Corso di Algebra 1 - a.a. 2009-2010
Prova scritta del 7.7.2010

1. Per quali interi n l'equazione
$$15x + 6y = n$$
ha soluzioni intere? Si determinino inoltre tutte le soluzioni intere positive di tale equazione per $n = 63$.

2. Sia G un gruppo, a un elemento di G e
$$H_a = \{g \in G \ : \ aga^{-1} = g^{-1}\}.$$
   (a) Dimostrare che, se G è abeliano, allora H_a è un sottogruppo di G.
   (b) Nel caso in cui $G = D_3$, trovare un elemento a di D_3 tale che H_a non sia un sottogruppo di D_3.

3. Sia $H = \{(1), (12)(35), (13)(25), (15)(23)\} \subset S_5$.
   (a) Dimostrare che H è un sottogruppo di S_5 isomorfo a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
   (b) H è un sottogruppo normale di S_5?

4. Sia A un anello, X un insieme e A^X l'anello delle funzioni da X verso A. Dimostrare che per ogni sottoinsieme Y di X l'insieme
$$I_Y = \{f \in A^X \ : \ f(y) = 0 \ \forall y \in Y\}$$
è un ideale di A^X e che l'anello quoziente A^X/I_Y è isomorfo a A^Y.

5. Dimostrare che per ogni intero positivo n l'insieme
$$\{f \in \mathbb{Z}[X] \ : \ n|f(6)\}$$
è un ideale di $\mathbb{Z}[X]$. Per quali valori di n tale ideale è primo e per quali massimale?

Soluzioni

1. L'equazione data ha soluzioni intere se e solo se n è un multiplo di $\mathrm{mcd}(15, 6) = 3$.

   Se $n = 63$, semplificando per 3 l'equazione è equivalente a $5x+2y = 21$. Le soluzioni intere di tale equazione sono tutte e sole della forma

   $$\begin{cases} x = x_0 + 2t \\ y = y_0 - 5t \end{cases}$$

   (con $t \in \mathbb{Z}$), dove (x_0, y_0) è una soluzione particolare. È facile vedere che si può prendere per esempio $x_0 = 1$ e $y_0 = 8$. Poiché $x = 1+2t > 0$ se e solo se $t \geq 0$ e $y = 8 - 5t > 0$ se e solo se $t \leq 1$, le soluzioni sono positive solo per $t = 0, 1$, e quindi sono $(1, 8)$ e $(3, 3)$.

2. (a) Se G è abeliano $aga^{-1} = g$ per ogni $g \in G$, quindi

   $$H_a = \{g \in G \ : \ g = g^{-1}\},$$

   che è un sottogruppo di G perché chiaramente $1 \in H_a$ e se $g_1, g_2 \in H_a$, allora
   $$(g_1g_2^{-1})^{-1} = g_2g_1^{-1} = g_2^{-1}g_1 = g_1g_2^{-1},$$
   quindi $g_1g_2^{-1} \in H_a$.

   (b) Per esempio H_1 non è un sottogruppo di D_3. Infatti anche in questo caso $H_1 = \{g \in G \ : \ g = g^{-1}\}$, ma in D_3 gli elementi che coincidono con il proprio inverso sono l'identità e le tre riflessioni di ordine 2. Dunque H_1 ha cardinalità 4 e non può essere un sottogruppo di D_3 per il teorema di Lagrange.

3. (a) Poiché H è finito e non vuoto, per dimostrare che è un sottogruppo basta verificare che è chiuso rispetto al prodotto. Siano dunque $\sigma, \tau \in H$: se $\sigma = (1)$ o $\tau = (1)$, chiaramente $\sigma\tau \in H$; se $\sigma = \tau$, $\sigma\tau = \sigma^2 = (1) \in H$; nei rimanenti casi è facile vedere che $\sigma\tau$ è l'unico elemento di H diverso da σ, τ e (1). Dunque H è un sottogruppo di S_5 di ordine 4, necessariamente isomorfo a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, dato che non è ciclico perché tutti i suoi elementi diversi da (1) hanno ordine 2.

   (b) H non è normale in S_5, infatti $(1, 4) \in S_5$, $(1, 2)(3, 5) \in H$, ma

   $$(1, 4)(1, 2)(3, 5)(1, 4)^{-1} = (2, 4)(3, 5) \notin H.$$

4. I_Y non è vuoto perché contiene la funzione identicamente nulla da X verso A (che è lo 0 di A^X). Inoltre per ogni $f, g \in I_Y$ si ha

$$(f+g)(y) = f(y) + g(y) = 0 + 0 = 0$$

per ogni $y \in Y$, dunque $f + g \in I_Y$. Analogamente per ogni $f \in I_Y$ e per ogni $h \in A^X$ si ha $fh, hf \in I_Y$. Questo dimostra che I_Y è un ideale di A^X.

La funzione $\alpha\colon A^X \to A^Y$ definita da $\alpha(f) = f|_Y$ è un omomorfismo di anelli: infatti ovviamente $\alpha(1) = 1$ e per ogni $f, g \in A^X$ vale

$$\alpha(f+g) = (f+g)|_Y = f|_Y + g|_Y = \alpha(f) + \alpha(g)$$

e analogamente $\alpha(fg) = \alpha(f)\alpha(g)$. Chiaramente $\ker(\alpha) = I_Y$, e inoltre α è suriettiva: data $h \in A^Y$, si ha $h = \alpha(\tilde{h})$ con $\tilde{h} \in A^X$ una qualunque funzione definita come h su Y e arbitrariamente su $X \setminus Y$. Dunque per il primo teorema di isomorfismo concludiamo che $A^Y \cong A^X/I_Y$.

5. L'insieme $I_n = \{f \in \mathbb{Z}[X] \ : \ n|f(6)\}$ è un ideale di $\mathbb{Z}[X]$: chiaramente $0 \in I_n$; se $f, g \in I_n$, cioè $n|f(6)$ e $n|g(6)$, anche $f + g \in I_n$ perché $n|(f+g)(6) = f(6)+g(6)$; infine, se $f \in I_n$ e $h \in \mathbb{Z}[X]$, anche $fh \in \mathbb{Z}[X]$ perché $n|(fh)(6) = f(6)h(6)$.

   I_n è primo se e solo se I_n è massimale se e solo se n è primo. Infatti se n non è primo esistono $a, b \in \mathbb{Z}$ con $a, b > 1$ e $n = ab$, e quindi I_n non è primo perché $a, b \notin I_n$ mentre $ab \in I_n$. Tenendo conto che ogni ideale massimale è anche primo, resta da dimostrare che se n è primo, allora I_n è massimale. Sia dunque J un ideale di $\mathbb{Z}[X]$ tale che $I_n \subsetneq J$. Per definizione esiste $f \in J \setminus I_n$ e facendo la divisione con resto di f per $X - 6$ trovo $g \in \mathbb{Z}[X]$ e $r \in \mathbb{Z}$ tali che $f = (X-6)g + r$. Poiché $X - 6 \in I_n \subset J$, ne segue che anche $r \in J \setminus I_n$, da cui $n \nmid r$. D'altra parte anche $n \in I_n \subset J$, per cui $J \supset (r, n)$. Ora, essendo n primo e $n \nmid r$, si ha $\operatorname{mcd}(r, n) = 1$, quindi $J = \mathbb{Z}[X]$ e pertanto I_n è massimale.

   In alternativa e più semplicemente si può osservare che la funzione $\mathbb{Z}[X] \to \mathbb{Z}/n\mathbb{Z}$, $f \mapsto \overline{f(6)}$ è un omomorfismo suriettivo di anelli con nucleo I_n. Dunque I_n è un ideale per ogni n, ed è primo o massimale se e solo se $\mathbb{Z}[X]/I_n$ è un dominio o un campo. Poiché $\mathbb{Z}[X]/I_n \cong \mathbb{Z}/n\mathbb{Z}$ per il primo teorema di isomorfismo, queste ultime condizioni sono tra loro equivalenti e sono verificate se e solo se n è primo.