Corso di Laurea in Matematica
compito di Algebra I del 10 luglio 2012
SOLUZIONE

Esercizio 1. *Siano A, B, C insiemi e, come consuetudine $C^B = \{f \mid f : B \to C\}$, $C^A = \{g \mid g : A \to C\}$; infine, sia fissata un'applicazione* <u>*suriettiva*</u> *$\alpha : A \to B$. Si definisca quindi l'applicazione $\chi : C^B \to C^A$ ponendo,*

$$\chi(f) = f \circ \alpha$$

per ogni $f \in C^B$. Si provi che χ è un'applicazione iniettiva.

Siano $f, g \in C^B$ tali che $\chi(f) = \chi(g)$, ovvero $f \circ \alpha = g \circ \alpha$. Ora, dato $b \in B$, esiste, poiché α è suriettiva, $a \in A$ tale che $b = \alpha(a)$; dunque

$$f(b) = f(\alpha(a)) = (f \circ \alpha)(a) = (g \circ \alpha)(a) = g(\alpha(a)) = g(b)$$

il che dimostra che $f = g$. Pertanto, χ è un'applicazione iniettiva.

Esercizio 2. Sull'insieme $A = \mathbb{N} \times \mathbb{N}$ si definisca la relazione $\lhd$ ponendo, per ogni $(a, b), (c, d) \in A$,

$$(a, b) \lhd (c, d) \quad \text{se} \quad \begin{cases} a \leq c \\ a + d \leq b + c \end{cases} .$$

1. *Si provi che $\lhd$ è una relazione d'ordine e che non è totale.*

– Riflessività. Per ogni $(a, b) \in A$ (quindi $a, b \in \mathbb{N}$) si ha banalmente $a \leq a$ e $a + b \leq b + a$; dunque $(a, b) \lhd (a, b)$.
– Antisimmetria. Siano $(a, b), (c, d) \in A$ con $(a, b) \lhd (c, d)$ e $(c, d) \lhd (a, b)$; allora

$$\begin{cases} a \leq c \\ a + d \leq b + c \end{cases} \qquad e \qquad \begin{cases} c \leq a \\ c + b \leq d + a \end{cases}$$

da cui segue subito $c = a$ e $d = (c + b) - a = a + b - a = b$.
– Transitività. Siano $(a, b), (c, d), (e, f) \in A$ con $(a, b) \lhd (c, d)$ e $(c, d) \lhd (e, f)$; allora

$$\begin{cases} a \leq c \\ a + d \leq b + c \end{cases} \qquad e \qquad \begin{cases} c \leq e \\ c + f \leq d + e \end{cases}$$

da cui si ricava: $a \leq e$, e
$a + f = a + d - d + f \leq b + c - d + f = (c + f) - d + b \leq e + d - d + b = e + b$
Dunque $(a, b) \lhd (e, f)$.
Quindi $(A, \lhd)$ è un insieme parzialmente ordinato. L'ordine non è totale perché, ad esempio $(0, 0) \not\lhd (1, 2)$ e $(1, 2) \not\lhd (0, 0)$.

2. *Osservato che per ogni $(a, b) \in A$ si ha $(a, b) \lhd (a + 1, b)$, si provi che l'insieme parzialmente ordinato $(A,\lhd)$ non ha né elementi massimali né minimali.*

Sia $(a, b) \in A$. Allora, come si verifica subito dalla definizione $(a, b) \lhd (a + 1, b)$ e $(a, b + 1) \lhd (a, b)$. Questo prova che $(A,\lhd)$ non ha elementi massimali né minimali.

3. *Posto $x = (0, 0)$ e $y = (1, 2)$, si provi che $\inf_A\{x, y\} = (0, 1)$.*

Sia $u = (a, b) \in A$; allora $u \lhd x$ se e solo se $a \leq 0$ e $a + 0 \leq b + 0$, cioè se e solo se $a = 0$; mentre $u \lhd y$ se e solo se $a \leq 1$ e $a + 2 \leq b + 1$, ovvero se e solo se $a = 0, 1$ e $b \geq a + 1$. Pertanto l'insieme degli elementi minimanti di $\{x, y\}$ è

$$\mathcal{M} = \{(0, b) \in A \mid b \geq 1\}.$$

Ora, per ogni $b \geq 1$ si ha $(0, b) \lhd (0, 1)$. Ne consegue che $(0, 1)$ è il massimo di $\mathcal{M}$ e dunque è l'estremo superiuore di $\{x, y\}$.

Esercizio 3. *Sia $A = \{\frac{m}{n} \in \mathbb{Q} \mid m \in \mathbb{Z}, (n, 7) = 1\}$.*

1. *Si provi che A è un sottoanello dell'anello $\mathbb{Q}$.*

Chiaramente $1 = \frac{1}{1} \in A$. Siano $x = \frac{m}{n}, y = \frac{m'}{n'} \in A$; allora

$$x - y = \frac{mn' - m'n}{nn'} \qquad e \qquad xy = \frac{mm'}{nn'}$$

sono elementi di A dato che, essendo 7 un numero primo, 7 non divide nn'. Questo prova che A è un sottoanello di $\mathbb{Q}$.

2. *Si determini l'insieme degli elementi invertibili $U(A)$.*

Per l'unicità dfgli elementi inversi in $\mathbb{Q}$, un elemento $\frac{m}{n}$ di A è invertibile in A se e soltanto se $m \neq 0$ e il suo inverso in $\mathbb{Q}$, cioè $\frac{n}{m}$, appartiene ad A, e ciò si verifica se e soltanto se 7 non divide m. Pertanto

$$U(A) = \left\{\frac{m}{n} \in A \middle| (m, 7) = 1\right\} = \left\{\frac{m}{n} \in \mathbb{Q} \middle| (m, 7) = (n, 7) = 1\right\}.$$

3. *Si provi che $I = A \setminus U(A)$ è un ideale di A e che è principale, determinandone esplicitamente un generatore.*

Per quanto visto al punto precedente $7 = \frac{7}{1} \in I$; inoltre per ogni $\frac{m}{n} \in A$ si ha $7 \cdot \frac{m}{n} = \frac{7m}{n} \in A \setminus U(A) = I$; quindi $(7) \subseteq I$. Viceversa, se $u = \frac{m}{n} \in A$ allora $\frac{m}{n} \in I$ se e sole se $7|m$ ovvero se e solo se esiste $m' \in \mathbb{Z}$ tale che $u = \frac{7m'}{n} = 7 \cdot \frac{m'}{n}$ con $\frac{m'}{n} \in A$. Quindi $I \subseteq (7)$. In conclusione, $I = (7)$.

4. *Qual è la caratteristica di A? Sia infine $\phi : A \to \mathbb{K}$ un omomorfismo suriettivo con $\mathbb{K}$ un campo: qual è la caratteristica di $\mathbb{K}$?*

La caratteristica di A coincide con quella di $\mathbb{Q}$, quindi è 0.
Sia $\phi : A \to \mathbb{K}$ un omomorfismo suriettivo con $\mathbb{K}$ un campo e sia $K = \ker(\phi)$. Per il Teorema di omomorfismo $A/K \simeq \mathbb{K}$. Quindi, K è un ideale massimale di A; in particolare K è proprio e perciò non contiene elementi invertibili di A; quindi $K \subseteq I$ e dunque (per la massimalità di K) $K = I$. Quindi $\mathbb{K} \simeq A/I$. Ora

$$7 \cdot (1 + I) = 7 + I = I = 0_{A/I}$$

e quindi A/I ha caratteristica uguale a 7. Lo stesso, per quanto detto, vale per $\mathbb{K}$.

Esercizio 4. *Si fattorizzi come prodotto di irriducibili il polinomio*

$$x^4 - x^2 - 2 \in \mathbb{K}[x]$$

con $\mathbb{K} = \mathbb{Z}/2\mathbb{Z},\ \mathbb{Q},\ \mathbb{Q}[\sqrt{2}]$.

– $\mathbb{K} = \mathbb{Z}/2\mathbb{Z}$. Allora $x^4 - x^2 - 2 = x^4 + x^2 = x^2(x^2 + 1) = x^2(x + 1)^2$. In questo caso, il polinomio si fattorizza come il prodotto di fattori lineari.

– $\mathbb{K} = \mathbb{Q}$. Allora $x^4 - x^2 - 2 = x^4 + x^2 - 2x^2 - 2 = x^2(x^2 + 1) - 2(x^2 + 1) = (x^2 - 2)(x^2 + 1)$, e i polinomi $x^2 - 2$, $x^2 + 1$ sono irriducibili in $\mathbb{Q}[x]$. .

– $\mathbb{K} = \mathbb{Q}[\sqrt{2}]$. Allora $x^4 - x^2 - 2 = (x^2 - 2)(x^2 + 1) = (x - \sqrt{2})(x + \sqrt{2})(x^2 + 1)$, è un fattorizzazioni in irriducibili in $\mathbb{Q}[\sqrt{2}][x]$. Infatti, poiché ha grado 2, se $x^2 + 1$ fosse riducibile, il campo $\mathbb{Q}[\sqrt{2}]$ dovrebbe contenere le sue radici, che sono i numeri complessi i e $-i$, e questo non è il caso dato che $\mathbb{Q}[\sqrt{2}]$ è contenuto nel campo $\mathbb{R}$ dei numeri reali.