Lösningar till tentamen i Algebraiska Strukturer 2006-09-01

1. a) Ja, ty $m*n = |m - n| = |-(m - n)| = |n - m| = n*m$ om $m,n \in \mathbf{N}$
b) Nej, t.ex. är $1*(2*3) = 1*1 = 0$ medan $(1*2)*3 = 1*3 = 2$
c) Ja, 0 är netralt element ty $|m - 0| = |m| = m = |-m| = |0 - m|$ om $m \in \mathbf{N}$.
d) Varje element i $\mathbf{N}$ är sin egen invers ty $m*m = |m - m| = 0$

2. (a) $\alpha^2=(23)(67)$, $\alpha^3=(15)(2637)$, $\alpha^4=$ Id. Alltså är $o(\alpha)=4$.
$\beta^2=(17)(23)$, $\beta^3=(1273)(46)$, $\beta^4=$ Id. Alltså är $o(\beta)=4$.

(b) $\gamma=\alpha\beta=(16425)$ har ordning 5 ty $\gamma^2=(14562)$, $\gamma^3=(12654)$, $\gamma^4=(15246)$ och $\gamma^5=$ id
$\beta\alpha=(15346)$ har ordning 5 av liknande skäl.

Man kan också i (a) och (b) använda ett resultat i kursboken som säger att ordningen av en permutation är största gemensamma nämnaren av cyklernas längd. I (a) får man då t.ex. $o(\alpha)=MGM(2,4)=4$ och $o(\beta)=MGM(2,4)=4$.

3. Se kursboken för Lagranges sats.

4. (a) Låt I vara ett ideal i $R=\mathbf{Z}_4$. Om $[1] \in I$ fås $[m]=[m][1] \in I$ för alla element $[m] \in \mathbf{Z}_4$ så att $I=\mathbf{Z}_4$. Om $[-1] \in I$ fås $[1]=[-1][-1] \in I$ och återigen att $I=\mathbf{Z}_4$. Om $I \not\subset \mathbf{Z}_4$ gäller alltså $I \subset \{[0], [2]\}$ och eftersom $[0]$ tillhör varje ideal att $I=\{[0], [2]\}$ eller $I=\{[0]\}$ som verkligen är ideal då de är abelska delgrupper av $\mathbf{Z}_4$ som är slutna under multiplikation med element i $\mathbf{Z}_4$. Alltså ges idealen i $\mathbf{Z}_4$ av $\mathbf{Z}_4$, $\{[0], [2]\}$ och $\{[0]\}$.

(b) Enligt övningsuppgift i kursboken gäller att ringarna $\mathbf{Z}_6$ och $\mathbf{Z}_2 \times \mathbf{Z}_3$ är isomorfa som ringar. Men om R_1, R_2 är ringar med etta och I ett ideal i $R=R_1 \times R_2$ så gäller för varje element $(i_1, i_2) \in I$ att $(i_1, 0)=(i_1, i_2)(1,0) \in I$ och att $(0, i_2)=(i_1, i_2)(0,1) \in I$. Omvänt om $(i_1, 0) \in I$ och $(0, i_2) \in I$ så är $(i_1, i_2)=(i_1, 0)+(0, i_2) \in I$. Alltså gäller för varje ideal $I \subseteq R_1 \times R_2$ att $I=I_1 \times I_2$ för $I_1=\{i_1 \in R_1 : (i_1, 0) \in I\}$ och $I_2=\{i_2 \in R_2 : (0, i_2) \in I\}$. Vidare är då I_1 ideal i R_1 och I_2 ideal i R_2 eftersom I_1 resp. I_2 är bilderna av I under projektionerna av $R_1 \times R_2$ på R_1 resp. R_2 vilka båda är ringhomomorfier. Men i en kropp finns bara de två triviala idealen. Om vi tillämpar detta på kropparna $\mathbf{Z}_2$ och $\mathbf{Z}_3$ får vi därför att det finns högst fyra möjliga ideal i $\mathbf{Z}_2 \times \mathbf{Z}_3$, nämligen $\mathbf{Z}_2 \times \mathbf{Z}_3$, $\{[0]_2\} \times \mathbf{Z}_3$, $\mathbf{Z}_2 \times \{[0]_3\}$ och $\{[0]_2\} \times \{[0]_3\}$. Det finns därför också högst fyra ideal i $\mathbf{Z}_6$. Men det är lätt att konstuera fyra ideal i $\mathbf{Z}_6$ genom att utgå från de fyra abelska delgrupperna i $\mathbf{Z}_6$. Idealen i $\mathbf{Z}_6$ är därför : $\mathbf{Z}_6$, $\{[0]_6, [2]_6, [4]_6\}$, $\{[0]_6, [3]_6\}$ och $\{[0]_6\}$.

(c) Vi visade i (b) att för varje direkt produkt av två kroppar $K_1 \times K_2$ det finns högst 4 ideal nämligen $K_1 \times K_2$, $\{0\} \times K_2$, $K_1 \times \{0\}$ och $\{0\} \times \{0\}$. Om vi tillämpar det här så får vi de möjliga idealen $\mathbf{R} \times \mathbf{R}$, $\{0\} \times \mathbf{R}$, $\mathbf{R} \times \{0\}$ och $\{0\} \times \{0\}$. Att alla dessa verkligen är ideal i $\mathbf{R} \times \mathbf{R}$ inses av att $\{0\} \times \mathbf{R}$, $\mathbf{R} \times \{0\}$ är kärnor till de naturliga ringhomomorfierna från $\mathbf{R} \times \mathbf{R}$ till $\mathbf{R}$.

(d) Antag först att I är ett ideal i $\mathbf{R}[t]/(t^2)$ som ej ligger i bilden av (t) under restklass-homomorfin från $\mathbf{R}[t]$ till $\mathbf{R}[t]/(t^2)$. Då innehåller I ett en restklass som kan representeras av $a+bt$ där a,b är rella tal med $a \neq 0$. Eftersom I är ett ideal gäller då även att
$[a^{-1}+(t^2)][a+bt+(t^2)] = 1+a^{-1}bt+(t^2) \in I$ och att $[1+a^{-1}bt+(t^2)][1-a^{-1}bt+(t^2)]=1+(t^2) \in I$.

Men om identiteten $1+(t^2)\in I$ gäller $I=\mathbf{R}[t]/(t^2)$. Alltså ligger varje äkta ideal i $\mathbf{R}[t]/(t^2)$ i bilden av (t) under ringhomomorfin från $\mathbf{R}[t]$ till $\mathbf{R}[t]/(t^2)$. Om detta ideal är skilt från nollidealet finns då någon restklass $bt+(t^2)$ med $b\neq 0$ i I. Men då måste varje klass $ct+(t^2)\in I$, ty $ct+(t^2)=[cb^{-1}+(t^2)][\,bt+(t^2)]$ i $\mathbf{R}[t]/(t^2)$. Alltså är detta ideal I då bilden av (t) under ringhomomorfin från $\mathbf{R}[t]$ till $\mathbf{R}[t]/(t^2)$ och detta I är det enda icke-triviala idealet i $\mathbf{R}[t]/(t^2)$. De övriga två idealen är ringen själv och nollidealet $\{0+(t^2)\}$.

5. Detta är en övninguppgift i kursboken. Den löses i fyra steg.

Steg 1 : Man visar att man får en väldefineierad avbildningen ϕ: $R/J\rightarrow R/I$ genom att låta $\phi(r+J)\rightarrow r+I$ för $r\in R$. Här utnyttjas förstås att $J\subseteq I$.

Steg 2 : Man visar att ϕ är en ringhomomorfi. Låt r_1+J , r_2+J vara två restklasser i R/J. Då är: $\phi((r_1+J)+(r_2+J))=\phi(((r_1+r_2)+J))=(r_1+r_2)+I=(r_1+I)+(r_2+I)=\phi(r_1+J)+\phi(r_2+J)$ och $\phi((r_1+J)(r_2+J))=\phi(r_1r_2+J)=r_1r_2+I=(r_1+I)(r_2+I)=\phi(r_1+J)\,\phi\,(r_2+J)$.

Steg 3 : Man konstaterar att ker $\phi=I/J$. Enligt sats i kursboken är därför I/J ett ideal i R/J.

Steg 4: Man noterar att ϕ är surjektiv. Enligt fundamentala homomorfisatsen för ringar är därför $(R/J)/\ker\phi=(R/J)/(I/J)$ isomorf med R/I som ring.

6. x^2+1 är irreducibelt som polynom över $\mathbf{Z}_p$ om och endast om den saknar en linjär faktor koefficienter i $\mathbf{Z}_p$. Enligt faktorsatsen är därför x^2+1 irreducibelt som polynom över $\mathbf{Z}_p$ om och endast om x^2+1 saknar nollställe i $\mathbf{Z}_p$. Men detta senare är ekvivalent med att -1 är en kvadrat i den multiplikativa gruppen $U(\mathbf{Z}_p)$ med p-1 element. Vi får tre fall.

Fall 1: $p=2$. Då är $x^2+1=(x+1)^2$ ej irreducibelt.

Fall 2: $p\equiv 3 \pmod 4$. Då är $o(U(\mathbf{Z}_p))\equiv 2 \pmod 4$ så att $U(\mathbf{Z}_p)$ saknar element av ordning 4 enligt Lagragnges sats. Alltså kan då ej -1 vara en kvadrat i den multiplikativa gruppen $U(\mathbf{Z}_p)$. Således är x^2+1 är irreducibelt som polynom över $\mathbf{Z}_p$ om $p\equiv 3 \pmod 4$.

Fall 3: $p\equiv 1 \pmod 4$. Enligt sats i kursboken är $U(\mathbf{Z}_p)$ en cyklisk grupp. Efttersom $o(U(\mathbf{Z}_p))=p-1\equiv 0 \pmod 4$ ger en annan sats om cykliska grupper att det finns element av ordning 4 i $o(U(\mathbf{Z}_p))$. Dessa har då kvadrat -1 eftersom det bara kan finnas ett element av ordning 2 i en cykisk grupp. Alltså är x^2+1 ej irreducibelt som polynom över $\mathbf{Z}_p$ om $p\equiv 1 \pmod 4$.

7. Grupperna A_4 och $S_3\times S_2$ har samma ordning 12 så vi måste hitta något annat sätt att visa att de ej är isomorfa. Man kan t.ex. utnyttja att S_4 och därmed A_4 saknar element av ordning 6. Detta är klart eftersom ordningen av ett permutation i S_n är minsta gemensamma multipeln av längderna av de ingående cyklerna. För att få en permutation av ordning 6 i S_4 skulle alltså någon av de fem partitionerna av 4 dvs. 4 , 3+1, 2+2, 2+1+1 eller 1+1+1+1 ha termer vars MGM är 6. Men detta gäller ej. Alltså saknar S_4 och $A_4\subset S_4$ element av ordning 6.

Men i $S_3\times S_2$ finns elementet $\{(123),(12)\}$ och detta element skulle under en isomorfi till A_4 avbildas på ett element av ordning 5. Alltså är A_4 och $S_3\times S_2$ icke-isomorfa grupper.