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

Prova scritta del 17.2.2017

1. Sia p un numero primo e si consideri il sistema di congruenze

$$\begin{cases} 6x \equiv 3 \mod 15 \\ 3^x \equiv 9 \mod p. \end{cases}$$

   (a) Trovare le soluzioni del sistema per $p = 7$ e $p = 11$.

   (b) Dimostrare che il sistema ha sempre soluzioni se $p \not\equiv 1 \mod 5$.

2. Sia G un gruppo. Per ogni intero positivo n sia H_n il sottoinsieme di G costituito dagli elementi il cui ordine divide n.

   (a) Dimostrare che, se H_n è un sottogruppo di G, allora è normale in G.

   (b) Dimostrare che, se G è abeliano, allora H_n è un sottogruppo di G per ogni n.

   (c) Nel caso in cui $G = A_4$, determinare per quali valori di n H_n è un sottogruppo di G.

3. Sia A un anello e, dati due ideali I e J di A, sia $B = A/(I \cap J)$.

   (a) Esiste un omomorfismo suriettivo di anelli da B a A/I?

   (b) Dimostrare che, se I e J sono primi e $b \in B$ verifica $b^2 = 0$, allora $b = 0$.

   (c) Sempre assumendo che I e J siano primi, dimostrare che B è un dominio se e solo se $I \subseteq J$ o $J \subseteq I$.

4. Sia $p = X^4 + 2X^3 - 3X^2 - 5X + 2$ e $A = \mathbb{Q}[X]/(p)$. Per ogni $f \in \mathbb{Q}[X]$ sia inoltre $\overline{f} = f + (p) \in A$.

   (a) Fattorizzare p in $\mathbb{Q}[X]$.

   (b) Posto $f_a = X^3 - 3X + a$, determinare i valori $a \in \mathbb{Q}$ tali che $\overline{f_a}$ non è invertibile in A.

   (c) Dimostrare che ogni elemento non nullo e non invertibile di A è un divisore di zero.

Soluzioni

1. (a) Essendo $\mathrm{mcd}(6,15)=3$, la prima congruenza ha soluzione, e questa è unica modulo $\frac{15}{3}=5$. In effetti tale congruenza è equivalente a $2x \equiv 1 \mod 5$, le cui soluzioni sono $x \equiv 3 \mod 5$. D'altra parte, la seconda congruenza ha chiaramente sempre la soluzione $x=2$, e dunque, per $p \neq 3$, $x \in \mathbb{N}$ è soluzione se e solo se $x \equiv 2 \mod n_p$, dove indichiamo con n_p l'ordine di $\overline{3}$ in $\mathbb{Z}/p\mathbb{Z}^*$ (si noti che $n_p \mid (p-1) = \#(\mathbb{Z}/p\mathbb{Z}^*)$ per il teorema di Lagrange). Risulta $n_7 = 6$ (dato che $\overline{3}^6 = \overline{1}$, mentre $\overline{3}^1 = \overline{3}, \overline{3}^2 = \overline{2}, \overline{3}^3 = \overline{6} \neq \overline{1}$ in $\mathbb{Z}/7\mathbb{Z}$) e $n_{11} = 5$ (dato che $\overline{3}^5 = \overline{1}$, mentre $\overline{3}^1 = \overline{3}, \overline{3}^2 = \overline{9} \neq \overline{1}$ in $\mathbb{Z}/11\mathbb{Z}$). Dunque le soluzioni del sistema per $p=7$ coincidono con gli $x \in \mathbb{N}$ che verificano il sistema

$$\begin{cases} x \equiv 3 \mod 5 \\ x \equiv 2 \mod 6. \end{cases}$$

Poiché $\mathrm{mcd}(5,6)=1$, per il teorema cinese del resto tale sistema ha un'unica soluzione modulo $5 \cdot 6 = 30$, che si vede facilmente essere $x \equiv 8 \mod 30$. Invece il sistema dato non ha soluzioni per $p=11$, perché ovviamente non ci sono soluzioni del sistema

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

(b) Per $p=3$ ogni $x>0$ è soluzione della seconda congruenza, dunque il sistema ha soluzione in questo caso. Per $p \neq 3$, come visto nel punto precedente, le soluzioni del sistema sono gli $x \in \mathbb{N}$ che verificano il sistema

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

Se $p \not\equiv 1 \mod 5$, cioè $5 \nmid (p-1)$, si ha anche $5 \nmid n_p$. Allora $\mathrm{mcd}(5, n_p) = 1$, per cui il sistema ha un'unica soluzione modulo $5n_p$ per il teorema cinese del resto.

2. (a) Per dimostrare questo, dato che H_n è un sottogruppo per ipotesi, basta vedere che per ogni $g \in G$, $gHg^{-1} \subseteq H$. Ma se $h \in H$, cioè – per definizione di H – l'ordine di h è un naturale k divisore di n,

l'ordine di ghg^{-1} è anch'esso k perché il coniugio con g definisce un automorfismo (interno) di G. [Alternativamente, basta calcolare

$$(ghg^{-1})^k = ghg^{-1}ghg^{-1}\dots ghg^{-1} = gh^kg^{-1} = gg^{-1} = 1,$$

da cui si deduce che ghg^{-1} ha un ordine che divide k (e in effetti allo stesso modo si vede che l'ordine è proprio k)]. Di conseguenza ghg^{-1} appartiene ad H_n.

(b) Evidentemente, $1 \in H_n$. Se $h \in H_n$ e k è il suo ordine, $(h^{-1})^k = (h^k)^{-1} = 1$, per cui l'ordine di h^{-1} divide k (in effetti è proprio k) e $h^{-1} \in H_n$. Infine, se G è abeliano e $h_1, h_2 \in H_n$ hanno ordine rispettivamente k_1, k_2, sia m il minimo comune multiplo tra k_1 e k_2: allora $m|n$ e

$$(h_1h_2)^m = h_1h_2h_1h_2\dots h_1h_2 = (h_1)^m(h_2)^m = 1$$

giacché m è un multiplo sia di k_1, sia di k_2. Questo dimostra che l'ordine di h_1h_2 divide m, e quindi $h_1h_2 \in H_n$.

(c) Innanzitutto, ricordiamo che in A_4 sono presenti l'identità 1, 3 elementi di ordine 2 (le doppie trasposizioni) e 8 elementi di ordine 3 (i 3-cicli). Perciò banalmente per tutti gli n primi con 2 e 3 avremo $H_n = \{1\}$, che è un sottogruppo. Rimane il caso in cui n sia multiplo di 2 e/o di 3. Se n è multiplo di 2 ma non di 3, controllando nella lista degli elementi si vede che H_n consta dell'identità e delle doppie trasposizioni, che formano in effetti un sottogruppo; se n è multiplo di 3, ma non di 2, H_n risulta contenere l'identità e tutti i 3-cicli, che evidentemente non formano un sottogruppo anche perché si tratta di 9 elementi in tutto, e 9 non divide l'ordine di A_4 che è 12; infine, se n è multiplo di 6 si ottiene $H_n = A_4$ che è ovviamente un sottogruppo. Perciò nel caso $G = A_4$ i valori di n per cui H_n è un sottogruppo sono tutti gli n tranne i multipli dispari di 3.

3. (a) L'esistenza di un tale omomorfismo ci è garantita dal terzo teorema di isomorfismo per anelli: infatti, I è un ideale di A che contiene $I \cap J$ e perciò $I/(I \cap J)$ è un ideale di $A/(I \cap J)$ e l'omomorfismo (suriettivo) di passaggio al quoziente

$$B = A/(I \cap J) \to \big(A/(I \cap J)\big)/\big(I/(I \cap J)\big)$$

composto con l'isomorfismo

$$\big(A/(I \cap J)\big)/\big(I/(I \cap J)\big) \cong A/I$$

dà un omomorfismo con le proprietà richieste.

(b) Sia $b \in B$ tale che $b^2 = 0$. Questo significa che $b = a + (I \cap J)$ per un opportuno elemento $a \in A$ tale che $a^2 \in I \cap J$. Ma se dunque $a^2 \in I$ e $a^2 \in J$, poiché entrambi gli ideali sono primi dalla prima relazione deduciamo che $a \in I$ e dalla seconda che $a \in J$, cioè che $a \in I \cap J$: il che equivale a dire che $b = 0$ nell'anello B.

(c) Supponiamo che non sia né $I \subseteq J$, né $J \subseteq I$; allora esistono elementi $x \in I \setminus J$ e $y \in J \setminus I$. Ma allora $xy \in IJ \subseteq I \cap J$ mentre $x, y \notin I \cap J$: ciò dimostra che $I \cap J$ non è primo, e quindi $B = A/(I \cap J)$ non è un dominio.

Viceversa, se $I \subseteq J$ (o $J \subseteq I$) si ha che $I \cap J = I$ (o $I \cap J = J$), ed evidentemente B è un dominio, essendo il quoziente di A per l'ideale primo I (o J, rispettivamente).

4. (a) Le eventuali radici razionali di p vanno cercate in $\{\pm 1, \pm 2\}$. Poiché $f(1) = -3$, $f(-1) = 3$, $f(2) = 12$ e $f(-2) = 0$, l'unica radice razionale di p è -2. Dunque p è divisibile per $X + 2$, e risulta $p = (X + 2)(X^3 - 3X + 1)$. Questa è la fattorizzazione completa di p, perché $X^3 - 3X + 1$ è irriducibile in $\mathbb{Q}[X]$ (essendo di terzo grado e senza radici razionali, dato che -2 non è una sua radice).

(b) Dato $f \in \mathbb{Q}[X]$, per definizione $\overline{f}$ è invertibile in A se e solo se esiste $g \in \mathbb{Q}[X]$ tale che $\overline{f}\overline{g} = \overline{1}$. Tale uguaglianza vale se e solo se esiste $h \in \mathbb{Q}[X]$ tale che $fg + ph = 1$. Ne segue che $\overline{f}$ è invertibile in A se e solo se $(f, p) = (1)$ in $\mathbb{Q}[X]$. Essendo $\mathbb{Q}[X]$ un dominio a ideali principali, $(f, p) = (1)$ se e solo se $\mathrm{mcd}(f, p) = 1$. Posto $p_1 = X + 2$ e $p_2 = X^3 - 3X + 1$, per il punto precedente si ottiene allora (tenendo conto che $\mathbb{Q}[X]$ è un dominio a fattorizzazione unica) che $\overline{f_a}$ non è invertibile in A se e solo se $p_1 \mid f_a$ o $p_2 \mid f_a$. Ora, $f_a(-2) = a - 2 = 0$ se e solo se $a = 2$, per cui $p_1 \mid f_a$ se e solo se $a = 2$. D'altra parte $p_2 \mid f_a$ se e solo se $a = 1$ (la divisione di f_a per p_2 ha quoziente 1 e resto $a - 1$). Si conclude perciò che $\overline{f_a}$ non è invertibile in A se e solo se $a = 1, 2$.

(c) Dato $a \in A$, necessariamente della forma $a = \overline{f}$ per qualche $f \in \mathbb{Q}[X]$, per quanto visto al punto precedente a non è invertibile se e solo se $p_1 \mid f$ o $p_2 \mid f$. Inoltre $a \neq \overline{0}$ se e solo se $p = p_1 p_2 \nmid f$. Per l'unicità della fattorizzazione di f, si ottiene allora che, se a è non nullo e non invertibile, $p_1 \mid f$ e $p_2 \nmid f$ o $p_2 \mid f$ e $p_1 \nmid f$. Si può supporre che $p_1 \mid f$ (diciamo $f = p_1 g$) e $p_2 \nmid f$, e in questo caso a è un divisore di zero in A perché $b := \overline{p_2} \in A$ soddisfa $b \neq \overline{0}$ (visto che $p = p_1 p_2 \nmid p_2$) e $ab = \overline{f}\overline{p_2} = \overline{pg} = \overline{0}$.