CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II, RECUPERO)
10 DICEMBRE 2014

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 *campo*. Ricordando di giustificare le risposte:

(i) $(\mathbb{N}, +, \cdot)$ è un anello?

(ii) Se S è un insieme, $(\mathcal{P}(S), \triangle, \smallsetminus)$ è un anello?

(iii) Se S è un insieme e $|S| > 1$, $(\mathcal{P}(S), \triangle, \cap)$ è un campo?

Dare un esempio di campo infinito ed uno di campo finito.

Esercizio 2. Si considerino le applicazioni

$$\varphi_3 \colon x \in \mathbb{Z}_{125} \mapsto \bar{3}x \in \mathbb{Z}_{125}; \qquad \text{e} \qquad \varphi_5 \colon x \in \mathbb{Z}_{125} \mapsto \bar{5}x \in \mathbb{Z}_{125}.$$

(i) φ_3 è iniettiva? φ_3 è suriettiva? φ_5 è iniettiva? φ_5 è suriettiva? Quale proprietà algebrica, che differenzia $\bar{3}$ e $\bar{5}$ in $\mathbb{Z}_{125}$, influisce sull'iniettività di φ_3 e φ_5?

(ii) Determinare gli interi positivi n tali che $\varphi_n \colon x \in \mathbb{Z}_{125} \mapsto \bar{n}x \in \mathbb{Z}_{125}$ sia biettiva.

(iii) Detto $\mathcal{R}_{\varphi_5}$ il nucleo di equivalenza di φ_5, descrivere esplicitamente $[\bar{0}]_{\mathcal{R}_{\varphi_5}}$, e calcolare le cardinalità di $[\bar{0}]_{\mathcal{R}_{\varphi_5}}$ e di $\vec{\varphi}_5(\mathbb{Z}_{125})$.

Esercizio 3. Si definisca in $\mathbb{Z}$ la relazione binaria Σ ponendo, per ogni $a, b \in \mathbb{Z}$:

$$a \mathrel{\Sigma} b \iff (\exists h \in 2\mathbb{N})(a + h = b).$$

(i) Verificare che Σ è una relazione d'ordine e che non è totale.

(ii) Fissato $x \in 2\mathbb{Z}$, quali sono gli elementi $y \in \mathbb{Z}$ confrontabili con x? E se, invece, $x \in \mathbb{Z} \smallsetminus 2\mathbb{Z}$?

(iii) Determinare, se esistono (o spiegare perché non esistono), gli elementi minimali, massimali, minimo, massimo in $(\mathbb{Z}, \Sigma)$.

(iv) Dimostrare che, se X è una parte di $\mathbb{Z}$ tale che (X, Σ) sia un reticolo, (X, Σ) è necessariamente totalmente ordinato.

Esercizio 4. Si definisca in $\mathbb{Z} \times \mathbb{Z}$ l'operazione binaria $*$ ponendo, per ogni $a, b, c, d \in \mathbb{Z}$;

$$(a, b) * (c, d) = (a + c + 2, -bd).$$

Dando per noto (e quindi *non* verificando) che questa operazione è commutativa e associativa,

(i) determinare (se esiste) l'elemento neutro di $(\mathbb{Z} \times \mathbb{Z}, *)$. Nel caso, stabilire quali sono gli elementi simmetrizzabili, descrivendone i corrispondenti simmetrici;

(ii) determinare una parte infinita A di $\mathbb{Z} \times \mathbb{Z}$ che sia chiusa rispetto a $*$ e tale che $(A, *)$ sia un gruppo;

(iii) determinare una parte propria infinita B di $\mathbb{Z} \times \mathbb{Z}$ che sia chiusa rispetto a $*$ e tale che $(B, *)$ non sia un gruppo;

(iv) determinare una parte infinita C di $\mathbb{Z} \times \mathbb{Z}$ che non sia chiusa rispetto a $*$.

Esercizio 5. Per $p = 2$ e per $p = 7$ si consideri il polinomio $f_p := x^4 - \bar{2}x^3 + x^2 - \bar{1} \in \mathbb{Z}_p[x]$ e

(i) si scriva f_p come prodotto di polinomi irriducibili monici in $\mathbb{Z}_p[x]$.

(ii) Solo per $p = 7$, si costruisca l'associato monico $\tilde{g}$ di $g := \bar{4}x^4 - x^3 - \bar{3}x^2 - \bar{4}$ in $\mathbb{Z}_7[x]$. $\tilde{g}$ è associato a f_7?