CORSO DI LAUREA TRIENNALE IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I E II)
21 MAGGIO 2018

Svolgere i seguenti esercizi,

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

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

Esercizio 1. Dare la definizione di *dominio di integrità* e di *campo*. Inoltre,

(*i*) Determinare gli interi n compresi tra 7 e 10 (inclusi) per i quali gli elementi invertibili dell'anello $\mathbb{Z}_n$ siano esattamente 6.

(*ii*) Per ciascuno degli anelli $\mathbb{Z}_n$ così individuati, si specifichi la struttura di $\mathbb{Z}_n$ (se è un campo e se è un dominio di integrità), e si dica se $\mathbb{Z}_n \smallsetminus \{\bar{0}\}$ è chiuso rispetto a $+$ e/o rispetto a $\cdot$.

(*iii*) Dire poi in quali di questi anelli la classe $[3]_n$ è invertibile e determinarne la classe inversa, facendo uso di un'opportuna equazione congruenziale.

Esercizio 2. Sia $A = \{1, 2, 3, 4, 5, 6, 7\}$ e sia F l'insieme delle applicazioni $f \colon A \to A$ tali che $f(1) = f(2) \neq f(3)$.

(*i*) Scrivere (senza calcolare) $|F|$;

(*ii*) Quante delle applicazioni appartenenti ad F sono iniettive? E quante suriettive?

Esercizio 3. Siano $A = \{n \in \mathbb{N} \mid n < 100\}$ e $f \colon n \in A \mapsto \mathrm{rest}(n^2, 5) \in \{0, 1, 2, 3, 4\}$.

(*i*) Vero o falso?:

(a) per ogni $n \in \mathbb{Z}$, $\mathrm{rest}(n^2, 5) = (\mathrm{rest}(n, 5))^2$;

(b) per ogni $n \in \mathbb{Z}$, $[\mathrm{rest}(n^2, 5)]_5 = ([\mathrm{rest}(n, 5)]_5)^2$.

(*ii*) f è iniettiva? f è suriettiva?

(*iii*) Detto $\sim$ il nucleo di equivalenza di f, si calcolino $|A/{\sim}|$ e $|[12]_\sim|$.

Esercizio 4. In $S = \mathbb{Z}_{15} \times \mathbb{Z}_{15}$ si definisca l'operazione binaria $*$ ponendo, per ogni $(a, b), (c, d) \in S$, $(a, b) * (c, d) = (acd, bd)$.

(*i*) Decidere se $*$ è commutativa e se è associativa, se ammette elementi neutri destra, a sinistra, neutri e, nel caso in cui la domanda abbia senso, quali elementi di S sono simmetrizzabili rispetto a $*$.

(*ii*) Posto $X = \{\bar{0}, \bar{1}, \bar{6}\} \subseteq \mathbb{Z}_{15}$, dopo aver verificato che ogni elemento di X è idempotente in $(\mathbb{Z}_{15}, \cdot)$, decidere se $T := \mathbb{Z}_{15} \times X$ è una parte chiusa in $(S, *)$. Nel caso lo sia, rispondere per $(T, *)$ alle stesse domande poste sopra per $(S, *)$ e dire che tipo di struttura è $(T, *)$.

Esercizio 5. Sia σ la relazione binaria definita in $\mathbb{N}$ ponendo, per ogni $a, b \in \mathbb{N}$,

$$a \;\sigma\; b \iff \big((a|b \wedge 2a < b) \vee a = b\big).$$

σ è una relazione d'ordine? Se lo è rispondere alle domande che seguono.

(*i*) Determinare gli eventuali elementi minimali, massimali, minimo, massimo in $(\mathbb{N}, \sigma)$. $(\mathbb{N}, \sigma)$ è un reticolo? Nel caso, decidere se è complementato, distributivo, booleano.

(*ii*) Posto $X = \{2^n \mid n \in \{0, 2, 3, 4, 5, 7\}\}$, si disegni il diagramma di Hasse di (X, σ). (X, σ) è un reticolo? Nel caso, decidere se è complementato, distributivo, booleano.

Esercizio 6. In $\mathbb{Z}_{13}[x]$ si considerino i polinomi $f = \bar{3}x^5 + x^4 + \bar{8}x^3 + \bar{6}$, $g = x^3 + \bar{6}x + \bar{6}$ e $d = x^2 + x + \bar{7}$.

(*i*) Determinare l'associato monico di f.

Sapendo che d divide in $\mathbb{Z}_{13}[x]$ sia f che g,

(*ii*) è vero che ogni radice di d è radice sia di f che di g?

(*iii*) Decomporre g in prodotto di polinomi irriducibili.