

CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II, RECUPERO)
12 OTTOBRE 2016

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. (i) Dare la definizione di *partizione* di un insieme.

(ii) Sia $A = \{1, 2, 3, 4, 5, 6\}$. Fornire, se possibile, un esempio di partizione \mathcal{F} di A tale che, detta σ la relazione di equivalenza associata a \mathcal{F} , valgano per σ queste tre proprietà:

$$1 \notin [3]_\sigma; \quad \{1, 2\} \subseteq [4]_\sigma; \quad [5]_\sigma \cap [6]_\sigma \neq \emptyset.$$

(iii) Quante sono, in tutto, le partizioni di A per le quali valga la condizione richiesta in (ii)?

Esercizio 2. Sia α la relazione binaria definita in \mathbb{Q} da: $(\forall a, b \in \mathbb{Q})(a \alpha b \iff (\exists n \in \mathbb{Z})(b = a^n))$.

(i) α è una relazione d'ordine? [Suggerimento: ogni numero razionale $a \neq 0$ ha inverso a^{-1} .] Se lo è, identificare gli eventuali minimo e massimo di (\mathbb{Q}, α) .

Sia poi β la relazione binaria indotta da α su \mathbb{Z} , cioè quella definita da:

$$(\forall a, b \in \mathbb{Z})(a \beta b \iff (\exists n \in \mathbb{Z})(b = a^n)).$$

(ii) β è una relazione d'ordine? [Suggerimento: nel ragionare sull'antisimmetria può essere utile considerare gli interi $0, 1$ e -1 separatamente da tutti gli altri. Ricordare: $0^0 = 1$.] Se lo è, identificare gli eventuali minimo e massimo di (\mathbb{Z}, β) e rispondere anche alle domande che seguono.

(iii) Quali tra $0, 1, 2, 3$ e 4 sono elementi minimali in (\mathbb{Z}, β) ?

(iv) (\mathbb{Z}, β) è un reticolo?

(v) Vero o falso?

(a) $(\forall n, m \in \mathbb{N})(2^n \beta 2^m \iff n \leq m)$;

(b) $(\forall n, m \in \mathbb{N})(2^n \beta 2^m \iff n \mid m)$.

(vi) Sia $X = \{2^n \mid n \in \mathbb{N}\}$. (X, β) è un reticolo?

(vii) Disegnare diagramma di Hasse di (Y, β) , dove $Y = \{y \in X \mid y \leq 1000\}$.

Esercizio 3. Per ogni $m \in \mathbb{N}^*$, sia f_m l'applicazione: $x \in \mathbb{Z}_m \mapsto \overline{20}x + \overline{8} \in \mathbb{Z}_m$.

(i) Dimostrare che f_{49} è un'applicazione biettiva e scriverne l'inversa.

(ii) Caratterizzare gli elementi dell'insieme $M = \{m \in \mathbb{N}^* \mid f_m \text{ è biettiva}\}$ ed elencare gli elementi di $S := \{m \in M \mid m \leq 15\}$.

Esercizio 4. Sia $G = \mathcal{U}(\mathbb{Z}_9)$, il gruppo degli invertibili dell'anello \mathbb{Z}_9 .

(i) Elencare gli elementi di G . Quanti sono?

Detto $E = \{1, -1\}$ il gruppo degli invertibili di \mathbb{Z} , sia $*$ l'operazione binaria in $G \times E$ definita ponendo, per ogni $a, b \in G$ e $\varepsilon, \delta \in E$, $(a, \varepsilon) * (b, \delta) = (ab^\varepsilon, \varepsilon\delta)$.

(ii) Provare che $(G \times E, *)$ è un gruppo. È abeliano? Quanti elementi ha?

(iii) Provare che $\{(\overline{1}, 1), (\overline{8}, 1)\}$ è una parte chiusa di $G \times E$.

Esercizio 5. Vero o falso?

(i) Esiste un campo F tale che il polinomio $x^2 - 1$ sia irriducibile in $F[x]$.

(ii) Per ogni campo F , il polinomio $x^2 + 1$ è irriducibile in $F[x]$.

(iii) Ogni polinomio di grado dispari in $\mathbb{R}[x]$ ammette radice in \mathbb{R} .

(iv) Ogni polinomio di grado dispari in $\mathbb{R}[x]$ non è irriducibile in \mathbb{R} .

(v) Per ogni intero $n \geq 6$, esiste in $\mathbb{Q}[x]$ un polinomio di grado n che non ammette radici in \mathbb{Q} ed è prodotto di tre polinomi irriducibili.

Scrivere come prodotto di polinomi irriducibili in $F[x]$ il polinomio $x^4 - 2$ in ciascuno dei casi $F = \mathbb{R}$, $F = \mathbb{Q}$, $F = \mathbb{Z}_7$.