Corso di Laurea in Matematica
I compito di ALGEBRA I – 12 gennaio 2015
Soluzioni

Esercizio 1. *Siano A, B insiemi, $f : A \to B$ e $g : B \to A$ applicazioni tali che g è suriettiva e $f \circ g = \iota_B$.*

1. *Si provi che $g = f^{-1}$;*
2. *si dica se, in generale, l'affermazione del punto precedente rimane vera anche senza l'ipotesi che g sia suriettiva.*

Soluzione. 1. Siano f e g come nelle ipotesi. Sia $a \in A$; poiché g è suriettiva esiste $b \in B$ tale che $g(b) = a$, e siccome $f \circ g = \iota_B$, si ha

$$b = \iota_B(b) = (f \circ g)(b) = f(g(b)) = f(a).$$

Dunque $(g \circ f)(a) = g(f(a)) = g(b) = a$. Poiché questo vale per ogni $a \in A$ si conclude che $g \circ f = \iota_A$ e pertanto $g = f^{-1}$.

altra soluzione. Poiché g è suriettiva ha una inversa destra $h : A \to B$, cioè tale che $g \circ h = \iota_A$. Ma allora, poiché per ipotesi g ha anche un'inversa sinistra (che è f), per quanto visto a teoria, g è invertibile e $f = h = g^{-1}$.

2. NO. Si considerino, ad esempio, $f : \{0, 1\} \to \{0\}$ e $g : \{0\} \to \{0, 1\}$, dove f è definita nel solo modo possibile e $g(0) = 0$. Allora $f \circ g = \iota_B$, dove $B = \{0\}$, ma f non è invertibile.

Attenzione: **non assumere g suriettiva**" significa che non si fa alcuna ipotesi su g, e NON significa **assumere che g non è suriettiva.**

Esercizio 2. *Sull'insieme $\mathcal{A} = \{X \subseteq \mathbb{Z} \mid |X| < \infty\}$ si definisca la relazione $\lhd$ ponendo, per ogni $X, Y \in \mathcal{A}$,*

$$X \lhd Y \text{ se } \begin{cases} X \cap \mathbb{N} \subseteq Y \cap \mathbb{N} \\ X \cap \mathbb{N}^- \supseteq Y \cap \mathbb{N}^- \end{cases}$$

dove $\mathbb{N}^- = \{z \in \mathbb{Z} \mid z < 0\}$.

1. *Si provi che $\lhd$ è una relazione d'ordine su $\mathcal{A}$ e si dica se è totale;*
2. *si dica se l'insieme parzialmente ordinato $(\mathcal{A}, \lhd)$ ha elementi minimali;*
3. *avendo posto, per $n \in \mathbb{N}$, $B_n = \{x \in \mathbb{Z} \mid -n \leq x \leq n\}$, si determini, se esiste, l'estremo superiore del sottoinsieme $\mathcal{B} = \{B_n \mid 0 \leq n \leq 5\}$.*

Soluzione. 1. *riflessività.* Sia $X \in \mathcal{A}$; allora per definizione di inclusione $X \cap N \subseteq X \cap N$ e $X \cap \mathbb{N}^- \supseteq X \cap \mathbb{N}^-$; quindi $X \lhd X$.

antisimmetria. Siano $X, Y \in \mathcal{A}$ tali che $X \lhd Y$ e $Y \lhd X$. Allora

$$\begin{cases} X \cap \mathbb{N} \subseteq Y \cap \mathbb{N} \\ X \cap \mathbb{N}^- \supseteq Y \cap \mathbb{N}^- \end{cases} \quad \text{e} \quad \begin{cases} Y \cap \mathbb{N} \subseteq X \cap \mathbb{N} \\ Y \cap \mathbb{N}^- \supseteq X \cap \mathbb{N}^- \end{cases}$$

quindi, per la doppia inclusione $X \cap \mathbb{N} = Y \cap \mathbb{N}$ e $X \cap \mathbb{N}^- \subseteq Y \cap \mathbb{N}^-$. Poiché $\mathbb{Z} = \mathbb{N} \cup \mathbb{N}^-$, si conclude

$$X = X \cap \mathbb{Z} = (X \cap \mathbb{N}) \cup (X \cap \mathbb{N}^-) = (Y \cap \mathbb{N}) \cup (Y \cap \mathbb{N}^-) = Y \cap \mathbb{Z} = Y.$$

transitività. Siano $X, Y, T \in \mathcal{A}$ tali che $X \lhd Y$ e $Y \lhd T$. Allora

$$\begin{cases} X \cap \mathbb{N} \subseteq Y \cap \mathbb{N} \\ X \cap \mathbb{N}^- \supseteq Y \cap \mathbb{N}^- \end{cases} \quad \text{e} \quad \begin{cases} Y \cap \mathbb{N} \subseteq T \cap \mathbb{N} \\ Y \cap \mathbb{N}^- \supseteq T \cap \mathbb{N}^- \end{cases}$$

da cui segue $X \cap \mathbb{N} \subseteq T \cap \mathbb{N}$ e $X \cap \mathbb{N}^- \supseteq T \cap \mathbb{N}^-$, ovvero $X \lhd T$.
Pertanto $(\mathcal{A}, \lhd)$ è un insieme parzialmente ordinato.
Non è totale; ad esempio se $X = \{0\}$ e $Y = \{1\}$, allora $X, Y \in \mathcal{A}$, ma $X \not\lhd Y$ e $Y \not\lhd X$.

2. Non ci sono elementi minimali. Infatti, sia $X \in \mathcal{A}$; poiché X è finito esiste $z \in \mathbb{N}^- \setminus X$. Sia $Y = X \cup \{z\}$; allora $Y \in \mathcal{A}$ e $Y \neq X$; inoltre

$$\begin{cases} Y \cap \mathbb{N} = X \cap \mathbb{N} \subseteq X \cap \mathbb{N} \\ Y \cap \mathbb{N}^- = \{z\} \cup (X \cap \mathbb{N}^-) \supseteq X \cap \mathbb{N}^- \end{cases}$$

ovvero $Y \lhd X$. Dunque X non è minimale.

3. Sia $M \in \mathcal{A}$ un maggiorante di $\mathcal{B} = \{B_n \mid 0 \leq n \leq 5\}$. Allora $B_n \lhd M$, per $0 \leq n \leq 5$. Da $B_0 = \{0\} \lhd M$, segue in particolare $\emptyset = B_0 \cap \mathbb{N}^- \supseteq M \cap \mathbb{N}^-$, cioè $M \cap \mathbb{N}^- = \emptyset$, ovvero

$$M \subseteq \mathbb{N}. \tag{1}$$

Mentre da $B_5 \lhd M$ segue in particolare $B_5 \cap \mathbb{N} \subseteq M \cap \mathbb{N} = M$, dunque

$$\{0, \ldots, 5\} \subseteq M. \tag{2}$$

Si verifica ora facilmente, per definizione, che le condizioni (1) e (2) sono anche sufficienti a che M sia un maggiorante di $\mathcal{B}$. Dunque, l'insieme dei maggioranti di $\mathcal{B}$ in $(\mathcal{A}, \lhd)$ è

$$\mathcal{M} = \{M \in \mathcal{A} \mid \{0, \ldots, 5\} \subseteq M \subseteq \mathbb{N}, \}.$$

Sia infine $S = \{0 \ldots, 5\}$. Allora $S \in \mathcal{M}$ e per ogni $Y \in \mathcal{M}$, $S \lhd Y$. Quindi S è il minimo di $\mathcal{M}$, cioè l'estremo superiore di $\mathcal{B}$ in $(\mathcal{A}, \lhd)$.

Esercizio 3. *Fissato un numero primo positivo p, sia $D = \mathbb{Z} \setminus p\mathbb{Z}$ (ovvero, $D = \{z \in \mathbb{Z} \mid p \not| z\}$). Su $D \times D$ si definisca la relazione ω ponendo, per ogni $(a, b), (c, d) \in D \times D$*

$$(a, b)\omega(c, d) \quad \textit{se} \quad p | ad - bc.$$

1. *Si provi che ω è una relazione d'equivalenza su $D \times D$;*

2. *si provi che l'insieme $\{(1,k) \in D \times D \mid 1 \leq k \leq p-1\}$ è un sistema di rappresentanti per l'insieme quoziente $(D \times D)/\omega$.*

Soluzione. 1. *riflessività.* Sia $(a,b) \in D \times D$; allora p divide $ab - ba = 0$, dunque $(a,b)\omega(a,b)$.
simmetria. Siano $(a,b),(c,d) \in D \times D$ tali che $(a,b)\omega(c,d)$; allora, per definizione p divide $ad-bc$, dunque p divide $-(ad-bc) = cb-da$ e pertanto $(c,d)\omega(a,b)$.
transitività. Siano $(a,b),(c,d),(e,f) \in D\times D$ tali che $(a,b)\omega(c,d)$ e $(c,d)\omega(e,f)$; allora, per definizione, p divide $ad-bc$ e divide $cf-de$. Dunque

$$p|(ad-bc)f + b(cf-de) = adf - bde = (af-be)d$$

poiché p è un primo e $p \not| d$ deve essere $p|af-be$, e quindi $(a,b)\omega(e,f)$. Abbiamo così provato che ω è una relazione d'equivalenza su $D \times D$.

2. Sia $(a,b) \in D \times D$. Poiché $(p,a) = 1$ la congruenza

$$ax \equiv b \pmod{p} \tag{3}$$

ammette soluzioni (o, anche, l'equazione diofantea $ax + yp = b$ ammette soluzioni). Osserviamo che se x è una soluzione allora $x \not\equiv 0 \pmod{p}$; quindi $x \equiv k \pmod{p}$ per qualche $1 \leq k \leq p-1$. Per tale k si ha

$$p|ak - b = ak - b \cdot 1$$

quindi $(a,b)\omega(1,k)$, ovvero $[(a,b)]_\omega = [(1,k)]_\omega$. Questo mostra che

$$(D \times D)/\omega = \{[(1,k)]_\omega | 1 \leq k \leq p-1\}.$$

Resta da provare che le classi $[(1,k)]_\omega$ con $1 \leq k \leq p-1$ sono tutte distinte. Siano quindi $1 \leq k \leq k' \leq p-1$ tali che $[(1,k')]_\omega = [(1,k)]_\omega$; allora $(1,k')\omega(1,k)$ e quindi $p|k'-k$. Poiché $0 \leq k'-k < p$, questo implica $k = k'$ come si voleva.

Esercizio 4. *Si risolva in $\mathbb{Z}$ il seguente sistema alle congruenze:*

$$\begin{cases} x^{100} + 66x^{66} + 100x^{10} \equiv 1 \pmod{35} \\ (6x)^{14} \equiv x + 2 \pmod{7} \end{cases}$$

Soluzione. Il sistema non ha soluzioni. Sia per assurdo $x \in \mathbb{Z}$ che soddisfa la prima congruenza; allora in particolare, dato che 5 divide 35,

$$x^{100} + 66x^{66} + 100x^{10} \equiv 1 \pmod{5} \tag{4}$$

che possiamo riscrivere (riducendo modulo 5 i coefficienti)

$$x^{100} + x^{66} \equiv 1 \pmod{5} \tag{5}$$

Osserviamo subito che deve essere

$$x \not\equiv 0 \pmod 5 \tag{6}$$

Possiamo quindi applicare il Teorema di Fermat; poiché $100 = 4 \cdot 25$ e $66 = 4 \cdot 16 + 2$, si ha $x^{100} \equiv 1 \pmod 5$ e $x^{66} \equiv x^2 \pmod 5$. Dunque da (5) segue

$$1 + x^2 \equiv 1 \pmod 5$$

ovvero

$$x^2 \equiv 0 \pmod 5$$

che significa (dato che 5 è un numero primo)

$$x \equiv 0 \pmod 5$$

che è in contraddizione con (6). Pertanto, (4) (e dunque nemmeno il sistema) ammette soluzioni intere.