CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II, RECUPERO)
18 MAGGIO 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. Dare la definizione di *anello* e quella di *divisore dello zero* in un anello. Fornire poi un esempio di divisore dello zero (non nullo) in un anello ed un esempio di anello privo di divisori dello zero non nulli.

Esercizio 2. Per ogni $n \in \mathbb{N}$, sia $D^*(n)$ l'insieme dei divisori propri di n in $\mathbb{N}$ (ad esempio, $D^*(6) = \{1, 2, 3\}$). Posto $S = \mathbb{N}^* \smallsetminus \{1\}$, consideriamo l'applicazione $\varphi \colon n \in S \mapsto \max D^*(n) \in \mathbb{N}^*$.

(*i*) φ è iniettiva? φ è suriettiva?

(*ii*) Calcolare l'immagine $\vec{\varphi}(\{n \in \mathbb{N} \mid 1 < n < 10\})$ e l'antiimmagine $\overleftarrow{\varphi}(\{5\})$.

Sia $\mathcal{R}$ il nucleo di equivalenza di φ e sia $\mathcal{R}'$ il nucleo di equivalenza della restrizione di φ a $X := \{n \in \mathbb{N} \mid 1 < n < 10\}$.

(*iii*) Descrivere le classi $[5]_{\mathcal{R}}$ e $[10]_{\mathcal{R}}$ in $S/\mathcal{R}$.

(*iv*) Quanti elementi ha $X/\mathcal{R}'$? Descrivere $[6]_{\mathcal{R}'}$.

Sia Σ la relazione d'ordine definita in S da: $\quad (\forall a, b \in S)\big(a \; \Sigma \; b \iff (a = b \;\vee\; 2\varphi(a) \mid \varphi(b)\big)$.

(*v*) Determinare gli elementi minimali e gli elementi massimali in (S, Σ).

Posto $A = \{4, 8, 12, 17, 24, 40, 1200\}$,

(*vi*) si disegni il diagramma di Hasse di (A, Σ).

(*vii*) (A, Σ) è un reticolo? Nel caso, è distributivo? È complementato?

(*viii*) Determinare, se esiste, un $a \in A$ tale che $(A \smallsetminus \{a\}, \Sigma)$ sia un reticolo distributivo.

(*ix*) Determinare, se esiste, un $n \in S$ tale che $(A \cup \{n\}, \Sigma)$ sia un reticolo booleano.

Esercizio 3. Si consideri, nell'insieme $\mathbb{Z}_{15}$, l'operazione binaria $*$ definita ponendo $a * b = \bar{6}(a+b) - \bar{5}ab$ per ogni $a, b \in \mathbb{Z}_{15}$.

(*i*) Si stabilisca se $*$ è commutativa e se è associativa.

(*ii*) Determinare $a \in \mathbb{Z}_{15}$ tale che $a * \bar{1} = \bar{1}$ e stabilire se tale a è un elemento neutro di $(\mathbb{Z}_{15}, *)$.

(*iii*) Che tipo di struttura è $(\mathbb{Z}_{15}, *)$?

(*iv*) Si trovi, in $(\mathbb{Z}_{15}, *)$, una parte chiusa di cardinalità 2 (suggerimento, si parta dall'elemento $\bar{5}$).

(*v*) Se la domanda ha senso, si elenchino gli elementi simmetrizzabili in $(\mathbb{Z}_{15}, *)$ (suggerimento: assegnato $a \in \mathbb{Z}$, il MCD positivo d tra $6 - 5a$ e 15 è uno tra 1 e 3 (perché?). Se $d = 1$, $\bar{a}$ è simmetrizzabile in $(\mathbb{Z}_{15}, *)$? E se $d = 3$?)

Esercizio 4. Si trovi un primo p tale che il polinomio $f = \bar{3}x^4 + x^3 + x + \bar{2} \in \mathbb{Z}_p[x]$ sia divisibile, in $\mathbb{Z}_p[x]$, per $x^2 + 1$. Quanti di tali primi p esistono? Per il fissato primo p,

(*i*) Si scomponga f come prodotto di polinomi irriducibili in $\mathbb{Z}_p[x]$.

(*ii*) Quanti sono i polinomi associati a f in $\mathbb{Z}_p[x]$? Se possibile, se ne scriva uno monico.