\,(\forall n \in \mathbb{N}\,(\exists c \in (\mathbb{N}/\alpha)(n \in c)))$

Si, qualunque elemento di N ha una classe di equivalenza

iii) $\forall \alpha \in E\,(\forall n \in \mathbb{N}\,(\exists! c \in (\mathbb{N}/\alpha)(n \in c)))$

è vero

v) $\forall \alpha, \beta \in E\,(\exists c \in (\mathbb{N}/\alpha)((\exists d \in (\mathbb{N}/\beta)(c \cap d \neq \emptyset)))$

è ovvio $\qquad [1]_\alpha \cap [1]_\beta \neq \emptyset$

Domande Orali

CHIESTO A TUTTI

- Induzione II forma con DIM
  - perchè y ha un minimo (è un insieme ben ordinato)
- Differenza tra buon ordine e ordine totale
- Perchè buon ordine → ordine totale
- Defi. a parole dei polinomi e costruire l'anello dei polinomi
  ↳ Una successione che ad un certo punto diventa 0
- Teorema fondamentale dell'aritmetica
- Divisione Lunga tra polinomi
- Def. di fattoriale
- Coefficiente binomiale
- Dimostrare che $\sum_{k=0}^{n} \binom{n}{k} = 2^n$
- Da anello booleano a reticolo booleano
- Ogni sottoinsieme ha una propria funzione caratteristica
- Teorema di isomorfismo tra insiemi
- Definire la congruenza
- Congruenza modulo n
- Definizione di $\mathbb{Z}_m$
- Chi è $\mathbb{Z}_0$