Corso di Laurea in Matematica

compito di Algebra I del 11 giugno 2012

SOLUZIONE

Esercizio 1. *Dato un intero $n \geq 3$, sia $I_n = \{0, 1, 2, \dots, n\}$. Su $A = I_n \times I_n$ si definisca una relazione $\trianglelefteq$ ponendo, per $(a, b), (c, d) \in A$,*

$$(a, b) \trianglelefteq (c, d) \qquad \text{se} \qquad a(a - c) = 0 \text{ e } b \leq d\,.$$

(1) *Si provi che $\trianglelefteq$ è una relazione di ordine su A.*

– Riflessività. Per ogni $(a, b) \in A$ si ha $a(a - a) = 0$ e $b \leq b$; dunque $(a, b) \trianglelefteq (a, b)$.
– Antisimmetria. Siano $(a, b), (c, d) \in A$ tali che $(a, b) \trianglelefteq (c, d)$ e $(c, d) \trianglelefteq (a, b)$. Allora, in particolare, $b \leq d$ e $d \leq b$, dunque $b = d$. Inoltre, sempre per definizione di $\trianglelefteq$, si ha $a(a - c) = 0 = c(c - a)$; quindi se $a = 0$ segue che $c = 0$, se $a \neq 0$ allora $a = c$. In ogni caso, $a = c$ e dunque $(a, b) = (c, d)$ come si voleva.

(2) *Si determinino gli elementi massimali/minimali e/o massimo/minimo (se esistono) dell'insieme parzialmente ordinato $(A, \trianglelefteq)$.*

Minimali. Si osserva che per ogni $(a, b) \in A$, $(0, 0) \trianglelefteq (a, b)$: infatti $0(0 - a) = 0$ e $0 \leq b$. Dunque $(0, 0)$ è il minimo di A e pertanto è anche l'unico minimale.
Massimali. Si osserva che per ogni $(a, b) \in A$ se $b \neq n$ allora $(a, b + 1) \in A$ e $(a, b) \trianglelefteq (a, b + 1)$. Quindi, se $b \neq n$ allora (a, b) non è massimale. Consideriamo ora gli elementi del tipo (a, n). Notato che $(0, 0)$ (che come abbiamo visto è il minimo) non è certo massimale, ci restano gli elementi (a, b) con $1 \leq a \leq n$: se $(a, n) \trianglelefteq (c, d)$ allora, $a(a - c) = 0$ e $n \leq d$. Poiché $a \neq 1$ dalla prima identità segue $c = a$, mentre dalla seconda segue $d = n$; pertanto $(c, d) = (a, n)$. Abbiamo provato così che (a, n) è un elemento massimale per ogni $1 \leq a \leq n$. Poiché il numero di massimali è superiore a uno, non esistono massimi.

(3) *Si determini (se esiste) l'estremo inferiore in A di $B = \{(i, 2) \, : \, 1 \leq i \leq n\}$.*

Si comincia cercando di individuare l'insieme dei minoranti di B. Se (a, b) è un minorante di B allora $(a, b) \trianglelefteq (i, 2)$ per ogni $1 \leq i \leq n$; ovvero,

$$\begin{cases} a(a - i) = 0 \\ b \leq 2 \end{cases}$$

per ogni $1 \leq i \leq n$. Questo forza $a = 0$; infatti, se $a \neq 0$ allora, prendendo $i \neq a$ si ha $a(a - i) \neq 0$ e dunque $(a, b) \not\trianglelefteq (i, 2)$. D'altra parte si vede subito che per $0 \leq b \leq 2$, l'elemento $(0, b)$ è un minorante di B. Quindi, l'insieme dei minoranti di B è $\{(0, 0), (0, 1), (0, 2)\}$, il cui massimo è - come si vede subito - $(0, 2)$. In conclusione $sup(B) = (0, 2)$.

Esercizio 2. *Sia* $\Delta(1) = 5$ *e per ogni* $n \geq 1$ *si ponga* $\Delta(n+1) = 5^{\Delta(n)}$. *Si dimostri che, per ogni* $n \geq 1$ *si ha*

$$4^{\Delta(n)} \equiv 1 \pmod{11}$$

Per ogni $n \geq 1$, $\Delta(n)$ è una potenza e quindi anche un multiplo di 5 [ad esempio $\Delta(3) = 5^{5^5}$]. Quindi, per $n \geq 1$, esiste $k \in \mathbb{N}$ tale che $\Delta(n) = 5k$. Pertanto

$$4^{\Delta(n)} = 4^{5k} = (4^5)^k \equiv 1 \pmod{11}.$$

Esercizio 3. *Sia* R *un dominio di integrità e sia* $a \in R$ *un elemento non nullo e non invertibile; si provi che* $\{0\} \neq (a^2) \neq (a)$. *Si deduca che un dominio d'integrità con un numero finito di ideali è un campo.*

Sia $a \in R$ un elemento non invertibile e non nullo del dominio d'integrità R. Da $a \neq 0$ segue, poiché R è un dominio d'integrità $a^2 \neq 0$; quindi $\{0\} \neq (a)$. Chiaramente $(a^2) \subseteq (a)$; se fosse $(a^2) = (a)$ esisterebbe un $r \in R$ tale che $a = a^2$ da cui, per la legge di cancellazione, $1 = ar$, che è una contraddizione perché a non è invertibile per ipotesi. Dunque $(a^2) \neq (a)$.

Per la seconda parte, supponiamo che R sia un dominio d'integrità con un numero finito di ideali. R è un anello commutativo per definizione; consideriamo allora un generico elemento $0 \neq a \in R$. Se a non è invertibile, allora per il punto precedente $(a) \supsetneq (a^2) \supsetneq \{0\}$; riproducendo la cosa su a^2 e andando avanti, si ottiene una catena **infinita** di ideali

$$(a) \supsetneq (a^2) \supsetneq (a^4) \supsetneq \dots$$

contro le ipotesi su R. Dunque, a è invertibile, e questo prova che R è un campo.

Esercizio 4. *Sia* $\psi : \mathbb{Q}[x] \to \mathbb{C} \times \mathbb{C}$ *definito da* $\psi(f) = (f(1), f(i))$.

(a) *Si provi che* ψ *è un omomorfismo di anelli.*

Siano $f, g \in \mathbb{Q}[x]$. Allora

$\psi(fg) = (fg(1), fg(i)) = (f(1)g(1), f(i)g(i)) = (f(1), f(i))(g(1), g(i)) = \psi(f)\psi(g)$,

$\psi(f+g) = ((f+g)(1), (f+g)(i)) = (f(1) + g(1), f(i) + g(i)) =$
$= (f(1), f(i)) + (g(1), g(i)) = \psi(f) + \psi(g)$,

inoltre $\psi(1) = (1, 1) = !_{\mathbb{C}\times\mathbb{C}}$.

Quindi, ψ è un omomorfismo di anelli.

(b) *Si determini un generatore di* $I = Ker(\psi)$.

Poiché $\mathbb{Q}$ è un campo e $\{0\} \neq I$ è un ideale di $\mathbb{Q}[x]$, I è principale e un suo generatore è un suo qualsiasi elemento (non-nullo) di grado minimo. Abbiamo

$$I = \{f \in \mathbb{Q}[x] \mid \psi(f) = o\} = \{f \in \mathbb{Q}[x] \mid f(1) = 0 = f(i)\}$$

quindi $g = (x-1)(x^2+1) \in I$.
Ora, se $0 \neq f \in I$, allora f ha radici 1 e i in $\mathbb{C}$, quindi, in $\mathbb{Q}[x]$, f è diviso sia dal polinomio $x-1$ che dal polinomio x^2+1; poiché tali polinomi sono coprimi, si conclude che $g = (x-1)(x^2+1)$ divide f. Dunque $I = (g)$.

(c) *Si dica se* $1 + x + x^2 + I$ *è invertibile in* $\mathbb{Q}[x]/I$ *e, se lo è, se ne determini l'inverso.*

Il polinomio $f = x^2+x+1$ è coprimo con $g = (x-1)(x^2+1) = x^3-x^2+x-1$ (che è un generatore dell'ideale I), quindi $f + I$ è un elemento invertibile di $\mathbb{Q}[x]/I$. Con l'algoritmo di Euclide su trova

$$3 = (2x^2 - 3x + 2)f - (2x + 1)g$$

quindi l'inverso di $f + I$ in $\mathbb{Q}[x]/I$ è $(2/3x^2 - x + 2/3) + I$.

(d) *Si determinino gli elementi nilpotenti di* $\mathbb{Q}[x]/I$.

Sia $h+I$ un elemento di $\mathbb{Q}[x]/I$ per cui esiste $n \geq 1$ tale che $(h+I)^n = 0_{\mathbb{Q}[x]/I} = I$. Allora $h^n + I = I$, cioè $h^n \in I = (g)$. Quindi $g \mid h^n$.
Questo vuol dire che sia $u = x-1$ che $v = x^2+1$ sono fattori di h^n in $\mathbb{Q}[x]$. Poiché sia u e v sono irriducibili, ciò implica che entrambi dividono h (se $h = q_1 \dots q_s$ è una fattorizzazione in irriducibili di h in $\mathbb{Q}[x]$, allora $q_1^n \dots q_s^n$ lo è di h^n). Pertanto sia u che v sono fattori irriducibili di h; siccome sono coprimi, ne segue che $g = uv$ divide h e dunque che $h + I = I = 0_{\mathbb{Q}[x]/I}$. In conclusione, l'anello $\mathbb{Q}[x]/I$ non contiene elementi nilpotenti.