CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II, RECUPERO)
17 GENNAIO 2017

Svolgere i seguenti esercizi,

giustificando pienamente tutte le risposte.

Sui fogli consegnati vanno indicati: *nome, cognome, matricola e gruppo di appartenenza (I, II o recupero).* **Non è necessario consegnare la traccia.**

Esercizio 1. Dare la definizione di polinomio *irriducibile* (a coefficienti in un campo).

Esercizio 2. Dati gli insiemi $S := \{1, 3, 8, 15, 22\}$ e $X := \{3, 5, 7\}$, si determinino, elencandone gli elementi:

$$A = \{p \in X \mid (\exists x \in S)(p|x)\}; \qquad B = \{p \in X \mid (\exists! x \in S)(p|x)\};$$
$$C = \{p \in X \mid (\exists! x \in S)(p \nmid x)\}; \qquad D = \{p \in X \mid (\forall x \in S)(p \nmid x)\}.$$

(i) L'insieme costituito da alcuni di questi quattro insiemi è una partizione di X. Determinarlo.
(ii) Detta F questa partizione, descrivere l'insieme delle coppie ordinate in $X \times X$ che costituisce la relazione di equivalenza corrispondente a F.

Esercizio 3. Si consideri l'applicazione $f\colon x \in \mathbb{N} \mapsto \text{rest}(x, 8) \in \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$.
(i) f è iniettiva? f è suriettiva?
(ii) Detto σ il nucleo di equivalenza di f, quante sono le classi di equivalenza in $\mathbb{N}/\sigma$? Descrivere esplicitamente gli elementi di ciascuna classe.
(iii) Scrivere un'applicazione biettiva da $[0]_\sigma$ a $[1]_\sigma$.

Definiamo la relazione d'ordine Σ in $\mathbb{N}$ ponendo, per ogni $x, y \in \mathbb{N}$,

$$x \;\Sigma\; y \iff \big(x = y \vee f(x) \text{ divide propriamente } f(y)\big).$$

(iv) Si determinino in $(\mathbb{N}, \Sigma)$ gli eventuali elementi minimali, massimali, minimo, massimo. $(\mathbb{N}, \Sigma)$ è un reticolo?
(v) Disegnare il diagramma di Hasse di (L, Σ), dove $L = \{0, 1, 2, 3, 4, 5, 6, 7\}$. Stabilire se (L, Σ) è un reticolo e, nel caso, se è distributivo, complementato, booleano.

Esercizio 4. Si consideri l'operazione binaria $*$ definita in $\mathbb{Z}_{20}$ da:

$$(\forall a, b \in \mathbb{Z}_{20}) \qquad a * b = ab - a + \bar{3}b - \bar{6}.$$

(i) Per ogni a e b in $\mathbb{Z}_{20}$, calcolare $a * \bar{0}$ e $\bar{0} * b$.
(ii) Sfruttando quanto appena fatto,
  (a) calcolare $\bar{1} * \bar{0}$ e $\bar{0} * \bar{1}$; decidere se $*$ è commutativa;
  (b) calcolare $(\bar{0} * \bar{1}) * \bar{0}$ e $\bar{0} * (\bar{1} * \bar{0})$; decidere se $*$ è associativa;
  (c) determinare tutti i $b \in \mathbb{Z}_{20}$ tali che $\bar{0} * b = \bar{0}$. Usare questo risultato per stabilire se $(\mathbb{Z}_{20}, *)$ è dotata di elementi neutri a destra;
  (d) stabilire se $(\mathbb{Z}_{20}, *)$ è dotata di elementi neutri a sinistra.

Sia $Y = \{[n]_{20} \mid n \in \mathbb{Z} \wedge n \equiv_5 2\}$. È possibile dimostrare che, per ogni $a \in \mathbb{Z}_{20}$ e $b \in Y$,

$$a * b = ab - a - b + \bar{2}. \tag{$\mathcal{P}$}$$

Utilizzando questa proprietà ($\mathcal{P}$):
(iii) verificare che Y è una parte chiusa di $(\mathbb{Z}_{20}, *)$;
(iv) stabilire se l'operazione indotta da $*$ su Y è associativa e se è commutativa. $(Y, *)$ ha elemento neutro?
(v) Nel caso la domanda abbia senso, per ciascuno di $\bar{7}$ e $\overline{12}$ stabilire se è invertibile in $(Y, *)$ e, se lo è, trovarne l'inverso.
(vi) Dimostrare la proprietà ($\mathcal{P}$).

Esercizio 5. Per ogni primo (positivo) p si consideri il polinomio

$$f_p = x^4 + x^3 - \overline{35}x^2 - \overline{36}x + \overline{34} \in \mathbb{Z}_p[x].$$

Dopo aver enunciato il teorema di Ruffini generalizzato,
(i) lo si usi per determinare l'insieme T dei primi p tali che f_p sia divisibile (in $\mathbb{Z}_p[x]$) per $x^2 - \bar{1}$.
(ii) Per ogni $p \in T$ si scriva f_p come prodotto di polinomi monici irriducibili in $\mathbb{Z}_p[x]$.