Lösningar till tentamen i algebraiska strukturer (MAL 600 , MAN 290) 2006-03-18

1. Detta är en teorifråga. Se kursboken.

2a) Neutrala elementet $e=e_G\in Z(G)$, ty $eg=g=ge$ för alla $g\in G$. Vidare är $Z(G)$ multiplikativt sluten ty om $w, z\in Z(G)$, så gäller $(wz)g= w(zg)= w(gz)= (wg)z=(gw)z=g(wz)$ för alla $g\in G$. $Z(G)$ är även sluten under inversbildning. Ty om $z\in Z(G)$ gäller för alla $g\in G$ att $g^{-1}z = zg^{-1}$ och därmed att $(g^{-1}z)^{-1} =(zg^{-1})^{-1}$ med V.L. $= z^{-1}g$ och H.L.$= g\, z^{-1}$.
Enligt kriterium för delgrupper i kursboken är därför $Z(G)$ en delgrupp av G.

b) Låt $\varphi : G\to H$ vara en isomorfi och $z\in Z(G)$. För att visa att $\varphi(z)\in Z(H)$, låt $h\in H$. Då finns $g\in G$ med $\varphi(g)= h$ så att $\varphi(z)h=\varphi(z)\varphi(g)=\varphi(zg) = \varphi(gz) =\varphi(g)\varphi(z)= h\varphi(z)$. Alltså gäller $\varphi(z) \in Z(H)$ och att $\varphi(Z(G))\subseteq Z(H)$. Eftersom även $\varphi^{-1}: H\to G$ är en isomorfi ger samma argument att $\varphi^{-1}(Z(H))\subseteq Z(G)$. Detta visar att φ avbildar $Z(G)$) bijektivt på $Z(H)$ och därmed att de är isomorfa grupper.

3) Låt $\varphi: A\to A$ vara en additiv grupphomomorfi. Då är enligt resultat i kursboken $\varphi(ma)= m\varphi(a)$ för alla $a\in A$ och $m\in\mathbf{Z}$. Speciellt är $\varphi([m]_n)=\varphi(m[1]_n)=m\varphi([1]_n)$ om $A= \mathbf{Z}_n$. Men $m\varphi([1]_n)$ beror bara på restklassen av m(mod n) och kan uppfattas som produkten $[m]_n\otimes\varphi([1]_n)$ av $[m]_n$ och $\varphi([1]_n)$ *i* $\mathbf{Z}_n$. Alltså ges varje additiv grupphomomorfi $\varphi: \mathbf{Z}_n \to \mathbf{Z}_n$ av $\varphi([m]_n)= [m]_n\otimes[k]_n$ för något entydigt bestämt element $[k]_n\in\mathbf{Z}_n$. Omvänt, om $[k]_n\in\mathbf{Z}_n$ så är avbildningen $\varphi_{[k]}: \mathbf{Z}_n \to \mathbf{Z}_n$, $\varphi([m]_n)= [m]_n\otimes[k]_n$ en additiv grupphomomorfi ty $\varphi([m]_n\oplus[m´]_n)= ([m]_n\oplus[m´]_n)\otimes[k]_n= ([m]_n\otimes[k]_n)\oplus([m´]_n\otimes[k]_n) =\varphi([m]_n\oplus\varphi([m´]_n)$ p.g.a. distributiva lagen i ringen $\mathbf{Z}_n$.

3a) Vi har sett ovan att samtliga grupphomomorfier $\varphi: \mathbf{Z}_n \to \mathbf{Z}_n$ är av typen $\varphi_{[k]}$ där $[k]\in\mathbf{Z}_n$. Här är $\varphi_{[0]}$ nollavbildningen som ej är en isomorfi. Om $[k]$ har en multiplikativ invers $[l]$ i $\mathbf{Z}_n$ så är däremot $\varphi_{[l]}(\varphi_{[k]}([m]))= \varphi_{[l]}([m] \otimes[k]) =([m] \otimes[k]) \otimes[l]) = [m] \otimes([k]\otimes[l])= [m] \otimes[1] = [m]$. Alltså är $\varphi_{[k]}$ då injektiv och därmed bijektiv enligt Dirichlets lådprincip. Om n är ett primtal så är alltså $\varphi_{[k]} : \mathbf{Z}_n \to \mathbf{Z}_n$ en gruppisomorfi för $[k]\neq [0]$ i $\mathbf{Z}_n$ eftersom $\mathbf{Z}_n$ då är en kropp. Vi har därmed visat att det finns för varje primtal n finns precis n-1 gruppisomorfier $\varphi: \mathbf{Z}_n \to \mathbf{Z}_n$ och att dessa ges av $\varphi_{[1]}$, ... , $\varphi_{[n-1]}$.

(b) Enligt ovan ges de additiva gruppisomorfierna $\varphi: \mathbf{Z}_n \to \mathbf{Z}_n$ av de avbildningar $\varphi_{[k]}$ som är injektiva. Men om n-1 vore bijektiva skulle alla $\varphi_{[k]}$ med $[k]\neq [0]$ vara injektiva. Speciellt skulle för $[k]\neq [0]$ då gälla att $\varphi_{[k]}([m])= [0] \Rightarrow [m]= [0]$ och att $[m] \otimes[k]= [0] \Rightarrow [m]= [0]$. Det kan därför bara inträffa att det finns n-1 gruppisomorfier då $\mathbf{Z}_n$ är ett integritetsområde och detta gäller bara om n är ett primtal.

4. Om en surjektiv ringhomomorfi $\mathbf{Q} \to \mathbf{Z}_n$ hade funnits så skulle det enligt fundamentala homomorifsatsen för ringar även finnas ett ideal i $\mathbf{Q}$ sådant att $\mathbf{Q}/I$ och $\mathbf{Z}_n$ är isomorfa som ringar. Men ett ideal i $\mathbf{Q}$ är endera $\{0\}$ eller kroppen själv, eftersom om $l/m\in I$ med $l\neq 0$ vi måste ha att $(m/l)(l/m)=1\in I$ och därmed att $I= \mathbf{Q}$. Men varken $\mathbf{Q}/\{0\}= \mathbf{Q}$ eller $\mathbf{Q}/ \mathbf{Q} = \{0\}$ är isomorfa med $\mathbf{Z}_n$ eftersom varje sådan ring måste ha samma antal element n som $\mathbf{Z}_n$. Alltså finns ingen surjektiv ringhomomorfi från $\mathbf{Q}$ till $\mathbf{Z}_n$.

5. Detta är en teorifråga. Se kursboken.

6a) Ett andragradspolynomet över $\mathbf{Z}_2$ kan bara vara reducibelt om det har en förstagradsfaktor och därmed ett nollställe i $\mathbf{Z}_2$. Men x^2+x+1 saknar sådan nollställen ty såväl 0^2+0+1 som 1^2+1+1 är lika med 1 i $\mathbf{Z}_2$. Alltså är x^2+x+1 irreducibelt i $\mathbf{Z}_2[x]$.

b) Om ett femtegradspolynom $f(x)= g(x)h(x)$ för två polynom $g(x)$, $h(x) \in \mathbf{Z}_2[x]$ så måste grad g +grad h =5 och endera $g(x)$ eller $h(x)$ ha grad högst två. För att visa att polynomet $f(x) = (x^2+x+1)(x^3+x) +1$ är irreducibelt över $\mathbf{Z}_2$ räcker det därför visa att det inte har någon andragradsfaktor. Men $f(0)= (0^2+0+1)(0^3+0) +1=1$ och $f(1)= (1^2+1+1)(1^3+1) +1=1$. Alltså kan inte $f(x)$ ha någon förstagradsfaktor. $f(x)$ kan därför inte heller ha någon andragradsfaktor som är reducibel i $\mathbf{Z}_2[x]$. Enda återstående möjlighet för $f(x)$ att vara reducibel är därför att det har en irreducibel andragradsfaktor. Men enligt a) är x^2+x+1 det enda irreducibla andragrads-polynomet i $\mathbf{Z}_2[x]$. En direkt inspektion visar emellertid att $(x^2+x+1)(x^3+x) +1$ ej är jämnt delbart med (x^2+x+1). Alltså är $f(x)= (x^2+x+1)(x^3+x) +1$ irreducibelt över $\mathbf{Z}_2$.

7. Om A_4 och $A_3 \times S_2$ vore isomorfa skulle det finnas en bijektion mellan dem. Men den alternerande gruppen A_n består av alla jämna element i S_n och har därmed index 2 i S_n. Alltså har A_4 ordning 12, A_3 ordning 3 och $A_3 \times S_2$ ordning 6. Det kan därför inte finnas någon bijektion mellan A_4 och $A_3 \times S_2$.