

**CORSO DI LAUREA TRIENNALE IN INFORMATICA**  
**PROVA SCRITTA DI ALGEBRA (GRUPPI I E II)**  
**20 GIUGNO 2018**

Svolgere i seguenti esercizi,

—————→ *giustificando pienamente tutte le risposte.* ←————

Sui fogli consegnati vanno indicati: **nome, cognome, matricola, gruppo di appartenenza** e eventuale superamento della **prova in itinere**. **Chi ha superato quest'ultima è esentato dai primi due esercizi.**

**Non** è necessario consegnare la traccia.

solo per chi non ha superato la prova in itinere

**Esercizio 1.** Si considerino le applicazioni  $f: x \in \mathbb{Z} \rightarrow \frac{x+1}{3} \in \mathbb{Q}$  e  $g: x \in \mathbb{Q} \rightarrow \frac{x+1}{3} \in \mathbb{Q}$ . Di ciascuna di esse si dica se è iniettiva, se è suriettiva, se è biettiva e si scriva esplicitamente l'inversa, se questa esiste.

**Esercizio 2.** In  $S = \mathbb{Z}_8 \times \mathbb{Z}_8$  si definisca l'operazione binaria  $*$  ponendo, per ogni  $(a, b), (c, d) \in S$ ,  $(a, b) * (c, d) = (a + c + \bar{2}, bd)$ . 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 è  $(S, *)$ ?
- (ii) Posto  $P = \{\bar{a} \in \mathbb{Z}_8 \mid a \text{ è pari}\}$  e  $D = \{\bar{a} \in \mathbb{Z}_8 \mid a \text{ è dispari}\}$ , quali tra  $P \times P, \mathbb{Z}_8 \times D, D \times P, D \times \mathbb{Z}_8$ , sono e quali non sono parti chiuse in  $(S, *)$ ? Qualcuna di queste, munita dell'operazione indotta da  $*$ , è un gruppo?

**Esercizio 3.** Enunciare il teorema sulla divisione con resto sia in  $\mathbb{Z}$  che nell'anello dei polinomi su un campo.

**Esercizio 4.** Siano  $B = \{n \in \mathbb{N} \mid n < 10\}$  e  $A = \mathcal{P}(B) \setminus \{\emptyset\}$ . Consideriamo in  $A$  la relazione di equivalenza  $\sim$  e la relazione d'ordine  $\rho$  definite da:  $\forall X, Y \in A$

$$X \sim Y \iff |X| = |Y|; \quad \text{e} \quad X \rho Y \iff (X = Y \vee |X| < |Y|).$$

- (i) Quanto vale  $|A/\sim|$ ? Se  $X \in A$  e  $|X| = n$ , quanto vale  $|[X]_{\sim}|$ ?
- (ii) Determinare gli eventuali elementi minimali, massimali, minimo, massimo in  $(A, \rho)$ .  $(A, \rho)$  è un reticolo? Nel caso, decidere se è complementato, distributivo, booleano.
- (iii) Dire, per un arbitrario  $X \in A$ , quali elementi di  $A$  non sono confrontabili con  $X$  rispetto a  $\rho$ . Quanti sono?
- (iv) Rispetto a  $\rho$ , costruire un sottoinsieme totalmente ordinato  $C$  di  $A$  tale che  $|C| = 10$  e decidere se esiste  $D \subseteq A$  tale che  $C \subset D$  e  $D$  sia totalmente ordinato.
- (v) Costruire, se possibile, sottoinsiemi  $U$  e  $V$  di  $A$  che, ordinati da  $\rho$ , abbiano diagrammi di Hasse



e stabilire, per ciascuno di essi, se è un reticolo e, nel caso, se è distributivo, complementato, booleano.

**Esercizio 5.** Dato un insieme  $P$  di 17 caratteri, sia  $W$  l'insieme delle stringhe di caratteri in  $P$  di lunghezza 10. Esprimere (senza calcolare!),  $|W|$ , il numero  $\lambda_1$  delle stringhe in  $W$  prive di ripetizioni ed il numero  $\lambda_2$  delle stringhe in  $W$  prive di occorrenze consecutive di uno stesso carattere.

**Esercizio 6.** Sia  $f = x^3 + \bar{2}x^2 - \bar{2} \in \mathbb{Z}_7[x]$ . Dopo aver calcolato  $f(\bar{1})$  e  $f(\bar{2})$  si scriva  $f$  come prodotto di polinomi monici irriducibili in  $\mathbb{Z}_7[x]$ .

- (i) A quali tra  $\bar{3}x^3 + x^2 - \bar{1}$  e  $\bar{3}x^3 - x^2 + \bar{1}$  è associato  $f$  in  $\mathbb{Z}_7[x]$ ?
- (ii) Quanti sono i polinomi monici di grado 4 in  $\mathbb{Z}_7[x]$  che hanno sia  $\bar{1}$  che  $\bar{2}$  come radici?

**Esercizio 7.** Si trovino tutte le soluzioni (in  $\mathbb{Z}$ ) dell'equazione congruenziale  $30x \equiv_{74} 4$ .