CORSO DI LAUREA TRIENNALE IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II E III)
4 MARZO 2022

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*) Se φ e θ sono formule, $(\exists x)(\varphi \vee \theta)$ equivale alla negazione di $(\forall x)((\neg\varphi) \vee (\neg\theta))$?
(*ii*) Siano $a, b, c \in \mathbb{Z}$. Quando, per definizione, c è un minimo comune multiplo tra a e b in $\mathbb{Z}$?

Esercizio 2. Si consideri l'applicazione $f\colon (x, y) \in \mathbb{Z} \times \mathbb{Z} \mapsto |x - y| \in \mathbb{N}$.
(*i*) f è iniettiva? f è suriettiva?
(*ii*) Descrivere $\overleftarrow{f}(\{0\})$ e $\overleftarrow{f}(\varnothing)$.
Indicato con σ il nucleo di equivalenza di f,
(*iii*) per ogni $n \in \mathbb{N}$, descrivere $[(0, n)]_\sigma$ e $\big[(0, n)\big]_\sigma \cap \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a = 0 \vee b = 0\}$;
(*iv*) verificare: $(\forall a, b \in \mathbb{Z})\big((\exists! n \in \mathbb{N})([(a, b)]_\sigma = [(n, 0)]_\sigma)\big)$.
Sia ora $S = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid |a - b| > 1\}$ e sia ρ la relazione d'ordine definita in S da: per ogni $(a, b), (c, d) \in S$[‡]

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

(*v*) La relazione ρ è totale?
(*vi*) Determinare in (S, ρ) eventuali minimo, massimo, elementi minimali, elementi massimali.
(*vii*) (S, ρ) è un reticolo?
Sia poi $T = \{-2, 4, 8, -16, 12, 36, -144, 288\} \times \{0\} \subseteq S$.
(*viii*) Disegnare il diagramma di Hasse di (T, ρ);
(*ix*) (T, ρ) è un reticolo? Nel caso, è distributivo? Complementato? Booleano?

Esercizio 3. In $\mathbb{R}_0^+ = \{r \in \mathbb{R} \mid r \geq 0\}$ si consideri l'operazione binaria $*$ ponendo per ogni $a, b \in \mathbb{R}_0^+$, $a * b = \max\{a, b\}$, dove il massimo è inteso rispetto all'ordinamento usuale dei numeri reali.
(*i*) Decidere se $*$ è commutativa e se è associativa.
(*ii*) $\mathbb{N}$ è una parte chiusa di $(\mathbb{R}_0^+, *)$? L'intervallo reale semiaperto $[0, 1[$ è una parte chiusa di $(\mathbb{R}_0^+, *)$?
(*iii*) Verificare se in $(\mathbb{R}_0^+, *)$ esistono elementi neutri a destra, neutri a sinistra, neutri.
(*iv*) Determinare in $(\mathbb{R}_0^+, *)$ gli elementi cancellabili e, se la domanda ha senso, quelli simmetrizzabili. Che tipo di struttura (semigruppo, monoide, gruppo) è $(\mathbb{R}_0^+, *)$?
(*v*) Stabilire se l'operazione indotta in $(\mathbb{R}_0^+, *)$ dall'ordinaria moltiplicazione tra numeri reali è distributiva rispetto a $*$.
(*vi*) Di quale costruzione teorica generale studiata nel corso la definizione di $*$ è un esempio?
(*vii*) Se ridefinissimo $*$ come operazione in $\mathbb{R}$ anziché in $\mathbb{R}_0^+$ (ponendo comunque $a * b = \max\{a, b\}$ per ogni $a, b \in \mathbb{R}$), cambierebbe qualcosa nelle risposte alle domande precedenti?

Esercizio 4. Esiste un numero intero u tale che $81u - 1$ sia multiplo di 23? Nel caso, trovarne uno.

Esercizio 5. Per ogni numero naturale $n > 1$, denotiamo con f_n il polinomio $\bar{7}x^3 + \bar{3}x^2 + x + \bar{1} \in \mathbb{Z}_n[x]$.
(*i*) Determinare l'insieme N_1 dei numeri naturali $n > 1$ tali che f_n sia monico.
(*ii*) Determinare l'insieme N_2 dei numeri naturali $n > 1$ tali che f_n abbia grado 2.
(*iii*) Determinare l'insieme N_3 dei numeri naturali $n > 1$ tali che f_n abbia grado 1.
(*iv*) Enunciare la formula (o regola) di addizione dei gradi e determinare, al variare di n in $N_1 \cup N_2 \cup N_3$, tutti i polinomi g di $\mathbb{Z}_n$ tali che per f e g valga la formula di addizione dei gradi.
(*v*) Per quali $n \in N_1 \cup N_2 \cup N_3$ il polinomio f_n è cancellabile in $\mathbb{Z}_n[x]$?

[‡]il simbolo '$\longleftrightarrow$', esattamente come '$\iff$', indica il connettivo bicondizionale

Es 1

$\exists x(\varphi \vee \theta)$ i) NO, la negazione $\exists x(\varphi \vee \theta)$ è $\forall x(\neg\varphi \wedge \neg\theta)$

ii) $a, b, c \in \mathbb{Z}$ c è mcm tra a e b se $a|c \wedge b|c$ e $\forall d\,(a|d \wedge b|d \Rightarrow c|d)$

Es 2

$f: (x,y) \in \mathbb{Z} \times \mathbb{Z} \mapsto |x-y| \in \mathbb{N}$

i) INIETTIVA: NO

$\forall a, b \in \mathbb{Z} \times \mathbb{Z}\ (f(a) = f(b) \Rightarrow a = b)$

NO, $a = (1,0)$ $b = (2,1)$

$f(a) = 1$ $f(b) = 1$ $a \neq b$

SURIETTIVA: SI

$\forall c \in \mathbb{N}\ \exists a \in \mathbb{Z} \times \mathbb{Z}\ (c = f(a))$

è vero, ad esempio le coppie $(x, 0)$ allora $x \in \mathbb{Z}$

ii) $\overleftarrow{f}(\{0\}) = \{(x,x) \mid x \in \mathbb{Z}\}$

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

σ nucleo di equiv. di f

iii) $\forall n \in \mathbb{N}$ $[(0,n)]_\sigma =$ è l'insieme di tutte le coppie il cui f è n
secondo = // perchè si prende il valore assoluto.

iv) $(\forall a, b \in \mathbb{Z})(\exists!\, n \in \mathbb{N})([(a,b)]_\sigma = [(n,0)]_\sigma$
è uno perchè $|a-b|$ è un valore unico, $f(n,0) = |n-0| = n$, quindi sono equivalenti

$S = \{(a,b) \in \mathbb{Z} \times \mathbb{Z} \mid |a-b| > 1\}$

$\rho : \forall (a,b),(c,b) \in S \ \big((a,b)\,\rho\,(c,b) \longleftrightarrow \big((a,b)=(c,d) \vee |a-b| \mid |c-d| \big)\big)$

↳ in teoria chiede: div propri, dovrei togliere se stesso, ma le coppie possono essere uguali, quindi se stesso soddisfa comunque la rel.

v) Totale : NO

$\forall x,y \in S \quad x \rho y \vee y \rho x$,

$x=(3,1) \quad y=(4,1) \qquad 2 \nmid 3 \vee 3 \nmid 2$,

non sono confrontabili.

vi) massimo e massimali non ci sono

minimali : $\{(x,y) \mid |x-y| \text{ è primo}\}$

minimo : non c'è

vii) RETICOLO : NO

No, non esiste l'inf per tutte le coppie. $(a,b) : |a-b| = 2$

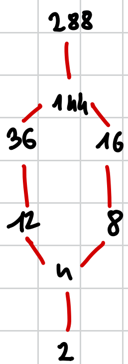
$(c,d) : |c-d| = 3$

queste due coppie non hanno inf.

$T = \{-2, 4, 8, -16, 12, 36, -144, 288\} \times \{0\} \subseteq S$

possiamo considerare ρ la relazione divide, e le coppie $(x,0) \in T$ con $|x|$

viii)



1x) RETICOLO: SI

Distributivo: SI

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$$

$$12 \wedge (36 \vee 16) = (12 \wedge 36) \vee (12 \wedge 16)$$

$$12 \wedge 144 = 12 \vee 4$$

$$12 = 12$$

COMPLEMENTATO: NO

ESERCIZIO 3

$\mathbb{R}_0^+$ $\quad * : \forall a, b \in \mathbb{R}_0^+ \left(a * b = \max\{a, b\} \right)$

i) commutativa: SI
$\forall a, b \in \mathbb{R}_0^+ (a * b = b * a)$, è vero, il max di due numeri non dipende dall'ordinamento.

associativa: SI
$\forall a, b, c \; ((a * b) * c = a * (b * c))$ è vero, è il max tra 3 numeri

ii) $\mathbb{N}$ è chiusa, il max di $x, y \in \mathbb{N}$ è $x \vee y$, entrambi in $\mathbb{N}$

$[0, 1[: \{x \in \mathbb{R}_0^+ \mid 0 \leq x < 1\}$, ed è sempre chiusa

iii) NEUTRO: 0 essendo commut. considero solo quello a sx

$\forall x \in \mathbb{R}_0^+ (x * \varepsilon = x)$

neutro è 0

VI) Cancellabili: NO

$\forall b,c\ (a*b = a*c \Rightarrow b=c)$

$3*2 = 3*1 \Rightarrow 2=1$ Falso.
V F

Simmetrizzabili: $\{0\}$

$a*\bar{a} = 0$ solo 0 con se stesso

MONOIDE COMMUTATIVO

V) · è distributiva rispetto $*$

$(a*b)\cdot c = (a\cdot c)*(b\cdot c)$

$a=1$
$b=2$
$c=3$

$2\cdot 3 = 3 * 6$

$6 = 6$

Sì, perché $(a*b)\cdot c$ moltiplica il max(a,b) con c, mentre $(a\cdot c)*(b\cdot c)$ moltiplica prima entrambi i valori con c e poi ne fa il max.

$a<b \Rightarrow ac<bc$

VI) ??

VII) Sì, non ci sarebbe più il neutro, sarebbe un semigruppo commut. e non un monoide commutativo.

Esercizio 4

$$81u - 1 \equiv_{23} 0$$

$\overline{12}\, u \equiv_{23} 1$

$MCD(12, 23) = 1$

$1 \mid 1$

$23 = 12 \cdot 1 + 11$

$12 = 11 \cdot 1 + 1$

$\overline{2} \cdot \overline{12}\, u \equiv_{23} \overline{1} \cdot \overline{2}$

$\overline{24}\, u \equiv_{23} \overline{2}$

$\overline{1}\, u \equiv_{23} \overline{2}$

$u = \overline{2}$

$1 = 12 + 11(-1) =$

$= 12 + (23 + 12(-1))(-1) =$

$= 12 + 23(-1) + 12(1) =$

$= 12(2) + 23(-1)$