

CORSO DI LAUREA TRIENNALE IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I E II)
16 GENNAIO 2019

Svolgere i seguenti esercizi,



giustificando pienamente tutte le risposte.



Sui fogli consegnati vanno indicati: **nome, cognome, matricola, gruppo di appartenenza**. Chi ha superato la **prova in itinere**, e sceglie di avvalersene, è esentato dai primi due esercizi ma deve **specificare anche questa scelta** sui fogli consegnati.

Non è necessario consegnare la traccia.

solo per chi non usufruisce del superamento della prova in itinere

Esercizio 1. Di ciascuna delle applicazioni $f: x \in \mathbb{Z} \mapsto \{x, -x\} \in \mathcal{P}(\mathbb{Z})$ e $g: X \in \mathcal{P}(\mathbb{Z}) \mapsto X \cap \{1, 2\} \in \mathcal{P}(\{1, 2\})$ si dica se è iniettiva e se è suriettiva. Si descriva poi esplicitamente $g \circ f$ e si elenchino gli elementi di $W := \{x \in \mathbb{Z} \mid (g \circ f)(x) \neq \emptyset\}$.

Esercizio 2. In $S = \mathbb{Q} \times \mathbb{Q}^*$ si definisca l'operazione binaria $*$ ponendo, per ogni $(a, b), (c, d) \in S$,
$$(a, b) * (c, d) = (a + c + 1, 3bd).$$

Sapendo che $*$ è associativa e commutativa,

- (i) decidere se $*$ ammette elemento neutro e, nel caso, quali elementi di S siano simmetrizzabili e quali cancellabili rispetto a $*$. Che tipo di struttura (semigruppato, monoide, gruppo) è $(S, *)$?
- (ii) $T := \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ è chiusa rispetto a $*$? Nel caso lo sia, che tipo di struttura è $(T, *)$?

Esercizio 3. Consideriamo la relazione di binaria \mathcal{R} definita in \mathbb{Q} da: $\forall a, b \in \mathbb{Q}$

$$a \mathcal{R} b \iff (\exists z \in \mathbb{Z})(a = b + z).$$

- (i) Provare che \mathcal{R} è una relazione di equivalenza;
- (ii) descrivere $[0]_{\mathcal{R}}$, $[3]_{\mathcal{R}}$ e $[1/2]_{\mathcal{R}}$.

Esercizio 4. Dare la definizione di *partizione*. Posto $A = \{1, 2, 3, 4, 5\}$ e $\mathcal{F} = \{\{1, 3\}, \{2, 4\}, \{5\}\}$,

- (i) decidere se \mathcal{F} è una partizione di A .
- (ii) Esiste una relazione di equivalenza \sim in A tale che $A/\sim = \mathcal{F}$? Se esiste, descriverne una elencando le coppie del suo grafico.
- (iii) Quante sono le partizioni \mathcal{V} di A tali che $|\mathcal{V}| = 2$?

Esercizio 5. Decomporre $f = x^4 - \bar{4} \in \mathbb{Z}_5[x]$ come prodotto di polinomi monici irriducibili in $\mathbb{Z}_5[x]$.

- (i) In $\mathbb{Z}_5[x]$, f ha fattori irriducibili di grado 3?
- (ii) In generale, se un polinomio di grado 4 a coefficienti in un campo è privo di radici, questo polinomio può avere un fattore di grado 3?
- (iii) Quanti sono i polinomi di grado 5 in $\mathbb{Z}_5[x]$ che hanno sia $\bar{1}$ che $\bar{2}$ come radici?

Esercizio 6. Si definisca in \mathbb{Z} la relazione binaria ρ ponendo, per ogni $a, b \in \mathbb{Z}$,

$$a \rho b \iff (a \leq b \wedge a|b).$$

- (i) Verificare che ρ è una relazione d'ordine. È totale?
- (ii) In (\mathbb{Z}, ρ) , 1 è minimo? 1 è minimale?
- (iii) In (\mathbb{Z}, ρ) , 0 è massimo? 0 è massimale?
- (iv) Sempre con riferimento a ρ , descrivere $X_2 = \{n \in \mathbb{Z} \mid n \text{ è confrontabile con } -2\}$.
- (v) In (\mathbb{Z}, ρ) , -2 è massimale? -2 è minimale?
- (vi) Più in generale, rispondere alle stesse domande in (iv) e (v) sostituendo 2 con un arbitrario primo positivo p .
- (vii) (\mathbb{Z}, ρ) è un reticolo?
- (viii) Posto $Y = \{-2, 2, 4, 6, 8, 24\}$, disegnare il diagramma di Hasse di (Y, ρ) e decidere se (Y, ρ) è un reticolo, un reticolo distributivo, un reticolo complementato.

Esercizio 7. In \mathbb{Z}_{72} , stabilire quali tra $[7]_{72}$ e $[27]_{72}$ sono invertibili, trovandone poi gli inversi utilizzando l'algoritmo euclideo.