Corso di Algebra 1 - a.a. 2009-2010
Prova scritta del 19.9.2011

1. Dimostrare che $12 \mid (5^{2n-1} + 7)$ per ogni intero $n \geq 1$.

2. Un sottogruppo H di un gruppo G si dice *caratteristico* se $\varphi(H) = H$ per ogni automorfismo φ di G.

   (a) Dimostrare che, se H è caratteristico in G, allora è anche normale in G.

   (b) Dimostrare che, se K è un sottogruppo normale di G e H è un sottogruppo caratteristico di K, allora H è normale in G.

3. Sia G un gruppo e H un suo sottogruppo di indice n.

   (a) Dimostrare che, se H è normale, allora $g^n \in H$ per ogni $g \in G$.

   (b) Fornire un esempio in cui esiste $g \in G$ tale che $g^n \notin H$.

4. Sia A un anello commutativo e sia $I = \{a \in A \,:\, a^2 = 0\}$.

   (a) Dimostrare che, se $1 + 1 = 0$ in A, allora I è un ideale di A.

   (b) Verificare se I è un ideale nel caso in cui $A = (\mathbb{Z}/9\mathbb{Z})[X]/(X^2)$.

5. Sia I l'ideale di $\mathbb{Z}[X]$ generato dai polinomi $3X + 3$ e $X^2 + X + 1$.

   (a) Dimostrare che $3 \in I$.

   (b) Dire se l'anello quoziente $\mathbb{Z}[X]/I$ è un dominio e/o un campo.

Soluzioni

1. Poiché $5^2 = 25 \equiv 1 \mod 12$, per ogni $n \geq 1$ si ha
$$5^{2n-1} + 7 = 5(5^2)^{n-1} + 7 \equiv 5 + 7 \equiv 0 \mod 12.$$

2. (a) Per ogni $g \in G$ la funzione $\varphi_g \colon G \to G$ definita da $a \mapsto gag^{-1}$ è un automorfismo (interno) di G. Dunque, se H è un sottogruppo caratteristico di G, per definizione si ha $\varphi_g(H) = H$. Essendo $\varphi_g(H) = gHg^{-1}$, si conclude che $gHg^{-1} = H$ per ogni $g \in G$, cioè H è normale in G.
   (b) Per ogni $g \in G$ vale $\varphi_g(K) = K$ (perché K è normale in G), per cui $\varphi_g|_K \colon K \to K$ è un automorfismo di K. Quindi (essendo H caratteristico in K) $H = \varphi_g|_K(H) = \varphi_g(H)$ per ogni $g \in G$, il che dimostra che H è normale in G.

3. (a) Nel gruppo quoziente G/H si ha $g^n H = (gH)^n = H$ per il teorema di Lagrange, quindi $g^n \in H$ per ogni $g \in G$.
   (b) Se $G = S_3$, $H = \{(1), (1,2)\}$ (per cui $n = 3$) e $g = (1,3)$, si ha $(1,3)^3 = (1,3) \notin H$.

4. (a) $I \neq \emptyset$ perché $0 \in I$. Se $a, b \in I$, allora
$$(a+b)^2 = a^2 + b^2 + 2ab = 2ab = (1+1)ab = 0,$$
il che dimostra che $a + b \in I$. Infine, se $a \in A$ e $b \in I$, allora $ab \in I$ perché $(ab)^2 = a^2b^2 = 0$.
   (b) I non è un ideale di $(\mathbb{Z}/9\mathbb{Z})[X]/(X^2)$: infatti $\overline{3}, \overline{X} \in I$, ma $\overline{3}+\overline{X} \notin I$ perché $(\overline{3} + \overline{X})^2 = \overline{6X} \neq \overline{0}$.

5. (a) $3 = 3(X^2 + X + 1) - X(3X + 3) \in I$.
   (b) Essendo $3X + 3 = 3(X + 1)$, per la prima parte
$$I = (3, X^2 + X + 1).$$
Allora, posto $J = (3)$, per il terzo teorema di isomorfismo
$$\mathbb{Z}[X]/I \cong (\mathbb{Z}[X]/J)/(I/J).$$
Si ha $J = 3\mathbb{Z}[X]$, per cui $\mathbb{Z}[X]/J \cong (\mathbb{Z}/3\mathbb{Z})[X]$, e in questo isomorfismo I/J corrisponde all'ideale generato da $X^2 + X + 1$. Se ne deduce che
$$\mathbb{Z}[X]/I \cong (\mathbb{Z}/3\mathbb{Z})[X]/(X^2 + X + 1)$$
non è né un dominio né un campo perché $X^2 + X + 1 = X^2 - 2X + 1 = (X - 1)^2$ è riducibile in $(\mathbb{Z}/3\mathbb{Z})[X]$.