CORSO DI LAUREA TRIENNALE IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I E II)
1 OTTOBRE 2019

Svolgere i seguenti esercizi,

⟶ ***giustificando pienamente tutte le risposte.*** ⟵

Sui fogli consegnati vanno indicati: **nome**, **cognome**, **matricola**, **gruppo di appartenenza**.
Non è necessario consegnare la traccia.

Esercizio 1. Enunciare i teoremi sull'esistenza di quoziente e resto nella divisione tra interi e nella divisione tra polinomi a coefficienti in un campo.

(*i*) Quali e quanti sono i possibili resti di numeri interi nella divisione per -7?
(*ii*) Quali e quanti sono i possibili resti di polinomi in $\mathbb{Z}_2[x]$ nella divisione per x^2?

Esercizio 2. Siano $\mathbb{P}$ l'insieme dei numeri interi positivi primi, $U = \{p \in \mathbb{P} \mid 15 \text{ divide } p\}$, $K = \{p \in \mathbb{P} \mid 2 \neq p \Rightarrow p = 17\}$, $H = \{p \in \mathbb{P} \mid p > 170000000\}$. Elencare gli elementi di U, di K e di $H \triangle H$.

Esercizio 3. Siano $A = \{n \in \mathbb{N} \mid n < 10\}$, $C = \mathcal{P}(A) \times \mathcal{P}(A)$ e $f\colon (X,Y) \in C \mapsto |X \cup Y| \in \mathbb{N}$.

(*i*) Stabilire se f è iniettiva e se f è suriettiva. In particolare, determinare $|\vec{f}(C)|$.
(*ii*) Determinare $|C/\mathcal{R}|$, dove $\mathcal{R}$ è il nucleo di equivalenza di f.
(*iii*) Descrivere esplicitamente $\big[\,(\{1\},\{1\})\,\big]_{\mathcal{R}}$, e dire quanti elementi ha.
(*iv*) Esiste una ed una sola coppia $(X,Y) \in C$ tale che $\big|\,\big[(X,Y)\big]_{\mathcal{R}}\,\big| = 1$. Spiegare perché, giustificando sia l'esistenza che l'unicità di tale coppia.

Siano poi σ e ρ le relazioni d'ordine definite in C ponendo, per ogni $X, Y, Z, T \in \mathcal{P}(A)$,

$$(X,Y)\ \sigma\ (Z,T) \iff \big((X,Y) = (Z,T) \vee |X \cup Y| < |Z \cup T|\,\big)$$
$$(X,Y)\ \rho\ (Z,T) \iff \big((X,Y) = (Z,T) \vee |X \cup Y| \text{ divide propriamente } |Z \cup T|\,\big).$$

(*v*) Determinare sia in (C,σ) che in (C,ρ) eventuali minimo, massimo, elementi minimali, elementi massimali.
(*vi*) (C,σ) è un reticolo? (C,ρ) è un reticolo?
(*vii*) Considerata la parte $T = \big\{(\{1\},\{1\}), (\{1\},\{2\}), (\{1\},\{2,3\}), (\{1,2,3\},\{4,5,6\})\big\}$ di C, disegnare i diagrammi di Hasse di (T,σ) e (T,ρ). Questi due insiemi ordinati sono reticoli? Sono isomorfi tra loro?

Esercizio 4. Si considerino le due operazioni binarie $\oplus$ e $*$ in $\mathbb{Z}_{128}$ definite ponendo, per ogni $a, b \in \mathbb{Z}_{128}$,

$$a \oplus b = a + b - \bar{3} \qquad \text{e} \qquad a * b = \bar{3}a + \bar{3}b - ab - \bar{6}.$$

(*i*) Sia $V := \{a \in \mathbb{Z}_{128} \mid a * \overline{29} = \overline{61}\}$. $V = \varnothing$? Se $V \neq \varnothing$, si trovi un elemento di V e si dica se $|V| = 1$.

Dando per noto che $R = (\mathbb{Z}_{128}, \oplus, *)$ è un anello commutativo,

(*ii*) si determini lo zero 0_R di R;
(*iii*) si stabilisca se R è unitario determinandone, nel caso, l'unità 1_R (suggerimento: si parta dalla ricerca degli $a \in \mathbb{Z}_{128}$ tali che $a * \bar{0} = \bar{0}$);
(*iv*) Dare la definizione di divisore dello zero in R. Dopo aver calcolato $\overline{1} * \overline{3}$ e $\overline{1} * \overline{67}$, si stabilisca se, in R, $\overline{1}$ è un divisore dello zero, se è cancellabile e se è invertibile.
(*v*) Se la domanda ha senso, si decida se, in R, $\overline{7}$ è invertibile e se $\overline{8}$ è invertibile (***non*** *è richiesto* il calcolo degli eventuali inversi).

Esercizio 5. Si determini l'insieme B dei numeri primi positivi p tali che il polinomio

$$f_p = x^4 + \bar{3}x^3 - \bar{3}x^2 + \bar{2} \in \mathbb{Z}_p[x]$$

abbia $\bar{2}$ come radice. Per ogni $p \in B$ si scriva poi f_p come prodotto di polinomi monici irriducibili in $\mathbb{Z}_p[x]$.