Corso di Algebra 1 - a.a. 2016-2017

Prova scritta dell'8.9.2017

1. Trovare tutte le coppie (x, y) di numeri interi che risolvono il sistema

$$\begin{cases} x + y \equiv 7 \mod 9 \\ xy \equiv 2 \mod 3 \end{cases}$$

2. Sia G il gruppo $\mathbb{Z} \times \mathbb{Z}$ e $h = (1, 2) \in G$.
   (a) Trovare, se esiste, $g \in G$ tale che il sottogruppo generato da g e h sia tutto il gruppo G.
   (b) Sia H il sottogruppo di G generato dal solo h: è vero che H è isomorfo a $\mathbb{Z}$ e che G/H è isomorfo a $\mathbb{Z}$?
   (c) Sia ora K il sottogruppo di G generato da $(4, 6)$: è vero che G/K è isomorfo a $\mathbb{Z}$?

3. Sia A un anello commutativo.
   (a) Dimostrare che $B := \{(p, a) \in A[X] \times A : p(0) = a\}$ è un sottoanello di $A[X] \times A$.
   (b) Dimostrare che $\tilde{I} := \{(p, a) \in B : a \in I\}$ è un ideale di B per ogni ideale I di A.
   (c) Dimostrare che $\tilde{I}$ è un ideale di $A[X] \times A$ se e solo se $I = \{0\}$.

4. Sia A un dominio a fattorizzazione unica e I un ideale primo non nullo di A.
   (a) Dimostrare che esiste $p \in I$ con p irriducibile in A.
   (b) Dimostrare che, se p è come nel punto precedente e I è principale, allora $I = (p)$.

Soluzioni

1. Il sistema non ha soluzioni. Infatti, è immediato verificare che la seconda congruenza è soddisfatta se e solo se $x \equiv 1 \mod 3$ e $y \equiv 2 \mod 3$ o viceversa $x \equiv 2 \mod 3$ e $y \equiv 1 \mod 3$. In entrambi i casi risulta $x + y \equiv 0 \mod 3$, mentre la prima congruenza implica $x + y \equiv 1 \mod 3$.

2. (a) Per esempio, $g = (0, 1)$ ha la proprietà richiesta. Infatti, ogni elemento (a, b) di G appartiene al sottogruppo generato da g e h, dato che

$$(a, b) = a(1, 2) + (b - 2a)(0, 1) = ah + (b - 2a)g.$$

   (b) Poiché $nh = (n, 2n) = (0, 0)$ se e solo se $n = 0$, per definizione l'ordine di h è infinito. Ciò dimostra che H è un gruppo ciclico infinito, e quindi $H \cong \mathbb{Z}$. Per dimostrare che anche $G/H \cong \mathbb{Z}$, per il primo teorema di isomorfismo per gruppi basta trovare un omomorfismo suriettivo $f\colon G \to \mathbb{Z}$ con $\ker(f) = H$. Ora, per ogni scelta di $x, y \in \mathbb{Z}$, la funzione

$$\begin{aligned} f_{x,y}\colon G &\to \mathbb{Z} \\ (a, b) &\mapsto ax + by \end{aligned}$$

   è un omomorfismo di gruppi (risulta infatti

$$\begin{aligned} f_{x,y}((a, b) + (c, d)) = f_{x,y}((a + c, b + d)) &= (a + c)x + (b + d)y \\ &= ax + by + cx + dy = f_{x,y}((a, b)) + f_{x,y}((c, d)) \end{aligned}$$

   per ogni $a, b, c, d \in \mathbb{Z}$). L'immagine di $f_{x,y}$ è $x\mathbb{Z}+y\mathbb{Z} = \mathrm{mcd}(x, y)\mathbb{Z}$, dunque $f_{x,y}$ è suriettivo se e solo se $\mathrm{mcd}(x, y) = 1$. Inoltre $H \subseteq \ker(f_{x,y})$ se e solo se $h \in \ker(f_{x,y})$ se e solo se $0 = f_{x,y}((1, 2)) = x+2y$, cioè se e solo se $x = -2y$. Scegliendo in particolare $x = -2$ e $y = 1$, risulta anche $\ker(f_{-2,1}) = H$: se infatti $(a, b) \in \ker(f_{-2,1})$, cioè $0 = f_{-2,1}((a, b)) = -2a + b$, si trova

$$(a, b) = (a, 2a) = a(1, 2) = ah \in H.$$

   In conclusione l'omomorfismo $f = f_{-2,1}$ ha tutte le proprietà cercate, e pertanto $G/H \cong \mathbb{Z}$.

(c) G/K non è isomorfo a $\mathbb{Z}$. Si può dimostrarlo per esempio osservando che $(2,3) \notin K$ mentre $2(2,3) = (4,6) \in K$. Questo implica che in G/K l'elemento $(2,3) + K$ ha ordine 2, mentre in $\mathbb{Z}$ non esistono elementi di ordine 2 (hanno tutti ordine infinito, tranne 0 che ha ordine 1).

3. (a) Chiaramente $(1,1) \in B$. Dati poi $(p,a), (q,b) \in B$, anche $(p,a) - (q,b) = (p-q, a-b) \in B$ (perché $(p-q)(0) = p(0) - q(0) = a - b$) e $(p,a)(q,b) = (pq, ab) \in B$ (perché $(pq)(0) = p(0)q(0) = ab$).

(b) Chiaramente $(0,0) \in \tilde{I}$. Se $(q,b), (r,c) \in \tilde{I}$, anche $(q,b) + (r,c) = (q+r, b+c) \in \tilde{I}$, visto che $b + c \in I$ (essendo I un ideale di A) e $(q,b) + (r,c) \in B$ (essendo B un sottoanello di $A[X] \times A$ per il punto precedente). Se infine $(p,a) \in B$ e $(q,b) \in \tilde{I}$, anche $(p,a)(q,b) = (pq, ab) \in \tilde{I}$, visto che $ab \in I$ (essendo I un ideale di A) e $(p,a)(q,b) \in B$ (essendo B un sottoanello di $A[X] \times A$).

In alternativa, si può dimostrare che $\tilde{I}$ è un ideale di B semplicemente osservando che è la controimmagine dell'ideale I attraverso l'omomorfismo di anelli $B \to A$ definito da $(p,a) \mapsto a$ (si tratta di un omomorfismo in quanto composizione degli omomorfismi dati dall'inclusione di B in $A[X] \times A$ e dalla proiezione $A[X] \times A \to A$).

(c) Essendo in ogni caso un ideale di B per il punto precedente, $\tilde{I}$ è un ideale di $A[X] \times A$ se e solo se $(p,a)(q,b) = (pq, ab) \in \tilde{I}$ per ogni $(p,a) \in A[X] \times A$ e per ogni $(q,b) \in \tilde{I}$. Tale condizione è certamente verificata se $I = \{0\}$, perché allora $b = 0 = q(0)$, e quindi $(pq)(0) = p(0)q(0) = 0 = ab$ e $ab = 0 \in I$. Viceversa, sia I un ideale di A tale che $\tilde{I}$ sia un ideale di $A[X] \times A$. Preso $b \in I$, per definizione $(b,b) \in \tilde{I}$, dunque anche $(0,1)(b,b) = (0,b) \in \tilde{I}$. In particolare $(0,b) \in B$, e questo implica $b = 0$, per cui $I = \{0\}$.

4. (a) Per ipotesi esiste $0 \neq a \in I$. Poiché $a \notin A^*$ (altrimenti si avrebbe $I = A$), a ha una fattorizzazione non vuota come prodotto di irriducibili, cioè esistono $n > 0$ e $p_1, \ldots, p_n \in A$ irriducibili tali che $a = p_1 \cdots p_n$. Dunque $p_1 \cdots p_n \in I$, e segue allora subito dalla definizione di ideale primo che esiste $i \in \{1, \ldots, n\}$ tale che $p = p_i \in I$.

(b) Sia $a \in I$ tale che $I = (a)$. Poiché $p \in I = (a)$, esiste $b \in A$ tale che $p = ab$. Dato che p è irriducibile e (come già osservato) $a \notin A^*$, deve essere $b \in A^*$. Allora p e a sono associati, e quindi $(p) = (a) = I$.