Durata della prova: 1h 30'

# Esame di Logica e Algebra

**Politecnico di Milano – Ingegneria Informatica – 18 Febbraio 2022**

| **Docente:** | **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) 2, b) 3, c) 2, d) 3+1 )
   Si consideri la relazione $R$ su $\mathbb{Z}_6$ definita da

$$([x]_6, [y]_6, ) \in R \text{ se e solo se } [y]_6 + [2x]_6 = [0]_6$$

   (a) Dopo averne disegnato il grafo d'adiacenza, stabilire le proprietà soddisfatte da $R$.

   (b) Si stabilisca se $R$ è una funzione. In caso lo sia, costruire l'insieme quoziente $\mathbb{Z}_6/\ker(R)$ e verificare se può esistere un'inversa destra.

   (c) Si stabilisca se $R$ è d'ordine ed in caso contrario verificare se esiste la chiusura d'ordine di $R$. In caso esista, disegnarne il diagramma di Hasse ed elencare eventuali elementi massimali, minimali, massimi e minimi.

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

$$\forall x\, (\, S(a, p(x, f(x))) \Rightarrow S(a, p(f(x), x))\, )$$

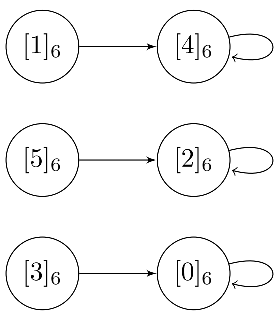
   Si stabilisca se è vera, falsa o soddisfacibile ma non vera nell'interpretazione avente come dominio l'insieme di tutte le relazioni binarie su di un certo insieme in cui $S$ interpreta la relazione di inclusione, $p$ il prodotto di relazioni, $f$ è interpretata dalla funzione che restituisce la relazione inversa e $a$ è la relazione identica. La formula è logicamente valida o insoddisfacibile?

**Soluzioni:**

(a) Per ogni $[x]_6 \in \mathbb{Z}_6$, le coppie che appartengono ad $R$ sono tutte e sole quelle del tipo $([x]_6, [-2x]_6)$ da cui segue che:

$$R = \{([0]_6, [0]_6), ([1]_6, [4]_6), ([2]_6, [2]_6), ([3]_6, [0]_6), ([4]_6, [4]_6), ([5]_6, [2]_6)\}$$

da cui otteniamo il seguente grafo d'adiacenza:



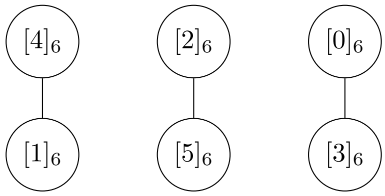

Dal grafo d'adiacenza si vede subito che $R$ soddisfa le seguenti proprietà: antisimmetrica (nessun arco, eccetto gli autoanelli, ha la doppia freccia), transitiva, seriale (da ogni vertice parte un arco).

(b) Poichè per ogni $[x]_6 \in \mathbb{Z}_6$ esiste un solo un elemento, cioè $[-2x]_6$, tale che $([x]_6, [-2x]_6) \in R$, segue che $R$ è chiaramente una funzione. Tra l'altro non è iniettiva dato che, per esempio, $[1]_6$ e $[4]_6$ hanno la stessa immagine pur essendo classi distinte.
Abbiamo che $\ker(R) = Id_{\mathbb{Z}_6} \cup \{([1]_6, [4]_6), ([4]_6, [1]_6), ([5]_6, [2]_6), ([2]_6, [5]_6), ([3]_6, [0]_6), ([0]_6, [3]_6)\}$ da cui segue che

$$\mathbb{Z}_6/\ker(R) = \{[[1]_6]_R, [[5]_6]_R, [[3]_6]_R\},$$

dove $[[1]_6]_R = \{[1]_6, [4]_6\}, [[5]_6]_R = \{[5]_6, [2]_6\}, [[3]_6]_R = \{[3]_6, [0]_6\}$.

(c) $R$ non è d'ordine nonostante sia transitiva e antisimmetrica poichè non è riflessiva. Se chiudiamo riflessivamente, cioè consideriamo $R \cup Id_{\mathbb{Z}_6}$, chiaramente rimane antisimmetrica e quindi questa nuova relazione risulta essere la chiusura d'ordine di $R$. Il diagramma di Hasse è il seguente:




da cui si vede subito che non si hanno massimi e minimi, mentre l'insieme dei massimali è $\{[4]_6, [2]_6, [0]_6\}$ e quello dei minimali $\{[1]_6, [5]_6, [3]_6\}$.

(d) La formula si può tradurre nel seguente modo: per ogni relazione $R$ su $X$, se $Id_X \subseteq R \cdot R^{-1}$, allora $Id_X \subseteq R^{-1} \cdot R$. Questa affermazione è falsa dato che se si considera $X = \{a, b\}$ ed $R = \{(a, b), (b, b)\}$, abbiamo $R \cdot R^{-1} = \{(a, a), (b, b)\}$ e $R^{-1} \cdot R = \{(b, b)\}$, quindi l'antecedente ($Id_X \subseteq R \cdot R^{-1}$) è soddisfatto, mentre il conseguente non lo è e pertanto l'intera formula, essendo la chiusura universale di una formula non vera, risulta falsa. Pertanto la formula non è logicamente valida e non è nemmeno insoddisfacibile: basta interpretare $S$ come la relazione vuota su di un qualunque insieme (rende falso l'antecedente e quindi vera l'intera formula).

2. (Punteggio: a) 3, b) 1, c) 2, d) 3+1 )

Si consideri l'insieme $A = \mathbb{Z} \times \mathbb{Z}$ strutturato ad anello rispetto alle seguenti operazioni:

$$(a,b) + (c,d) = (a+c, b+d)$$
$$(a,b) \cdot (c,d) = (ac, bd)$$

(a) Si verifichi che la relazione $R$ così definita:

$$(a,b)\, R\, (c,d) \text{ se e solo se } a+b \equiv c+d \pmod 5$$

è una congruenza del gruppo $(\mathbb{Z} \times \mathbb{Z}, +)$. È anche una congruenza dell'anello $(\mathbb{Z} \times \mathbb{Z}, +, \cdot)$?

(b) Si consideri l'anello $(\mathbb{Z}_3 \times \mathbb{Z}_5, +, \cdot)$ dove somma e prodotto sono definiti componente per componente come per l'anello $A$. Trovare le soluzioni dell'equazione $([2]_3, [3]_5) \cdot (x,y) = ([1]_3, [2]_5)$.

(c) Si consideri l'applicazione $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}_3 \times \mathbb{Z}_5$ definita da $f(a,b) = ([a]_3, [b]_5)$. Si mostri che $f$ è un omomorfismo tra l'anello $A$ e l'anello $(\mathbb{Z}_3 \times \mathbb{Z}_5, +, \cdot)$.

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

$$\forall x\, (\, \neg E(x,a) \wedge \exists y (\neg E(y,a) \wedge E(p(x,y),a)) \Rightarrow \neg \exists y E(p(x,y),b)\, )$$

e si dica se è vera, falsa, soddisfacibile ma non vere nell'interpretazione che ha come dominio l'anello $(\mathbb{Z}_3 \times \mathbb{Z}_5, +, \cdot)$ e nella quale $a = ([0]_3, [0]_5)$ è lo zero dell'anello, $b$ l'elemento $([1]_3, [1]_5)$, $p(x,y)$ è interpretato dall'operazione prodotto dell'anello, mentre $E(x,y)$ interpreta l'uguaglianza. La formula è logicamente valida o logicamente contraddittoria?

**Soluzione:**

(a) Verifichiamo che $R$ è una relazione di equivalenza. La riflessività e la simmetria di $R$ seguono subito dalla riflessività e dalla simmetria della congruenza modulo 5, infatti se $(a,b), (c,d) \in R$ allora $a+b \equiv a+b \pmod 5$ e, se $a+b \equiv c+d \pmod 5$ allora $c+d \equiv a+b \pmod 5$. Verifichiamo che $R$ è transitiva: siano $(a,b), (c,d), (e,f) \in R$ tali che $(a,b)\, R\, (c,d), (c,d)\, R\, (e,f)$, allora abbiamo $[a+b]_5 = [c+d]_5$ e $[c+d]_5 = [e+f]_5$ da cui segue che $[a+b]_5 = [e+f]_5$. Pertanto $(a,b)\, R\, (e,f)$ e quindi $R$ è transitiva.
Mostriamo la compatibilità rispetto all'addizione: siano $(a,b), (c,d), (e,f), (g,h) \in \mathbb{Z} \times \mathbb{Z}$ tali che $(a,b)\, R\, (c,d)$ e $(e,f)\, R\, (g,h)$, allora $[a+b]_5 = [c+d]_5$ e $[e+f]_5 = [g+h]_5$ da cui segue che:

$$[(a+e)+(b+f)]_5 = [e+f]_5 + [a+b]_5 = [g+h]_5 + [c+d]_5 = [(c+g)+(d+h)]_5$$

quindi $(a+e, b+f)\, R\, (c+g, d+h)$ e quindi si ha la compatibilità rispetto all'addizione. La relazione non è però una congruenza di anelli, infatti $(1,2)\, R\, (4,4)$ (dato che $[1+2]_5 = [3]_5 = [8]_5 = [4+4]_5$) e $(1,0)\, R\, (1,0)$ ma $(1,0) \cdot (1,2) = (1,0)$ e $(1,0) \cdot (4,4) = (4,0)$ ma $(1,0)$ non è in relazione con $(4,0)$ dato che $[1+0]_5 \neq [4+0]_5$.

(b) Risolvere l'equazione $([2]_3, [3]_5) \cdot (x,y) = ([1]_3, [2]_5)$ equivale a cercare $x \in \mathbb{Z}_3$, $y \in \mathbb{Z}_5$ tali che $[2]_3 \cdot x = [1]_3$ e $[3]_5 \cdot y = [2]_3$. Dato che $\mathbb{Z}_3$ e $\mathbb{Z}_5$ sono campi, tutti gli elementi non nulli sono invertibili rispetto alla moltiplicazione quindi si ha:

$$x = [2]_3^{-1} \cdot [1]_3 = [2]_3 \cdot [1]_3 = [2]_3, \quad y = [3]_5^{-1} \cdot [2]_5 = [2]_5 \cdot [2]_5 = [4]_5.$$

(c) Verifichiamo che $f$ è un omomorfismo di anelli. Infatti

$$f((a,b)\cdot(c,d)) = f(ac, bd) = ([ac]_3, [bd]_5) = ([a]_3, [b]_5) \cdot ([c]_3, [d]_5) = f(a,b) \cdot f(c,d)$$

$$f((a,b)+(c,d)) = f(a+c, b+d) = ([a+c]_3, [b+d]_5) = ([a]_3+[c]_3, [b]_5+[d]_5) = ([a]_3, [b]_5)+([c]_3, [d]_5) = f(a,b)+f(c,d).$$

(d) La formula si traduce nel seguente modo: se $x = ([x_1]_3, [x_2]_5) \neq ([0]_3, [0]_5)$ (che è zero dell'anello $(\mathbb{Z}_3 \times \mathbb{Z}_5, +, \cdot)$) ed esiste un $y = ([a]_3, [b]_5) \neq ([0]_3, [0]_5)$ tale che $([x_1]_3, [x_2]_5) \cdot ([a]_3, [b]_5) = ([0]_3, [0]_5)$, allora $x$ non è invertibile, cioè non esiste $z = ([z_1]_3, [z_2]_5)$ tale che $([z_1]_3, [z_2]_5) \cdot ([x_1]_3, [x_2]_5) = ([1]_3, [1]_5)$. Ricapitolando, la formula ci dice che se $x$ è un divisore dello zero allora non è invertibile e pertanto la formula assegnata è vera in questa interpretazione in quanto è noto dalla teoria che in un anello finito i divisori dello zero sono tutti e soli gli elementi non invertibili.
Osserviamo che questa formula è vera per un qualunque anello anche non finito infatti se $x$ fosse invertibile e divisore dello zero allora esisterebbe $y$ diverso dallo zero tale che $xy = 0$ e $x^{-1}x = 1$, quindi moltiplicando primo e secondo membro dell'equazione $xy = 0$ a sinistra per $x^{-1}$ avremmo $(x^{-1}x)y = 0$ e quindi si arriverebbe all'assurdo $y = 0$. Nel nostro caso particolare potevamo anche dedurre che se $y = ([a]_3, [b]_5) \neq ([0]_3, [0]_5)$ allora almeno una componente è diversa dalla classe nulla, per esempio $[a]_3 \neq [0]_3$, quindi se $x = ([x_1]_3, [x_2]_5)$ fosse invertibile e divisore dello zero, allora avremmo che esisterebbe $[z_1]_3$ tale che $[z_1]_3 \cdot [x_1]_3 = [1]_3$ e $[x_1]_3 \cdot [a]_3 = [0]_3$. Anche qui, con lo stesso accorgimento di moltiplicare primo e secondo membro della precedente equazione a sinistra per $[z_1]_3$, arriveremmo all'assurdo $[a]_3 = [0]_3$.
La formula non è logicamente contraddittoria poichè è vera nella precedente interpretazione. Non è neppure logicamente valida poichè ad esempio non è vera nell'interpretazione avente come dominio l'insieme dei numeri interi e nella quale $a$ è interpretata da 0, $b$ è interpretata da 1, $p(x,y)$ è interpretato dall'operazione di moltiplicazione fra interi mentre $E(x,y)$ interpreta la relazione $\geq$. In tal caso infatti l'antecedente è soddisfatto se ad $x$ assegniamo un valore negativo, ad esempio -1 (esiste sempre un $y$ negativo che moltiplicato per $x$ ci dà un valore positivo), ma non è vero che $x \cdot y$ è sempre minore di 1 (ad esempio basta porre $y = -10$). Pertanto l'intera formula è falsa in questa interpretazione poichè è chiusura universale di un formula non vera.

3. (Punteggio: a) 4, b) 5 )

(a) Si mostri che nella teoria L è possibile dedurre la formula $(C \Rightarrow B) \Rightarrow (C \Rightarrow \neg A)$ dalla formula $A \Rightarrow \neg B$;

(b) Mostrare usando il metodo della risoluzione del primo ordine che la seguente formula:

$$\mathcal{F} = \exists x \exists y \neg\, (\, A(f(x), f(y)) \Rightarrow A(x, y)\,) \Rightarrow \forall x \exists y A(f(x), y)$$

non è logicamente valida.

**Soluzione:**

(a) Dobbiamo mostrare che $A \Rightarrow \neg B \vdash_L (C \Rightarrow B) \Rightarrow (C \Rightarrow \neg A)$. Dal teorema di correttezza e completezza forte, questo è equivalente a richiedere che $A \Rightarrow \neg B \models (C \Rightarrow B) \Rightarrow (C \Rightarrow \neg A)$. I modelli $v$ di $A \Rightarrow \neg B$ sono quelli tali che $v(A) = 0$ e che assegnano a $B$ e $C$ valori arbitrari oppure quelli tali che $v(A) = 1, v(B) = 0$ e che assegnano a $C$ valore arbitrario. D'altro canto $(C \Rightarrow B) \Rightarrow (C \Rightarrow \neg A)$ è falsa quando $(C \Rightarrow B)$ è vera e $(C \Rightarrow \neg A)$ è falsa. Poichè $(C \Rightarrow \neg A)$ è falsa solo quando $C$ ed $A$ assumono valore 1, affinchè $(C \Rightarrow B)$ risulti vera è necessario che $B$ assuma valore 1. Segue che i modelli $w$ di $(C \Rightarrow B) \Rightarrow (C \Rightarrow \neg A)$ sono tutti quelli diversi dall'interpretazione $v$ tale che $v(A) = v(B) = v(C) = 1$ e quindi tutti i modelli di $A \Rightarrow \neg B$ sono modelli anche per $(C \Rightarrow B) \Rightarrow (C \Rightarrow \neg A)$ che pertanto risulta essere conseguenza semantica di $A \Rightarrow \neg B$.

(b) Dobbiamo verificare che non vale $\models \mathcal{F}$. Dal teorema di correttezza e completezza per refutazione, questo equivale a mostrare che dall'insieme di clausole di $\neg\mathcal{F}$ non si può ricavare la clausola vuota. Portiamo la formula $\neg\mathcal{F}$ in FNP:

$$\begin{aligned}
\neg\mathcal{F} =& \neg\, (\exists x \exists y \neg\, (\, A(f(x), f(y)) \Rightarrow A(x, y)\,) \Rightarrow (\forall x \exists y A(f(x), y))) = \\
& \neg\, (\forall x \forall y (\neg\, (\, A(f(x), f(y)) \Rightarrow A(x, y)) \Rightarrow (\forall x \exists y A(f(x), y))\,)) = \\
& \neg\, (\forall x \forall y \forall t \exists w (\neg\, (\, A(f(x), f(y)) \Rightarrow A(x, y)) \Rightarrow A(f(t), w)\,)) = \\
& \exists x \exists y \exists t \forall w \neg\, (\neg A(f(x), f(y)) \vee A(x, y) \vee A(f(t), w)\,) = \\
& \exists x \exists y \exists t \forall w\, (A(f(x), f(y)) \wedge \neg A(x, y) \wedge \neg A(f(t), w)\,)\,.
\end{aligned}$$

Ora portiamola in forma di Skolem introducendo le nuove costanti $a, b, c$:

$$\forall w\, (A(f(a), f(b)) \wedge \neg A(a, b) \wedge \neg A(f(c), w)\,)$$

da cui otteniamo le clausole: $\{A(f(a), f(b))\}, \{\neg A(a, b)\}, \{\neg A(f(c), w)\}$. Ora, dato che $A(f(a), f(b))$ non può essere unificato né con $A(a, b)$ né con $A(f(c), w)$, è evidente che non si possono ottenere altre clausole per risolvente, e quindi nemmeno la clausola vuota.