ALGEBRA E LOGICA MATEMATICA
I prova in itinere
21 novembre 2005

Esercizio 1

Sia X={a,b,c,d,e} e sia R la relazione definita dalla matrice di incidenza

$$M=\begin{bmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

a) si costruisca la chiusura riflessiva e transitiva ρ di R e si verifichi che è una relazione d'ordine
b) si trovino gli elementi massimali e minimali di X rispetto a ρ e si dica se sono massimi e minimi
c) si stabilisca se X è un reticolo rispetto a ρ e in caso affermativo si dica se tale reticolo è distributivo e/o complimentato.
d) (Facoltativo) Si provi che se un insieme finito parzialmente ordinato, ammette massimo e minimo è un reticolo.

Esercizio 2

Si consideri l'insieme $Z \times Z$ strutturato ad anello rispetto alle seguenti operazioni

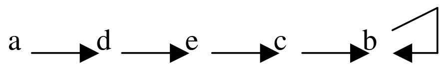
$$(a,b)+(c,d) = (a+c, b+d)$$
$$(a,b) \cdot (c,d) = (ac,bd)$$

a) Si verifichi se la relazione R così definita
$$(a,b)\ R\ (c,d) \iff a \equiv c \pmod 3 \text{ e } b \equiv d \pmod 5$$
è una congruenza sull'anello (Z x Z , + , ·).
b) In caso affermativo si determini la struttura quoziente $\frac{Z \times Z}{R}$ e, considerata la classe di equivalenza [(0,0)] a cui appartiene lo zero dell'anello, si mostri che è un ideale I.
c) Si consideri l'applicazione
$$f:\ Z \times Z \to Z_3 \times Z_5$$
tale che $f((a,b)) = ([a]_3, [b]_5)$, ove $[a]_n$ indica la classe di resti di a modulo n
e si mostri che è un omomorfismo di anelli.
d) Si determinino infine i divisori dello zero e gli elementi invertibili dell'anello $Z_3 \times Z_5$.
e) Si mostri che $\frac{Z \times Z}{I}$ è isomorfo a $Z_3 \times Z_5$.

TRACCIA DI SOLUZIONE

Esercizio 1.

a) Il grafo corrispondente ad R è il seguente:

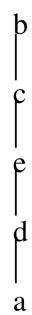


ed è quindi evidente che la matrice associata alla chiusura riflessiva e transitiva ρ di R è la seguente

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

che per costruzione è la matrice di incidenza di una relazione riflessiva e transitiva. Inoltre la relazione ρ è antisimmetrica perché per ogni coppia i,j tale che $a_{ij}= 1$ si ha $a_{ji}=0$.

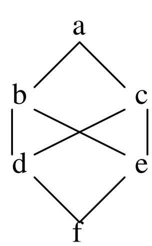
b) Dunque ρ è una relazione d'ordine e il diagramma di Hasse di X rispetto a ρ è il seguente



da cui risulta immediatamente che X è un insieme totalmente ordinato con a minimo e b massimo (come si poteva rilevare subito anche dalla matrice di incidenza), Ovviamente non ci sono altri massimali e minimali.

c) X con la relazione d'ordine ρ è un reticolo (perché ogni insieme totalmente ordinato lo è), è distributivo (non contiene sottoreticoli della forma proibita) non è complementato perché ad esempio c non ha complementi (o perché se fosse complementato sarebbe un'algebra di Boole e quindi non potrebbe avere ordine 5).

d) Esistono insiemi parzialmente ordinati finiti con massimo e minimo che non sono reticoli, ad esempio l'insieme il cui diagramma di Hasse è il seguente:



per cui non esiste sup{d,e}, ad esempio.

Esercizio 2

a) Per verificare che la relazione R è una relazione di congruenza su $Z\times Z$ dobbiamo prima di tutto verificare che è una relazione di equivalenza e poi che è compatibile con le operazioni di $Z\times Z$. Verifichiamo dunque che R è
   - riflessiva, cioè $((a,b),(a,b))\in R$: infatti $a\equiv a \pmod 3$ e $b\equiv b \pmod 5$
   - simmetrica, cioè $((a,b),(c,d))\in R$ implica $((c,d),(a,b))\in R$: infatti se è $((a,b),(c,d))\in R$ si ha $a\equiv c \pmod 3$ e $b\equiv d \pmod 5$ da cui per la simmetria delle congruenze modulo n si ricava $c\equiv a \pmod 3$ e $d\equiv b \pmod 5$, cioè $((c,d),(a,b))\in R$
   - transitiva, cioè $((a,b),(c,d))\in R$ e $((c,d),(e,f))\in R$ implicano $((a,b),(e,f))\in R$: infatti da $((a,b),(c,d))\in R$ si ha $a\equiv c \pmod 3$ e $b\equiv d \pmod 5$ e da $((c,d),(e,f))\in R$ si ha $c\equiv e \pmod 3$ e $d\equiv f \pmod 5$, ora per la transitività delle congruenze modulo n, da $a\equiv c \pmod 3$ e da $c\equiv e \pmod 3$ si ricava $a\equiv e \pmod 3$, da $b\equiv d \pmod 5$ e da $d\equiv f \pmod 5$ si ricava $b\equiv f \pmod 5$, cioè $((a,b),(e,f))\in R$
   - compatibile con la somma, cioè $((a,b),(c,d))\in R$ e $((e,f),(g,h))\in R$ implicano $((a+e,b+f),(c+g,d+h))\in R$: infatti da $((a,b),(c,d))\in R$ si ha $a\equiv c \pmod 3$ e $b\equiv d \pmod 5$ e da $((e,f),(g,h))\in R$ si ha $e\equiv g \pmod 3$ e $f\equiv h \pmod 5$, ora essendo le congruenze modulo n congruenza su $<Z,+,\cdot>$, da $a\equiv c \pmod 3$ e da $e\equiv g \pmod 3$ si ricava $a+e\equiv c+g \pmod 3$, da $b\equiv d \pmod 5$ e da $f\equiv h \pmod 5$ si ricava $b+f\equiv d+h \pmod 5$, cioè $((a+e,b+f),(c+g,d+h))\in R$
   - compatibile col prodotto, cioè $((a,b),(c,d))\in R$ e $((e,f),(g,h))\in R$ implicano $((a\cdot e,b\cdot f),(c\cdot g,d\cdot h))\in R$: infatti da $((a,b),(c,d))\in R$ si ha $a\equiv c \pmod 3$ e $b\equiv d \pmod 5$ e da $((e,f),(g,h))\in R$ si ha $e\equiv g \pmod 3$ e $f\equiv h \pmod 5$, ora essendo le congruenze modulo n congruenza su $<Z,+,\cdot>$, da $a\equiv c \pmod 3$ e da $e\equiv g \pmod 3$ si ricava $a\cdot e\equiv c\cdot g \pmod 3$, da $b\equiv d \pmod 5$ e da $f\equiv h \pmod 5$ si ricava $b\cdot f\equiv d\cdot h \pmod 5$, cioè $((a\cdot e,b\cdot f),(c\cdot g,d\cdot h))\in R$

b) Per determinare la struttura quoziente $Z\times Z/R$, dobbiamo descrivere le classi di equivalenza rispetto ad R e definire le operazioni tra le classi. Per definizione preso un elemento $(a,b)\in Z\times Z$, (n,m) appartiene alla R-classe di (a,b) se e solo se $((a,b),(n,m))\in R$ cioè se e solo se $a\equiv n \pmod 3$ e $b\equiv m \pmod 5$, dunque se e solo se $n\in [a]_3$ e $m\in [b]_5$. Dunque la R-classe $[(a,b)]$ di (a,b) è costituita dall'insieme $\{(n,m)\mid n\in [a]_3 \text{ e } m\in [b]_5\}=[a]_3\times[b]_5=\{(a+3h,b+3k)\mid h,k\in Z\}$. Le operazioni su tali classi sono le operazioni indotte per cui $[(a,b)]+ [(c,d)]= [(a+c,b+d)]$, $[(a,b)]\cdot[(c,d)]= [(a\cdot c,b\cdot d)]$. La R-classe $[(0,0)]$ è dunque l'insieme $I=\{(3h,5k)\mid h,k\in Z\}$. Dobbiamo verificare che I è un ideale (come sappiamo deve essere la R-classe dello zero di un anello quando R è una congruenza), per verificarlo dobbiamo provare che presi comunque $(3h_1,5k_1),(3h_2,5k_2)\in I$ e $(a,b)\in Z\times Z$ si ha $(3h_1,5k_1)-(3h_2,5k_2)\in I$ e $(a,b)\cdot(3h_1,5k_1)\in I$ (si può tralasciare la verifica che $(3h_1,5k_1)\cdot(a,b)\in I$ perché il prodotto è ovviamente commutativo), infatti è $(3h_1,5k_1)-(3h_2,5k_2)=(3h_1-3h_2,5k_1-5k_2)=(3(h_1-h_2),5(k_1-k_2))\in I$ e $(a,b)\cdot(3h_1,5k_1) =(a\cdot 3h_1,b\cdot 5k_1) =(3(ah_1), 5(bk_1))\in I$ essendo h_1-h_2, k_1-k_2, ah_1, $bk_1\in Z$.

c) La f è ovviamente una applicazione di $Z\times Z$ su $Z_3\times Z_5$ per verificare che è un omomorfismo basta verificare che conserva somma e prodotto:
   $f((a,b)+(c,d))=f((a+b,c+d))=([a+c]_3,[b+d]_5)=([a]_3+[c]_3,[b]_5+[d]_5)=([a]_3,[b]_5)+([c]_3,[d]_5) =f((a,b))+f((c,d))$
   $f((a,b)\cdot(c,d))=f((a\cdot b,c\cdot d))=([a\cdot c]_3,[b\cdot d]_5)=([a]_3\cdot [c]_3,[b]_5\cdot [d]_5)=([a]_3,[b]_5)\cdot([c]_3,[d]_5) =f((a,b)) \cdot f((c,d))$
   Dunque f è un omomorfismo.

d) Gli elementi della forma $([0]_3,[b]_5)$ e $([a]_3,[0]_5)$ con $a,b\neq 0$ sono divisori dello zero di $Z_3\times Z_5$, infatti $([0]_3,[b]_5)\cdot([a]_3,[0]_5)= ([0]_3,[0]_5)$, invece gli elementi delle forma $([a]_3,[b]_5)$ con $a,b\neq 0$ sono invertibili, infatti essendo 3,5 numeri primi sia $[a]_3$ sia $[b]_5$ ammettono inverso $[c]_3$, $[d]_5$

rispettivamente in Z_3 e in Z_5 , e dunque $([c]_3 , [d]_5)$ è l'inverso di $([a]_3 , [b]_5)$, essendo $([a]_3 , [b]_5) \cdot ([c]_3 , [d]_5)= ([a\cdot c]_3 , [b\cdot d]_5)= ([1]_3 , [1]_5)$

e) E' facile verificare che l'omomorfismo f del punto c) è una epimorfismo , infatti ogni coppia $([a]_3,[b]_5)$ ha almeno come controimmagine in f (a,b). Inoltre è immediato osservare che le controimmagini di $([0]_3,[0]_5)$ rispetto ad f sono esattamete gli elementi dell'ideale I, e che R è la congruenza su $Z\times Z$ indotta da I (oppure direttamente che ker f è la relazione R) dunque l'asserto segue immediatamente dal I teorema di fattorizzazione degli omomorfismi.