Durata della prova: 1h 30'

Esame di Logica e Algebra, 6 febbraio 2023 **Politecnico di Milano – Ingegneria Informatica –**			
Punti prec. lab.	**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)2, (c)2, (d)3, (e)3)
   Si consideri l'anello $(\mathbb{Z}_6, +, \cdot)$ della classi di resto modulo 6 e la relazione binaria R su $\mathbb{Z}_6$ definita nel seguente modo:

$$\forall [x]_6, [y]_6 \in \mathbb{Z}_6 \qquad ([x]_6, [y]_6) \in R \text{ se e solo se } [x]_6 \cdot [y]_6 = [4]_6 \vee [x]_6 + [y]_6 = [0]_6$$

   (a) Si disegni il grafo d'adiacenza di R e si stabilisca quali proprietà soddisfa R.

   (b) Si determini la chiusura di equivalenza T di R e si descriva l'insieme quoziente $\mathbb{Z}_6/T$.

   (c) Si stabilisca, motivando la risposta, se esiste la chiusura d'ordine S di R e, in caso affermativo, la si determini.

   (d) Si determinino i valori di a, con $a \in \{0, 1, 2, 3, 4, 5\}$, per i quali l'equazione congruenziale $[a]_6 \cdot [x]_6 + [2]_6 = [3]_6$ ammette soluzione.

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

$$\forall x \forall y (E(f(g(y, x), a), b) \Rightarrow \exists z (\neg E(z, x) \wedge E(f(g(y, z), a), b)))$$

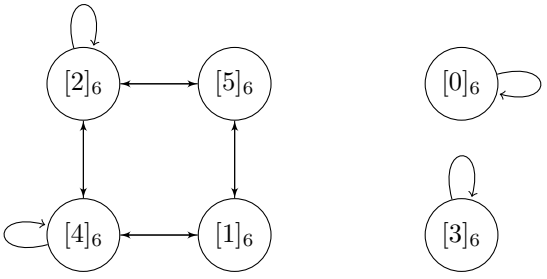
   e si stabilisca se è vera, falsa oppure soddisfacibile ma non vera nell'interpretazione avente come dominio $\mathbb{Z}_6$, in cui la lettera predicativa E interpreta la relazione di uguaglianza, le lettere funzionali f e g interpretano rispettivamente l'operazione di addizione e di moltiplicazione, le costanti a, b interpretano gli elementi $[2]_6$, $[3]_6$ di $\mathbb{Z}_6$.

   Soluzioni:

   (a) Da un esplicito calcolo otteniamo che

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

   e quindi il grafo d'adiacenza di R è il seguente



   La relazione gode solo delle proprietà simmetrica (ogni arco ha la doppia freccia) e seriale (da ogni vertice parte almeno un arco).

   (b) La chiusura d'equivalenza T di R è la chiusura riflessiva, simmetrica e transitiva di R e quindi segue che

$$T = (\{[1]_6, [2]_6, [4]_6, [5]_6\} \times \{[1]_6, [2]_6, [4]_6, [5]_6\}) \cup \{([3]_6, [3]_6), ([0]_6, [0]_6)\}.$$

   Pertanto l'insieme quoziente è $\mathbb{Z}_6/T = \{[[1]_6]_T, [[3]_6]_T, [[0]_6]_T\}$, dove $[[1]_6]_T = \{[1]_6, [2]_6, [4]_6, [5]_6\}$, $[[3]_6]_T = \{[3]_6\}$, $[[0]_6]_T = \{[0]_6\}$.

   (c) Non può esistere la chiusura d'ordine di R essendo R non antisimmetrica, infatti ogni relazione H che contiene R contiene anche le coppie $([1]_6, [5]_6), ([5]_6, [1]_6)$, quindi non potrà mai essere antisimmetrica.

   (d) L'equazione congruenziale è equivalente a $[a]_6 \cdot [x]_6 = [1]_6$ quindi è soddisfatta dagli elementi invertibili in $\mathbb{Z}_6$. Sappiamo che gli elementi invertibili sono solo quelli primi con $n = 6$, quindi l'equazione avrà soluzione solo per $a \in \{1, 5\}$.

(e) La formula data si può interpretare nel seguente modo: "per ogni $x, y \in \mathbb{Z}_6$, se l'equazione $yx + [2]_6 = [3]_6$ ha soluzione, allora esiste un elemento $z \in \mathbb{Z}_6$ tale che $z \neq x$ e z soddisfa l'equazione $yz + [2]_6 = [3]_6$". Osserviamo che, essendo la formula chiusa, essa è o vera o falsa, non può essere soddisfacibile ma non vera. La precedente affermazione può anche essere riformulata come segue: "per ogni $x, y \in \mathbb{Z}_6$, se l'equazione $yx = [1]_6$ ha soluzione, allora esiste uno $z \in \mathbb{Z}_6$ tale che $z \neq x$ che soddisfa $yz = [1]_6$". Questa affermazione è falsa, infatti, per ogni $y \in \mathbb{Z}_6$, se l'equazione $yx = [1]_6$ ha soluzione, allora x deve essere uguale all'inverso moltiplicativo di y che sappiamo essere unico quindi non può esistere un altro z diverso da x che sia inverso di y. Pertanto la formula assegnata è falsa in questa interpretazione.

2. (Punteggio: (a)3, (b)4, (c)2)

(a) Si provi che nella teoria L si ha
$$\neg(A \Rightarrow C) \vdash_L (A \Rightarrow B) \Rightarrow \neg(B \Rightarrow C)$$

(b) Si mostri lo stesso risultato utilizzando la teoria della risoluzione.

(c) Tenendo presente il risultato del punto a) si mostri che la f.b.f. della logica del primo ordine
$$\neg(A(x,y) \Rightarrow C(x)) \Rightarrow ((A(x,y) \Rightarrow \forall y A(y,x)) \Rightarrow \neg(\forall y A(y,x) \Rightarrow C(x)))$$
è logicamente valida.

Soluzione:

(a) Dal teorema di correttezza e completezza (forte) per la teoria L abbiamo che
$$\neg(A \Rightarrow C) \vdash_L (A \Rightarrow B) \Rightarrow \neg(B \Rightarrow C) \text{ sse } \neg(A \Rightarrow C) \vDash (A \Rightarrow B) \Rightarrow \neg(B \Rightarrow C)$$
quindi dobbiamo verificare che ogni modello di $\neg(A \Rightarrow C)$ lo è anche di $(A \Rightarrow B) \Rightarrow \neg(B \Rightarrow C)$. I modelli di $\neg(A \Rightarrow C)$ sono chiaramente le interpretazioni v tali che $v(A) = 1, v(C) = 0$ e $v(B) \in \{0,1\}$. E' facile verificare tramite la tavola di verità che tali modelli di $\neg(A \Rightarrow C)$ sono anche modelli di $(A \Rightarrow B) \Rightarrow \neg(B \Rightarrow C)$.

(b) Per usare la risoluzione, richiamiamo prima il risultato che lega l'insoddisfacibilità di un insieme di f.b.f. alla conseguenza semantica:

$\neg(A \Rightarrow C) \vDash (A \Rightarrow B) \Rightarrow \neg(B \Rightarrow C)$ sse $\Gamma = \{(A \Rightarrow C), \neg((A \Rightarrow B) \Rightarrow \neg(B \Rightarrow C))\}$ è un insieme insoddisfacibile

Dato che $\neg((A \Rightarrow B) \Rightarrow \neg(B \Rightarrow C)) \equiv \neg((\neg A \vee B) \Rightarrow (B \wedge \neg C)) \equiv (\neg A \vee B) \wedge (\neg B \vee C)$, otteniamo l'insieme di clausole $\{\{\neg A, B\}, \{\neg B, C\}\}$ che con l'insieme di clausole di $\neg(A \Rightarrow C)$, genera $\Gamma^c = \{\{A\}, \{\neg C\}, \{\neg A, B\}, \{\neg B, C\}\}$. Dal teorema di correttezza e completezza per refutazione sappiamo che Γ è un insieme di formule insoddisfacibile se e solo se $\Gamma^c \vdash_R \square$. La clausola $\{\neg B\}$ si ottiene come risolvente di $\{\neg C\}$ e $\{\neg B, C\}$, la clausola $\{B\}$ si ottiene come risolvente di $\{A\}$ e $\{\neg A, B\}$, infine la clausola vuota si ottiene come risolvente di $\{\neg B\}$ e di $\{B\}$.

(c) Dal primo punto sappiamo che $\neg(A \Rightarrow C) \vDash (A \Rightarrow B) \Rightarrow \neg(B \Rightarrow C)$, quindi dal teorema di deduzione semantica otteniamo che
$$\vDash \neg(A \Rightarrow C) \Rightarrow ((A \Rightarrow B) \Rightarrow \neg(B \Rightarrow C))$$
cioè $\neg(A \Rightarrow C) \Rightarrow ((A \Rightarrow B) \Rightarrow \neg(B \Rightarrow C))$ è una tautologia. Si osservi che la formula data nell'esercizio è un esempio di tautologia, infatti prendendo la precedente tautologia e facendo le sostituzioni $A \to A(x,y)$, $C \to C(x)$, $B \to \forall y A(y,x)$ otteniamo la formula data. Essendo quindi un esempio di tautologia, la formula assegnata è logicamente valida.

3. (Punteggio: (a)4, (b)3, (c)2)
Si consideri l'insieme A delle matrici quadrate di ordine 2 ad elementi in $\mathbb{Z}_7$ strutturato ad anello rispetto alle usuali operazioni di somma e prodotto di matrici.

(a) Si consideri il suo sottoinsieme B così definito

$$B = \left\{ \begin{pmatrix} a & [0]_7 \\ b & a \end{pmatrix} \mid \quad a, b \in \mathbb{Z}_7 \right\}$$

e si mostri che è un anello rispetto alle stesse operazioni definite in A.

(b) Si determinino i divisori dello zero di B.

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

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

e si dica se è vera, falsa, soddisfacibile ma non vera nell'interpretazione che ha come dominio l'insieme B e nella quale la lettera predicativa $E(x, y)$ è da interpretare come l'uguaglianza, la lettera funzionale $f(x, y)$ come il prodotto di matrici e le costanti a e b rispettivamente come la matrice nulla e la matrice:

$$\begin{pmatrix} [0]_7 & [0]_7 \\ [1]_7 & [0]_7 \end{pmatrix}$$

Soluzioni:

(a) Usiamo il criterio dei sottoanelli (visto che nel testo è specificato che l'insieme A è un anello). Prese due generiche matrici

$$\alpha = \begin{pmatrix} a & [0]_7 \\ b & a \end{pmatrix}, \beta = \begin{pmatrix} c & [0]_7 \\ d & c \end{pmatrix} \in B$$

mostriamo che $\alpha\beta \in B$ e $\alpha - \beta \in B$. Risulta che:

$$\begin{pmatrix} a & [0]_7 \\ b & a \end{pmatrix} \begin{pmatrix} c & [0]_7 \\ d & c \end{pmatrix} = \begin{pmatrix} ca & [0]_7 \\ cb + ad & ca \end{pmatrix} \in B, \quad \begin{pmatrix} a & [0]_7 \\ b & a \end{pmatrix} - \begin{pmatrix} c & [0]_7 \\ d & c \end{pmatrix} = \begin{pmatrix} a - c & [0]_7 \\ b - d & a - c \end{pmatrix} \in B$$

dato che $ca, cb + ad, a - c, b - d \in \mathbb{Z}_7$, gli elementi sulla diagonale principale sono uguali e l'elemento di posto (1,2) è nullo. Pertanto B è un sottoanello di A e segue che è esso stesso un anello.

(b) Ricordiamo che un divisore dello zero di un anello A è un elemento $a \in A$ diverso dallo zero per il quale esiste un elemento $b \in A$, anch'esso diverso da zero, tale che $ab = 0$. Per determinare i divisori dello zero impostiamo la seguente equazione:

$$\begin{pmatrix} a & [0]_7 \\ b & a \end{pmatrix} \begin{pmatrix} c & [0]_7 \\ d & c \end{pmatrix} = \begin{pmatrix} [0]_7 & [0]_7 \\ [0]_7 & [0]_7 \end{pmatrix}$$

con almeno uno tra a, b diverso da $[0]_7$ e almeno uno tra c, d diverso da $[0]_7$. Quest'ultima equazione è equivalente al sistema $ca = [0]_7, cb + ad = [0]_7$. Dato che $\mathbb{Z}_7$ è un campo la prima equazione è soddisfatta se uno tra a e c è uguale a zero. Consideriamo i due casi:

- Se $a = [0]_7$, allora dalla seconda equazione deduciamo che c o b sono uguali a zero. Ma dato che b deve essere diverso da zero, necessariamente $c = [0]_7$. In questo caso i divisori dello zero sono della forma:

$$\begin{pmatrix} [0]_7 & [0]_7 \\ b & [0]_7 \end{pmatrix} \begin{pmatrix} [0]_7 & [0]_7 \\ d & [0]_7 \end{pmatrix} = \begin{pmatrix} [0]_7 & [0]_7 \\ [0]_7 & [0]_7 \end{pmatrix}$$

con $b, d \neq [0]_7$.
- Nel caso $c = [0]_7$, la seconda equazione è soddisfatta se almeno uno tra a o d è uguale a zero, quindi necessariamente $a = [0]_7$ (ricordando che almeno uno tra c, d dev'essere diverso da $[0]_7$). Pertanto anche in questo caso i divisori dello zero sono della forma determinata nel caso precedente.

(c) La formula dell'esercizio si traduce con "per ogni $x \in B$, se esiste un $y \in B$ diverso dalla matrice nulla tale che xy è la matrice nulla, allora esiste una matrice $y \in B$ tale che xy mi dia la matrice $\begin{pmatrix} [0]_7 & [0]_7 \\ [1]_7 & [0]_7 \end{pmatrix}$". Prendendo x uguale alla matrice nulla, vediamo subito che l'antecedente è soddisfatto mentre non esisterà nessuna matrice y tale che

$$xy = \begin{pmatrix} [0]_7 & [0]_7 \\ [1]_7 & [0]_7 \end{pmatrix}$$

dato che xy è la matrice nulla per tutte le possibili matrici $y \in B$. Segue che questa formula è falsa poiché è la chiusura universale di una formula non vera.