

CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II, RECUPERO)
22 MARZO 2017

Svolgere i seguenti esercizi,

giustificando pienamente tutte le risposte.

Sui fogli consegnati vanno indicati: *nome, cognome, matricola e gruppo di appartenenza (I, II o recupero)*. **Non è necessario consegnare la traccia.**

Esercizio 1. Dare la definizione di *polinomio irriducibile* a coefficienti in un campo.

Il polinomio $f = (x^2 + 1)(x^2 + 2)$ è irriducibile in $\mathbb{Q}[x]$?

Esercizio 2. Dati $S = \{1, 2, 3, 4, 5\}$ e $T = \{1, 2, 3\}$, si determini il numero delle applicazioni costanti da S a T , quello delle applicazioni iniettive da S a T , quello delle applicazioni iniettive da T a S .

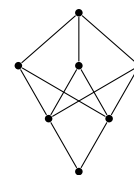
Esercizio 3. Si considerino l'applicazione $f: (x, y) \in \mathbb{Z} \times \mathbb{Z} \mapsto xy + 1 \in \mathbb{Z}$ ed il suo nucleo di equivalenza \sim .

- (i) f è iniettiva?
- (ii) f è suriettiva?
- (iii) Determinare le coppie $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ tali che $|(x, y)_{\sim}| = 2$ e quelle tali che $|(x, y)_{\sim}| = 4$.
- (iv) Descrivere in modo esplicito $|(0, 7)_{\sim}|$.
- (v) Provare che, per ogni $n \in \mathbb{Z} \setminus \{0\}$ si ha: $(\forall m \in \mathbb{Z})((1, m) \in |(1, n)_{\sim}| \iff n = m)$.
 Determinare quindi un sottoinsieme A di $\mathbb{Z} \times \mathbb{Z}$ tale che l'applicazione $g: (x, y) \in A \mapsto xy + 1 \in \mathbb{Z}$ sia biettiva, calcolandone poi l'inversa.

Sia ora σ la relazione d'ordine definita in $\mathbb{Z} \times \mathbb{Z}$ da: $\forall a, b \in \mathbb{Z} \times \mathbb{Z}$

$$a \sigma b \iff (a = b \vee f(a) < f(b)).$$

- (vi) Si determinino in $(\mathbb{Z} \times \mathbb{Z}, \sigma)$ gli eventuali elementi minimali, massimali, minimo, massimo.
- (vii) $(\mathbb{Z} \times \mathbb{Z}, \sigma)$ è totalmente ordinato?
- (viii) Si determini una parte X di $\mathbb{Z} \times \mathbb{Z}$ tale che (X, σ) sia rappresentata dal diagramma di Hasse disegnato a destra.
- (ix) (X, σ) è un reticolo?
- (x) Esiste $a \in X$ tale che $(X \setminus \{a\}, \sigma)$ sia un reticolo? Nel caso, indicare un tale a .



Esercizio 4. Si definiscano le due operazioni binarie \oplus e \circ in \mathbb{Z}_{23} ponendo, per ogni $a, b \in \mathbb{Z}_{23}$:

$$a \oplus b = a + b + \bar{1}; \quad a \circ b = ab + a + b.$$

- (i) Verificare che $(\mathbb{Z}_{23}, \oplus, \circ)$ è un anello commutativo unitario.
- (ii) Determinarne gli elementi invertibili. $(\mathbb{Z}_{23}, \oplus, \circ)$ è un campo?
- (iii) Se possibile, calcolare l'inverso di $\bar{6}$ in $(\mathbb{Z}_{23}, \oplus, \circ)$.
- (iv) Sia $V = \{-\bar{2}, \bar{0}\} \subseteq \mathbb{Z}_{23}$. V è una parte chiusa in (\mathbb{Z}_{23}, \circ) ? V è un sottoanello di $(\mathbb{Z}_{23}, \oplus, \circ)$?

Esercizio 5.

- (i) Verificare che ogni polinomio $f \in \mathbb{Z}_5[x]$ che ammetta $\bar{2}$ e $\bar{4}$ come radici è divisibile per $x^2 - x + \bar{3}$.
- (ii) Scrivere tutti i polinomi in $\mathbb{Z}_5[x]$ che siano di grado 4, prodotto di quattro polinomi monici irriducibili e che ammettano come radici solo $\bar{2}$ e $\bar{4}$. Quanti sono questi polinomi?