KTH Teknikvetenskap

SF2703 Algebra grundkurs
Lösningsförslag med bedömningskriterier till tentamen
Måndagen den 9 mars 2009

---

(1) a) Definiera vad som menas med centralisatorn till ett element g i en grupp G. **(1)**

b) Visa att om H är en normal delgrupp i en grupp G så finns det en naturlig surjektiv homomorfi $G \longrightarrow G/H$ vars kärna är H. **(2)**

c) Fyll i resterande element i grupptabellen

$*$	u	v	w	x	y	z
u	w				v	
v		x				
w				w		
x	u					
y						u
z			y			

och motivera noggrant. **(2)**

d) Ge ett exempel där den symmetriska gruppen S_n verkar på en mängd X så att den alternerande gruppen A_n är stabilisatorn för något element x i X. **(2)**

e) Visa att gruppen G måste vara abelsk om $G/Z(G)$ är cyklisk. **(2)**

---

a). Centralisatorn, $C_G(g)$, till ett element g i G ges av

$$C_G(g) = \{g \in G | hg = gh, \quad \forall h \in G\},$$

dvs delmängden av alla elemtent i G som kommuterar med g. Vi kan också skriva $hgh^{-1} = g$ istället för $hg = gh$.

b). Vi kan definiera $\Phi : G \longrightarrow G/H$ genom

$$\Phi(g) = gH, \qquad \forall g \in G.$$

Detta är en homomorfi eftersom

$$\Phi(gh) = ghH = ghHH = gHhH = \Phi(g)\Phi(h), \qquad \forall g, h \in G,$$

eftersom H är normal och därmed $hH = Hh$, för alla $h \in G$. Homomorfin är surjektiv per definition, och kärnan ges av

$$\ker \Phi = \{g \in G | gH = H\} = \{g \in G | g \in H\} = H,$$

vilket skulle visas.

c). Till att börja med kan vi identifiera identitetselementet, e, genom att se att $wx = w$, vilket innebär att $x = e$, efter multiplikation till vänster med w^{-1}. Alltså kan vi fylla i raden och kolonnen som hör till $x = e$ och får då

$*$	u	v	w	x	y	z
u	w			u	v	
v		x		v		
w				w		
x	u	v	w	x	y	z
y				y		u
z			y	z		

Eftersom gruppens ordning är 6, vet vi att elementens ordning kan vara 1, 2, 3 eller 6 och eftersom $u^2 = w \neq e$, måste u ha ordning tre eller sex.

Om ordningen av u är sex är gruppen cyklisk och det finns bara ett element av ordning två som därmed måste vara $u^3 = v$. Därmed måste y och z vara u^4 och u^5 i någon ordning, men vi har att $yz = u$, enligt tabellen vilket motsäger att $yz = u^4 u^5 = u^9 = u^3$. Alltså kan inte ordningen av u vara sex.

Vi vet nu att u har ordning tre och vi får $uw = wu = e$. Därmed är också w ordning tre och $w^2 = w^{-1} = u$. När vi fyller i detta får vi

$*$	u	v	w	x	y	z
u	w		x	u	v	
v		x		v		
w	x		u	w		
x	u	v	w	x	y	z
y				y		u
z			y	z		

I första raden fattas bara y och z. Eftersom z redan finns med i sista kolonnen måste $uv = z$ och $uz = y$. På samma sätt fattas y och z i tredje kolonnen, och vi får $vw = z$ och $yw = v$. Vi har nu fått

$*$	u	v	w	x	y	z
u	w	z	x	u	v	y
v		x	z	v		
w	x		u	w		
x	u	v	w	x	y	z
y			v	y		u
z			y	z		

I tre av raderna saknas nu tre element, men vi kan i alla tre fallen bara sätta dem på ett sätt så att inte ett element förekommer två gånger i en kolonn. När vi väl gjort detta blir den sista raden given. Resultatet blir:

$*$	u	v	w	x	y	z
u	w	z	x	u	v	y
v	y	x	z	v	u	w
w	x	y	u	w	z	v
x	u	v	w	x	y	z
y	z	w	v	y	x	u
z	v	u	y	z	w	x

Vi skulle också ha kunnat använda oss av kunskapen att det bara finns en icke-cyklisk grupp av ordning 6 upp till isomorfi, S_3, för att förenkla räkningarna något. Efter att ha identifierat u och w som element av ordning 3, vet vi att v, y och z måste vara transpositionerna.

d). I och med att A_n har index två i S_n måste banan till ett element som har stabilisator A_n innehålla två element. Vi kan lika gärna ersätta X med denna bana och ser då att vi kan välja en mängd X med två element. A_n fixerar nu det ena elementet, men då måste även det andra elementet fixeras. De udda permutationerna ska inte fixera något av elementen. Vi ser att vi kan låta X vara $\{\pm 1\}$ och låta S_n verka genom multiplikation med tecknet på permutationen

$$\sigma.x = \text{sgn}\sigma \cdot x, \qquad x \in \{\pm 1\}$$

Ett annat sätt som fungerar i allmänhet för en delgrupp H i en grupp G är att låta G verka på vänstersidoklasserna till H, dvs

$$g.hH = (gh)H.$$

Då fixeras sidoklassen $H = eH$ precis av H, eftersom $gH = H$ om och endast om $g \in H$. Alltså kan vi låta S_n verka på $X = S_n/A_n$ på detta sätt och få stabilisatorn A_n till den triviala sidoklassen.

e). Om $G/Z(G)$ är cyklisk kan den genereras av ett enda element, säg $gZ(G)$. Vi får då att

$$G/Z(G) = \langle gZ(G) \rangle = \{g^i Z(G) | i \in \mathbb{Z}\}.$$

Eftersom unionen av sidoklasserna till $Z(G)$ är hela G betyder det att alla element kan skrivas som

$$g^i z, \qquad i \in \mathbb{Z}, z \in Z(G),$$

men två godtyckliga sådana element kommuterar med varandra eftersom

$$(g^i z)(g^j z') = g^i g^j z z' = g^j g^i z' z = (g^j z')(g^i z),$$

där vi använt att $g^i g^j = g^{i+j} = g^j g^i$ och att $z, z' \in Z(G)$. Alltså är G abelsk och i själva verket är $Z(G) = G$ och $G/Z(G) = \{e\}$.

Bedömningskriterier.

a) Korrekt definition av centralisatorn, **1 poäng**.

b)
- Korrekt konstruktion av homomorfin inklusive kontroll att det är en homomorfi, **1 poäng**
- Korrekt motivering till att kärnan är H, **1 poäng**

c)
- Korrekt ifylld tabell, **1 poäng**
- Korrekt utförlig motivering till tabellen, **1 poäng**

d)
- Korrekt exempel, **1 poäng**
- Korrekt motivering till att stabilisatorn är A_n, **1 poäng**

e)
- Korrekt slutsats om att det finns ett $g \in G$ så att elementen i G kan skrivas $g^i z$, för $i \in \mathbb{Z}$, $z \in Z(G)$, **1 poäng**
- Korrekt slutförd motivering till att G är abelsk, **1 poäng**

(2) a) Definiera vad som menas med en p-grupp. **(1)**

b) Låt p vara ett primtal. Använd klassekvationen för att visa att centret i en p-grupp inte kan vara trivialt. **(2)**

c) Låt H och K vara normala delgrupper i en grupp G. Visa att $G/(H \cap K)$ är abelsk om G/H och G/K båda är abelska. (*Ledning*: Se på homomorfin $G \longrightarrow (G/H) \times (G/K)$). **(2)**

d) Låt A vara en ändlig abelsk grupp och p ett primtal som delar ordningen av A. Visa att kärnan till homomorfin, $\Phi : A \longrightarrow A$, som ges av $\Phi(a) = a^p$, är p-delgrupp. (*Ledning*: Använd struktursatsen för ändliga abelska grupper.) **(2)**

e) Låt G vara symmetrigruppen för en dodekaeder. Det är känt att $|G| = 60$. Bestäm antalet 3- och 5-Sylowdelgrupper till G. **(2)**

---

a). Om p är ett primtal är G en p-grupp om $|G| = p^n$ för något heltal $n > 0$.

b). Antag att $|G| = p^n$, för något positivt heltal n. Enligt klassekvationen är nu

$$p^n = |G| = |Z(G)| + \sum_{i=1}^{s} \frac{p^n}{|C_G(g_i)|}$$

där $g_1, g_2, \ldots, g_s$ är representanter för de icke-triviala konjugatklasserna. Därmed är alla dessa termer delbara med p, liksom vänsterledet. Alltså måste även $|Z(G)|$ vara delbart med p och vi kan inte ha $Z(G) = \{e\}$, vilket skulle visas.

c). Vi kan definiera en homomorfi

$$G \longrightarrow (G/H) \times (G/K)$$

genom $\Phi(g) = (gH, gK)$ för alla g i G. Kärnan till denna homomorfi ges av

$$\ker \Phi = \{g \in G | gH = H, gK = K\} = \{g \in G | g \in H, g \in K\} = H \cap K.$$

Enligt första isomorfisatsen har vi att $G/(H \cap K) \cong \mathrm{im}\Phi$, men denna måste vara abelsk om G/H och G/K är abelska eftersom $\mathrm{im}\Phi$ är en delgrupp av $(G/H) \times (G/K)$ som i så fall är abelsk.

d). Enligt struktursatsen för ändliga abelska grupper kan vi skriva A som en produkt av cykliska grupper:

$$A \cong Z_{n_1} \times Z_{n_2} \times \cdots \times Z_{n_s}.$$

Det räcker nu att visa påståendet för en cyklisk grupp eftersom kärnan till $\Phi : A \longrightarrow A$ är produkten av kärnorna till motsvaranade homomorfier $\Phi_i : Z_{n_i} \longrightarrow Z_{n_i}$, $i = 1, 2, \ldots, s$. Eftersom $|A|$ är delbart med p är n_1 delbart med p. Om n_i inte är delbart med p måste $\Phi_i : Z_{n_i} \longrightarrow Z_{n_i}$ vara en isomorfi, eftersom det inte kan finnas något element av ordning p i Z_{n_i}. Om n_i är delbart med p finns precis p element av ordning p i i Z_{n_i}. Alltså är kärnan till Φ en produkt av cykliska grupper av ordning p och därmed en p-delgrupp till A.

Vi kan också argumentera genom att $B = \ker \Phi$ är en delgrupp där alla element uppfyller $x^p = e$. Alltså kan det inte finnas någon annan primtalsfaktor än p i ordningen till B, eftersom det då enligt Cauchys sats skulle finnas element av ordning q, men

$x^p = x^q = e$ innebär att $x = e$, om p och q är olika primtal. Det räcker nu att se att Cauchys sats säger att B inte kan vara trivial, eftersom det finns minst ett element av ordning p i A och detta ligger också i B.

e). Antalet 3-Sylowdelgrupper ska vara kongruent med 1 modulo 3 och en delare i 20. För varje par av motstående hörn i dodekaedern finns rotationer av ordning tre som bevarar dodekaedern. Det innebär att det finns minst tio 3-Sylowdelgrupper, eftersom antalet hörn är 20, men det finns inga större delare i 20 som är kongruenta med 1 modulo 3. Alltså finns precis tio 3-Sylowdelgrupper i G.

Antalet 5-Sylowdelgrupper ska vara kongruent med 1 modulo 5 och en delare i 12. Därmed kan det antingen vara 1 eller 6. För varje par av motstående sidor finns rotationer av ordning fem som bevarar dodekaedern. Därmed finns minst sex 5-Sylowdelgrupper. Alltså finns precis sex 5-Sylowdelgrupper i G.

Bedömningskriterier.

a) Korrekt definition av p-grupp, **1 poäng**.

b)
- Korrekt formulerad klassekvation, **1 poäng**
- Korrekt motivering till att p delat $|Z(G)|$, **1 poäng**

c)
- Korrekt motivering till att kärnan till homomorfin är $H \cap K$, **1 poäng**
- Korrekt slutfört bevis av att gruppen är abelsk, **1 poäng**

d)
- Korrekt motivering till att kärnan är cyklisk av ordning p för varje cyklisk faktor, **1 poäng**
- Korrekt slutfört bevis av att kärnan är en p-delgrupp, **1 poäng**

e)
- Korrekt motiverat antal 3-Sylowdelgrupper, **1 poäng**
- Korrekt motiverat antal 5-Sylowdelgrupper, **1 poäng**

---

(3) a) Definiera vad som menas med en skevkropp (divisionsring). **(1)**
b) Visa att en homomorfi från en kropp till en ring antingen är injektiv eller trivial, dvs noll för alla element. **(2)**
c) Låt R vara en kommutativ ring med etta. Visa att ett ideal I i R är ett äkta ideal om och endast om 1 inte ligger i I. **(2)**
d) Skriv $\mathbb{Z}[i]/(1+11i)$ som en produkt av kroppar. **(2)**
e) Låt G vara en cyklisk grupp av ordning n och låt k vara en kropp. Visa att gruppringen $k[G]$ är isomorf med $k[x]/(x^n-1)$. **(2)**

---

a). En skevkropp är en ring med etta där varje element utom noll är inverterbart.

b). Låt $\Phi : k \longrightarrow R$ vara en homomorfi från en kropp k till en ring R. Då är $\ker \Phi$ ett ideal i k. En homomorfi är injektiv om och endast om dess kärna är trivial. Om Φ inte är injektiv finns alltså ett nollskilt element $a \in \ker \Phi$, men eftersom k är en kropp är a inverterbart och $(a) = (1) = k$. Alltå är $\ker \Phi = k$ och Φ är konstant noll, dvs trivial.

c). Om I är ett äkta ideal kan inte 1 ligga i I eftersom vi då har $I \supseteq (1) = R$, vilket motsäger att I är äkta. Om 1 inte ligger i I så är $I \neq R$ och därmed är I ett äkta ideal.

d). De Gaussiska heltalen är ett område med unik faktorisering och vi kan faktorisera $1 + 11i$ i irreducibla faktorer. Genom att titta på normen $N(1 + 11i) = 1^2 + 11^2 = 122 = 2 \cdot 61$. Eftersom både 2 och 61 är primtal är den enda möjligheten till att $1 + 11i$ inte är irreducibelt att det är en produkt av två irreducibla element med norm 2 och 61. Det finns fyra Gaussiska heltal med norm 2, och dessa skiljer bara genom multiplikation med enheter; $(1 + i)$, $-1 + i$, $-1 - i$ och $1 - i$. Det räcker därmed att se om $1 + 11i$ är delbart med $1 + i$. Vi provar och ser att $1 + 11i = (1 + i)(6 + 5i)$. Eftersom detta är en faktorisering av $1 + 11i$ i irreducibla faktorer får vi enligt kinesiska restsatsen att

$$\mathbb{Z}[i]/(1+11i) \cong \mathbb{Z}[i]/(1+i) \times \mathbb{Z}[i]/(6+5i)$$

där faktorerna är kroppar eftersom $1 + i$ och $6 + 5i$ är irreducibla element i $\mathbb{Z}[i]$. (Vi kan också se att $\mathbb{Z}[i]/(1 + i) \cong \mathbb{Z}_2$ och $\mathbb{Z}[i]/(6 + 5i) \cong \mathbb{Z}_{61}$, exempelvis genom att räkna antalet element i kvoterna. Därmed får vi att $\mathbb{Z}[i]/(1 + 11i) \cong \mathbb{Z}_2 \times \mathbb{Z}_{61}$.)

e). Om $G = \langle g \rangle$ så kan vi skriva $G = \{g^0, g^1, \ldots, g^{n-1}\}$. Elementen i gruppringen $k[G]$ är därmed linjärkombinationer

$$a_0 g^0 + a_1 g^1 + \cdots + a_{n-1} g^{n-1}$$

där $a_0, a_!, \ldots, a_{n-1}$ är element i k. Vi ser att dessa ser ut som polynom och det är naturligt att se om det går att definiera en ringhomomorfi

$$\Phi : k[x] \longrightarrow k[G]$$

genom

$$\Phi(a_0 + a_1 x + \cdots + a_m x^m) = a_0 + a_1 g + \cdots + a_m g^m,$$

som vi också skulle kunna skriva $\Phi(f(x)) = f(g)$. På grund av att multiplikationen i $k[G]$ bygger på att $g^i g^j = g^{i+j}$ och att additionen sker termvis får vi att

$$\Phi(f(x) + h(x)) = f(g) + h(g) = \Phi(f(x)) + \Phi(h(x))$$

och

$$\Phi(f(x) \cdot h(x)) = f(g) \cdot h(g) = \Phi(f(x)) \cdot \Phi(h(x)),$$

för polynom $f(x), h(x) \in k[x]$, dvs Φ är en homomorfi.

För att se att $k[G] \cong k[x]/(x^n - 1)$ räcker det nu enligt isomorfisatsen att se att Φ är surjektiv med kärna $(x^n - 1)$. På grund av utseendet av elementen i $k[G]$ ovan ser vi att Φ är surjektiv och att det inte kan finnas något polynom av grad lägre än n i kärnan. Däremot ser vi att $\Phi(x^n) = g^n = 1$, dvs $\Phi(x^n - 1) = 0$. Alltså måste $(x^n - 1)$ vara generatorn till $\ker \Phi$. (Ett ideal i en polynomring i en variabel över en kropp genereras av polynomet av lägsta grad i idealet.)

Bedömningskriterier.

a) Korrekt definition av skevkropp, **1 poäng**.

b)
- Korrekt motivering till att kärnan är icke-trivial om homomorfin inte är injektiv, **1 poäng**
- Korrekt motivering till att homomorfin är trivial om kärnan innehåller ett nollskilt element, **1 poäng**

c)
- Korrekt bevis för att ett äkta ideal inte innehåller ettan, **1 poäng**
- Korrekt bevis för att ett ideal som inte innehåller ett är äkta, **1 poäng**

d)
- Korrekt faktorisering av $1 + 11i$, **1 poäng**
- Korrekt användning av kinesiska restsatsen för att skriva ringen som en produkt av kroppar, **1 poäng**

e)
- Korrekt motiverad homomorfi $k[x] \longrightarrow k[G]$, **1 poäng**
- Korrekt motivering till att kärnan är $(x^n - 1)$ och att detta leder till den önskade isomorfin, **1 poäng**
