Corso di Algebra 1 - a.a. 2014-2015

Prova scritta dell'1.7.2015

1. Per quali numeri primi p il sistema di congruenze

$$\begin{cases} x^3 \equiv -1 \mod p \\ x \equiv 4 \mod 30 \end{cases}$$

   non ha soluzione?

   Determinare inoltre tutte le soluzioni per $p = 7$.

2. Sia H un sottogruppo di ordine 6 di A_5.

   (a) Dimostrare che esistono un 3-ciclo τ e una doppia trasposizione σ tali che $H =< \tau, \sigma >$.

   (b) Dimostrare che H è isomorfo al gruppo diedrale D_3.

3. Si consideri la seguente domanda relativa a un anello A:

   Esistono in A due ideali non nulli I e J tali che $I \cap J = \{0\}$?

   (a) Dimostrare che la risposta alla domanda è no se A è un dominio.

   (b) Sia $A = \mathbb{Z}/n\mathbb{Z}$ con n un intero positivo. Dimostrare che la risposta alla domanda è no se e solo se n è una potenza di un numero primo.

4. Siano A un anello commutativo, $I \neq A$ un suo ideale e $a \in A$. Sia inoltre $J = \{P \in A[X] : P(a) \in I\} \subseteq A[X]$.

   (a) Dimostrare che J è un ideale di $A[X]$ e $J \neq A[X]$.

   (b) Dimostrare che J è primo se e solo se I è primo.

   (c) Dimostrare che $J = (X - a, I)$.

Soluzioni

1. La prima congruenza ha sempre almeno la soluzione $x \equiv -1 \mod p$. Essendo $30 = 2 \cdot 3 \cdot 5$, ne segue che, per il teorema cinese del resto, il sistema ha sempre soluzione se $p > 5$. Se $p = 2$ la prima congruenza equivale a $x \equiv 1 \mod 2$, mentre la seconda implica $x \equiv 0 \mod 2$. Analogamente, se $p = 3$ la prima congruenza equivale a $x \equiv 2 \mod 3$, mentre la seconda implica $x \equiv 1 \mod 3$. Infine, se $p = 5$ il sistema ha la soluzione $x \equiv 4 \mod 30$. In conclusione il sistema non ha soluzione se e solo se $p = 2$ o $p = 3$.

   Se $p = 7$ le soluzioni della prima congruenza sono $x \equiv 3, 5, 6 \mod 7$. Perciò le soluzioni del sistema sono l'unione delle soluzioni di ciascuno dei seguenti sistemi

$$\begin{cases} x \equiv 3 \mod 7 \\ x \equiv 4 \mod 30 \end{cases} \qquad \begin{cases} x \equiv 5 \mod 7 \\ x \equiv 4 \mod 30 \end{cases} \qquad \begin{cases} x \equiv 6 \mod 7 \\ x \equiv 4 \mod 30 \end{cases}$$

   Per il teorema cinese del resto ciascuno di tali sistemi ha un'unica soluzione modulo $7 \cdot 30 = 210$. Un semplice calcolo mostra che le soluzioni cercate sono allora $x \equiv 94, 124, 34 \mod 210$.

2. (a) Ogni gruppo di ordine 6 è ciclico o isomorfo a D_3, dunque contiene sia elementi di ordine 2 che elementi di ordine 3. Esistono quindi $\sigma, \tau \in H$ tali che $\text{ord}(\sigma) = 2$ e $\text{ord}(\tau) = 3$. Dato che gli elementi non banali di A_5 sono solo le doppie trasposizioni (di ordine 2), i 3-cicli (di ordine 3) e i 5-cicli (di ordine 5), σ deve essere una doppia trasposizione e τ un 3-ciclo. Posto $H' =< \sigma, \tau >$ resta solo da dimostrare che $H' = H$. Chiaramente H' è un sottogruppo di H e H' contiene il sottogruppo generato da σ (di ordine 2) e il sottogruppo generato da τ (di ordine 3). Indicando con n l'ordine di H', per il teorema di Lagrange si ha allora $2, 3 \mid n \mid 6$. Da ciò segue che $\text{mcm}(2, 3) = 6 \mid n$ e pertanto $n = 6$, cioè $H' = H$.

   (b) Come osservato nel punto precedente, A_5 (e quindi H) non contiene elementi di ordine 6. Perciò H non può essere ciclico, e quindi deve essere isomorfo a D_3.

3. (a) Se $I, J \neq \{0\}$, esistono $0 \neq a \in I$ e $0 \neq b \in J$. Poiché A è un dominio, $0 \neq ab \in IJ \subseteq I \cap J$, per cui $I \cap J \neq \{0\}$.

   (b) Sia $n = p^m$ con p numero primo e $m \in \mathbb{N}$. Dati I e J ideali non nulli di $\mathbb{Z}/n\mathbb{Z}$ (notiamo che questo implica $n > 1$, cioè $m > 0$), va dimostrato che $I \cap J \neq \{\bar{0}\}$. Ricordando che ogni ideale di $\mathbb{Z}/n\mathbb{Z}$ è della forma $n'\mathbb{Z}/n\mathbb{Z}$ con n' divisore positivo di n e un tale ideale è nullo se e solo se $n' = n$, esistono $h, k \in \mathbb{N}$ con $h, k < m$ tali che $I = p^h\mathbb{Z}/p^m\mathbb{Z}$ e $J = p^k\mathbb{Z}/p^m\mathbb{Z}$. Si può supporre $h \leq k$, e allora $I \cap J = J \neq \{\bar{0}\}$.

Se invece n non è una potenza di un numero primo, esistono interi $1 < n_1, n_2 < n$ tali che $n = n_1 n_2$ e $\mathrm{mcd}(n_1, n_2) = 1$. Allora $I = n_1\mathbb{Z}/n\mathbb{Z}$ e $J = n_2\mathbb{Z}/n\mathbb{Z}$ sono ideali non nulli di $\mathbb{Z}/n\mathbb{Z}$ (come osservato nel punto precedente) tali che $I \cap J = \{\bar{0}\}$. Per dimostrare quest'ultima uguaglianza basta osservare che, dato $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ (con $a \in \mathbb{Z}$), si ha $\bar{a} \in I$ se e solo se $n_1 \mid a$, e analogamente $\bar{a} \in J$ se e solo se $n_2 \mid a$. Dunque $\bar{a} \in I \cap J$ se e solo se $n_1, n_2 \mid a$ se e solo se $\mathrm{mcm}(n_1, n_2) = n \mid a$ se e solo se $\bar{a} = \bar{0}$.

4. (a) La funzione $f \colon A[X] \to A$ definita da $f(P) = P(a)$ è un omomorfismo di anelli (detto di valutazione in a), ed è chiaro che $J = f^{-1}(I)$. Allora J è un ideale perché controimmagine di un ideale attraverso un omomorfismo di anelli. Inoltre $1 \notin J$ perché $f(1) = 1 \notin I$.

   (b) Indicando con $\pi \colon A \to A/I$ la proiezione naturale,
$$f' = \pi \circ f \colon A[X] \to A/I$$
è un omomorfismo suriettivo di anelli, dato che lo sono sia π che f (f è suriettivo perché $b = f(b)$ per ogni $b \in A$). Essendo inoltre
$$\ker(f') = f^{-1}(\ker(\pi)) = f^{-1}(I) = J,$$
per il primo teorema di isomorfismo c'è un isomorfismo di anelli $A/I \cong A[X]/J$. Allora J è primo se e solo se $A[X]/J$ è un dominio se e solo se A/I è un dominio se e solo se I è primo.

   (c) Chiaramente $I \subset J$ e $X - a \in J$, dunque basta dimostrare che $J \subseteq (X - a, I)$. Dato $P \in J$ si può fare la divisione con resto di P per $X - a$ (essendo $X - a$ monico), cioè esistono $Q, R \in A[X]$ tali che
$$P = (X - A)Q + R$$
con $R = 0$ o $\deg(R) < \deg(X - a) = 1$. Risulta quindi $R \in A$, da cui segue $f(R) = R$. Si ha inoltre
$$R = P - (X - a)Q \in J$$
(perché J è un ideale e $P, X - a \in J$), e questo implica, per definizione di J, che $f(R) \in I$. Allora $R = f(R) \in I$ e l'uguaglianza $P = (X - A)Q + R$ dimostra che $P \in (X - a, I)$.