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

Prova scritta del 3.7.2017

1. Trovare le soluzioni $(x, k) \in \mathbb{Z} \times \mathbb{N}$ del sistema di congruenze

$$\begin{cases} x^k \equiv 2 \mod 7 \\ k \equiv 8 \mod 15. \end{cases}$$

2. Sia G il gruppo $S_3 \times \mathbb{Z}/4\mathbb{Z}$.
   (a) Dimostrare che esiste un sottogruppo di G di ordine 8.
   (b) Sia H un sottogruppo di G di ordine 8. Dimostrare che in H esiste un elemento della forma (a, b) con a trasposizione, mentre non esiste un elemento della forma (c, d) con c 3-ciclo.
   (c) Dimostrare che non esiste un sottogruppo normale di G di ordine 8.

3. Sia A un dominio che verrà considerato come sottoanello del suo campo dei quozienti K. Dato $c \in K$, sia $\alpha_c \colon A[X] \to K$ l'omomorfismo di anelli definito da $\alpha_c(f) = f(c)$.
   (a) Dimostrare che α_c non è iniettivo.
   (b) Dimostrare che α_c è suriettivo se e solo se $\ker(\alpha_c)$ è un ideale massimale.
   (c) Dimostrare che α_c non è suriettivo se $A = \mathbb{Z}$.

4. Si considerino i polinomi a coefficienti interi $f = X^4 - 2X^3 - 2X^2 + X + 6$ e $g = X^5 - 3X^2 - 4X - 6$.
   (a) Trovare $p \in \mathbb{Z}[X]$ monico di terzo grado tale che $(f, g) = (p)$ in $\mathbb{Q}[X]$.
   (b) Dimostrare che $(f, g) \neq (p)$ in $\mathbb{Z}[X]$. Dedurre che (f, g) non è un ideale principale in $\mathbb{Z}[X]$.

Soluzioni

1. Dato che $\mathrm{mcd}(2,7) = 1$, risolvere la prima congruenza equivale a risolvere l'equazione $\overline{x}^k = \overline{2}$ in $\mathbb{Z}/7\mathbb{Z}^*$. Fissato $\overline{x} \in \mathbb{Z}/7\mathbb{Z}^*$, esiste una soluzione k se e solo se $\overline{2} \in \langle\overline{x}\rangle$, e in tal caso la soluzione è unica modulo l'ordine di $\overline{x}$ (che coincide con l'ordine di $\langle\overline{x}\rangle$) in $\mathbb{Z}/7\mathbb{Z}^*$. Chiaramente $\overline{2} \notin \langle\overline{1}\rangle = \{\overline{1}\}$ e $\overline{2} \notin \langle\overline{6}\rangle = \{\overline{1}, \overline{6}\}$, mentre $\overline{2} \in \langle\overline{2}\rangle = \langle\overline{4}\rangle = \{\overline{1}, \overline{2}, \overline{4}\}$ e $\overline{2} \in \langle\overline{3}\rangle = \langle\overline{5}\rangle = \mathbb{Z}/7\mathbb{Z}^*$. Inoltre $\overline{2} = \overline{2}^1 = \overline{3}^2 = \overline{4}^2 = \overline{5}^4$, per cui le soluzioni della prima congruenza sono le coppie $(x,k) \in \mathbb{Z} \times \mathbb{N}$ che verificano una delle condizioni seguenti:

$$\begin{cases} x \equiv 2 \mod 7 \\ k \equiv 1 \mod 3 \end{cases} \quad \begin{cases} x \equiv 3 \mod 7 \\ k \equiv 2 \mod 6 \end{cases} \quad \begin{cases} x \equiv 4 \mod 7 \\ k \equiv 2 \mod 3 \end{cases} \quad \begin{cases} x \equiv 5 \mod 7 \\ k \equiv 4 \mod 6. \end{cases}$$

   Per ottenere le soluzioni del sistema di partenza, si tratta allora, in ciascuno di questi quattro casi, di risolvere un sistema della forma

$$\begin{cases} k \equiv a \mod n \\ k \equiv 8 \mod 15 \end{cases}$$

   (con $n = 3$ o 6). Tale sistema ha soluzione se e solo se $8 - a$ è un multiplo di $\mathrm{mcd}(n, 15) = 3$, e in questo caso la soluzione è unica modulo $\mathrm{mcm}(n, 15)$ (che vale 15 se $n = 3$ e 30 se $n = 6$). Dunque non ci sono soluzioni se $x \equiv 2, 5 \mod 7$ (visto che $a = 1, 4$), mentre la soluzione è unica modulo 30 se $x \equiv 3 \mod 7$ ($a = 2$ e $n = 6$) e modulo 15 se $x \equiv 4 \mod 7$ ($a = 2$ e $n = 3$). Esplicitamente si trova subito che le soluzioni cercate sono le coppie $(x,k) \in \mathbb{Z} \times \mathbb{N}$ che verificano una delle condizioni seguenti:

$$\begin{cases} x \equiv 3 \mod 7 \\ k \equiv 8 \mod 30 \end{cases} \qquad \begin{cases} x \equiv 4 \mod 7 \\ k \equiv 8 \mod 15. \end{cases}$$

2. (a) Osservando che, in generale, $H_1 \times H_2$ è un sottogruppo di $G_1 \times G_2$ se H_i è un sottogruppo di G_i per $i = 1, 2$, basta prendere come H_1 il sottogruppo generato da una trasposizione in $G_1 = S_3$ e $H_2 = G_2 = \mathbb{Z}/4\mathbb{Z}$. Infatti $\#H_1 = 2$ e $\#H_2 = 4$, per cui $\#(H_1 \times H_2) = 8$.

   (b) Se c è un 3-ciclo, $\mathrm{ord}((c,d)) = \mathrm{mcm}(\mathrm{ord}(c), \mathrm{ord}(d))$ è un multiplo di 3 (essendo $\mathrm{ord}(c) = 3$), e quindi non divide 8. Ne segue che $(c,d) \notin H$ per il teorema di Lagrange. Questo dimostra che, se $(a,b) \in H$, allora a può essere solo una trasposizione o l'elemento neutro. Non è possibile che sia $a = 1$ per ogni $(a,b) \in H$, altrimenti $H \subseteq \{1\} \times \mathbb{Z}/4\mathbb{Z}$ avrebbe ordine al massimo 4.

(c) Per assurdo sia H un sottogruppo normale di G di ordine 8. Per il punto precedente esiste $h = (a, b) \in H$ con a trasposizione. Poiché le trasposizioni sono tra loro coniugate in S_3, data un'altra trasposizione $a' \neq a$ esiste $c \in S_3$ tale che $a' = cac^{-1}$. Posto $g := (c, d)$ per qualche $d \in \mathbb{Z}/4\mathbb{Z}$, $h' := ghg^{-1} \in H$ per la normalità di H, e risulta $h' = (a', b)$. Essendo H un sottogruppo, $hh' = (aa', 2b) \in H$, e questo contraddice il punto precedente perché aa' è un 3-ciclo.

3. (a) Per definizione di campo dei quozienti, esistono $a, b \in A$ con $b \neq 0$ tali che $c = \frac{a}{b}$. Allora $\alpha_c(bX - a) = bc - a = 0$, il che dimostra che $0 \neq bX - a \in \ker(\alpha_c)$, e dunque α_c non è iniettivo.

   (b) $\ker(\alpha_c)$ è massimale se e solo se $A[X]/\ker(\alpha_c)$ è un campo. Essendo $A[X]/\ker(\alpha_c) \cong \mathrm{im}(\alpha_c)$ per il primo teorema di isomorfismo, basta dimostrare che α_c è suriettivo se e solo se $\mathrm{im}(\alpha_c)$ è un campo. È ovvio che, se α_c è suriettivo, allora $\mathrm{im}(\alpha_c) = K$ è un campo. Se viceversa $L := \mathrm{im}(\alpha_c)$ è un campo, chiaramente $A \subseteq L$ (dato che $a = \alpha_c(a)$ per ogni $a \in A$). Preso inoltre $x \in K$, esistono $y, z \in A$ con $z \neq 0$ tali che $x = \frac{y}{z}$. Osservando che nel campo L la moltiplicazione è definita come in K (perché L è un sottoanello di K in quanto immagine di un omomorfismo di anelli), dal fatto che $y, z \in A \subseteq L$ si deduce che $z^{-1} \in L$ e quindi anche $x = yz^{-1} \in L$. Ciò dimostra che $L = K$, cioè α_c è suriettivo.

   (c) Se $c = \frac{m}{n}$ con $m, n \in \mathbb{Z}$ e $n \neq 0$, per ogni $f = \sum_{i=0}^{d} a_i X^i \in \mathbb{Z}[X]$ si ha

$$\alpha_c(f) = f(c) = \sum_{i=0}^{d} a_i c^i = \sum_{i=0}^{d} a_i \frac{m^i}{n^i} = \frac{\sum_{i=0}^{d} a_i m^i n^{d-i}}{n^d},$$

   per cui ogni elemento nell'immagine di α_c si può scrivere come frazione con denominatore una potenza di n. Scelto allora un numero primo p che non compare nella fattorizzazione di n (cosa possibile perché i numeri primi sono infiniti), $\frac{1}{p}$ non si può scrivere in questa forma (altrimenti p dividerebbe n^d e quindi n), cioè $\frac{1}{p} \notin \mathrm{im}(\alpha_c)$.

4. (a) Essendo $\mathbb{Q}[X]$ un dominio euclideo e quindi a ideali principali (perché $\mathbb{Q}$ è un campo), un generatore dell'ideale (f, g) è dato da $\mathrm{mcd}(f, g)$, che può essere calcolato con l'algoritmo di Euclide. Facendo la divisione con resto di g per f si trova $g = (X+2)f + r$ con $r = 6X^3 - 12X - 18$. Risulta poi $f = \frac{1}{6}(X - 2)r$, dunque

r è l'ultimo resto non nullo e $\mathrm{mcd}(f,g) = r$. Inoltre $r = 6p$ con $p = X^3 - 2X - 3$ per cui p è il generatore cercato di (f,g) in $\mathbb{Q}[X]$ (r e p sono associati in $\mathbb{Q}[X]$, dato che $6 \in \mathbb{Q}[X]^* = \mathbb{Q}^*$).

(b) Se fosse $(f,g) = (p)$ in $\mathbb{Z}[X]$, esisterebbero $h, k \in \mathbb{Z}[X]$ tali che $fh + gk = p$, ma il termine noto di $fh + gk$ è necessariamente pari (poiché sono pari i termini noti di f e di g), mentre quello di p è dispari. Supponiamo poi per assurdo che (f,g) sia principale in $\mathbb{Z}[X]$, cioè che esista $p' \in \mathbb{Z}[X]$ tale che $(f,g) = (p')$ in $\mathbb{Z}[X]$. Chiaramente tale uguaglianza vale anche in $\mathbb{Q}[X]$, e dunque $(p') = (p)$ in $\mathbb{Q}[X]$. Essendo $\mathbb{Q}[X]$ un dominio, questo implica che p e p' sono associati, cioè esiste $a \in \mathbb{Q}[X]^* = \mathbb{Q}^*$ tale che $p' = ap$. D'altra parte $p, p' \in \mathbb{Z}[X]$ e p è monico, per cui deve essere $a \in \mathbb{Z}$. Inoltre p' divide f e g in $\mathbb{Z}[X]$, e questo implica, tenendo conto che f e g sono monici, che il coefficiente direttivo di p' (che coincide con a) deve essere 1 o -1. Quindi $p' = \pm p$, ma questo dà la contraddizione $(p) = (p') = (f,g)$ in $\mathbb{Z}[X]$.