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

AVVERTENZA: Il testo fornito in classe presentava - rispetto alle intenzioni - un errore nella definizione della relazione nell'esercizio 2. Nella valutazione degli elaborati ho ovviamente tenuto conto di questo, e nella presente soluzione ho ripristinato la versione corretta del problema.

Esercizio 1. *Sia A un insieme finito e non vuoto. Su $\mathcal{P}(A)$ si definisca una relazione ω ponendo, per ogni $X, Y \in \mathcal{P}(A)$, $X\omega Y \Leftrightarrow |X\Delta Y|$ è pari.*

1. Si provi che ω è una relazione d'equivalenza su $\mathcal{P}(A)$.

- Per ogni $X \in \mathcal{P}(A)$, $|X\Delta X| = |\emptyset| = 0$ e quindi $X\omega X$; dunque ω è riflessiva.
- Siano $X, Y \in \mathcal{P}(A)$ tali che $X\omega Y$. Allora $|X\Delta Y|$ è pari; ma, poiché Δ è commutativa, $Y\Delta X = X\Delta Y$; quindi $Y\omega X$. Dunque, ω è simmetrica.
- Per la transitività, osserviamo prima che se U, V sono insiemi finiti di ordine pari allora

$$|U\Delta V| = |U \cup V)| - |U \cap V| = |U| + |V| - 2|U \cap V|$$

è pari. Siano ora $X, Y, Z \in \mathcal{P}(A)$ tali che $X\omega Y$ e $Y\omega Z$; allora $|X\Delta Y|$ e $|Y\Delta Z|$ sono pari e quindi, per quanto osservato e per l'associatività di Δ:

$$|X\Delta Z| = |X\Delta\emptyset\Delta Z| = |X\Delta(Y\Delta Y)\Delta Z| = |(X\Delta Y)\Delta(Y\Delta Z)|$$

è pari. Dunque $X\omega Z$ e questo prova che ω è transitiva.
In conclusione, ω è una relazione d'equivalenza.

2. Si provi che $|\mathcal{P}(A)/\omega| = 2$.

Sia $X \in \mathcal{P}(A)$; allora $X\Delta\emptyset = X$, quindi

$$[\emptyset]_\omega = \{X \in \mathcal{P}(A) \mid |X| \text{ pari}\}.$$

Sia ora $a \in A$, allora $\{a\} \notin [\emptyset]_\omega$ e per ogni $X \in \mathcal{P}(A)$,

$$X\Delta\{a\} = \begin{cases} X \setminus \{a\} & se \quad a \in X \\ X \cup \{a\} & se \quad a \notin X \end{cases}$$

quindi: $|X\Delta\{a\}|$ è pari $\Leftrightarrow |X|$ è dispari. Pertanto

$$[\{a\}]_\omega = \{X \in \mathcal{P}(A) \mid |X| \text{ dispari}\}.$$

Dunque $\mathcal{P}(A)/\omega = \{[\emptyset]_\omega, [\{a\}]_\omega\}$.

Esercizio 2. *Sia $A = \mathbb{N}^{\mathbb{N}}$ l'insieme di tutte le applicazioni $f : \mathbb{N} \to \mathbb{N}$. Su A si definisca la relazione $\preceq$ ponendo, per ogni $f, g \in A$,*

$$f \preceq g$$

se esiste $n \in \mathbb{N}$ tale che $0 \leq g(x) - f(x) \leq n$ per ogni $x \in \mathbb{N}$.

1. Si provi che $\preceq$ è una relazione d'ordine su A.

- Sia $f \in A$; allora, per ogni $x \in \mathbb{N}$, $0 = f(x) - f(x)$ e quindi $f \preceq f$. Dunque $\preceq$ è riflessiva.
- Siano $f, g \in A$ tali che $f \preceq g$ e $g \preceq f$. Allora, in particolare, per ogni $x \in \mathbb{N}$, $f(x) - g(x) \geq 0$ e $-(f(x) - g(x)) = g(x) - f(x) \geq 0$, il che implica $f(x) = g(x)$ per ogni $x \in \mathbb{N}$, ovvero $f = g$. Dunque $\preceq$ è antisimmetrica.
- Siano $f, g, h \in A$ tali che $f \preceq g$ e $g \preceq h$. Esistono allora $n, m \in \mathbb{N}$ tali che, per ogni $x \in \mathbb{N}$

$$\begin{cases} 0 \leq g(x) - f(x) \leq n \\ 0 \leq h(x) - g(x) \leq m \end{cases}$$

da cui, commando membro a membro: $0 \leq h(x) - f(x) \leq n + m$ per ogni $x \in \mathbb{N}$, quindi $f \preceq h$. Questo prova che $\preceq$ è transitiva.

Quindi $\preceq$ è una relazione d'ordine su A.

2. Si provi che $(A, \preceq)$ non ha minimo e che la funzione costante $x \mapsto 0$ è il suo unico elemento minimale.

Denotiamo con $\underline{0}$ la funzione costante $x \mapsto 0$ (per ogni $x \in \mathbb{N}$). Sia $g \in A$ tale che $g \preceq \underline{0}$; allora in particolare $g(x) \leq 0$ (e dunque $g(x) = 0$) per ogni $x \in \mathbb{N}$ e quindi $g = \underline{0}$, il che prova che $\underline{0}$ è un elemento minimale di $(A, \preceq)$.

Sia $f \in A$, $f \neq \underline{0}$; allora esiste $a \in \mathbb{N}$ tale che $f(a) \geq 1$; ponendo ora, per ogni $x \in \mathbb{N}$,

$$g(x) = \begin{cases} f(x) & se \quad x \neq a \\ f(a) - 1 & se \quad x = a \end{cases}$$

si ha un elemento $g \in A$ tale che $g \preceq f$ e $g \neq f$; dunque f non è minimale.

Quindi $\underline{0}$ è l'unico elemento minimale di $(A, \preceq)$.

Notiamo infine che $\underline{0} \not\preceq \iota_{\mathbb{N}}$ (dove $\iota_{\mathbb{N}}$ è l'applicazione identica su $\mathbb{N}$). Quindi $\underline{0}$ non è minimo e pertanto $(A, \preceq)$ non ha elemento minimo (perché se lo avesse questo dovrebbe coincidere con ogni minimale).

Esercizio 3. *Si dica per quali $x, y \in \mathbb{Z}$ si ha:*

$$\begin{cases} x^{512} - 512y \equiv 0 \pmod 7 \\ (xy)^{512} \equiv 1024 \pmod 7 \end{cases}$$

Poiché $512 \equiv 1 \pmod 7$ e $1024 \equiv 2 \pmod 7$, il sistema è equivalente a

$$\begin{cases} x^{512} - y \equiv 0 \pmod 7 \\ (xy)^{512} \equiv 2 \pmod 7 \end{cases}$$

A questo punto, abbiamo a che fare con esponenti da ridurre mediante il Teorema di Fermat. Occorre in primo luogo osservare che, per la seconda congruenza, xy non può essere multiplo di 7, quindi né x né y sono multipli di 7, e possiamo allora applicare il Teorema di Fermat:
Poiché $512 = 85(7-1) + 2$, e $7 \not| xy$, il sistema è equivalente a

$$\begin{cases} x^2 - y \equiv 0 \pmod 7 \\ (xy)^2 \equiv 2 \pmod 7 \end{cases}$$

Quindi $y \equiv x^2 \pmod 7$, e dunque, sostituendo nella seconda congruenza,

$$x^6 = (x^3)^2 \equiv 2 \pmod 7$$

congruenza che non ha soluzioni perché, proprio per il teorema di Fermat, per ogni $x \in \mathbb{Z}$ si ha $x \equiv 0 \pmod 7$ oppure $x^6 \equiv 1 \pmod 7$.

Esercizio 4. *Siano $n, m \in \mathbb{N}$ con $n \geq 2$, $m \geq 2$, e sia $d = (n, m)$. Si provi che porre, per ogni $a + n\mathbb{Z}$,*

$$\phi(a + n\mathbb{Z}) = a\frac{m}{d} + m\mathbb{Z}$$

dà una buona definizione di un'applicazione $\phi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$.

Siano $a, b \in \mathbb{Z}$ tali che rappresentino lo stesso elemento nel dominio $\mathbb{Z}/n\mathbb{Z}$, ovvero tali che $a + n\mathbb{Z} = b + n\mathbb{Z}$. Allora $a \equiv b \pmod n$, cioè $n|a - b$. Poiché $d = (n, m)$ divide n, d divide anche $a - b$. Quindi

$$a\frac{m}{d} - b\frac{m}{d} = (a-b)\frac{m}{d} = \frac{a-b}{d}m \in m\mathbb{Z}$$

e pertanto $a\frac{m}{d} + m\mathbb{Z} = b\frac{m}{d} + m\mathbb{Z}$, così provando che quella proposta dal testo è una buona definizione.