

**Linguaggio e Metodi della Matematica**

Prova scritta del 8 Febbraio 2006

**[Esercizio 1]**

Sia  $f : \mathbb{Z} \rightarrow \mathbb{Z}$  la funzione definita come

$$f(z) = \begin{cases} z + 1 & \text{se } z < 0 \\ z - 1 & \text{se } z \geq 0 \end{cases}$$

Si dica, giustificando ogni risposta, se  $f$  è iniettiva, surgettiva, bigettiva. Inoltre, a cosa corrispondono  $f^{-1}(-1)$ ,  $f^{-1}(0)$  e  $f^{-1}(1)$ ?

**Svolgimento**

$f$  non è iniettiva perché esistono due valori che hanno la stessa immagine. Infatti  $f(-1) = 0 = f(1)$  (o anche  $f(-2) = -1 = f(0)$ ).

$f$  è surgettiva perché per ogni  $n \in \mathbb{Z}$  possiamo trovare un elemento  $z \in \mathbb{Z}$  tale che  $f(z) = n$ .

Infatti, se  $n \geq 0$  allora basta prendere  $z = n + 1$  (si ha  $f(n + 1) = (n + 1) - 1 = n$ , essendo in questo caso  $n + 1 \geq 0$ ).

Se invece  $n < 0$  allora basta prendere  $z = n - 1$  (si ha  $f(n - 1) = (n - 1) + 1 = n$ , essendo in questo caso  $n - 1 < 0$ ).

$f$  non è bigettiva perché non è iniettiva.

$$f^{-1}(-1) = \{-2, 0\}, f^{-1}(0) = \{-1, 1\} \text{ e } f^{-1}(1) = \{2\}.$$

### [Esercizio 2]

Si dica, giustificando tutte le risposte, se le seguenti formule predicative sono equivalenti, e se sono tautologie, contraddizioni o soddisfacibili.

1.  $\forall x.P(x) \rightarrow \exists x.(P(x) \wedge \neg Q(x))$
2.  $\exists x.((P(x) \wedge Q(x)) \rightarrow \perp)$

### Svolgimento

Verifichiamo prima se le formule sono equivalenti, poi mostriamo che sono soddisfacibili.

$$\begin{aligned}\forall x.P(x) \rightarrow \exists x.(P(x) \wedge \neg Q(x)) &\equiv \neg(\forall x.P(x)) \vee \exists x.(P(x) \wedge \neg Q(x)) \quad (\text{implic.}) \\ &\equiv \exists x.\neg P(x) \vee \exists x.(P(x) \wedge \neg Q(x)) \quad (\text{neg. quantif.}) \\ &\equiv \exists x.(\neg P(x) \vee (P(x) \wedge \neg Q(x))) \quad (\text{distrib. quantif.}) \\ &\equiv \exists x.(\neg P(x) \vee \neg Q(x)) \quad (\text{semplif.})\end{aligned}$$

$$\begin{aligned}\exists x.((P(x) \wedge Q(x)) \rightarrow \perp) &\equiv \exists x.(\neg(P(x) \wedge Q(x)) \vee \perp) \quad (\text{implic.}) \\ &\equiv \exists x.\neg(P(x) \wedge Q(x)) \quad (\text{identità}) \\ &\equiv \exists x.(\neg P(x) \vee \neg Q(x)) \quad (\text{de morgan})\end{aligned}$$

Quindi le formule sono equivalenti.

Per mostrare che non sono tautologie si consideri l'interpretazione  $\mathcal{I}$  tale che  $D_{\mathcal{I}} = \{a\}$ ,  $TS_{\mathcal{I}}(P) = TS_{\mathcal{I}}(Q) = \{a\}$ . Infatti  $\mathcal{I} \models P(a)$  e quindi  $\mathcal{I} \not\models \neg P(a)$ , inoltre  $\mathcal{I} \models Q(a)$  e quindi  $\mathcal{I} \not\models \neg Q(a)$ . Dunque  $\mathcal{I} \not\models \neg P(a) \vee \neg Q(a)$ . Dato che  $a$  è l'unico valore nel dominio, si ha  $\mathcal{I} \not\models \exists x.(\neg P(x) \vee \neg Q(x))$ , che sappiamo essere equivalente alle due formule.

Analogamente, per mostrare che non sono contraddizioni si consideri l'interpretazione  $\mathcal{I}'$  tale che  $D_{\mathcal{I}'} = \{a\}$ ,  $TS_{\mathcal{I}'}(P) = \{a\}$  e  $TS_{\mathcal{I}'}(Q) = \emptyset$ . Infatti  $\mathcal{I}' \not\models Q(a)$  e quindi  $\mathcal{I}' \models \neg Q(a)$ . Dunque  $\mathcal{I}' \models \neg P(a) \vee \neg Q(a)$ . Ma allora  $\mathcal{I}' \models \exists x.(\neg P(x) \vee \neg Q(x))$  (scegliendo  $x = a$ ), che sappiamo essere equivalente alle due formule.

Le interpretazioni  $\mathcal{I}$  e  $\mathcal{I}'$  mostrano che le formule sono soddisfacibili.

**[Esercizio 3 - SOLO PER RECUPERO PRIMO COMPITINO]**

|     |     |       |
|-----|-----|-------|
| $P$ | $Q$ | $P Q$ |
| 0   | 0   | 1     |
| 0   | 1   | 1     |
| 1   | 0   | 1     |
| 1   | 1   | 0     |

Tutti i connettivi della logica proposizionale possono essere espressi in termini del solo operatore  $P|Q$  (si legge “P *nand* Q”) definito dalla tabella di verità a lato. Ad esempio,  $\neg P \equiv P|P$  e  $P \wedge Q \equiv (P|Q)|(P|Q)$ . Si scrivano delle formule equivalenti a  $P \vee Q$  e  $(P \rightarrow \neg Q) \rightarrow R$  usando il solo operatore *nand*.

**Svolgimento**

Dalle leggi di De Morgan sappiamo che

$$P \vee Q \equiv \neg(\neg P \wedge \neg Q)$$

Inoltre, come suggerito anche dal nome stesso dell’operatore si ha

$$\neg(A \wedge B) \equiv A|B$$

Quindi prendendo  $A = \neg P = P|P$  e  $B = \neg Q = Q|Q$  si ha

$$P \vee Q \equiv (P|P)|(Q|Q)$$

Per le leggi dell’implicazione sappiamo che

$$(P \rightarrow \neg Q) \rightarrow R \equiv \neg(P \rightarrow \neg Q) \vee R \equiv \neg(\neg P \vee \neg Q) \vee R$$

Inoltre, applicando De Morgan e doppia negazione si ottiene facilmente:

$$\neg(\neg P \vee \neg Q) \vee R \equiv (\neg\neg P \wedge \neg\neg Q) \vee R \equiv (P \wedge Q) \vee R$$

Per quanto visto sopra, sappiamo che

$$(P \wedge Q) \vee R \equiv ((P \wedge Q)|(P \wedge Q)|(R|R))$$

(usando *nand* per rimpiazzare l’*or*).

A questo punto basta rimpiazzare  $P \wedge Q$  con la formula equivalente  $(P|Q)|(P|Q)$  suggerita nel testo:

$$(P \rightarrow \neg Q) \rightarrow R \equiv (((P|Q)|(P|Q))((P|Q)|(P|Q))|(R|R))$$

Si ricorda che l’uso delle parentesi nelle formule con il *nand* è importante perché il *nand* non è associativo.

**[Esercizio 4 - SOLO PER RECUPERO PRIMO COMPITINO]**

Scrivere una formula della logica predicativa che formalizzi la frase “ $a$  è il più grande dei divisori primi di  $b$ ” sul dominio dei naturali positivi, sfruttando la costante 1, il simbolo di funzione  $\times$ , e i simboli di predicato  $=$ ,  $<$  e  $\leq$  con l’ovvio significato. (*Consiglio*: definire le formule per esprimere che “ $x$  è divisore di  $y$ ” e che “ $x$  è primo” per poi riusarle).

**Svolgimento**

Abbiamo visto a lezione che la formula  $\text{div}(x, y)$  che formalizza la frase “ $x$  è divisore di  $y$ ” può essere espressa come segue (essendo il dominio quello dei naturali non dobbiamo occuparci dei valori negativi e dello 0).

$$\forall x, y ( \text{div}(x, y) \leftrightarrow \exists a. (x \times a = y) )$$

Ricordando che un numero  $x$  è primo se è maggiore di 1 e non ha divisori più piccoli, la formula  $\text{prime}(x)$  che formalizza la frase “ $x$  è primo” può essere espressa come segue:

$$\forall x ( \text{prime}(x) \leftrightarrow 1 < x \wedge \forall a. (\text{div}(a, x) \rightarrow (a = 1 \vee a = x)) )$$

Adesso bisogna formalizzare il fatto che  $a$  è un divisore primo di  $b$  e che preso un qualsiasi altro divisore primo  $k$  di  $b$  si ha  $a$  maggiore o uguale a  $k$ :

$$\forall a, b ( \text{max\_div\_prime}(a, b) \leftrightarrow \text{div}(a, b) \wedge \text{prime}(a) \wedge \forall k. (\text{div}(k, b) \wedge \text{prime}(k) \rightarrow k \leq a) )$$

**[Esercizio 5]**

Si dica se le seguenti proprietà su insiemi sono valide, fornendo una dimostrazione formale in caso positivo oppure un controesempio in caso negativo:

1.  $\forall A, B, C. ((A \subseteq B \wedge A \cap B \subseteq C) \rightarrow (A \subseteq B \cap C))$
2.  $\forall A, B, C. ((A \subseteq B \wedge A \cap B \subseteq C) \rightarrow (B \subseteq C))$

**Svolgimento**

La proprietà  $\forall A, B, C. ((A \subseteq B \wedge A \cap B \subseteq C) \rightarrow (A \subseteq B \cap C))$  è valida, come dimostrato dalla seguente prova formale:

- |   |   |
|---|---|
| 1. $(A \subseteq B \wedge A \cap B \subseteq C)$  | (Ipotesi aggiuntiva)  |
| 2. $x \in A$  | (Ipotesi aggiuntiva)  |
| 3. $A \subseteq B$  | ( <b>A.E.</b> da 1)   |
| 4. $x \in B$  | ( <b>M.P.</b> <sub><math>\subseteq</math></sub> da 2 e 3)               |
| 5. $x \in A \cap B$   | ( <b>A.I.</b> <sub><math>\cap</math></sub> da 2 e 4)                    |
| 6. $A \cap B \subseteq C$   | ( <b>A.E.</b> da 1)   |
| 7. $x \in C$  | ( <b>M.P.</b> <sub><math>\subseteq</math></sub> da 5 e 6)               |
| 8. $x \in B \cap C$   | ( <b>A.I.</b> <sub><math>\cap</math></sub> da 4 e 7)                    |
| 9. $x \in A \rightarrow x \in B \cap C$   | ( <b>Imp.</b> da $\frac{[2]}{8}$ )                                      |
| 10. $A \subseteq B \cap C$  | ( <b><math>\forall G</math></b> <sub><math>\subseteq</math></sub> da 9) |
| 11. $(A \subseteq B \wedge A \cap B \subseteq C) \rightarrow (A \subseteq B \cap C)$                    | ( <b>Imp.</b> da $\frac{[1]}{10}$ )                                     |
| 12. $\forall A, B, C. ((A \subseteq B \wedge A \cap B \subseteq C) \rightarrow (A \subseteq B \cap C))$ | ( <b><math>\forall G</math></b> per tre volte da 11)                    |

La proprietà  $\forall A, B, C. ((A \subseteq B \wedge A \cap B \subseteq C) \rightarrow (B \subseteq C))$  non è valida, come dimostrato dal seguente semplice controesempio.

Prendiamo  $A = \{1\}$ ,  $B = \{1, 2\}$  e  $C = \{1, 3\}$ .

Ovviamente  $A \cap B = \{1\}$ , quindi:

- $A \subseteq B$ ;
- $A \cap B \subseteq C$ ;
- $B \not\subseteq C$ .

### [Esercizio 6]

Si considerino le stringhe di lunghezza 10 sull'alfabeto  $A = \{a, b\}$ . In quante di esse compaiono esattamente due simboli  $a$ ? E in quante di esse  $a$  compare al massimo due volte?

### Svolgimento

Ogni stringa che contiene esattamente due occorrenze di  $a$  è determinata univocamente dalle posizioni occupate dalle  $a$ . Quindi il problema si riconduce a scegliere due posizioni tra le dieci disponibili.

In questo modo il problema viene formulato in termini delle disposizioni **non ordinate** (perché se scambiamo le due  $a$  tra di loro otteniamo sempre la stessa stringa) di due elementi presi da un insieme di dieci, e quindi il numero di possibili scelte è

$$C(10, 2) = 10! / (2! \cdot (10 - 2)!) = 10! / (2! \cdot 8!) = (10 \cdot 9) / 2 = 45.$$

Le stringhe che contengono al massimo due occorrenze di  $a$  possono essere partizionate in tre insiemi disgiunti:

- $S_0$ , che comprende le stringhe senza  $a$ ;
- $S_1$ , che comprende le stringhe che contengono esattamente una occorrenza di  $a$ ;
- $S_2$ , che comprende le stringhe che contengono esattamente due occorrenze di  $a$ ;

L'insieme  $S_0$  contiene ovviamente una sola stringa ( $bbbbbbbbb$ ):  $|S_0| = 1$ .

La cardinalità dell'insieme  $S_2$  è stata calcolata sopra:  $|S_2| = 45$ .

La cardinalità dell'insieme  $S_1$  può essere calcolata in maniera analoga a quella di  $S_2$ : questa volta dobbiamo considerare le disposizioni di un solo elemento (la posizione dove mettere  $a$ , in tutte le altre posizioni dobbiamo mettere  $b$ ) preso da un insieme di dieci. Ovviamente:

$$C(10, 1) = 10! / (1! \cdot (10 - 1)!) = 10! / (1! \cdot 9!) = 10.$$

Si noti che in questo caso non fa differenza considerare le disposizioni ordinate o quelle non ordinate, perché si sceglie un solo elemento. Essendo gli insiemi disgiunti, per la regola della somma:

$$|S_0 \cup S_1 \cup S_2| = |S_0| + |S_1| + |S_2| = 1 + 10 + 45 = 56$$

**[Esercizio 7 - SOLO PER RECUPERO SECONDO COMPITINO]**

Date due relazioni  $R_1 \subseteq \mathbb{Z} \times \mathbb{Z}$  e  $R_2 \subseteq \mathbb{Z} \times \mathbb{Z}$ , la loro *composizione* è la relazione  $R_2 \circ R_1 = \{(n, m) \mid \exists k. (n R_1 k \wedge k R_2 m)\} \subseteq \mathbb{Z} \times \mathbb{Z}$ . Esistono due relazioni  $R$  e  $S$  tali che  $S \circ R = \{(1, 1)\}$  mentre  $R \circ S = \emptyset$ ? A cosa corrisponde la relazione  $R_{\geq} \circ R_{\leq}$ ?

**Svolgimento**

Non è possibile trovare due relazioni  $R$  e  $S$  tali che  $S \circ R = \{(1, 1)\}$  e  $R \circ S = \emptyset$ . Infatti, se  $S \circ R = \{(1, 1)\}$  vuol dire che esiste un qualche intero  $k$  tale che  $1 R k$  e  $k S 1$ , ma allora si avrebbe che  $(k, k) \in R \circ S$  e quindi  $R \circ S$  non potrebbe essere vuota.

Si ha  $R_{\geq} \circ R_{\leq} = \mathbb{Z} \times \mathbb{Z}$ . Infatti, dati due interi qualsiasi  $n$  e  $m$  si consideri  $k = \max(n, m)$ . Ovviamente essendo  $k$  il massimo dei due valori si ha  $n \leq k$  e  $k \geq m$ . Quindi:

- $(n, k) \in R_{\leq}$ , ovvero  $n R_{\leq} k$
- $(k, m) \in R_{\geq}$ , ovvero  $k R_{\geq} m$

Per definizione di composizione si ha dunque  $(n, m) \in (R_{\geq} \circ R_{\leq})$ , ovvero  $n (R_{\geq} \circ R_{\leq}) m$

**[Esercizio 8 - SOLO PER RECUPERO SECONDO COMPITINO]**  
Disegnare il diagramma di Hasse della relazione di divisibilità sul dominio  $\{2, 3, 4, 5, 15, 22, 176, 198\}$

**Svolgimento**

