

CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II, RECUPERO)
16 NOVEMBRE 2015

Svolgere i seguenti esercizi, *giustificando pienamente tutte le risposte*. Sui fogli consegnati vanno indicati: *nome, cognome, matricola e gruppo di appartenenza*. Non è necessario consegnare la traccia.

Esercizio 1. Si diano le definizioni di *applicazione iniettiva* e di *applicazione suriettiva*. Posto $X = \{n \in \mathbb{N} \mid n < 10\}$, si fornisca (o si spieghi perché non esiste) un esempio di:

- (i) un'applicazione iniettiva non suriettiva $f: \mathbb{N} \rightarrow \mathbb{N}$;
- (ii) un'applicazione suriettiva non iniettiva $g: \mathbb{N} \rightarrow \mathbb{N}$;
- (iii) un'applicazione iniettiva non suriettiva $h: X \rightarrow X$;
- (iv) un'applicazione suriettiva non iniettiva $k: X \rightarrow X$.

Esercizio 2.

(i) Si disegni il diagramma di Hasse dell'insieme $\{n \in \mathbb{N} \mid n < 9\}$ ordinato per divisibilità. Considerata la relazione d'ordine σ definita in \mathbb{Z} ponendo, per ogni $a, b \in \mathbb{Z}$,

$$a \sigma b \iff (a = b \text{ oppure } \text{rest}(a, 9) \text{ è un divisore proprio di } \text{rest}(b, 9)),$$

- (ii) determinare gli (eventuali) elementi minimali, massimali, minimo, massimo in (\mathbb{Z}, σ) ;
- (iii) stabilire se (\mathbb{Z}, σ) è un reticolo;
- (iv) decidere se in (\mathbb{Z}, σ) esiste una catena infinita.

Sia $A = \{2, 5, 10, 13, 18, 20, 22, 40, 50\}$.

- (v) Disegnare il diagramma di Hasse di (A, σ) ;
- (vi) stabilire se (A, σ) è un reticolo;
- (vii) trovare $x \in A$ tale che $(A \setminus \{x\}, \sigma)$ sia un reticolo e decidere se questo reticolo è distributivo, complementato, booleano (si ricorda che le risposte vanno giustificate in modo esauriente).

Esercizio 3. In $T = \mathbb{Z}_{10} \times \mathbb{Z}_{10} \times \mathbb{Z}_{10}$ si definisca l'operazione binaria $*$ ponendo, per ogni $a, b, c, x, y, z \in \mathbb{Z}_{10}$,

$$(a, b, c) * (x, y, z) = (ax, ay + bz, cz).$$

- (i) Sapendo che $*$ è associativa (non è richiesta verifica di questo fatto), dimostrare che $(T, *)$ è un monoide e che non è commutativo.

Sia $K = \{(a, b, c) \in T \mid a, c \in \mathcal{U}(\mathbb{Z}_{10})\}$;

- (ii) calcolare $|K|$;
- (iii) verificare che K è una parte chiusa rispetto a $*$;
- (iv) verificare che $(K, *)$ è un gruppo;
- (v) calcolare l'inverso in $(K, *)$ di $(\bar{7}, \bar{5}, \bar{7})$, svolgendo una equazione congruenziale utilizzando l'algoritmo euclideo.

Esercizio 4. Per ogni primo (positivo) p , sia f_p il polinomio

$$\bar{6}5x^5 + \bar{1}0x^4 + \bar{1}1x^3 + \bar{5}x^2 + \bar{7}x + \bar{1}2 \in \mathbb{Z}_p[x].$$

- (i) Trovare un primo q tale che f_q sia monico di grado 5 (quanti ce ne sono?).
- (ii) Trovare un primo r tale che f_r sia monico di grado 3 (quanti ce ne sono?).
- (iii) Decomporre f_q come prodotto di polinomi monici irriducibili in $\mathbb{Z}_q[x]$.
- (iv) Decomporre f_r come prodotto di polinomi monici irriducibili in $\mathbb{Z}_r[x]$.
- (v) f_r ha in $\mathbb{Z}_r[x]$ un divisore irriducibile di coefficiente (parametro) direttore $\bar{2}$?
- (vi) f_r ha in $\mathbb{Z}_r[x]$ un divisore irriducibile di grado 2?