Corso di Algebra 1 - a.a. 2009-2010
Prova scritta del 20.9.2010

1. Trovare tutte le soluzioni intere del sistema di congruenze

$$\begin{cases} x \equiv 5 \mod 8 \\ x^2 \equiv 1 \mod 7 \end{cases}$$

2. Sia G il gruppo $D_3 \times \mathbb{Z}/3\mathbb{Z}$ e sia

$$H = \{(R^i, [i]) \,:\, i \in \mathbb{Z}\} \subset G.$$

Dimostrare che H è un sottogruppo di G e dire se H è normale.

3. Siano n e m due interi positivi, $f\colon S_n \to S_m$ un omomorfismo di gruppi e τ e τ' due trasposizioni di S_n.

   (a) Dimostrare che τ e τ' sono coniugate in S_n, cioè che esiste $\sigma \in S_n$ tale che $\tau' = \sigma\tau\sigma^{-1}$.

   (b) Dimostrare che $f(\tau)$ e $f(\tau')$ hanno lo stesso segno in S_m.

   (c) Dimostrare che $f(A_n) \subseteq A_m$.

4. Sia A un anello. Per ogni $a \in A$ indichiamo con $\mathrm{ord}(a)$ l'ordine di a nel gruppo additivo $(A, +)$.

   (a) Dimostrare che se $\mathrm{ord}(1)$ è finito, allora $\mathrm{ord}(a) \mid \mathrm{ord}(1)$ per ogni $a \in A$.

   (b) Dimostrare che se $(A, +)$ è un gruppo ciclico di ordine n, allora A è isomorfo a $\mathbb{Z}/n\mathbb{Z}$ come anello.

5. Sia p un numero primo e

$$A = \{q \in \mathbb{Q} \,:\, \exists\, a, b \in \mathbb{Z} \text{ tali che } q = \frac{a}{b} \text{ e } p \nmid b\} \subset \mathbb{Q}.$$

   (a) Dimostrare che A è un sottoanello di $\mathbb{Q}$.

   (b) Dimostrare che

$$I = \{q \in \mathbb{Q} \,:\, \exists\, a, b \in \mathbb{Z} \text{ tali che } q = \frac{pa}{b} \text{ e } p \nmid b\}$$

   è un ideale di A. Dire inoltre se I è primo e/o massimale.

Soluzioni

1. La seconda congruenza è equivalente a $7 \mid (x^2 - 1) = (x-1)(x+1)$. Poiché 7 è primo, questo succede se e solo se $7 \mid (x-1)$ (cioè $x \equiv 1 \mod 7$) o $7 \mid (x+1)$ (cioè $x \equiv -1 \mod 7$). Dunque i valori di x cercati sono le soluzioni di uno dei due sistemi

$$\begin{cases} x \equiv 5 \mod 8 \\ x \equiv 1 \mod 7 \end{cases} \qquad \begin{cases} x \equiv 5 \mod 8 \\ x \equiv -1 \mod 7 \end{cases}$$

Essendo $\operatorname{mcd}(8,7) = 1$, per il teorema cinese del resto ciascun sistema ha un'unica soluzione modulo $8 \cdot 7 = 56$. Si trova facilmente che una soluzione particolare del primo sistema è per esempio $x = 29$ e del secondo $x = 13$. Dunque tutte le soluzioni cercate sono $x \equiv 29 \mod 56$ o $x \equiv 13 \mod 56$.

2. Chiaramente $H \neq \emptyset$, visto che per esempio $(R, [1]) \in H$. Se $a, b \in H$ con $a = (R^i, [i])$ e $b = (R^j, [j])$, allora

$$ab^{-1} = (R^i, [i])(R^j, [j])^{-1} = (R^i, [i])(R^{-j}, [-j]) = (R^{i-j}, [i-j]) \in H,$$

quindi H è un sottogruppo di G.

H non è normale in G: infatti, presi per esempio $g = (S, [0]) \in G$ e $h = (R, [1]) \in H$, si ha

$$ghg^{-1} = (S, [0])(R, [1])(S, [0]) = (SRS, [1]) = (R^{-1}, [1]) \notin H$$

(altrimenti esisterebbe $i \in \mathbb{Z}$ tale che $(R^{-1}, [1]) = (R^i, [i])$, da cui seguirebbe $i \equiv -1 \mod 3$ e $i \equiv 1 \mod 3$, quindi $-1 \equiv 1 \mod 3$, assurdo).

3. (a) Se $\tau = (a, b)$ e $\tau' = (a', b')$, è immediato verificare che ogni $\sigma \in S_n$ tale che $\sigma(a) = a'$ e $\sigma(b) = b'$ soddisfa $\tau' = \sigma\tau\sigma^{-1}$.

   (b) Da $\tau' = \sigma\tau\sigma^{-1}$ segue $f(\tau') = f(\sigma)f(\tau)f(\sigma)^{-1}$, quindi, denotando con $\epsilon\colon S_m \to \{\pm 1\}$ l'omomorfismo segno, si trova

$$\epsilon(f(\tau')) = \epsilon(f(\sigma))\epsilon(f(\tau))\epsilon(f(\sigma))^{-1} = \epsilon(f(\tau)).$$

   (c) Per quanto appena visto esiste $\alpha \in \{\pm 1\}$ tale che $\epsilon(f(\tau)) = \alpha$ per ogni trasposizione τ di S_n. Dato che ogni $\sigma \in A_n$ si può scrivere come prodotto di un numero pari di trasposizioni, diciamo $\sigma = \prod_{i=1}^{2k} \tau_i$, si ottiene dunque

$$\epsilon(f(\sigma)) = \prod_{i=1}^{2k} \epsilon(f(\tau_i)) = \alpha^{2k} = 1,$$

cioè $f(\sigma) \in A_m$.

4. (a) Se $\operatorname{ord}(1) = m$, si ha in particolare $m1 = 0$, quindi $ma = m(1a) = (m1)a = 0a = 0$ per ogni $a \in A$, da cui $\operatorname{ord}(a) \mid m$.

   (b) Per ipotesi esiste $a \in A$ tale che $\operatorname{ord}(a) = n$, e allora per quanto appena visto $n \mid \operatorname{ord}(1)$. D'altra parte $\operatorname{ord}(1) \mid n$ per il teorema di Lagrange, quindi deve essere $\operatorname{ord}(1) = n$ (per cui 1 è un generatore di $(A, +)$). Ne segue che l'(unico)omomorfismo di anelli $\mathbb{Z} \to A$ (definito da $k \mapsto k1$) è suriettivo e ha come nucleo $\operatorname{ord}(1)\mathbb{Z} = n\mathbb{Z}$. Per il primo teorema di isomorfismo per anelli si può concludere che A è isomorfo a $\mathbb{Z}/n\mathbb{Z}$.

5. (a) Chiaramente $1 = 1/1 \in A$. Inoltre se $q = a/b$ e $q' = a'/b'$ (con $p \nmid b$ e $p \nmid b'$) sono due elementi di A, anche $q - q' = (ab' - a'b)/(bb')$ e $qq' = (aa')/(bb')$ appartengono ad A, tenuto conto che $p \nmid (bb')$.

   (b) $I \neq \emptyset$ perché $0 = (p0)/1 \in I$. Siano poi $q = (pa)/b$ e $q' = (pa')/b'$ due elementi di I e $r = c/d \in A$ (con $p \nmid b$, $p \nmid b'$ e $p \nmid d$). Allora anche $q + q' = (p(ab' + a'b))/(bb')$ e $rq = (pca)/(db)$ appartengono a I (usando di nuovo il fatto che $p \nmid (bb')$ e $p \nmid (db)$), il che dimostra che I è un ideale di A.

   I è un ideale massimale (dunque anche primo) di A. Sia infatti J un ideale di A tale che $I \subsetneq J$: per definizione esiste $q \in J \setminus I$, quindi esistono $a, b \in \mathbb{Z}$ tali che $q = a/b$ con $p \nmid a$ e $p \nmid b$. Visto che $q^{-1} = b/a \in A$, q è un'unità di A, e pertanto $J = A$.