CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II, RECUPERO)
5 SETTEMBRE 2013

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

Esercizio 1. Fornire la definizione di applicazione *iniettiva* e di applicazione *suriettiva*. Di ciascuna delle due applicazioni

$$f\colon A \in \mathcal{P}(\mathbb{Z}) \mapsto \mathbb{N} \smallsetminus A \in \mathcal{P}(\mathbb{Z}) \qquad \text{e} \qquad g\colon A \in \mathcal{P}(\mathbb{N}) \mapsto \mathbb{N} \smallsetminus A \in \mathcal{P}(\mathbb{Z}).$$

dire se è iniettiva e se è suriettiva.

Esercizio 2. In $\mathbb{Z}_{10}$ si definisca l'operazione $*$ ponendo, per ogni $a, b \in \mathbb{Z}_{10}$, $\quad a*b = \bar{3}ab+\bar{2}a-\bar{3}b+\bar{4}$.

(*i*) $*$ è commutativa? $*$ è associativa?

(*ii*) Siano $P = \{[n]_{10} \mid n \text{ è un intero pari}\}$ e $D = \{[n]_{10} \mid n \text{ è un intero dispari}\}$. P è una parte chiusa in $(\mathbb{Z}_{10}, *)$? D è una parte chiusa in $(\mathbb{Z}_{10}, *)$?

(*iii*) Si trovino, se esistono, tutti e soli gli $a \in \mathbb{Z}_{10}$ tali che $a * \bar{0} = \bar{0}$ ed i $b \in \mathbb{Z}_{10}$ tali che $\bar{0} * b = \bar{0}$.

(*iv*) Usando il risultato di (*iii*), stabilire se esiste in $(\mathbb{Z}_{10}, *)$ elemento neutro.

Esercizio 3.

(*i*) Dato un monoide $(M, \cdot)$, è sempre vero che l'insieme U degli elementi invertibili di M ne costituisce una parte chiusa? E, nel caso lo sia, U, munito dell'operazione indotta, è necessariamente un gruppo?

(*ii*) Si elenchino gli elementi di $\mathcal{U}(\mathbb{Z}_9)$, l'insieme degli invertibili di $(\mathbb{Z}_9, \cdot)$.

Si definisca in $\mathbb{Z}_9$ la relazione binaria ρ ponendo, per ogni $a, b \in \mathbb{Z}_9$,

$$a \;\rho\; b \iff (\exists u \in \mathcal{U}(\mathbb{Z}_9))(ua = b).$$

(*iii*) Stabilire se ρ è una relazione di equivalenza.

(*iv*) Nel caso in cui ρ sia di equivalenza, elencare gli elementi di $[\bar{0}]_\rho$, $[\bar{1}]_\rho$, $[\bar{2}]_\rho$, $[\bar{3}]_\rho$; elencare poi gli elementi di $\mathbb{Z}_9/\rho$ e dire quanto vale $|\mathbb{Z}_9/\rho|$.

Esercizio 4. Si verifichi che la relazione $\mathcal{R}$, definita in $\mathcal{P}(\mathbb{N})$ ponendo, per ogni $X, Y \in \mathcal{P}(\mathbb{N})$,

$$X \;\mathcal{R}\; Y \iff X \subseteq Y \wedge |Y \smallsetminus X| \neq 1,$$

è una relazione d'ordine.

(*i*) $\mathcal{R}$ è di ordine totale?

(*ii*) Determinare in $(\mathcal{P}(\mathbb{N}), \mathcal{R})$ gli eventuali minimo, massimo, elementi minimali, elementi massimali.

(*iii*) Posto $X = \{0, 1, 2\}$, disegnare il diagramma di Hasse di $(\mathcal{P}(X), \mathcal{R})$.

(*iv*) $(\mathcal{P}(X), \mathcal{R})$ è un reticolo? Se lo è, è distributivo? È complementato?

(*v*) Indicare, se possibile, una parte P di $\mathcal{P}(\mathbb{N})$ tale che $|P| = 4$ e $(P, \mathcal{R})$ sia un reticolo booleano.

Esercizio 5. Si determini un primo p tale che il polinomio $f = \overline{10}x^4 + \bar{6}x^3 + \bar{3}x - \bar{6} \in \mathbb{Z}_p[x]$ sia monico di terzo grado.

(*i*) Tale p è univocamente determinato?

(*ii*) Decomporre f in prodotto di polinomi monici irriducibili in $\mathbb{Z}_p[x]$?

(*iii*) Esiste in $\mathbb{Z}_p[x]$ un polinomio irriducibile di secondo grado che divida f?