Corso di Algebra 1 - a.a. 2017-2018

Prova scritta del 20/09/2018

1. Si consideri la congruenza $x^y \equiv 4 \mod 15$.
   (a) Trovare le soluzioni intere positive y quando $x = 2018$.
   (b) Trovare le soluzioni intere x quando $y = 2018$.

2. Siano G e G' due gruppi. Dimostrare che l'unico omomorfismo $G \to G'$ è quello banale in ciascuno dei seguenti casi.
   (a) G è finito e $G' = \mathbb{Z}$.
   (b) $G = \mathbb{Q}$ e $G' = \mathbb{Z}$.
   (c) $G = A_4$ e $G' = D_4$.

3. Dati un anello A e un ideale sinistro I di A, sia
$$B := \{b \in A \,:\, cb \in I \ \forall c \in I\}.$$
   (a) Dimostrare che $I \subseteq B$.
   (b) Dimostrare che B è un sottoanello di A.
   (c) Se B' è un sottoanello di A contenente I, dimostrare che I è un ideale bilatero di B' se e solo se $B' \subseteq B$.

4. Dato un campo K, per ogni intero positivo n sia
$$f_n := \sum_{i=0}^{n} (n+1-i)X^i = X^n + 2X^{n-1} + \cdots + nX + n + 1 \in K[X].$$
   (a) Dimostrare che $(f_n, f_{n+1}) = K[X]$ se e solo se $n \neq -2$ in K.
   (b) Nel caso in cui $K = \mathbb{Z}/3\mathbb{Z}$, trovare il più piccolo $n > 1$ tale che f_n sia irriducibile.
   (c) Nel caso in cui $K = \mathbb{Z}/2\mathbb{Z}$, esiste $n > 1$ tale che f_n sia irriducibile?

Soluzioni

1. Osserviamo preliminarmente che, essendo $15 = 3 \cdot 5$ con $\mathrm{mcd}(3,5) = 1$, risolvere la congruenza data equivale a risolvere il sistema

$$\begin{cases} x^y \equiv 4 \equiv 1 \mod 3 \\ x^y \equiv 4 \mod 5. \end{cases}$$

   (a) Poiché $2018 \equiv 2 \mod 3$ e $2018 \equiv 3 \mod 5$, si tratta di risolvere il sistema

$$\begin{cases} 2^y \equiv 1 \mod 3 \\ 3^y \equiv 4 \mod 5. \end{cases}$$

   Dato che $\overline{2}$ ha ordine 2 in $\mathbb{Z}/3\mathbb{Z}^*$, le soluzioni della prima congruenza sono $y \equiv 0 \mod 2$. Similmente, 3 ha ordine 4 in $\mathbb{Z}/5\mathbb{Z}^*$ e $\overline{3}^2 = \overline{4}$, dunque le soluzioni della seconda congurenza sono $y \equiv 2 \mod 4$. Si conclude che le soluzioni cercate sono gli interi positivi y che verificano il sistema

$$\begin{cases} y \equiv 0 \mod 2 \\ y \equiv 2 \mod 4, \end{cases}$$

   cioè $y \equiv 2 \mod 4$.

   (b) Il sistema da risolvere è

$$\begin{cases} x^{2018} \equiv 1 \mod 3 \\ x^{2018} \equiv 4 \mod 5. \end{cases}$$

   Ragionando come nel punto precedente, abbiamo che, per ogni valore di x, le soluzioni intere positive y di $x^y \equiv 1 \mod 3$ sono: nessuna se $x \equiv 0 \mod 3$; ogni y se $x \equiv 1 \mod 3$; y pari se $x \equiv 2 \mod 3$. Poiché 2018 è pari, si ottiene che le soluzioni della prima congruenza sono $x \equiv 1, 2 \mod 3$. Analogamente, le soluzioni intere positive y di $x^y \equiv 4 \mod 5$ sono: nessuna se $x \equiv 0, 1 \mod 5$; $y \equiv 2 \mod 4$ se $x \equiv 2, 3 \mod 5$; y dispari se $x \equiv 4 \mod 5$. Essendo $2018 \equiv 2 \mod 4$, si ottiene che le soluzioni della seconda congruenza sono $x \equiv 2, 3 \mod 5$. Dunque le soluzioni cercate sono gli interi x che verificano il sistema

$$\begin{cases} x \equiv 1, 2 \mod 3 \\ x \equiv 2, 3 \mod 5, \end{cases}$$

   cioè $x \equiv 2, 7, 8, 13 \mod 15$.

2. (a) Se $f\colon G \to \mathbb{Z}$ è un omomorfismo di gruppi, $\mathrm{im}(f)$ è un sottogruppo di $\mathbb{Z}$, dunque della forma $n\mathbb{Z}$ per qualche $n \in \mathbb{N}$. D'altra parte $\mathrm{im}(f)$ è finito perché G lo è, quindi necessariamente $n = 0$. Questo dimostra che $f(g) = 0$ per ogni $g \in G$, cioè f è l'omomorfismo banale.

   (b) Se $f\colon \mathbb{Q} \to \mathbb{Z}$ è un omomorfismo di gruppi (additivi), per ogni $q \in \mathbb{Q}$ e per ogni intero positivo n si ha

$$f(q) = f(n\frac{q}{n}) = nf(\frac{q}{n}) \in n\mathbb{Z}.$$

   Questo chiaramente implica $f(q) = 0$, per cui, come prima, f è l'omomorfismo banale.

   (c) Sia $f\colon A_4 \to D_4$ un omomorfismo. Per ogni 3-ciclo $\sigma \in A_4$, si ha $\mathrm{ord}(f(\sigma)) \mid \mathrm{ord}(\sigma) = 3$, dunque $\mathrm{ord}(f(\sigma))$ può essere solo 1 o 3. Poiché D_4 (che ha ordine 8) non contiene elementi di ordine 3, necessariamente $\mathrm{ord}(f(\sigma)) = 1$, cioè $f(\sigma) = 1$. Ciò dimostra che $\ker(f)$ contiene tutti i 3-cicli di A_4, che sono 8. D'altra parte $\ker(f)$ è un sottogruppo di A_4, e quindi (per il teorema di Lagrange) $\#\ker(f) \mid \#A_4 = 12$. Se ne deduce che $\#\ker(f) = 12$, cioè $\ker(f) = A_4$, il che prova che f è l'omomorfismo banale.

3. (a) Preso $d \in I$, per ogni $c \in I \subseteq A$ si ha $cd \in I$ (perché I è un ideale sinistro di A). Per definizione di B, questo dimostra che $d \in B$.

   (b) Chiaramente $1 \in B$ perché $c1 = c \in I$ per ogni $c \in I$. Se poi $b, b' \in B$ (cioè $cb, cb' \in I$ per ogni $c \in I$), va dimostrato che anche $b - b', bb' \in B$. Essendo I un sottogruppo di A, si ha $c(b - b') = cb - cb' \in I$ per ogni $c \in I$, il che prova $b - b' \in B$. Inoltre per ogni $c \in I$ si ha $cb \in I$ e quindi anche $(cb)b' = c(bb') \in I$, il che prova $bb' \in B$.

   (c) Osserviamo che, essendo I un ideale sinistro di A e B' un sottoanello di A contenente I, ovviamente I è un ideale sinistro anche di B'. Dunque I è un ideale bilatero di B' se e solo se verifica l'ulteriore condizione $cb' \in I$ per ogni $c \in I$ e per ogni $b' \in B'$. Ora, per definizione di B, questo succede se e solo se ogni elemento b' di B' è un elemento di B, cioè se e solo se $B' \subseteq B$.

4. (a) Dato che $f_{n+1} = Xf_n + n + 2$, risulta

$$n + 2 = f_{n+1} - Xf_n \in I := (f_n, f_{n+1}).$$

   Se $n \neq -2$, $n + 2 \in K \setminus \{0\} = K^* = K[X]^*$, per cui $I = K[X]$ (un ideale che contiene un'unità è tutto l'anello). Se invece $n = -2$,

$f_{n+1} = Xf_n \in (f_n)$, e quindi $I = (f_n) \subsetneq K[X]$ ($f_n \notin K[X]^* = K^*$ perché $\deg(f) = n > 0$).

(b) Il numero cercato è $n = 3$. Infatti

$$f_2 = X^2 + \overline{2}X + \overline{3} = X^2 + \overline{2}X = X(X + \overline{2})$$

non è irriducibile, mentre

$$f_3 = X^3 + \overline{2}X^2 + \overline{3}X + \overline{4} = X^3 + \overline{2}X^2 + \overline{1}$$

è irriducibile perché di terzo grado e senza radici in $\mathbb{Z}/3\mathbb{Z}$, come è immediato verificare.

(c) No. Infatti, se n è dispari (per cui $\overline{n+1} = \overline{0}$), f_n non è irriducibile perché ha la radice $\overline{0}$. Se invece $n = 2m$ è pari, f_n non è irriducibile perché si ha

$$f_n = X^{2m} + X^{2m-2} + \cdots + X^2 + \overline{1} = \sum_{i=0}^{m} X^{2i} = (\sum_{i=0}^{m} X^i)^2.$$