ALGEBRA 1 PB-Z
III. 23 III 2012

Esercizio 1. Dato un insieme X, sia $A = \mathcal{P}(X)$ l'insieme delle parti di X.

I. Si mostri che entrambi $(A, \cap)$ e $(A, \cup)$ sono dei monoidi commutativi.

Sia $\mathcal{C}_X : A \to A$ l'applicazione che a $B \in A$ associa il suo complementare in X:

$$A \ni B \mapsto \mathcal{C}_X(B) = X \setminus B \in A$$

II. Tenendo presenti le leggi di de Morgan, si mostri che $\mathcal{C}_X : (A, \cup) \to (A, \cap)$ e $\mathcal{C}_X : (A, \cap) \to (A, \cup)$ sono isomorfismi di monoidi ([1]).

III. Si mostri che gli isomorfismi qui sopra definiti sono uno inverso dell'altro, ossia, che $\mathcal{C}_X \circ \mathcal{C}_X = \mathrm{Id}_{(A,\cup)}$ e $\mathcal{C}_X \circ \mathcal{C}_X = \mathrm{Id}_{(A,\cap)}$.

Soluzione. I. Occorre mostrare che entrambe le operazioni binarie $\cap : A \times A \to A$ e $\cup : A \times A \to A$ sono (i) associative, (ii) tali da ammettere un elemento neutro, (iii) commutative. Ossia, occorre mostrare (i) che per ogni $B_1, B_2, B_3 \in A$ risulta $(B_1 \cap B_2) \cap B_3 = B_1 \cap (B_2 \cap B_3)$ e $(B_1 \cup B_2) \cup B_3 = B_1 \cup (B_2 \cup B_3)$, (ii) che esistono $E_\cap, E_\cup \in A$ tali che per ogni $B \in A$ risulti $E_\cap \cap B = B = B \cap E_\cap$ e $E_\cup \cup B = B = B \cup E_\cup$, (iii) che per ogni $B_1, B_2 \in A$ risulta $B_1 \cap B_2 = B_2 \cap B_1$ e $B_1 \cup B_2 = B_2 \cup B_1$. Essendo (i) e (iii) evidentemente vere, ci limitiamo a mostrare (ii); ora, a tal fine basta osservare che gli elementi $E_\cap = X$ e $E_\cup = \emptyset$ soddisfanoano le equazioni che servono a definire gli elementi neutri di $\cap$ e, rispettivamente, $\cup$.

II. Si inizi osservando che, per il principio del terzo escluso, l'applicazione $\mathcal{C}_X : A \to A$ è bigettiva (si noti che, nell'osservare questo fatto, la cui natura è puramente logico-insiemistica, non è necessario tenere in considerazione le strutture algebriche $\cap$ e $\cup$ che abbiamo definito su A). Ora, $\mathcal{C}_X$ è un omomorfismo di semigruppi (da $(A, \cap)$ a $(A, \cup)$ e viceversa) se e solo se per ogni $B_1, B_2 \in A$ entrambe le formule $\mathcal{C}_X(B_1 \cap B_2) = \mathcal{C}_X(B_1) \cup \mathcal{C}(B_2)$ e $\mathcal{C}_X(B_1 \cup B_2) = \mathcal{C}_X(B_1) \cap \mathcal{C}(B_2)$ sono vere; ossia, se e solo se per ogni $B_1, B_2 \in A$ entrambe le formule $X \setminus (B_1 \cap B_2) = (X \setminus B_1) \cup (X \setminus B_2)$ e $X \setminus (B_1 \cup B_2) = (X \setminus B_1) \cap (X \setminus B_2)$ sono vere; ossia se e solo se le leggi di de Morgan sono vere. Infine si osservi che $\mathcal{C}_X(E_\cap) = \mathcal{C}_X(X) = \emptyset = E_\cup$ e $\mathcal{C}_X(E_\cup) = \mathcal{C}_X(\emptyset) = X = E_\cap$, come deve essere (il termine "deve" viene dal fatto che ogni omomorfismo di semigruppi tra semigruppi che in realtà son dei monoidi è anche un omomorfismo di monoidi).

III. Basta mostrare le identità a livello insiemistico, 'ché $\mathcal{C}_X$ preserva tutte le strutture. Ora, per ogni $B \in A$ risulta $\mathcal{C}_X \circ \mathcal{C}_X(B) = \mathrm{Id}_A(B)$: infatti, $\mathcal{C}_X \circ \mathcal{C}_X(B) = \mathcal{C}_X(\mathcal{C}_X(B)) = \mathcal{C}_X(X \setminus B) = X \setminus (X \setminus B) = B = \mathrm{Id}_A(B)$.

---

[1] Dati $(A_1, \star_1)$ e $(A_2, \star_2)$ due monoidi, chiameremo **isomorfismo di monoidi** tra $(A_1, \star_1)$ e $(A_2, \star_2)$ ogni applicazione $A_1 \to A_2$ che sia e (I.) bigettiva e (II.) un omomorfismo di monoidi.

Esercizio 2. Sia $A = \{a, b, c, d\}$ un insieme.

I. Si consideri la famiglia $P = \{\{a\}, \{b, c\}, \{d\}\}$ di sottoinsiemi di A. Si dica se P è una partizione di A e, in caso affermativo, si descriva esplicitamente la relazione di equivalenza R_P ad essa associata.

II. Si consideri la relazione $R = \{(a, a), (b, b), (c, c), (d, d), (a, d), (b, c), (c, b), (d, a)\}$ su A. Si dica se R è di equivalenza e, in caso affermativo, si descriva esplicitamente la partizione P_R ad essa associata.

Soluzione. I. Una verifica immediata ci permette di dire che P è una partizione di A. La relazione di equivalenza $R_P \subseteq A \times A$ associata a P è

$$R_P = \{\ (a, a), (b, b), (b, c), (c, b), (c, c), (d, d)\ \}.$$

II. La relazione $R \subseteq A \times A$ è evidentemente di equivalenza. La partizione $P_R \subseteq \mathcal{P}(A)$ associata a R è

$$P_R = \{\{a, d\}, \{b, c\}\}.$$

Esercizio 3. Da quanto raccontato a lezione, sappiamo che su $\mathbb{Z}$ sono ben definite le operazioni di addizione e moltiplicazione. Manipolando classi di equivalenza, rappresentanti et cætera, si mostri che **I.** entrambe queste operazioni sono associative; **II.** la moltiplicazione è distributiva rispetto all'addizione.

Soluzione. I. Più. L'operazione di addizione è associativa se e solo se per ogni $[m, s]$, $[\mu, \sigma]$, $[M, S] \in \mathbb{Z}$ risulta $([m, s] + [\mu, \sigma]) + [M, S] = [m, s] + ([\mu, \sigma] + [M, S])$; ossia, se e solo se per ogni $[m, s]$, $[\mu, \sigma]$, $[M, S] \in \mathbb{Z}$ risulta $[m + \mu, s + \sigma] + [M, S] = [m, s] + [\mu + M, \sigma + S]$; ossia, se e solo se per ogni $[m, s]$, $[\mu, \sigma]$, $[M, S] \in \mathbb{Z}$ risulta $[m+\mu+M, s+\sigma+S] = [m+\mu+M, s+\sigma+S]$; ossia, sempre. **I. Per.** L'operazione di moltiplicazione è associativa se e solo se per ogni $[m, s]$, $[\mu, \sigma]$, $[M, S] \in \mathbb{Z}$ risulta $([m, s] \cdot [\mu, \sigma]) \cdot [M, S] = [m, s] \cdot ([\mu, \sigma] \cdot [M, S])$; ossia, se e solo se per ogni $[m, s]$, $[\mu, \sigma]$, $[M, S] \in \mathbb{Z}$ risulta $[m \cdot \mu + s \cdot \sigma,\ m \cdot \sigma + \mu \cdot s] \cdot [M, S] = [m, s] \cdot [\mu \cdot M + \sigma \cdot S,\ \mu \cdot S + M \cdot \sigma]$; ossia, se e solo se per ogni $[m, s]$, $[\mu, \sigma]$, $[M, S] \in \mathbb{Z}$ risulta $[(m \cdot \mu + s \cdot \sigma) \cdot M + (m \cdot \sigma + \mu \cdot s) \cdot S,\ (m \cdot \mu + s \cdot \sigma) \cdot S + M \cdot (m \cdot \sigma + \mu \cdot s)] = [m \cdot (\mu \cdot M + \sigma \cdot S) + s \cdot (\mu \cdot S + M \cdot \sigma),\ m \cdot (\mu \cdot S + M \cdot \sigma) + s \cdot (\mu \cdot M + \sigma \cdot S)]$; ossia, sempre.

II. L'operazione di moltiplicazione si distribuisce su quella di addizione se e solo se per ogni $[m, s]$, $[\mu_1, \sigma_1]$, $[\mu_2, \sigma_2] \in \mathbb{Z}$ risulta $[m, s] \cdot ([\mu_1, \sigma_1] + [\mu_2, \sigma_2]) = [m, s] \cdot [\mu_1, \sigma_1] + [m, s] \cdot [\mu_2, \sigma_2]$; ossia, se e solo se per ogni $[m, s]$, $[\mu_1, \sigma_1]$, $[\mu_2, \sigma_2] \in \mathbb{Z}$ risulta $[m, s] \cdot [\mu_1 + \mu_2, \sigma_1 + \sigma_2] = [m \cdot \mu_1 + s \cdot \sigma_1, m \cdot \sigma_1 + \mu_1 \cdot s] + [m \cdot \mu_2 + s \cdot \sigma_2, m \cdot \sigma_2 + \mu_2 \cdot s]$; ossia, se e solo se per ogni $[m, s]$, $[\mu_1, \sigma_1]$, $[\mu_2, \sigma_2] \in \mathbb{Z}$ risulta $[m \cdot (\mu_1 + \mu_2) + s \cdot (\sigma_1 + \sigma_2), m \cdot (\sigma_1 + \sigma_2) + (\mu_1 + \mu_2) \cdot s] = [m \cdot \mu_1 + s \cdot \sigma_1 + m \cdot \mu_2 + s \cdot \sigma_2, m \cdot \sigma_1 + \mu_1 \cdot s + m \cdot \sigma_2 + \mu_2 \cdot s]$; ossia, sempre.

Esercizio 4. Siano $\mathbb{N}$ l'insieme dei numeri naturali e $\mathbb{Z}$ l'insieme dei numeri interi. Si mostri che **I.** esistono biiezioni tra $\mathbb{N}$ e $\mathbb{Z}$, ossia che $|\mathbb{Z}| = |\mathbb{N}|$; **II.** ogni omomorfismo di monoidi $\alpha : (\mathbb{N}, +) \to (\mathbb{Z}, +)$ è della forma $\alpha(n) = A \cdot n$, con $A \in \mathbb{Z}$; **III.** l'unico omomorfismo tra i monoidi (additivi e moltiplicativi) $(\mathbb{N}, +, \cdot)$ e $(\mathbb{Z}, +, \cdot)$ è l'applicazione $\varrho : (\mathbb{N}, +, \cdot) \to (\mathbb{Z}, +, \cdot)$ definita da $\mathbb{N} \ni n \mapsto \varrho(n) = n \in \mathbb{Z}$.

Soluzione. I. Per mostrare che $|\mathbb{Z}| = |\mathbb{N}|$, basta mostrare che entrambe le disuguaglianze $|\mathbb{N}| \leq |\mathbb{Z}|$ e $|\mathbb{Z}| \leq |\mathbb{N}|$ sono vere (questo grazie al teorema di Schroeder-Bernstein). Ora, per mostrare la prima disuguaglianza, è sufficiente considerare l'applicazione (evidentemente iniettiva) $\varrho : \mathbb{N} \to \mathbb{Z}$ definita ponendo $\mathbb{N} \ni n \mapsto \varrho(n) = n \in \mathbb{Z}$. Per msotrare la seconda disuguaglianza, invece, basta (1.) ricordare che, data una qualsiasi relazione di equivalenza ϵ su un qualsivoglia insieme X, allora $|X/\epsilon| \leq |X|$, 'ché esiste sempre almeno un'applicazione suriettiva $\pi_\epsilon : X \to X/\epsilon$ (per esempio la proiezione canonicamente associata a ϵ); (2.) ricordare che $\mathbb{Z} = (\mathbb{N} \times \mathbb{N})/\sim$; (3.) ricordare che $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$; (4.) scrivere $|\mathbb{Z}| = |(\mathbb{N} \times \mathbb{N})/\sim| \leq |\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$. Un esempio esplicito di bigezione tra $\mathbb{Z}$ e $\mathbb{N}$ è dato dall'applicazione $\gamma : \mathbb{Z} \to \mathbb{N}$ definita ponendo $[0, 0] \mapsto \gamma([0, 0]) = 0$ e, per $a \in \mathbb{N} \setminus \{0\}$, $[a, 0] \mapsto \gamma([a, 0]) = 2a$, $[0, a] \mapsto \gamma([0, a]) = 2a - 1$.

II. Un'applicazione $\alpha : (\mathbb{N}, +) \to (\mathbb{Z}, +)$ che sia anche un omomorfismo di monoidi è tale che $\alpha(n) = n \cdot \alpha(1)$ (infatti $\alpha(n) = \alpha(1 + ... + 1) = \alpha(1) + ... + \alpha(1) = n \cdot \alpha(1)$). Scrivendo $A = \alpha(1)$ e usando la commutatività della moltiplicazione in $\mathbb{Z}$, abbiamo infine che α è l'applicazione $\mathbb{N} \ni n \mapsto \alpha(n) = A \cdot n$. Si osservi che, come deve essere, l'immagine di $0 \in \mathbb{N}$ è $0 \in \mathbb{Z}$.

III. Dal punto II., sappiamo che ogni applicazione ϱ che sia un omomorfismo tra i monoidi additivi e moltiplicativi $(\mathbb{N}, +, \cdot)$ e $(\mathbb{Z}, +, \cdot)$ ha la forma $\varrho(n) = P \cdot n$, 'ché ϱ è un omomorfismo tra i monoidi additivi. Ora, imponendo la codizione $\varrho(1) = 1$, che viene dal volere che ϱ sia un omomorfismo tra i monoidi moltiplicativi, abbiamo $P = 1$ (infatti $1 = \varrho(1) = P \cdot 1$ implica $P = 1$) e, quindi, ϱ è l'applicazione $\mathbb{N} \ni n \mapsto \varrho(n) = n \in \mathbb{Z}$.

Esercizio 5. Fissato $m \in \mathbb{Z}$, $m \geq 2$, si definisca su $\mathbb{Z}$ la relazione $\equiv_m$ ponendo

$$\forall a_1, a_2 \in \mathbb{Z}, \quad a_1 \equiv_m a_2 \Leftrightarrow \exists\, q \in \mathbb{Z} \text{ tale che } a_1 = a_2 + qm.$$

Dire se la relazione $\equiv_m$ è di equivalenza.

Soluzione. Riflessività. Per ogni $a \in \mathbb{Z}$ risulta $a \equiv_m a$, 'ché, prendendo $q = 0$, è possibile scrivere $a = a + qm$.

Simmetria. Se $a_1, a_2 \in \mathbb{Z}$ sono tali che $a_1 \equiv_m a_2$, allora $a_2 \equiv_m a_1$, 'ché, detto $q \in \mathbb{Z}$ l'intero tale che $a_1 = a_2 + qm$, abbiamo che l'intero $Q = -q$ è tale che $a_2 = a_1 + Qm$.

Transitività. Se $a_1, a_2, a_3 \in \mathbb{Z}$ sono tali che $a_1 \equiv_m a_2$ e $a_2 \equiv_m a_3$, allora $a_1 \equiv_m a_3$, 'ché, detti $q', q'' \in \mathbb{Z}$ gli interi tali che $a_1 = a_2 + q'm$ e $a_2 = a_3 + q''m$, abbiamo che l'intero $Q = q' + q''$ è tale che $a_1 = a_3 + Qm$ (e questo perché $a_1 = a_2 + q'm = (a_3 + q''m) + q'm = a_3 + (q' + q'')m$).