Durata della prova: 1h 30'

| | | | |
|---|---|---|---|
| | | | |

# Esame di Logica e Algebra

**Politecnico di Milano – Ingegneria Informatica – 22 Giugno 2022**

| **Docente e ultimo voto laboratorio:** | **Cognome:** | **Nome:** | **Codice persona:** |
|---|---|---|---|
| | | | |

**Tutte le risposte devono essere motivate. Gli esercizi vanno svolti su questi fogli, nello spazio sotto il testo e sul retro. I fogli di brutta non devono essere consegnati. I compiti privi di indicazione leggibile di nome e cognome non verranno corretti.**

1. (Punteggio: a) 3, b) 1+2, c) 4+1 )
Si consideri la relazione binaria $\rho$ su $X = \mathbb{Z} \times \mathbb{Z}$ definita nel seguente modo:

$$(a, b)\, \rho\, (c, d) \text{ se e solo se } ab - cd = 0$$

(a) Si mostri che $\rho$ è una relazione di equivalenza su $X$.

(b) Si mostri che $[(2, 3)]_\rho = [(1, 6)]_\rho$ e si verifichi che $\rho = \ker(f)$, dove $f : X \to \mathbb{Z}$ è definita da $f(a, b) = ab$.

(c) Si consideri la seguente formula della logica del primo ordine:

$$\forall x\, (\, A(a, x) \wedge A(f(x), x) \Rightarrow A(g(x, x), x)\, )$$

Si stabilisca se è vera, falsa o soddisfacibile ma non vera nell'interpretazione avente come dominio $D$ l'insieme di tutte le relazioni binarie su $X$ e nella quale la costante $a$ è interpretata dalla relazione identica su $X$, $A(x, y)$ è la relazione di inclusione di relazioni, $f(x)$ è la relazione inversa di $x$, e $g(x, y)$ è il prodotto tra le relazioni $x, y$. La formula è logicamente valida o logicamente contraddittoria?

**Soluzioni:**

(a) La relazione $\rho$ è riflessiva dato che $(a, b)\rho(a, b)$ dal momento che $ab = ab$; è anche simmetrica infatti se $(a, b)\rho(c, d)$ allora $ab = cd$ e quindi anche $(c, d)\rho(a, b)$. Infine $\rho$ è anche transitiva: se $(a, b)\rho(c, d)$ e $(c, d)\rho(e, f)$ allora $ab = cd = ef$ da cui segue che $(a, b)\rho(e, f)$.

(b) Dato che $2 \cdot 3 = 1 \cdot 6$, abbiamo che $(2, 3)\rho(1, 6)$ e quindi $[(2, 3)]_\rho = [(1, 6)]_\rho$. La relazione $\ker(f)$ mette in relazione due elementi $(a, b)$, $(c, d)$ se e solo se $f(a, b) = f(c, d)$ che è equivalente a $ab = cd$, cioè $(a, b)\rho(c, d)$. Pertanto $\rho = \ker(f)$.

(c) La formula si interpreta nel seguente modo: per ogni relazione binaria $R$ su $\mathbb{Z}$, se $I \subseteq R$ e $R^{-1} \subseteq R$, allora $R^2 \subseteq R$. In altre parole dice che ogni relazione binaria su $\mathbb{Z}$ che sia riflessiva e simmetrica è necessariamente anche transitiva. Questa formula è falsa, basta considerare ad esempio la relazione

$$R = I \cup \{(1, 2), (2, 1), (2, 3), (3, 2)\}$$

che è chiaramente riflessiva e simmetrica, ma non transitiva. La formula non è quindi logicamente valida, ma non è nemmeno logicamente contradditoria dato che risulta vera in una interpretazione avente un qualunque dominio non vuoto e in cui $A(x, y)$ sia interpretata dalla relazione vuota.

2. (Punteggio: a) 3, b) 3, c) 3 )

Si consideri la formula $f(A, B, C)$ della logica proposizionale che assume il valore di verità 1 se e solo se $v(A) = v(B) = v(C) = 1$ oppure $v(A) = v(C) = 1$ e $v(B) = 0$ oppure $v(B) = v(C) = 1$ e $v(A) = 0$.

(a) Si scriva una formula equivalente ad $f(A, B, C)$ che contenga solo i connettivi $\neg, \Rightarrow$.

(b) Si stabilisca, giustificando l'affermazione, se da $\neg A \Rightarrow B$ si può dedurre nel sistema formale $L$, la formula $f(A, B, C)$.

(c) Si dica se l'insieme $\Gamma = \{\neg A \Rightarrow B, \neg f(A, B, C)\}$ è insoddisfacibile.

**Soluzioni:**

(a) Usando la forma normale disgiuntiva abbiamo $f(A, B, C) \equiv (A \wedge B \wedge C) \vee (\neg A \wedge B \wedge C) \vee (A \wedge \neg B \wedge C)$. Semplificando la precedente formula abbiamo:

$$f(A, B, C) \equiv (B \wedge C) \vee (A \wedge \neg B \wedge C) \equiv (B \vee (A \wedge \neg B)) \wedge C \equiv ((B \vee A) \wedge (B \vee \neg B)) \wedge C \equiv (B \vee A) \wedge C$$

da cui, usando solo i connettivi $\neg, \Rightarrow$, otteniamo $f(A, B, C) \equiv (B \vee A) \wedge C \equiv \neg(C \Rightarrow \neg(\neg A \Rightarrow B))$.

(b) Dal teorema di correttezza e completezza forte abbiamo $\neg A \Rightarrow B \vdash_L \neg(C \Rightarrow \neg(\neg A \Rightarrow B))$ se e solo se $\neg A \Rightarrow B \models \neg(C \Rightarrow \neg(\neg A \Rightarrow B))$, quindi dobbiamo verificare che i modelli di $\neg A \Rightarrow B$ sono anche modelli di $\neg(C \Rightarrow \neg(\neg A \Rightarrow B))$ (che conosciamo dal testo!). Ora, un modello di $\neg A \Rightarrow B$ è $v(A) = 0, v(B) = 1$ e $v(C) = 0$ che però non è modello di $f(A, B, C)$. Pertanto da $\neg A \Rightarrow B$ non si può dedurre in $L$ la formula $f(A, B, C)$.

(c) L'insieme $\{\neg A \Rightarrow B, \neg f(A, B, C)\}$ è insoddisfacibile se e solo se $\neg A \Rightarrow B \models f(A, B, C)$ che, dal punto precedente, sappiamo essere una deduzione falsa. Infatti l'interpretazione $v(A) = 0, v(B) = 1$ e $v(C) = 0$ è modello di $\neg A \Rightarrow B$ ma non di $f(A, B, C)$, quindi è anche modello di $\neg f(A, B, C)$ e pertanto $\Gamma$ è soddisfacibile.

3. (Punteggio: a) 3, b) 3, c) 4 )
Si consideri l'insieme delle matrici quadrate di ordine 2 ad elementi in $\mathbb{Z}$ strutturato ad anello rispetto alle usuali operazioni di somma e prodotto di matrici ed il suo sottoinsieme $A$ così definito:

$$A = \left\{ \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} : a, b, c \in \mathbb{Z} \right\}.$$

Sia inoltre $f : Z \to A$ l'applicazione definita da $f(z) = \begin{pmatrix} 0 & 0 \\ z & 0 \end{pmatrix}$ per ogni $z \in \mathbb{Z}$.

(a) Si mostri che $A$ è un anello rispetto alle usuali operazioni di somma e prodotto di matrici.

(b) Si mostri che $f$ è un monomorfismo del gruppo additivo $(\mathbb{Z}, +)$ nel gruppo additivo $(A, +)$ e si dica se è anche un monomorfismo di anelli.

(c) Si considerino ora le seguenti formule della logica del primo ordine:

$$E(p(x, y), p(y, x))$$
$$\forall x \forall y \, (E(p(x, y), p(y, x)))$$

e si dica se sono vere, false, soddisfacibili ma non vere nell'interpretazione che ha come dominio $A$ e nella quale la lettera predicativa $E$ sia da interpretare come l'uguaglianza e la lettera funzionale $p$ come il prodotto tra matrici. Le formule sono logicamente valide?

**Soluzioni:**

(a) Dato che l'insieme delle matrici $2 \times 2$ a coefficienti interi costituisce un anello rispetto alle usuali somma e prodotto di matrici, usiamo il criterio di caratterizzazione dei sottoanelli e verifichiamo che per ogni $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}, \begin{pmatrix} \alpha & 0 \\ \beta & \gamma \end{pmatrix} \in A$ risulta che $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} - \begin{pmatrix} \alpha & 0 \\ \beta & \gamma \end{pmatrix} \in A$ e che $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \cdot \begin{pmatrix} \alpha & 0 \\ \beta & \gamma \end{pmatrix} \in A$. Abbiamo:

$$\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} - \begin{pmatrix} \alpha & 0 \\ \beta & \gamma \end{pmatrix} = \begin{pmatrix} a - \alpha & 0 \\ b - \beta & c - \gamma \end{pmatrix} \in A$$

$$\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \cdot \begin{pmatrix} \alpha & 0 \\ \beta & \gamma \end{pmatrix} = \begin{pmatrix} a\alpha & 0 \\ b\alpha + c\beta & c\gamma \end{pmatrix} \in A$$

Poichè è verificato il criterio di caratterizzazione dei sottoanelli segue che $(A, +, \cdot)$ è esso stesso un anello.

(b) Per ogni $z_1, z_2 \in \mathbb{Z}$, risulta che

$$f(z_1 + z_2) = \begin{pmatrix} 0 & 0 \\ z_1 + z_2 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ z_1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ z_2 & 0 \end{pmatrix} = f(z_1) + f(z_2)$$

e pertanto $f$ è un omomorfismo. Inoltre $f$ è iniettiva dato che $f(z_1) = f(z_2)$ se e solo se $\begin{pmatrix} 0 & 0 \\ z_1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ z_2 & 0 \end{pmatrix}$ e quindi se e solo se $z_1 = z_2$. Per verificare che $f$ sia un omomorfismo di anelli dobbiamo avere anche che $f(z_1 z_2) = f(z_1) \cdot f(z_2)$, che però in generale non è un'uguaglianza vera, infatti:

$$f(z_1 z_2) = \begin{pmatrix} 0 & 0 \\ z_1 z_2 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ z_1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ z_2 & 0 \end{pmatrix} = f(z_1) \cdot f(z_2)$$

Segue che $f$ è un monomorfismo di gruppi ma non di anelli.

(c) La prima formula non è chiusa ed è soddisfacibile, ad esempio è soddisfatta dall'assegnamento in cui $x = y = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. Il suo valore di verità si può dedurre dalla sua chiusura universale che è la seconda formula. Quest'ultima è falsa, infatti basta prendere $x = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$ e $y = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$ e si ha:

$$\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 2 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 2 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$$

Deduciamo pertanto che la prima formula è non vera ma solo soddisfacibile. Chiaramente dato che le due formule non sono vere, non sono nemmeno logicamente valide.