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

Svolgere i seguenti esercizi,

$\longrightarrow$ $\boxed{\textbf{\textit{giustificando pienamente tutte le risposte.}}}$ $\longleftarrow$

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

Esercizio 1. Dare la definizione di *sottogruppo* di un gruppo $(G, \cdot)$.
Sia S un insieme, e si consideri il gruppo $(\mathcal{P}(S), \triangle)$.

(i) Vero o falso? Se K è un elemento di $\mathcal{P}(S)$, allora $\{\varnothing, K\}$ è un sottogruppo di $(\mathcal{P}(S), \triangle)$.
(ii) Per ogni sottogruppo H di $(\mathcal{P}(S), \triangle)$ si definisce la relazione binaria $\mathcal{R}_H$ in $(\mathcal{P}(S), \triangle)$ ponendo, per ogni $L, T \in \mathcal{P}(S)$,
$$L \,\mathcal{R}_H\, T \iff L \triangle T \in H.$$
(a) Provare che $\mathcal{R}_H$ è una relazione di equivalenza.
(b) Descrivere $[\varnothing]_{\mathcal{R}_H}$.
(c) Nel caso in cui $H = \{\varnothing\}$, con quale ben nota relazione di equivalenza coincide $\mathcal{R}_H$?

Esercizio 2. Trovare tutte le soluzioni dell'equazione congruenziale $520x \equiv_{1210} 20$.

Esercizio 3. Sia $A = \{n \in \mathbb{N} \mid n < 20\}$, Si considerino l'applicazione $f\colon X \in \mathcal{P}(A) \mapsto |X \cup \{0\}| \in \mathbb{N}^*$ e la relazione d'ordine ρ definita in $\mathcal{P}(A)$ ponendo, per ogni $X, Y \in \mathcal{P}(A)$,
$$X \,\rho\, Y \iff (X = Y \vee f(X) < f(Y)).$$
(i) Stabilire se f è iniettiva e se f è suriettiva.
(ii) Determinare in $(\mathcal{P}(A), \rho)$ eventuali minimo, massimo, elementi minimali, elementi massimali.
(iii) $(\mathcal{P}(A), \rho)$ è totalmente ordinato? È un reticolo? Se lo è, è distributivo? È complementato?
(iv) Quali e quanti sono sono gli elementi di $(\mathcal{P}(A), \rho)$ non confrontabili con $B := \{n \in \mathbb{N} \mid n < 7\}$? (Il numero va ovviamente espresso senza eseguire calcoli.)
(v) In $(\mathcal{P}(A), \rho)$:
(a) qual è il massimo ordine possibile per un sottoinsieme totalmente ordinato (rispetto a ρ)?
(b) Individuare un sottoinsieme che sia un reticolo booleano di ordine 4.

Esercizio 4.
(i) Descrivere $C := \{a^3 \mid a \in \mathbb{Z}_7\}$, elencandone gli elementi e calcolando $|C|$.
(ii) Determinare un polinomio irriducibile $f \in \mathbb{Z}_7[x]$ che sia irriducibile e di grado 3 (si consiglia vivamente, se possibile, di fare uso di quanto visto al punto precedente).
(iii) Costruire, se esistono (o spiegare perché non esistono) polinomi $g, h \in \mathbb{Z}_7[x]$, entrambi di grado 5, tali che:
(a) g ammetta due radici distinte e sia prodotto di tre fattori irriducibili;
(b) h non ammetta radici in $\mathbb{Z}_7$ e sia prodotto di tre fattori irriducibili.