ALGEBRA PER INFORMATICA
Esame scritto - 22 maggio 2007

Esercizio 1

Si consideri l'anello $\mathbb{Z}/6\mathbb{Z}$.
a) Si determinino i divisori dello zero di $\mathbb{Z}/6\mathbb{Z}$. Quanti sono?
b) L'insieme degli elementi di $\mathbb{Z}/6\mathbb{Z}$ che sono zero o divisori dello zero è un ideale di $\mathbb{Z}/6\mathbb{Z}$? Giustificare la risposta.

Esercizio 2

Siano G un gruppo, N un sottogruppo normale di G e H un qualunque sottogruppo di G. Dimostrare che $N \cap H$ è un sottogruppo normale di H.

Esercizio 3

Sia G un gruppo e sia $G' = \{\Pi_{i=1}^{n} x_i y_i x_i^{-1} y_i^{-1} \colon n \in \mathbf{N}, x_i, y_i \in G\}$ il sottogruppo di G generato dagli elementi della forma $xyx^{-1}y^{-1}$ (chiamati *commutatori* di G). Dimostrare che G' è un sottogruppo normale di G.

Esercizio 4

(Lemma di Dedekind) Siano $H \leq K \leq G$ e $L \leq G$ sottogruppi. Dimostrare che $K \cap HL = H(K \cap L)$.

Esercizio 5

Dati i polinomi

$$f(x) = 18x^4 - 9x^3 - 41x^2 + 49x + 15 \qquad \text{e} \qquad g(x) = 6x^3 - 5x^2 - 13x + 20$$

appartenenti a $\mathbb{Q}[x]$ trovare il loro massimo comune divisore $M(x)$ e trovare due polinomi $\lambda(x), \mu(x) \in \mathbb{Q}[x]$ tali che $\lambda(x)f(x) + \mu(x)g(x) = M(x)$.

Esercizio 6

Sia R un anello commutativo e sia I un ideale di R. Sia inoltre $N(I) = \{x \in R \colon x^n \in I$ per qualche $n\}$. Dimostrare che $N(I)$ è un ideale di R che contiene I e che $N(N(I)) = N(I)$.

Esercizio 7

Sia $(R, +, \cdot)$ un anello con unità. Costruiamo un anello $\tilde{R}$ che ha come elementi gli elementi di R, come somma l'operazione $a \oplus b = a + b + 1$ e come prodotto l'operazione $a \otimes b = a \cdot b + a + b$ per $a, b \in R$. Dimostrare che $(\tilde{R}, \oplus, \otimes)$ è un anello, trovarne lo zero e l'unità e dimostrare che è isomorfo a R.

Esercizio 8

Dimostrare che l'anello $\mathbb{Z}/m\mathbb{Z}$ ha idempotenti non banali se e solo se m è divisibile per almeno due primi distinti.

Esercizio 9

Si scriva un campo K di 8 elementi spiegando nel dettaglio perché K è un campo.