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

Prova scritta del 10/07/2018

1. Trovare gli interi positivi x che risolvono il sistema

$$\begin{cases} x^2 \equiv x \mod 30 \\ 5^x \equiv 2 \mod 7 \end{cases}$$

2. Sia G un gruppo e sia H un sottogruppo di G. Dimostrare che le seguenti condizioni sono equivalenti:

   (a) l'unico sottogruppo normale di G contenente H è G stesso;

   (b) per ogni altro gruppo G', l'unico omomorfismo $G \to G'$ il cui nucleo contenga H è l'omomorfismo banale.

   Nel caso in cui $G = S_4$, trovare H non normale che non soddisfi tali condizioni.

3. (a) Dimostrare che

$$A := \left\{ \sum_{i \geq 0} a_i X^i \in \mathbb{Q}[X] \,:\, a_0 \in \mathbb{Z} \right\}$$

   è un sottoanello di $\mathbb{Q}[X]$.

   (b) Dimostrare che, per ogni sottogruppo G di $\mathbb{Q}$,

$$I_G := \left\{ \sum_{i \geq 0} a_i X^i \in \mathbb{Q}[X] \,:\, a_0 = 0,\ a_1 \in G \right\}$$

   è un ideale di A.

   (c) Stabilire se $I_{\mathbb{Q}}$ è un ideale principale di A.

4. Per ogni $a \in \mathbb{Z}$ sia $f_a := (2a+1)X^4 + (3a+4)X^2 - 10X + 5a$.

   (a) Esiste $a \in \mathbb{Z}$ tale che f_a sia irriducibile in $\mathbb{Z}/2\mathbb{Z}[X]$?

   (b) Fattorizzare f_{-1} in $\mathbb{Z}/3\mathbb{Z}[X]$.

   (c) Trovare il più piccolo intero positivo a tale che f_a sia irriducibile in $\mathbb{Q}[X]$ ma non in $\mathbb{Z}[X]$.

Soluzioni

1. Essendo $30 = 2 \cdot 3 \cdot 5$ con 2, 3 e 5 primi distinti (dunque a due a due coprimi), la prima congruenza è equivalente al sistema

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

Per ogni numero primo p le soluzioni di $x^2 \equiv x \mod p$ sono $x \equiv 0, 1 \mod p$: infatti x è soluzione se e solo se $p \mid (x^2 - x) = x(x-1)$ se e solo se $p \mid x$ o $p \mid (x-1)$. Tenendo conto che ogni intero x verifica $x \equiv 0, 1 \mod 2$, la prima congruenza è perciò equivalente al sistema

$$\begin{cases} x \equiv 0, 1 \mod 3 \\ x \equiv 0, 1 \mod 5 \end{cases}$$

D'altra parte, poiché (come è immediato verificare) l'ordine in $\mathbb{Z}/7\mathbb{Z}^*$ di $\overline{5}$ è 6 e $\overline{5}^4 = \overline{2}$, la seconda congruenza è verificata se e solo se $x \equiv 4 \mod 6$. Quest'ultima congruenza implica in particolare $x \equiv 1 \mod 3$, e quindi le soluzioni cercate sono le soluzioni del sistema

$$\begin{cases} x \equiv 0, 1 \mod 5 \\ x \equiv 4 \mod 6 \end{cases}$$

che si trovano facilmente essere $x \equiv 10, 16 \mod 30$.

2. Se vale (a) e $f\colon G \to G'$ è un omomorfismo tale che $H \subseteq \ker(f)$, allora $\ker(f) = G$ (perché $\ker(f)$ è un sottogruppo normale di G), per cui f è l'omomorfismo banale. Ciò dimostra (b).

Viceversa, assumendo (b), sia K un sottogruppo normale di G tale che $H \subseteq K$. L'omomorfismo di proiezione al quoziente $\pi\colon G \to G/K$ verifica $H \subseteq K = \ker(\pi)$, dunque π è l'omomorfismo banale. Essendo π anche suriettivo, G/K deve essere il gruppo banale, cioè $K = G$. Ciò dimostra (a).

Se infine $G = S_4$, si può per esempio prendere come H il sottogruppo generato dal 3-ciclo $(1, 2, 3)$. Infatti H non è normale (dato che $(3, 4)(1, 2, 3)(3, 4)^{-1} = (1, 2, 4) \notin H$), ma $H \subset A_4 \subsetneq S_4$ e A_4 è un sottogruppo normale di S_4.

3. (a) Chiaramente $1 \in A$. Dati $f = \sum_{i\geq 0} a_i X^i$ e $g = \sum_{i\geq 0} b_i X^i$ in A (cioè con $a_0, b_0 \in \mathbb{Z}$), anche $f - g = \sum_{i\geq 0}(a_i - b_i)X^i \in A$ (perché $a_0 - b_0 \in \mathbb{Z}$) e $fg = \sum_{i\geq 0} c_i X^i \in A$ (perché $c_0 = a_0 b_0 \in \mathbb{Z}$).

   (b) Chiaramente $I_G \subseteq A$ e $0 \in I_G$. Dati $f = \sum_{i\geq 0} a_i X^i$ e $g = \sum_{i\geq 0} b_i X^i$ in I_G (cioè con $a_0 = b_0 = 0$ e $a_1, b_1 \in G$), anche $f+g = \sum_{i\geq 0}(a_i + b_i)X^i \in I_G$ (perché $a_0 + b_0 = 0$ e $a_1 + b_1 \in G$). Se poi $h = \sum_{i\geq 0} c_i X^i \in A$ (cioè $c_0 \in \mathbb{Z}$), allora $hf = \sum_{i\geq 0} d_i X^i \in I_G$ (perché $d_0 = c_0 a_0 = 0$ e $d_1 = c_0 a_1 + c_1 a_0 = c_0 a_1 \in G$).

   (c) L'ideale
   $$I_{\mathbb{Q}} = \left\{ \sum_{i\geq 0} a_i X^i \in \mathbb{Q}[X] \,:\, a_0 = 0 \right\}$$
   non è principale. Infatti, come già visto nel punto precedente, per ogni $f = \sum_{i\geq 0} a_i X^i \in I_{\mathbb{Q}}$ e $h = \sum_{i\geq 0} c_i X^i \in A$, si ha $hf = \sum_{i\geq 0} d_i X^i$ con $d_1 = c_0 a_1 \in \langle a_1 \rangle$. Dato che $\langle a_1 \rangle \subsetneq \mathbb{Q}$ ($1 \notin \langle 0 \rangle = \{0\}$ e $\frac{a_1}{2} \notin \langle a_1 \rangle$ se $a_1 \neq 0$), questo implica chiaramente che $(f) \subsetneq I_{\mathbb{Q}}$ per ogni $f \in I_{\mathbb{Q}}$.

4. (a) No: infatti, se a è pari $f_a = X^4$, mentre se a è dispari
   $$f_a = X^4 + X^2 + \overline{1} = (X^2 + X + \overline{1})^2.$$

   (b) Si vede subito che l'unica radice in $\mathbb{Z}/3\mathbb{Z}$ di $f_{-1} = -X^4 + X^2 - X + \overline{1}$ è $\overline{1}$. Risulta in effetti $f_{-1} = -(X - \overline{1})(X^3 + X^2 + \overline{1})$; inoltre $\overline{1}$ è radice anche di $X^3 + X^2 + \overline{1}$ e $X^3 + X^2 + \overline{1} = (X - \overline{1})(X^2 - X - \overline{1})$. Dato che $X^2 - X - \overline{1}$ è irriducibile (perché di secondo grado senza radici), la fattorizzazione completa è
   $$f_{-1} = -(X - \overline{1})^2 (X^2 - X - \overline{1}).$$

   (c) Il valore cercato è $a = 2$. Infatti non può essere $a = 1$ perché $f_1 = 3X^4 + 7X^2 - 10X + 5$ è primitivo in $\mathbb{Z}[X]$ (per cui è irriducibile in $\mathbb{Q}[X]$ se e solo se lo è in $\mathbb{Z}[X]$). Invece
   $$f_2 = 5X^4 + 10X^2 - 10X + 10 = 5g$$
   (con $g = X^4 + 2X^2 - 2X + 2$) non è primitivo (e dunque non è irriducibile) in $\mathbb{Z}[X]$, mentre g è irriducibile in $\mathbb{Z}[X]$ (e quindi in $\mathbb{Q}[X]$) per il criterio di Eisenstein relativo al primo 2; ne segue che anche f_2 (essendo associato a g) è irriducibile in $\mathbb{Q}[X]$.