ALGEBRA E LOGICA MATEMATICA
5/2/2008
PARTE DI ALGEBRA

Esercizio 1

Sia $f : A \to B$ un'applicazione.

- Sia ρ una relazione di equivalenza su B, provare che la relazione σ definita su A ponendo $(a_1,a_2)\in \sigma$ se e solo se $(f(a_1),f(a_2))\in \rho$ è una relazione di equivalenza su A
- Nel caso particolare in cui A=R, B=Z, f associa ad ogni numero reale la sua parte intera e ρ è la relazione di congruenza modulo 4, descrivere la classe di equivalenza di ½ rispetto a σ.
- Data una relazione di equivalenza τ su A la relazione κ definita su B ponendo $(b_1,b_2)\in \kappa$ se e solo se esistono $a_1,a_2 \in A$ tali che $f(a_1)=b_1, f(a_2)=b_2$ e $(a_1,a_2)\in \tau$ è une relazione di equivalenza su B? Sempre o talvolta?

Esercizio 2

Sia $\langle Z_{15},+,\cdot\rangle$ l'anello delle classi di resti modulo 15. Sia U il sottoinsieme di Z_{15} costituito dalle classi che ammettono inverso rispetto al prodotto e verificare che U è un gruppo rispetto all'usuale prodotto $\cdot$ di Z_{15}, e che l'insieme $H=\{[1]_{15},[2]_{15},[4]_{15},[8]_{15}\}$ forma un sottogruppo normale di U.
Dimostrare che l'applicazione $f: \langle U,\cdot\rangle \to \langle Z_2,+\rangle$ definito ponendo $f(h)=[0]_2$ per ogni $h\in H$ e $f(k)=[1]_2$ per ogni elemento k di U che non sta in H è un omomorfismo di gruppi.
($[a]_{15}$ e $[a]_2$ denotano rispettivamente le classi di resti di a modulo 15 e modulo 2.)

TRACCIA DI SOLUZIONE.

Esercizio 1

Proviamo che σ gode delle proprietà:

- riflessiva : infatti $(a,a)\in\sigma$ in quanto essendo ρ riflessiva $(f(a),f(a))\in\rho$,
- simmetrica: sia $(a_1,a_2)\in\sigma$, allora $(f(a_1),f(a_2))\in\rho$ e per la simmetria di ρ $(f(a_e),f(a_1))\in\rho$ da cui $(a_2,a_1)\in\sigma$,
- transitiva: sia $(a_1,a_2)\in\sigma$ e $(a_2,a_3)\in\sigma$, allora $(f(a_1),f(a_2))\in\rho$ e $(f(a_2),f(a_3))\in\rho$ e per la transitività di ρ, $(f(a_1),f(a_3))\in\rho$ da cui $(a_1,a_3)\in\sigma$,

dunque ρ è una relazione di equivalenza su A.
Nel caso particolare in cui A=R, B=Z, $f:R\rightarrow Z$ associ ad ogni numero reale la sua parte intera e ρ sia la relazione di congruenza modulo 4, sia x un elemento della σ-classe di ½, questo implica che $f(x)\equiv f(1/2) \pmod 4$ ovvero $f(x)\equiv 0 \pmod 4$ ovvero $x=4h+r_1$ ove h è intero e r_1 è un numero reale con $0\leq r_1<1$, viceversa se $x=4h+r_1$ si ha $f(x)=4h\equiv 0=f(1/2) \pmod 4$, dunque la della σ-classe di ½ è $\{4h+r_1 \mid h\in Z, r_1\in R, 0\leq r_1<1\}$.
Se f non è suriettiva la relazione κ non è riflessiva, infatti non esiste alcun elemento associato da κ ad un $b\in B\backslash f(A)$. Se invece f è suriettiva la κ gode della proprietà riflessiva in quanto per ogni $b\in B=f(A)$ esiste un $a\in A$ tale che $f(a)=b$ e $(a,a)\in\tau$.
Inoltre κ è sempre simmetrica in quanto se $(b_1,b_2)\in\kappa$ esistono $a_1,a_2\in A$ tali che $f(a_1)=b_1$, $f(a_2)= b_2$ e $(a_1,a_2)\in\tau$ ma allora per la simmetria di τ si ha anche $(a_2,a_1)\in\tau$.
Supponiamo ora che sia $(b_1,b_2)\in\kappa$ e $(b_2,b_3)\in\kappa$, la prima dice che esistono $a_1,a_2\in A$ tali che $f(a_1)= b_1$, $f(a_2)= b_2$ e $(a_1,a_2)\in\tau$, dalla seconda abbiamo che esistono $a'_2,a_3\in A$ tali che $f(a'_2)= b2_1$, $f(a_3)= b_3$ e $(a'_2,a_3)\in\tau$ e dunque solo se f è iniettiva e quindi $a_2=a_2$ possiamo dedurre $(a_1,a_3)\in\tau$ e quindi $(b_1,b_3)\in\kappa$. La κ dunque non è in generale una relazione di equivalenza ma lo è nel caso f sia una relazione biunivoca.

Esercizio 2.

Gli elementi invertibili di Z_{15} sono le classi che hanno un rappresentante primo con 15 e dunque $U=\{[1]_{15},[2]_{15},[4]_{15},[7]_{15},[8]_{15},[11]_{15},[13]_{15},[14]_{15}\}$. U è un gruppo in quanto il prodotto di due elementi invertibili è sempre un elemento invertibile e le altre proprietà di gruppo sono ovviamente soddisfatte.
H è il sottogruppo ciclico di U generato da $[2]_{15}$ (ovvero è formato da tutte e sole le potenze di $[2]_{15}$, è quindi è chiuso rispetto al prodotto e questo baste essendo un sottoinsieme finito a garantire che è sottogruppo). U è un gruppo abeliano e quindi ogni suo sottogruppo, in particolare H è normale.
La f è un'applicazione da U a Z_2, bisogna quindi far vedere che conserva le operazioni ovvero che presi comunque $[x]_{15},[y]_{15}\in U$, $f([x]_{15}[y]_{15})= f([x]_{15})+f([y]_{15})$.
Se $[x]_{15},[y]_{15}\in H$ si ha ovviamente $[x]_{15}[y]_{15}\in H$ e dunque $f([x]_{15}[y]_{15})= [0]_2 = f([x]_{15})+f([y]_{15})$.
Dalla tavola di moltiplicazione di U si vede subito che se $[x]_{15},[y]_{15}\in U\backslash H$ si ha $[x]_{15}[y]_{15}\in H$ e dunque $f([x]_{15}[y]_{15})= [0]_2 = [1]_2 +[1]_2 = f([x]_{15})+f([y]_{15})$ e si vede anche che se $[x]_{15}\in H$ ed $[y]_{15}\in U\backslash H$ si ha $[x]_{15}[y]_{15}\in U\backslash H$ e dunque $f([x]_{15}[y]_{15})= [1]_2 = [0]_2 +[1]_2 = f([x]_{15})+f([y]_{15})$. Dunque la f è un omomorfismo. Il tutto poteva essere

svolto molto più rapidamente osservando che il gruppo quoziente U/H è un gruppo di ordine 2 , che c'è un omomorfismo naturale π_H da U ad U/H ed U/H è isomorfo a Z_2 mediante un isomorfismo φ che manda H in $[0]_2$ e $U \backslash H$ in $[1]_2$. E' immediato che $f=\pi_H \circ \varphi$ e dunque è un omomorfismo di U su Z_2.

ALGEBRA E LOGICA MATEMATICA
5/2/2008
PARTE DI LOGICA

Esercizio 1

Verificare che l'insieme di f.b.f. $\{\sim A, \sim A \Rightarrow (B \vee C), B \Rightarrow (A \vee C)\}$ è soddisfacibile. Trovare una formula di logica proposizionale $f(A,B,C)$ che non sia una contraddizione, non sia A e tale che l'insieme di f.b.f. $\{\sim A, \sim A \Rightarrow (B \vee C), B \Rightarrow (A \vee C), f(A,B,C)\}$ sia insoddisfacibile. La formula A è una conseguenza semantica di $\{\sim A \Rightarrow (B \vee C), B \Rightarrow (A \vee C), f(A,B,C)\}$? Verificare il risultato trovato tramite la risoluzione.

Esercizio 2

Si consideri la f.b.f.
$\mathcal{A}_1^2(x,y) \Rightarrow \sim \forall z\, \mathcal{A}_1^2(f_1^2(x,z), f_1^2(y,z))$.
Trovare una interpretazione in cui la formula sia vera ed una in cui sia soddisfacibile ma non vera.
Determinare la forma di Skolem della sua chiusura universale e dire se la formula così trovata è soddisfacibile (ovvero se esiste una interpretazione in cui è vera).
Discutere la verità della formula $\forall z\, \mathcal{A}_1^2(f_1^2(x,z), f_1^2(y,z)) \Rightarrow \sim \mathcal{A}_1^2(x,y)$.

TRACCIA DI SOLUZIONE.

Esercizio 1

Per verificare che l'insieme di f.b.f. $\{\sim A, \sim A \Rightarrow (B \vee C), B \Rightarrow (A \vee C)\}$ è soddisfacibile basta trovare modello per l'insieme cioè un assegnamento di valori di verità delle lettere enunciative che occorrono nelle formule che renda vere tutte e tre le formule dell'insieme. Ovviamente affinché sia $v(\sim A)=1$ deve essere $v(A)=1$ e quindi $v(B \vee C)=1$, per cui $v(B)=1$ o $v(C)=1$, inoltre se $v(B)=1$ allora affinché $v(B \Rightarrow (A \vee C))=1$ deve essere $v(A \vee C)=1$ e quindi $v(C)=1$. Ci sono quindi due modelli per il nostro insieme:

1) $v(A)=0$, $v(B)=0$, $v(C)=1$
2) $v(A)=0$, $v(B)=1$, $v(C)=1$.

Una formula $f(A,B,C)$ che non sia una contraddizione né A e tale che $\{\sim A, \sim A \Rightarrow (B \vee C), B \Rightarrow (A \vee C), f(A,B,C)\}$ sia insoddisfacibile è ad esempio $\sim(\sim A \Rightarrow (B \vee C)) \equiv \sim A \wedge \sim B \wedge \sim C$, tale formula è infatti la negazione di una formula dell'insieme e non può esistere alcun assegnamento che soddisfi insieme $f(A,B,C)$ e $\sim A \Rightarrow (B \vee C)$ e non è una contraddizione perché ha il modello $v(A)=v(B)=v(C)=0$.
La formula A è conseguenza semantica di $\{\sim A \Rightarrow (B \vee C), B \Rightarrow (A \vee C), f(A,B,C)\}$, infatti sappiamo che dato un insieme Γ di f.b.f. una f.b.f. $\mathcal{B}$ è conseguenza semantica di Γ se e solo se $\Gamma \cup \{\sim \mathcal{B}\}$ è insoddisfacibile , dunque dal fatto che $\{\sim A, \sim A \Rightarrow (B \vee C), B \Rightarrow (A \vee C), f(A,B,C)\} = \{\sim A \Rightarrow (B \vee C), B \Rightarrow (A \vee C), f(A,B,C)\} \cup \{\sim A\}$ sia insoddisfacibile segue che $\sim\sim A \equiv A$ è conseguenza semantica di $\{\sim A \Rightarrow (B \vee C), B \Rightarrow (A \vee C), f(A,B,C)\}$.
Per ritrovare questo risultato tramite la risoluzione , visto che come sappiamo la risoluzione è corretta e completa per reputazione dobbiamo provare che l'insieme $\{\sim A \Rightarrow (B \vee C), B \Rightarrow (A \vee C), f(A,B,C)\} \cup \{\sim A\}$ è insoddisfacibile ovvero che dall?insieme delle formule precedenti scritte in forma a clausole possiamo ricavare la clausola vuota .
La formula $\sim A \Rightarrow (B \vee C)$ in forma a clausole si riduce all'unica clausola $\{A,B,C\}$, la formula $B \Rightarrow (A \vee C)$ in forma a clausole si riduce all'unica clausola $\{A, \sim B, C\}$, la formula $f(A,B,C)$ che abbiamo scelto essere $\sim A \wedge \sim B \wedge \sim C$ è l'insieme delle tre clausole $\{\sim A\}, \{\sim B\}, \{\sim C\}$ ed inoltre abbiamo la formula $\sim A$ che è a sua volta una sola clausola già presente nell'insieme. Abbiamo dunque l'insieme di clausole $\{\{A,B,C\}, \{A, \sim B, C\}, \{\sim A\}, \{\sim B\}, \{\sim C\}\}$, per risoluzione dalla prima e seconda clausola ricaviamo $\{A,C\}$, da questa e da $\{\sim A\}$ ricaviamo la clausola $\{C\}$ che con la clausola $\{\sim C\}$ dà la clausola vuota.

Esercizio 2

Una interpretazione in cui la formula $\mathcal{A}_1^2(x,y) \Rightarrow \sim \forall z\, \mathcal{A}_1^2(f_1^2(x,z), f_1^2(y,z))$ sia vera molto semplice è del seguente tipo: su un qualsiasi dominio D si prende come funzione f_1^2 una qualsiasi operazione binaria su D e come relazione $\mathcal{A}_1^2$ la relazione vuota, allora nessun assegnamento di valori alle variabili soddisfa $\mathcal{A}_1^2(x,y)$ e quindi l'antecedente della formula è falso e la formula è vera.
Un'altra interpretazione è la seguente: prendiamo come dominio Z come operazione f_1^2 l'usuale prodotto su Z e come predicato $\mathcal{A}_1^2(x,y)$ il predicato $x<y$. La formula

diventa allora : “se x è minore di y allora non per tutti gli z xz<yz”. Tale formula è soddisfatta da tutti gli assegnamenti s per cui s(x)>s(y) , se invece s(s)<s(y) qualsiasi sia il valore s(z) esiste un assegnamento s’ tale che s’(x)=s(x), s’(y)=s(y) con s’(z)=0 per cui non accade che (s’)*(xz)<(s’)*(yz) in quanto (s’)*(xz)=0=(s’)*(yz).
Una interpretazione in cui la formula è soddisfacibile ma non vera è ad esempio la seguente: prendiamo come dominio Z come operazione f_1^2 l’usuale somma su Z e come predicato $\mathcal{A}_1^2(x,y)$ il predicato x=y. La formula dice allora : “se x è uguale ad y allora non per tutti gli z x+z=y+z”, è ovviamente soddisfatta da tutti gli assegnamenti s per cui s(x)≠s(y), ma non è soddisfatta dagli assegnamenti s’ per cui s’(x)=s’(y), in quanto non esiste alcun assegnamento s” tale che s”(x)=s’(x)=s’(y)=s”(y) per cui (s”)*(x+z) non è uguale a (s”)*(y+z).
La chiusura universale della formula considerata è
$\forall x\forall y(\mathcal{A}_1^2(x,y) \Rightarrow \sim\forall z\, \mathcal{A}_1^2(f_1^2(x,z),f_1^2(y,z))$ la cui forma normale prenessa è
$\forall x\forall y\exists z(\mathcal{A}_1^2(x,y) \Rightarrow \sim\mathcal{A}_1^2(f_1^2(x,z),f_1^2(y,z))$. La forma di Skolem è allora
$\forall x\forall y\exists z(\mathcal{A}_1^2(x,y) \Rightarrow \sim\mathcal{A}_1^2(f_1^2(x, f_2^2(x,y)),f_1^2(y, f_2^2(x,y)))$.
Poiché esiste una interpretazione in cui la formula di partenza è vera, in tale interpretazione la chiusura universale della formula è vera è quindi a maggior ragione soddisfacibile e noi sappiamo che la forma di Skolem di una forma soddisfacibile è soddisfacibile, quindi a formula in forma di Skolem cha abbiamo scritto è soddisfacibile , ovvero esiste una interpretazione in cui è soddisfacibile (e quindi vera essendo una f.b.f. chiusa).
Ricordiamo che la formula $(A\Rightarrow B)\Leftrightarrow(\sim B\Rightarrow\sim A)$ è una tautologia nella logica proposizionale e dunque la f.b.f
$(\mathcal{A}_1^2(x,y) \Rightarrow\sim\forall z\, \mathcal{A}_1^2(f_1^2(x,z),f_1^2(y,z))) \Leftrightarrow(\forall z\, \mathcal{A}_1^2(f_1^2(x,z),f_1^2(y,z)) \Rightarrow \sim\mathcal{A}_1^2(x,y))$
ottenuta da questa sostituendo la lettera A con la f.b.f. $\mathcal{A}_1^2(x,y)$ e la lettera B con la f.b.f. $\sim\forall z\, \mathcal{A}_1^2(f_1^2(x,z),f_1^2(y,z))$, essendo un esempio di tautologia, è logicamente valida e dunque $\forall z\, \mathcal{A}_1^2(f_1^2(x,z),f_1^2(y,z)) \Rightarrow \sim\mathcal{A}_1^2(x,y)$ è una formula logicamente equivalente a $\mathcal{A}_1^2(x,y) \Rightarrow\sim\forall z\, \mathcal{A}_1^2(f_1^2(x,z),f_1^2(y,z))$ e quindi come quest’ultima è soddisfacibile, ma non logicamente valida.