Corso di Laurea in Matematica 2014-2015

Alegbra I - prova scritta del 16 giugno 2015: soluzioni

Esercizio 1. *Sia p un numero primo fissato, e siano $a, b \in \mathbb{Z}$. Posto*

$$\Delta = \sum_{i=0}^{p} a^i b^{p-i},$$

si provi che $\Delta \equiv a \pmod{p}$ se $a \equiv b \pmod{p}$, mentre $\Delta \equiv a + b \pmod{p}$ nel caso in cui $a \not\equiv b \pmod{p}$.

Soluzione. 1. Supponiamo $a \equiv b \pmod{p}$. Allora, per ogni $0 \leq i \leq p$,

$$a^i b^{p-i} \equiv a^i a^{p-i} \equiv a^p \equiv a \pmod{p}$$

(dove, per l'ultima congruenza, si è applicata una conseguenza del Teorema di Fermat); quindi

$$\Delta \equiv \sum_{i=0}^{p} a = (p+1)a = a + pa \equiv a \pmod{p}.$$

2. Supponiamo $a \not\equiv b \pmod{p}$. Allora $a - b \not\equiv 0 \pmod{p}$. Ora

$$(a-b)\Delta = (a-b)(a^p + a^{p-1}b + \cdots + ab^{p-1} + b^p) = a^{p+1} - b^{p+1}.$$

Osservndo che, per il teorema di Fermat, si ha $x^{p+1} = x^x \equiv x^2 \pmod{p}$, per ogni $x \in \mathbb{Z}$, si deduce che

$$(a-b)\Delta \equiv a^2 - b^2 = (a-b)(a+b) \pmod{p},$$

ovvero p divide $(a-b)(\Delta - (a+b))$. Poiché p è un primo e non divide $a - b$, si conclude che p divide $\Delta - (a+b)$, ovvero che $\Delta \equiv a + b \pmod{p}$.

Esercizio 2. *Sia $\Omega = \{(x, y) \mid x, y \in (0, +\infty)\}$, l'insieme di tutti i punti nel piano cartesiano $\mathbb{R}^2$ le cui coordinate sono entrambe positive. Su Ω si definisca la relazione σ ponendo, per ogni $P = (x, y), P' = (x', y') \in \Omega$,*

$$P \sigma P'$$

se $P = P'$ oppure $y \leq y'$ e il coefficiente angolare della retta congiungente P con P' è ≥ 2 (con la convenzione che le rette verticali hanno ceoff. angolare $+\infty$).

(1) Si provi che σ è una relazione d'ordine su Ω e si dica se è totale.

(2) Si provi che per ogni $P, Q \in \Omega$ esiste $P \vee Q = \sup_\Omega(\{P, Q\})$.

(3) Sia $B = \{(x, y) \in \Omega \mid x, y \in \mathbb{N} \setminus \{0\}, y \geq 2x\}$; si dica se B ammette minimo e/o estremo inferiore.

SOLUZIONE. 1. *riflessività.* La proprietà riflessiva di σ è data per definizione.

antissimmetria. Siano $P = (x, y), P' = (x', y') \in \Omega$ con $P\sigma P'$ e $P'\sigma P$; supponiamo, per assurdo, $P \neq P'$, allora $y \leq y'$ e $y' \leq y$, da cui $y = y'$; quindi $x \neq x'$ e il coefficiente angolare della retta congiungente P a P' è 0, contro l'assunzione $P\sigma P'$.

transitività. Siano $P = (x, y), P' = (x', y'), P'' = ('', y'') \in \Omega$ con $P\sigma P'$ e $P'\sigma P''$; vogliamo provare $P\sigma P''$. Tale conclusione è banale se $P = P'$ oppure $P' = P''$, assumiamo quindi $P \neq P'$v e $P' \neq P''$. Allora $y \leq y' \leq y''$, quindi $y \leq y''$; inoltre la condizione sui coefficienti angolari fornisce le diseguaglianze

$$\begin{cases} y' - y \geq \\ y'' - y' \geq 2(x'' - x') \end{cases}$$

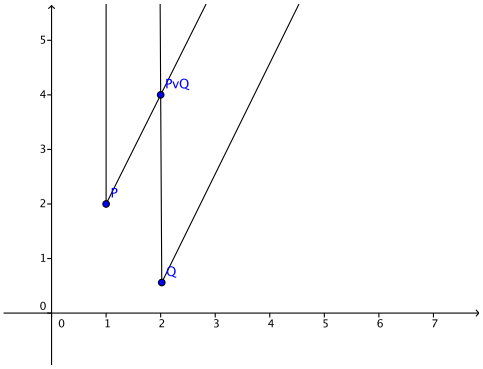
da cui:

$$y'' - y = (y'' - y') + (y' - y) \geq 2(x'' - x') + 2(x' - x) = 2(x'' - x);$$

quindi il coefficiente angolare della retta congiungente P a P'' è almeno 2, e pertanto $P\sigma P''$, come si voleva.

Questo prova che σ è una relazione d'ordine su Ω. Non è totale: ad esempio, posto $P = (1, 1)$ e $Q = (2, 2)$ si ha $P \not\sigma Q$ e $Q \not\sigma P$.

2. Siano $P = (x_0, y_0), Q = (x_1, y_1) \in \Omega$. La figura qui sotto fa capire cosa sta succedendo.



Possiamo supporre $x_1 \geq x_0$. Se $y_1 - y_0 \geq 2(x_1 - x_0)$, allora anche $y_1 \geq y_0$ e $P\sigma Q$ per cui $P \vee Q = Q$. Sia $y_1 - y_0 < 2(x_1 - x_0)$ e consideriamo il punto R di coordinate

$$\begin{cases} x_R = x_1 \\ y_R = 2(x_1 - x_0) + y_0 \end{cases}$$

Si prova dalla definizione che $P\sigma R$ (poiché R giace sulla retta di coeff. angolare 2 passante per P e $y_R \geq y_0$) e $Q\sigma R$ (poiché R giace sulla retta verticale passante per Q e $y_R = 2(x_1 - x_0) + y_0 \geq y_1 - y_0 + y_0 = y_1$; quindi R è maggiorante di

$\{P, Q\}$. D'altra parte se $T = (x_2, y_2)$ un maggiorante di $\{P, Q\}$; allora

$$\begin{cases} y_2 \geq y_i \\ y_2 - y_i \geq 2(x_2 - x_i) \end{cases}$$

per $i = 0, 1$. Quindi $y_2 \geq y_R$; inoltre

$$y_2 - y_R = y_2 - 2(x_1 - x_0) - y_0 \geq 2(x_2 - x_0) - 2(x_R - x_0) = 2(x_2 - x_R)$$

dunque il coeff. angolare della retta per R e T è maggiore o uguale a 2 e pertanto $R\sigma T$. Questo dimostra che $R = P \vee Q$.

3. Osserviamo che $(1, 2) \in B$. Sia $X = (a, b) \in B$ allora $1 \leq a, b \in \mathbb{N}$ e $b \geq 2a$. In particolare $b \geq 2$. Se $a = 1$ allora X giace sulla retta verticale per $(1, 2)$, quindi $(1, 2)\sigma X$. Se $a > 1$ allora $b - 2 \geq 2a - 2 = 2(a - 1)$, e dunque $(1, 2)\sigma X$. Questo prova che $(1, 2)$ è il minimo (e pertanto anche l'estremo inferiore) di B.

Esercizio 3. *Questioni sugli ideali primi.*

(1) *Sia $\phi : A \to B$ un omomorfismo di anelli e sia J un ideale primo di B; si provi che $\phi^{-1}(J)$ è un ideale primo di A.*
(2) *Sia $I_1 \supset I_2 \supset I_3 \dots$ una catena discendente di ideali primi dell'anello A; si provi che $\bigcap_{i \geq 1} I_i$ è un ideale primo di A.*
(3) *Sia A un P.I.D. e siano I, J ideali primi di A; si provi che se $I \supseteq J$ allora $I = J$ oppure $J = \{0_A\}$.*
(4) *Nell'anello $\mathbb{Z}[x]$ si trovino due ideali primi I, J non banali, distinti, e tali che $J \supset I$.*

Soluzione. 1. Che $\phi^{-1}(J)$ sia un ideale di A è una fatto provato a lezione, e si poteva dare per noto. Proviamo che $\phi^{-1}(J)$è un ideale proprio di A; infatti se, per assurdo, fosse $\phi^{-1}(J) = A$, allora, in particolare, $1_A \in \phi^{-1}(J)$, ovvero $1_B = \phi(1_A) \in J$, da cui l'assurdo $J = B$.

Proviamo quindi che $\phi^{-1}(J)$ ùprimo. Siano $x, y \in A$ tali che $xy \in \phi^{-1}(J)$; allora - tenendo conto che ϕ è un omomorfismo -

$$\phi(x)\phi(y) = \phi(xy) \in J,$$

e poiché J è un ideale primo di B, $\phi(x) \in J$ o $\phi(y) \in J$; dunque $x \in \phi^{-1}(J)$ oppure $y \in \phi^{-1}(J)$. Questo prova che $\phi^{-1}(J)$ è un ideale primo di A.

attenzione: $\phi^{-1}(\dots)$ indica la *controimmagine*; utilizzare ϕ^{-1} come una funzione da B ad A (come se ϕ fosse necessariamente invertibile) è un errore, ed è anche grave.

2. Sia $I = \bigcap_{i\geq 1} I_i$. Sappiamo dalla teoria che I è un ideale di A (*l'intersezione di una qualsiasi famiglia di ideali è un ideale*), ed è chiaramente proprio, dato che ciascun I_n è tale.

Siano $a, b \in A$ tali che $ab \in I$ e supponiamo $a \notin I$, allora esiste $n \in \mathbb{N}$ tale che $a \notin I_n$, e quindi, $a \notin A_k$ per ogni $k \geq n$ (dato che, in tal caso, $I_k \subseteq I_n$). Per la proprietà degli ideali primi, $b \in I_k$ per ogni $k \geq n$; inoltre $b \in I_i$ per ogni $0 \leq i \leq n$ dato che, in questo caso, $I_n \subseteq I_i$. Dunque $b \in I$, come si voleva provare.

3. Sappiamo dalla teoria che in un P.I.D. gli ideali primi non banali sono massimali. Quindi se I, J sono ideali primi di A (che è un P.I.D.) e $J \subseteq I$, allora $J = \{0_A\}$ oppure - appunto - J è massimale e dunque $I = J$ (dato che $I \neq A$ per definizione).

4. Si possono trovare tanti esempi; eccone uno

$$I = \{f \in \mathbb{Z}[x] \mid f(0) = 0\}, \qquad J = \{f \in \mathbb{Z}[x] \mid f(0) \in 2\mathbb{Z}\};$$

I, J sono ideali primi di $\mathbb{Z}[x]$ dato che sono, rispettivamente, il nucleo degli omomorfismi: $\sigma_0 : \mathbb{Z}[x] \to \mathbb{Z}$ e $\overline{\sigma}_0 : \mathbb{Z}[x] \to \mathbb{Z}/2\mathbb{Z}$, definiti da $\sigma_0(f) = f(0)$ e $\overline{\sigma}_0(f) = f(0) + 2\mathbb{Z}$, per ogni $f \in \mathbb{Z}[x]$; e sia $\mathbb{Z}$ che $\mathbb{Z}/2\mathbb{Z}$ sono domini d'integrità. Chiaramente, I e J sono distinti, non banali e $J \subseteq I$.

Esercizio 4. *Nell'anello dei polinomi $\mathbb{Q}[x]$ si consideri il sottoinsieme*

$$I = \{f \in \mathbb{Q}[x] \mid f(2) = f(1/2) = f(\sqrt{2}) = 0\}.$$

(1) Si provi che I è un ideale di $\mathbb{Q}[x]$.
(2) Si determinino tutti gli ideali massimali di $\mathbb{Q}[x]$ che contengono I.

Soluzione. 1. Chiaramente I non è vuoto (contiene il polinomio nullo). Siano $f, g \in I$; allora per ogni $b \in \{2, 1/2, \sqrt{2}\}$ si ha

$$(f - g)(b) = f(b) - g(b) = 0 - 0 = 0,$$

dunque $f - g \in I$. Similmente, se $f \in I$, $h \in \mathbb{Q}[x]$, per ogni $b \in \{2, 1/2, \sqrt{2}\}$,

$$(fh)(b) = f(b)h(b) = 0 \cdot h(b) = 0$$

e dunqeu $fh = hf \in I$. Questo dimostra che I è un ideale.

2. Poiché $\mathbb{Q}[x]$ è un P.I.D., l'ideale I è principale. Ora, se $f \in I$, allora f è diviso dai polinomi

$$g_1 = x - 2, \quad g_2 = x - \frac{1}{2}, \quad g_3 = x^2 - 2.$$

Siccome tali polinomi sono irriducibili (in $\mathbb{Q}[x]$) e a due a due non associati, ne segue che f è diviso dal loro prodotto $g = (x-2)(x-\frac{1}{2})(x^2-2)$. Dato che $g \in I$ si conclude che $I = (g)$ e gli ideali massimali di $\mathbb{Q}[x]$ contenenti I sono

$$(x - 2), \quad (x - 1/2), \quad (x^2 - 2).$$