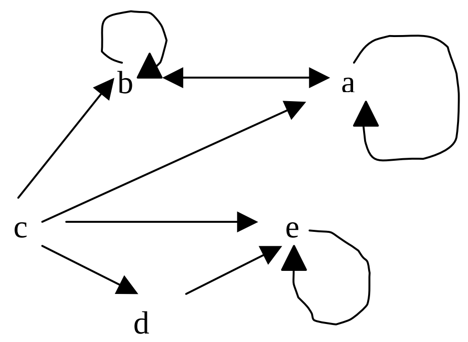
Algebra e logica matematica 1
Proff. Adami , Cherubini
I prova in itinere

1) Si considerino l'insieme X={a,b,c,d,e} e la relazione R su X rappresentata dal seguente grafo:



a) Dire di che proprietà gode R La chiusura riflessiva e simmetrica di R è una relazione di equivalenza su X? Qual è la relazione di equivalenza generata da R?
b) E' possibile trovare una relazione d'ordine su X contenente R? E' possibile trovare una funzione $f:X\rightarrow X$ contenuta in R? ed una funzione $f:X\rightarrow X$ contenuta in R e che ammetta inversa sinistra?
In caso di risposta affermativa ad una o più delle domande precedenti fornire un esempio di funzione che soddisfi le condizioni richieste.
c) Si consideri su X la relazione ρ così definita:

$(a,b)\in\rho$ se e solo se $\begin{cases} a = b, \quad \text{oppure} \\ (a,b)\in R \ \text{ e } \ (b,a)\in R \end{cases}$

Verificare che ρ è una relazione di equivalenza su X. Determinare l'insieme quoziente X/ ρ.
d) Verificare che la relazione T su X/ρ definita ponendo
$(\rho_a, \rho_b)\in T$ se e solo se $(a,b)\in R$ (ρ_a indica ovviamente la ρ-classe avente come rappresentante a) è antisimmetrica e transitiva.Verificare che la chiusura riflessiva di T è una relazione d'ordine su X/ρ e determinare se esistono elementi massimali, minimali, massimi e minimi di X/ρ rispetto a tale relazione . X/ρ è un reticolo rispetto a tale relazione?
Facoltativo: Nel punto d) non è richiesto di provare che la definizione di T è ben posta. Provarlo.

2) Dimostrare che nel gruppo moltiplicativo di Z_5 (classi di resti modulo 5) l'unica soluzione dell'equazione $x^3=\{1\}$ è la classe $\{1\}$.

3) Sia $<G,\cdot>$ un gruppo finito di ordine n e sia $h\in G$. Verificare che l'insieme $<h>$ delle potenze positive di h è un sottogruppo di $<G,\cdot>$. Provare poi che $h^n=e$ (dove e indica l'unità di $<G,\cdot>$) e che il minimo intero positivo r per cui $h^r=e$ è un divisore di n. Verificare che $<h>$ è un sottogruppo normale di $<G,\cdot>$ se e solo se se per ogni $g\in G$ esiste un intero positivo m tale che $h\cdot g=g\cdot h^m$.

TRACCIA DI SOLUZIONE

Esercizio 1)

a) La R è seriale in quanto da ogni vertice del suo grafo di incidenza esce un arco ed è transitiva come si verifica facilmente o attraverso la matrice di incidenza (in quanto il quadrato della matrice non aggiunge nuovi 1) o attraverso la considerazione delle coppie di archi tali che il primo abbia come vertice d'arrivo il vertice di partenza dell'altro.Tali coppie sono: (c,b), (b,a) in corrispondenza ai quali abbiamo l'arco (c,a); (c,b), (b,b) in corrispondenza ai quali abbiamo l'arco (c,b); (b,b), (b,a) in corrispondenza ai quali abbiamo l'arco (b,a); (b,a), (a,a) in corrispondenza ai quali abbiamo l'arco (b,a) ; (b,a), (a,b) in corrispondenza ai quali abbiamo l'arco (b,b); (a,b), (b,a) in corrispondenza ai quali abbiamo l'arco (a,a); (c,a), (a,a) in corrispondenza ai quali abbiamo l'arco (c,a) ; (c,d), (d,e) in corrispondenza ai quali abbiamo l'arco (c,e) ; (d,e), (e,e) in corrispondenza ai quali abbiamo l'arco (d,e); (c,e), (e,e) in corrispondenza ai quali abbiamo l'arco (c,e).
La chiusura riflessiva e simmetrica di R non è di equivalenza in quanto (a,c) e (c,e) appartengono a tale chiusura, mentre non ci appartiene (a,e). La relazione di equivalenza generata da R è la relazione universale, come si può verificare facendo la chiusura transitiva della chiusura riflessiva e simmetrica di R.

b) R non gode della proprietà antisimmetrica, pertanto nessuna relazione contenente R può essere antisimmetrica, dunque non esiste una relazione d'ordine contenente R. R è seriale e quindi se si considera la matrice di incidenza di R su ogni riga c'è almeno un 1 , sostituendo degli 1 con degli 0 nella matrice di incidenza di R in modo che su ogni riga rimanga esattamente un 1 si trova la matrice di incidenza di una relazione contenuta in R che è una funzione. Queste sostituzioni di 1 con 0 possono essere fare in 16 modi diversi , si ottengono quindi 16 possibili funzioni contenute in R, una di queste è ad esempio la funzione f: f(a)=a, f(b)=b, f(c)=b, f(d)=e, f(e)=e. Non può esserci una funzione contenuta in R che ammetta inversa sinistra perché per ammettere inversa sinistra una funzione deve essere suriettiva e quindi per ogni $x \in X$ in R dovrebbe esserci una coppia che ha come secondo elemento x, mentre non c'è alcuna coppia con secondo elemento c.

c) La ρ è riflessiva per definizione. E' simmetrica in quanto nella definizione a,b hanno lo stesso ruolo.Verifichiamo che è transitiva. Siano $(a,b)\in\rho$, $(b,c)\in\rho$. Se a=b o b=c, si ha immediatamente $(a,c)\in\rho$. Supponiamo allora $a\neq b$, $b\neq c$; $(a,b)\in\rho$ implica $(a,b)\in R$, $(b,a)\in R$, $(b,c)\in\rho$ implica $(b,c)\in R$, $(c,b)\in R$, da $(a,b)\in R$ e da $(b,c)\in R$ per la transitività di R otteniamo $(a,c)\in R$, analogamente da $(c,b)\in R$ e da $(b,a)\in R$ per la transitività di R otteniamo $(c,a)\in R$, dunque $(a,c)\in\rho$. Si osserva subito che per come è fatta R, si ha $\rho=\{(a,a),(a,b),(b,a),(b,b),(c,c),(d,d),(e,e)\}$. dunque $X/\rho=\{\rho_a, \rho_c, \rho_d, \rho_e\}$ con $\rho_a=\rho_b=\{a,b\}$, $\rho_c=\{c\}$,$\rho_d=\{d\}$,$\rho_e=\{e\}$.

d) Si verifica che $T=\{(\rho_a,\rho_a), (\rho_c,\rho_a), (\rho_c,\rho_d), (\rho_c,\rho_e), (\rho_e,\rho_e)\}$, è immediato verificare che T è antisimmetrica e transitiva, poiché la chiusura riflessiva di T conserva queste caratteristiche è una relazione d'ordine. Rispetto a tale relazione X/ρ ammette come unico elemento minimale ρ_c, che è anche un minimo e come elementi massimali ρ_a e ρ_e. X/ρ non è un reticolo rispetto a tale relazione in quanto non esiste ad esempio $\sup\{\rho_a,\rho_e\}$

Fac) Per verificare che T è ben posta dobbiamo dimostrare che la definizione non dipende dai rappresentanti usati per le ρ-classi. L'unica ρ-classe che ha più di un rappresentante è $\rho_a=\rho_b=\{a,b\}$, del resto guardando alla definizione di R si ha subito che (ρ_a,ρ_b), (ρ_b,ρ_a), (ρ_b,ρ_b), (ρ_c,ρ_b) stanno ancora in T, quindi anche scegliendo come rappresentante di ρ_a l'elemento b la definizione di T non cambia.

Esercizio 2)

Si può svolgere molto facilmente considerando le potenze terze dei quattro elementi del gruppo moltiplicativo di Z_5. Infatti $\{1\}^3=\{1\}$, $\{2\}^3=\{3\}$, $\{3\}^3=\{2\}$, $\{4\}^3=\{4\}$.
Si può anche svolgere osservando che il gruppo moltiplicativo di Z_5 ha ordine 4 quindi per quanto detto nell'esercizio successivo il minimo intero r tale che $a^r=\{1\}$, con a elemento del gruppo moltiplicativo di Z_5, è un divisore di 4 pertanto è 1,2 o 4. Una soluzione b dell'equazione $x^3=\{1\}$ è un elemento di Z_5 per cui $b^3=\{1\}$, quindi il minimo intero r tale che $b^r=\{1\}$ non può essere 4, se fosse 2 avremmo $b^2=\{1\}$ e $b^3=\{1\}$, cioè $b^2\cdot b=\{1\}\cdot b=\{1\}$ cioè $b=\{1\}$, se infine fosse 1 avremmo subito $b=\{1\}$.

Esercizio 3)

Poiché G è finito per dimostrare che $<h>$è sottogruppo basta provare che il prodotto di due elementi di $<h>$ sta in $<h>$. Siano $h_1,h_2\in<h>$ questo significa che esistono due interi positivi s,t tali che $h_1=h^s$, $h_2=h^t$, allora $h_1\cdot h_2=h^s\cdot h^t=h^{s+t}\in<h>$, perché $s+t>0$.
Poiché $<h>$ è un sottogruppo, $e\in<h>$, dunque esiste un intero positivo m tale che $e=h^m$. Sia r il minimo intero positivo tale che $e=h^r$, $<h>$ contiene esattamente r elementi. Infatti h, $h^2,\dots$, $e=h^r=h^0$ sono tutti elementi distinti in quanto se fosse $h^t=h^v$ con $t<v<r$ si avrebbe $e=h^{v-t}$ con $0<v-t<r$, assurdo. Inoltre per ogni $i>r$ si ha $h^i= h^{rq+s}$, con $0\le s<r$, cioè $h^i= e\cdot h^s$, quindi ogni potenza positiva di h coincide con uno degli elementi h, $h^2,\dots$, $e=h^r=h^0$. Dunque $|<h>|=r$ e per il teorema di Lagrange r divide n, sia allora $n=rt$, si ha $h^n= h^{rt}=(h^r)^t=e^t=e$.
Ora supponiamo che $<h>$ sia un sottogruppo normale, allora per ogni $g\in G$ e per ogni $h_1\in<h>$ deve essere $g^{-1}h_1g\in<h>$, in particolare $g^{-1}h\,g\in<h>$ dunque deve esistere un intero positivo m tale che $g^{-1}h\,g= h^m$, da cui moltiplicando a sinistra entrambi i membri per g, si ha $hg= gh^m$. Viceversa supponiamo che per ogni $g\in G$ esista un intero positivo m tale che $hg= gh^m$. Moltiplicando a sinistra per g^{-1} otteniamo $g^{-1}h\,g= h^m$, consideriamo ora un qualsiasi elemento $h_1\in<h>$, esiste un intero positivo s tale che $h_1=h^s$, allora $g^{-1}h_1g= g^{-1}h^sg= (g^{-1}hg)(g^{-1}hg)\dots(g^{-1}hg)$ s volte, da cui $g^{-1}h_1g=(g^{-1}hg)^s= (h^m)^s=h^{ms}\in<h>$, in quanto $sm>0$.