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

Prova scritta del 28.1.2015

1. Sia p un numero primo e n un intero non divisibile per p.

   (a) Dimostrare che esiste $x \in \mathbb{N}$ tale che

   $$\begin{cases} nx \equiv 1 \mod p \\ n^x \equiv 1 \mod p. \end{cases}$$

   (b) Determinare il minimo $x \in \mathbb{N}$ tale che

   $$\begin{cases} 3x \equiv 1 \mod 11 \\ 3^x \equiv 1 \mod 11. \end{cases}$$

2. Si consideri la permutazione $\sigma = (1, 2, 3)$ in S_5, sia H il sottogruppo di S_5 generato da σ e sia $K = \{\tau \in S_5 : \tau H \tau^{-1} = H\}$.

   (a) Dimostrare che K è un sottogruppo di S_5 e che $K \supseteq C(\sigma)$ (dove $C(\sigma) = \{\tau \in S_5 : \tau\sigma = \sigma\tau\}$).

   (b) Dimostrare che, dato $\tau \in S_5$, si ha $\tau \in K$ se e solo se $\tau(\{1, 2, 3\}) = \{1, 2, 3\}$.

   (c) Dimostrare che H è un sottogruppo normale di K e che K/H è isomorfo a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

3. Sia A un anello e siano I, J, K tre ideali di A.

   (a) Dimostrare che $I + (J \cap K) \subseteq (I + J) \cap (I + K)$.

   (b) Dimostrare che, se $A = \mathbb{Z}$, allora $I + (J \cap K) = (I + J) \cap (I + K)$.

4. Dato $q \in \mathbb{Q}$, sia $A_q = \mathbb{Q}[X]/(X^3 - 2X^2 + q)$.

   (a) Trovare un valore di q tale che A_q sia un campo.

   (b) Stabilire se A_0 e A_1 sono domini di integrità.

   (c) Dimostrare che A_0 e A_1 non sono isomorfi come anelli.

Soluzioni

1. (a) Essendo $\mathrm{mcd}(n,p)=1$, si ha $\bar{n}\in\mathbb{Z}/p\mathbb{Z}^*$, dove $\bar{n}$ indica la classe di n in $\mathbb{Z}/p\mathbb{Z}$. Dato un intero x, la congruenza $nx\equiv 1 \mod p$ è verificata se e solo se $\bar{n}\bar{x}=\bar{1}$ nel gruppo $\mathbb{Z}/p\mathbb{Z}^*$, cioè se e solo se $\bar{x}=\bar{n}^{-1}$. D'altra parte, per $x\in\mathbb{N}$ la congruenza $n^x\equiv 1 \mod p$ è equivalente a $\bar{n}^x=\bar{1}$ in $\mathbb{Z}/p\mathbb{Z}^*$, ed è quindi verificata se e solo se x è multiplo dell'ordine k di $\bar{n}$ in $\mathbb{Z}/p\mathbb{Z}^*$. Indicando con a un intero tale che $\bar{a}=\bar{n}^{-1}$, si tratta allora di dimostrare che esiste $x\in\mathbb{N}$ che sia soluzione del seguente sistema di congruenze:

$$\begin{cases} x\equiv a \mod p \\ x\equiv 0 \mod k. \end{cases}$$

Per il teorema di Lagrange k divide l'ordine di $\mathbb{Z}/p\mathbb{Z}^*$, cioè $p-1$, e dunque $\mathrm{mcd}(p,k)=1$. Segue dal teorema cinese del resto che il sistema ha un'unica soluzione modulo pk, e in particolare ammette soluzioni in $\mathbb{N}$.

(b) Mantenendo la notazione della prima parte (con $p=11$ e $n=3$), si può prendere $a=4$ (perché $\bar{3}\cdot\bar{4}=\bar{1}$), mentre risulta $k=5$. Per vedere quest'ultimo fatto basta osservare che l'ordine di $\bar{3}$ in $\mathbb{Z}/11\mathbb{Z}^*$ è un divisore di $11-1=10$, $\bar{3}^2\neq\bar{1}$ e $\bar{3}^5=\bar{1}$. Ci si è quindi ricondotti a risolvere il sistema

$$\begin{cases} x\equiv 4 \mod 11 \\ x\equiv 0 \mod 5. \end{cases}$$

Si trova facilmente che la soluzione generale del sistema è $x\equiv 15 \mod 55$, e quindi la soluzione minima in $\mathbb{N}$ è $x=15$.

2. (a) Ovviamente $(1)\in K$, dunque $K\neq\emptyset$. Se $\tau,\rho\in K$, allora

$$(\tau\rho)H(\tau\rho)^{-1}=(\tau\rho)H(\rho^{-1}\tau^{-1})=\tau(\rho H\rho^{-1})\tau^{-1}=\tau H\tau^{-1}=H,$$

e quindi $\tau\rho\in K$. Se poi $\tau\in K$, dall'uguaglianza $H=\tau H\tau^{-1}$ segue

$$\tau^{-1}H(\tau^{-1})^{-1}=\tau^{-1}(\tau H\tau^{-1})\tau=(\tau^{-1}\tau)H(\tau^{-1}\tau)=(1)H(1)=H,$$

e quindi $\tau^{-1}\in K$. Questo conclude la dimostrazione del fatto che K è un sottogruppo di S_5. Infine, se $\tau\in C(\sigma)$, allora $\tau\sigma\tau^{-1}=\sigma$, e dunque $\tau\sigma^i\tau^{-1}=(\tau\sigma\tau^{-1})^i=\sigma^i$ per ogni $i\in\mathbb{Z}$. Ne segue che $\tau\in K$ (visto che gli elementi di H sono della forma σ^i con $i=0,1,2$), il che dimostra che $C(\sigma)\subseteq K$.

(b) Per ogni $\tau \in S_5$ e per ogni 3-ciclo (a,b,c) si ha $\tau(a,b,c)\tau^{-1} = (\tau(a),\tau(b),\tau(c))$. Essendo $H = \{(1),(1,2,3),(1,3,2)\}$, si ottiene pertanto $\tau H\tau^{-1} = \{(1),(\tau(1),\tau(2),\tau(3)),(\tau(1),\tau(3),\tau(2))\}$. A questo punto è chiaro che $\tau \in K$ se e solo se $\{1,2,3\} = \{\tau(1),\tau(2),\tau(3)\} = \tau(\{1,2,3\})$.

(c) H è un sottogruppo di S_5 ovviamente contenuto in K, e dunque è un sottogruppo di K. Inoltre per ogni $\tau \in K$ vale $\tau H\tau^{-1} = H$ per definizione, e pertanto H è normale in K. Per il punto precedente gli elementi di K sono le permutazioni di S_5 che mandano in sè l'insieme $\{1,2,3\}$ (e necessariamente allora anche $\{4,5\}$). Se ne deduce che ogni $\tau \in K$ si scrive in modo unico come $\tau = \tau_1\tau_2$ con τ_1 che fissa 4 e 5 e τ_2 che fissa 1, 2 e 3. Si può identificare τ_1 con un elemento di $S(\{1,2,3\}) = S_3$ e τ_2 con un elemento di $S(\{4,5\}) \cong S_2$ (e in effetti si vede facilmente che K è isomorfo a $S_3 \times S_2 \cong S_3 \times \mathbb{Z}/2\mathbb{Z}$). Dunque $\#K = \#(S_3 \times S_2) = 12$, e poiché $\#H = 3$, si ha $\#(K/H) = \frac{\#K}{\#H} = \frac{12}{3} = 4$. Per concludere che $K/H \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ basta allora dimostrare che $g^2 = 1$ per ogni $g \in K/H$, cioè che $\tau^2 \in H$ per ogni $\tau \in K$. Scrivendo $\tau = \tau_1\tau_2$ come prima e osservando che τ_1 e τ_2 commutano, si trova infatti $\tau^2 = \tau_1^2\tau_2^2 = \tau_1^2$ (perché τ_2 può essere solo (1) o $(4,5)$). Se $\tau_1 \in H$, anche $\tau_1^2 \in H$; altrimenti τ_1 è una trasposizione (di due elementi di $\{1,2,3\}$), e anche in questo caso $\tau_1^2 = (1) \in H$.

3. (a) Dato $a \in I + (J \cap K)$, per definizione di somma di ideali esistono $b \in I$ e $c \in J \cap K$ tali che $a = b + c$. Essendo $c \in J$ e $c \in K$, questa stessa scrittura mostra che $a \in I + J$ e $a \in I + K$, quindi $a \in (I + J) \cap (I + K)$.

(b) Se $A = \mathbb{Z}$ esistono $a,b,c \in \mathbb{N}$ tali che $I = a\mathbb{Z}$, $J = b\mathbb{Z}$ e $K = c\mathbb{Z}$. Ricordando che dati due interi m e n si ha $m\mathbb{Z}+n\mathbb{Z} = \mathrm{mcd}(m,n)\mathbb{Z}$ e $m\mathbb{Z} \cap n\mathbb{Z} = \mathrm{mcm}(m,n)\mathbb{Z}$, risulta allora

$$I + (J \cap K) = \mathrm{mcd}(a, \mathrm{mcm}(b,c))\mathbb{Z},$$
$$(I + J) \cap (I + K) = \mathrm{mcm}(\mathrm{mcd}(a,b), \mathrm{mcd}(a,c))\mathbb{Z}.$$

Basta quindi dimostrare che per ogni $a,b,c \in \mathbb{N}$ vale

$$\mathrm{mcd}(a, \mathrm{mcm}(b,c)) = \mathrm{mcm}(\mathrm{mcd}(a,b), \mathrm{mcd}(a,c)).$$

Se $a = 0$ entrambi i membri valgono $\mathrm{mcm}(b,c)$, mentre se $b = 0$ o $c = 0$ entrambi i membri valgono a, per cui si può supporre $a,b,c > 0$. Scrivendo $a = \prod_p p^{\alpha_p}$ (dove la produttoria è su tutti i

numeri primi, gli α_p sono in $\mathbb{N}$ e solo un numero finito sono non nulli) e analogamente $b = \prod_p p^{\beta_p}$ e $c = \prod_p p^{\gamma_p}$, l'uguaglianza da dimostrare diventa

$$\prod_p p^{\min\{\alpha_p, \max\{\beta_p, \gamma_p\}\}} = \prod_p p^{\max\{\min\{\alpha_p, \beta_p\}, \min\{\alpha_p, \gamma_p\}\}}.$$

Per concludere è sufficiente allora osservare che

$$\min\{\alpha, \max\{\beta, \gamma\}\} = \max\{\min\{\alpha, \beta\}, \min\{\alpha, \gamma\}\}$$

per ogni $\alpha, \beta, \gamma \in \mathbb{N}$, visto che se $\alpha \geq \beta, \gamma$ entrambi i membri valgono $\max\{\beta, \gamma\}$ e altrimenti entrambi valgono α.

4. Posto $f_q = X^3 - 2X^2 + q$, l'anello A_q è un dominio (rispettivamente un campo) se e solo se l'ideale (f_q) è primo (rispettivamente massimale) in $\mathbb{Q}[X]$. Poiché $\mathbb{Q}[X]$ è un dominio a ideali principali (essendo $\mathbb{Q}$ un campo) e $f_q \neq 0$, si ha inoltre che (f_q) è primo se e solo se (f_q) è massimale se e solo se f_q è irriducibile. Pertanto A_q è un campo se e solo se A_q è un dominio se e solo se f_q è irriducibile in $\mathbb{Q}[X]$.

   (a) Per quanto detto sopra basta trovare un valore di q tale che f_q sia irriducibile in $\mathbb{Q}[X]$. Si può prendere per esempio $q = 2$: per il criterio di Eisenstein rispetto al primo 2, f_2 è irriducibile in $\mathbb{Z}[X]$, e quindi anche in $\mathbb{Q}[X]$.

   (b) A_0 e A_1 non sono domini, dato che f_0 e f_1 sono riducibili in $\mathbb{Q}[X]$. Infatti si trova facilmente che le loro fattorizzazioni come prodotto di irriducibili sono $f_0 = X^2(X-2)$ e $f_1 = (X-1)(X^2 - X - 1)$ (osservando che le radici di f_1 vanno cercate in $\{\pm 1\}$).

   (c) Basta dimostrare che in A_0 esiste un elemento $a \neq 0$ tale che $a^2 = 0$, mentre in A_1 no (chiaramente l'esistenza di un tale elemento è una proprietà preservata da ogni isomorfismo di anelli). In effetti, ricordando dal punto precedente che $f_0 = X^2(X-2)$, in A_0 basta prendere $a = X(X-2) + (f_0)$ (dato che $X(X-2) \notin (f_0)$, mentre $[X(X-2)]^2 \in (f_0)$). Invece $f_1 = gh$ con $g = X-1$ e $h = X^2 - X - 1$ irriducibili non associati in $\mathbb{Q}[X]$. Ne segue che (g) e (h) sono ideali coprimi tali che $(g)(h) = (f_1)$. Dal teorema cinese per anelli si deduce allora che $A_1 \cong B \times C$, con $B = \mathbb{Q}[X]/(g)$ e $C = \mathbb{Q}[X]/(h)$. Come già detto, l'irriducibilità di g e h implica che B e C sono campi, ed è allora ovvio che $(0,0)$ è l'unico elemento di $B \times C$ il cui quadrato è $(0,0)$.