Corso di Algebra 1 - a.a. 2009-2010

Prova scritta del 27.6.2011

1. Per quali valori interi positivi di n il sistema di congruenze

$$\begin{cases} x \equiv 4 \mod 6 \\ x \equiv n \mod n^2 \end{cases}$$

ha soluzione?

2. Sia G un gruppo e H un sottogruppo di G. Dimostrare che H è normale se e solo se la seguente condizione è verificata:

per ogni $a, b \in G$ si ha $ab \in H$ se e solo e $ba \in H$.

3. Sia $f\colon D_4 \to D_4$ l'applicazione definita da $f(R^i S^j) = R^{-i} S^j$, per ogni $i, j \in \mathbb{Z}$. Mostrare che f è ben definita e che è un automorfismo di D_4.

Sia G l'insieme $D_4 \times \mathbb{Z}/2\mathbb{Z}$ con l'operazione

$$(x_1, y_1) \cdot (x_2, y_2) = \begin{cases} (x_1 x_2, y_1 + y_2) & \text{se } y_1 = \bar{0} \\ (x_1 f(x_2), y_1 + y_2) & \text{se } y_1 = \bar{1} \end{cases}$$

Dimostrare che $(G, \cdot)$ è un gruppo e che $D_4 \times \{\bar{0}\}$ è un sottogruppo normale di G.

4. Sia A un anello commutativo e $A_0 = A^* \cup \{0\}$.

   (a) Dimostrare che se A_0 è un sottogruppo (additivo) di A, allora A_0 è un sottocampo di A.

   (b) Fornire un esempio in cui A_0 è un sottocampo di A e A non è un campo.

5. Sia $f\colon A \to B$ un omomorfismo di anelli e I, J due ideali di B.

   (a) Dimostrare che $f^{-1}(I) f^{-1}(J) \subseteq f^{-1}(IJ)$.

   (b) Nel caso in cui $f\colon \mathbb{R}[X] \to \mathbb{R}$ sia l'omomorfismo definito da $f(P) = P(0)$, dire se si ha $f^{-1}(I) f^{-1}(J) = f^{-1}(IJ)$ per ogni coppia di ideali I, J di $\mathbb{R}$.

Soluzioni

1. Se $n = \prod_p p^{a_p}$ (dove la produttoria è su tutti i primi p, $a_p \in \mathbb{N}$ e solo un numero finito di a_p è non nullo), per il teorema cinese del resto il sistema dato è equivalente a

$$\begin{cases} x \equiv 4 \mod 2 \\ x \equiv 4 \mod 3 \\ x \equiv n \mod p^{2a_p} \quad \text{per ogni } p \text{ tale che } a_p > 0 \end{cases}$$

   Sempre per il teorema cinese del resto, tale sistema ha soluzione se e solo se per ogni primo p ha soluzione il sottosistema costituito dalle congruze in cui il modulo è una potenza di p. Chiaramente questo succede se $p \neq 2, 3$ o $a_p = 0$. Inoltre, se $a_2 > 0$ (quindi $2 \mid n$), ogni soluzione di $x \equiv n \mod 2^{2a_2}$ verifica anche $x \equiv 4 \mod 2$. Infine, se $a_3 > 0$ (quindi $3 \mid n$), nessuna soluzione di $x \equiv n \mod 3^{2a_3}$ verifica $x \equiv 4 \mod 3$. Se ne conclude che il sistema ha soluzione se e solo $a_3 = 0$, cioè se e solo se $3 \nmid n$.

2. Supponiamo che H sia normale. Dati $a, b \in G$ tali che $ab \in H$, anche $ba = (a^{-1}a)(ba) = a^{-1}(ab)a \in H$. Analogamente, scambiando a e b, si dimostra che $ba \in H$ implica $ab \in H$.

   Viceversa, supponiamo che (per ogni $a, b \in G$) $ab \in H$ se e solo se $ba \in H$. Dati $g \in G$ e $h \in H$, si ha $h = (hg^{-1})g \in H$, quindi anche $ghg^{-1} \in H$, il che dimostra che H è normale.

3. f è ben definita perché se $R^i S^j = R^{i'} S^{j'}$ (cioè $i \equiv i' \mod 4$ e $j \equiv j' \mod 2$) anche $R^{-i} S^j = R^{-i'} S^{j'}$ (dato che $-i \equiv -i' \mod 4$). Inoltre, essendo $f^2 = \mathrm{id}_{D_4}$, f è biunivoca, ed è un omomorfismo (quindi un automorfismo) perché per ogni $i, j, k, l \in \mathbb{Z}$ si ha

$$\begin{aligned} f(R^i S^j) f(R^k S^l) = R^{-i} S^j R^{-k} S^l &= R^{-i-(-1)^j k} S^{j+l} \\ &= f(R^{i+(-1)^j k} S^{j+l}) = f(R^i S^j R^k S^l). \end{aligned}$$

   Per dimostrare che l'operazione $\cdot$ è associativa, cioè che

$$[(x_1, y_1) \cdot (x_2, y_2)] \cdot (x_3, y_3) = (x_1, y_1) \cdot [(x_2, y_2) \cdot (x_3, y_3)]$$

   per ogni $(x_i, y_i) \in G$ (con $i = 1, 2, 3$), distinguiamo alcuni casi a seconda dei valori di y_1 e y_2. Se $y_1 = y_2 = \bar{0}$,

$$[(x_1, \bar{0}) \cdot (x_2, \bar{0})] \cdot (x_3, y_3) = (x_1 x_2 x_3, y_3) = (x_1, \bar{0}) \cdot [(x_2, \bar{0}) \cdot (x_3, y_3)].$$

Se $y_1 = \bar{0}$ e $y_2 = \bar{1}$,

$$[(x_1, \bar{0}) \cdot (x_2, \bar{1})] \cdot (x_3, y_3) = (x_1 x_2, \bar{1}) \cdot (x_3, y_3) = (x_1 x_2 f(x_3), \bar{1} + y_3)$$
$$= (x_1, \bar{0}) \cdot (x_2 f(x_3), \bar{1} + y_3) = (x_1, \bar{0}) \cdot [(x_2, \bar{1}) \cdot (x_3, y_3)].$$

Se $y_1 = \bar{1}$ e $y_2 = \bar{0}$,

$$[(x_1, \bar{1}) \cdot (x_2, \bar{0})] \cdot (x_3, y_3) = (x_1 f(x_2), \bar{1}) \cdot (x_3, y_3) = (x_1 f(x_2) f(x_3), \bar{1} + y_3)$$
$$= (x_1 f(x_2 x_3), \bar{1} + y_3) = (x_1, \bar{1}) \cdot (x_2 x_3, y_3) = (x_1, \bar{1}) \cdot [(x_2, \bar{0}) \cdot (x_3, y_3)].$$

Se $y_1 = y_2 = \bar{1}$,

$$[(x_1, \bar{1}) \cdot (x_2, \bar{1})] \cdot (x_3, y_3) = (x_1 f(x_2), \bar{0}) \cdot (x_3, y_3) = (x_1 f(x_2) x_3, y_3)$$
$$= (x_1 f(x_2) f^2(x_3), y_3) = (x_1 f(x_2 f(x_3)), \bar{1} + \bar{1} + y_3)$$
$$= (x_1, \bar{1}) \cdot (x_2 f(x_3), \bar{1} + y_3) = (x_1, \bar{1}) \cdot [(x_2, \bar{1}) \cdot (x_3, y_3)].$$

Per concludere che $(G, \cdot)$ è un gruppo basta osservare che $(1, \bar{0})$ è l'elemento neutro e che ogni elemento di G ha l'inverso: esplicitamente per ogni $x \in D_4$ si ha $(x, \bar{0})^{-1} = (x^{-1}, \bar{0})$ e $(x, \bar{1})^{-1} = (f(x^{-1}), \bar{1})$.

Infine $D_4 \times \{0\}$ è un sottogruppo di G perché è un sottoinsieme finito, non vuoto e chiuso rispetto a $\cdot$, ed è normale perché ha indice 2.

4. (a) Osserviamo che in ogni caso $1 \in A^* \subset A_0$ e che A_0 è chiuso rispetto al prodotto: dati $a, b \in A^*$, anche $ab \in A^*$, mentre se $a = 0$ o $b = 0$, allora $ab = 0 \in A_0$. Da ciò segue che se A_0 è un sottogruppo di A, è anche un sottoanello; inoltre è anche un campo perché per ogni $a \in A_0 \setminus \{0\} = A^*$ esiste $a^{-1} \in A^* \subset A_0$.

   (b) Sia K un campo e $A = K[X]$. Essendo $K[X]^* = K^* = K \setminus \{0\}$, $A_0 = K$ è un sottocampo di A, che non è un campo.

5. (a) Se $a \in f^{-1}(I) f^{-1}(J)$, per definizione di prodotto di ideali esistono $b_1 \ldots, b_n \in f^{-1}(I)$ e $c_1 \ldots, c_n \in f^{-1}(J)$ tali che $a = \sum_{i=1}^n b_i c_i$. Essendo $f(b_i) \in I$ e $f(c_i) \in J$ per ogni $i = 1, \ldots, n$, otteniamo

$$f(a) = f(\sum_{i=1}^n b_i c_i) = \sum_{i=1}^n f(b_i) f(c_i) \in IJ,$$

   cioè $a \in f^{-1}(IJ)$.

   (b) L'uguaglianza non vale sempre. Infatti, se $I = J = \{0\}$ (quindi anche $IJ = \{0\}$), poiché $f^{-1}(\{0\}) = \ker(f) = (X)$, si ha

$$f^{-1}(I) f^{-1}(J) = (X)(X) = (X^2) \subsetneq (X) = f^{-1}(IJ).$$