



KTH Teknikvetenskap

SF2703 Algebra grundkurs
Lösningsförslag till tentamen
Tisdagen den 3 juni 2008

- (1) a) Definiera vad som menas med att en grupp G verkar på en mängd X . (1)
b) Visa att en gruppverkan av en grupp G på en mängd X är det samma som en homomorfi från G till den symmetriska gruppen S_X . (2)
c) Formulera och bevisa Lagranges sats för ändliga grupper. (2)
d) Är stabilisatorn av ett element vid en gruppverkan alltid en normal delgrupp? Ge bevis eller motexempel. (2)
e) Visa att om H och K är normala delgrupper i G som uppfyller $H \cap K = \{e\}$ och $HK = G$ så gäller att $G \cong H \times K$. (2)
-

a). Att G verkar på X betyder att det finns en funktion $\phi : G \times X \longrightarrow X$ som uppfyller

(i) $e.x = x$, för alla element x i X .

(ii) $g.(h.x) = (g * h).x$, för alla element x i X och alla element g och h i G .

där vi skriver $g.x$ för $\phi(g, x)$.

b). Om vi har en gruppverkan får vi för varje element g en funktion $\phi_g : X \longrightarrow X$ genom $\phi_g(x) = g.x$. Eftersom varje element g i G har en invers g^{-1} kan vi med (i) och (ii) få att

$$x = e.x = (g * g^{-1}).x = g.(g^{-1}.x) = \phi_g(\phi_{g^{-1}}(x)),$$

för alla $x \in X$, vilket visar att ϕ_g är inverterbar med invers g^{-1} . Alltså är ϕ_g ett element i S_X och vi har en funktion

$$\Phi : G \longrightarrow S_X$$

som ges av $\Phi(g) = \phi_g$, för $g \in G$. Det återstår att visa att Φ är en homomorfi. Vi använder oss nu av (ii) vilket ger att

$$\Phi(g * h) = \phi_{g*h} = \phi_g \circ \phi_h$$

eftersom

$$\phi_{g*h}(x) = (g * h).x = g.(h.x) = \phi_g(\phi_h(x))$$

för alla $x \in X$.

Vi har nu visat att en gruppverkan av G på X ger upphov till en homomorfi. Omvänt kan vi för en homomorfi $\Phi : G \longrightarrow S_X$ definiera $g.x = \Phi(g)(x)$ för alla (g, x) i $G \times X$, vilket är en gruppverkan eftersom

- (i) $e.x = \Phi(e)(x) = \text{Id}(x) = x$, eftersom en homomorfi tar e till enheten Id i S_X ,
- (ii) $g.(h.x) = \Phi(g)(\Phi(h)(x)) = (\Phi(g) \circ \Phi(h))(x) = \Phi(g * h)(x) = (g * h).x$.

Alltså har vi en bijektion mellan mängden av verkningar av G på X och mängden av homomorfier från G till S_X .

c). Lagranges sats säger att ordningen av en delgrupp H i en ändlig grupp G delar gruppens ordning.

För att bevisa satsen ser vi på sidoklasserna till H i G , dvs $\{gH | g \in G\}$. Eftersom $gH = g'H$ är detsamma som att $H = g^{-1}g'H$, så är de två sidoklasserna lika om och endast om $g^{-1}g' \in H$. Detta innebär en ekvivalensrelation på G som delas in i disjunkta ekvivalensklasser. Dessa ekvivalensklasser är lika med sidoklasserna och varje sidoklass innehåller precis $|H|$ element eftersom vi har en bijektion

$$H \longrightarrow gH$$

genom multiplikation med g till vänster. Eftersom alla sidoklasser har $|H|$ element och deras union är hela G får vi att $|G| = n|H|$ för något heltal n .

d). Om H är stabilisatorn till x vid verkan av G på X har vi att

$$H = \{h \in G | h.x = x\}$$

och för ett element g i G har vi att

$$gHg^{-1} = \{ghg^{-1} | h.x = x\}$$

Om detta skulle vara lika med H skulle vi ha att $ghg^{-1}.x = x$ för alla h som uppfyller $h.x = x$. Genom att verka med g^{-1} i bägge led får vi

$$hg^{-1}.x = g^{-1}.x \iff h.(g^{-1}.x) = g^{-1}.x$$

dvs h stabiliserar också $g^{-1}.x$. Vi kan alltså hitta motexempel om vi kan hitta ett h som bara fixerar ett element x , och där detta element inte fixeras av alla element i gruppen. Tag exempelvis $h = (12)$ i S_3 . Detta element fixerar endast 3 när S_3 verkar på $\{1, 2, 3\}$. Däremot fixeras inte 3 av övriga element i S_3 . Stabilisatorn till 3 är $\langle(12)\rangle$ som inte är en normal delgrupp i S_3 , då exempelvis $(23)^{-1}\langle(12)\rangle(23) = \langle(13)\rangle$.

e). Eftersom H och K är normala kan vi bilda kvoterna G/H och G/K . Vi kan också definiera en avbildning

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

genom $\Phi(g) = (gH, gK)$. Detta är en homomorfi av grupper eftersom

$$\Phi(g_1g_2) = (g_1g_2H, g_1g_2K) = (g_1Hg_2H, g_1Kg_2K) = \Phi(g_1)\Phi(g_2)$$

då H och K är normala.

Kärnan till Φ ges av de g som uppfyller $gH = H$ och $gK = K$, dvs de element i G som ligger i både H och K . Alltså är $\ker \Phi = H \cap K = \{e\}$ och enligt isomorfin satsen har vi att

$$\operatorname{im} \Phi \cong G / \ker \Phi = G / \{e\} \cong G.$$

Eftersom Φ är injektiv ger den en isomorfi mellan H och bilden av H i $G/H \times G/K$. Denna ligger helt i den andra faktorn eftersom H går på identiteten in G/H . På samma sätt får vi att K är isomorf med en delgrupp i G/H . Det återstår att visa att Φ är surjektiv, eftersom detta leder till att $H \cong G/K$ och $K \cong G/H$. För att visa detta behöver vi använda oss av att $G = HK$, dvs att varje element i G kan skrivas som hk för något element h i H och något element k i K .

Tag nu ett element (g_1H, g_2K) i $(G/H) \times (G/K)$. Vi skriver $g_1 = h_1k_1$ och $g_2 = h_2k_2$ och får

$$(g_1H, g_2K) = (h_1k_1H, h_2k_2K) = (h_1Hk_1, h_2K) = (h_2Hk_1, h_2k_1K) = (h_2k_1H, h_2k_1K) = \Phi(h_2k_1)$$

där vi har använt att $Hg = gH$ för alla element g i G och att $hH = H$ och $kK = k$ för alla h i H och k i K . Därmed har vi visat att Φ är surjektiv, och därmed följer att $G \cong H \times K$.

Bedömningskriterier.

- a) Korrekt definition av gruppverkan, **1 poäng**.
- b) – Korrekt bevis av att en gruppverkan ger en homomorfi, **1 poäng**.
– Korrekt bevis av att en homomorfi ger en gruppverkan, **1 poäng**.
- c) – Korrekt formulering av Lagranges sats, **1 poäng**.
– Korrekt bevis för Lagranges sats, **1 poäng**.
- d) Korrekt motexempel mot att stabilisatorn är normal, **2 poäng**.
- e) – Korrekt konstruktion av homomorfin Φ , **1 poäng**.
– Korrekt slutfört bevis av påståendet, **1 poäng**.

- (2) a) Definiera vad som menas med en p -Syldowdelgrupp. (1)
 b) Bestäm antalet 11-Syldowdelgrupper i en grupp av ordning 715. (2)
 c) Formulera Cauchys sats för ändliga grupper och bevisa den i specialfallet då gruppen är abelsk. (2)
 d) Bestäm antalet abelska grupper av ordning 60. (2)
 e) Låt G vara gruppen av inverterbara övertriangulära matriser med koefficienter i \mathbb{Z}_3 . Bestäm antalet element i G som är konjugerade med

$$h = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

(2)

a). För varje primtal p som delar ordningen av en ändlig grupp G är en p -Syldowdelgrupp i G en delgrupp av ordning p^m där $|G|/p^m$ inte är delbart med p , dvs p^m är den högsta potens av p som delar $|G|$.

b). Antalet 11-Syldowdelgrupper skall vara kongruent med 1 modulo 11 enligt Sylows sats. Vidare skall antalet vara en delare i $715/11 = 65$. Eftersom delarna i 65 är 1, 5, 13 och 65 och bara 1 är kongruent med 1 modulo 11 måste det finnas bara en enda 11-Syldowdelgrupp.

c). Cauchys sats för ändliga grupper säger att en ändlig grupp har ett element av ordning p för varje primtal p som delar gruppens ordning.

Fixera primtalet p . Satsen är sann för cykliska grupper eftersom dessa innehåller element av ordning d för varje delare d av gruppens ordning. Antag att A är den minsta abelska grupp som inte har något element av ordning p trots att p delar $|A|$. Då finns inget element i A som har ordning som är delbar med p . Om tar kvoten av A med en cyklisk delgrupp får vi därmed en grupp av ordning som är delbar med p . Enligt antagandet om minimaliteten hos A finns ett element, \bar{y} , av ordning p i $A/(x)$. Det betyder att $y + y + \dots + y = kx$ för något heltal k . Om x har ordning n så får vi nu att $pn\bar{y} = 0$, vilket innebär att y har ordning som är delbar med p om inte $n\bar{y} = 0$. Eftersom p inte delar n så finns a och b så att $ap + bn = 1$, vilket innebär att

$$\bar{y} = (ap + bn)\bar{y} = a(p\bar{y}) + b(n\bar{y}) = 0.$$

Alltså kan inte $n\bar{y} = 0$ och vi får att y har en ordning som är delbar med p , varför det finns ett element av ordning p i A . Detta är en motsägelse mot antagandet om A , vilket bevisar satsen.

d). Vi vet enligt struktursatsen för ändliga abelska grupper att alla abelska grupper är produkter av cykliska grupper. Vi kan dessutom dela upp en abelsk grupp som en produkt av cykliska grupper av primtalspotensordning. Vi faktorerar 60 och får $60 = 2 \cdot 2 \cdot 3 \cdot 5$, vilket innebär att en abelsk grupp av ordning 60 kan skrivas som

$$C_2 \times C_2 \times C_3 \times C_5$$

eller

$$C_4 \times C_3 \times C_5$$

och dessa båda grupper är inte isomorfa. Alltså finns två abelska grupper av ordning 60.

e). Vi beräknar först antalet element i G . Elementen på diagonalen kan väljas på 2^3 sätt så att matrisen blir inverterbar medan de övriga tre elementen kan väljas godtyckligt, dvs på 3^3 sätt. Alltså består G av $6^3 = 216$ element. För att se hur många av dessa som är konjugerade med den givna matrisen kan vi också se på centralisatorn eftersom konjugatklassen innehåller $|G|/|C_G(A)|$ element. Vi skriver upp vilka ekvationer som behöver gälla för att en matris i G skall kommutera med A och får

$$\begin{pmatrix} x_1 & x_2 & x_3 \\ 0 & x_4 & x_5 \\ 0 & 0 & x_6 \end{pmatrix} \begin{pmatrix} 2 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 & x_2 & x_3 \\ 0 & x_4 & x_5 \\ 0 & 0 & x_6 \end{pmatrix}$$

dvs

$$\begin{pmatrix} 2x_1 & x_1 + x_2 & x_2 + x_3 \\ 0 & x_4 & x_4 + x_5 \\ 0 & 0 & x_6 \end{pmatrix} = \begin{pmatrix} 2x_1 & 2x_2 + x_4 & 2x_3 + x_5 \\ 0 & x_4 & x_5 + x_6 \\ 0 & 0 & x_6 \end{pmatrix}.$$

Alltså får vi

$$\begin{array}{rcccc} x_1 & +2x_2 & & +2x_4 & = 0 \\ & x_2 & +2x_3 & & = 0 \\ & & & x_4 & +2x_5 = 0 \\ & & & & +2x_6 = 0 \end{array}$$

Vi kan välja x_3 och x_5 godtyckligt och $x_6 \neq 0$, vilket ger $3 \cdot 3 \cdot 2 = 18$ möjligheter. Sedan kommer en tredjedel av lösningarna att ha $x_1 = 0$ och vi får därmed 12 matriser i G som kommuterar med A . Alltså finns $216/12 = 18$ matriser som är konjugerade med A .

För att kunna kontrollera eventuella andra lösningsmetoder kommer här en lista på dessa arton matriser.

$$\begin{pmatrix} 2 & 2 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 1 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 1 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 2 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}, \\ \begin{pmatrix} 2 & 2 & 2 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 2 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 1 & 2 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 & 2 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}, \\ \begin{pmatrix} 2 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 2 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 1 & 2 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 & 2 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 2 & 2 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}.$$

Bedömningskriterier.

- a) Korrekt definition av Sylowdelgrupp, **1 poäng**.
 - b) – Korrekt krav på antalet Sylowdelgrupper, **1 poäng**
– Korrekt antal Sylowdelgrupper, **1 poäng**
 - c) – Korrekt formulering av Cauchys sats, **1 poäng**
– Korrekt bevis av Cauchys sats, **1 poäng**
 - d) – Korrekt användning av struktursatsen för ändliga abelska grupper, **1 poäng**
– Korrekt motiverad slutsats om antalet abelska grupper av ordning 60, **1 poäng**
 - e) – Korrekt användning av relation mellan centralisator och element i konjugatklassen, **1 poäng**
– Korrekt motiverat antal element i konjugatklassen, **1 poäng**
-

- (3) a) Definiera vad som menas med ett maximalideal i en ring. (1)
 b) Visa att $k[x]/(f(x))$ är en kropp om $f(x)$ är ett irreducibelt polynom och k är en kropp. (2)
 c) Låt R vara en kommutativ ring. Visa att $I = \bigcup_{n=1}^{\infty} I_n$ är ett ideal i R om $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$ är en kedja av ideal i R . (2)
 d) Låt k vara en kropp och antag att $a_0 a_n \neq 0$. Visa att $a_0 + a_1 x + \dots + a_n x^n$ är irreducibelt i $k[x]$ om och endast om $a_n + a_{n-1} x + \dots + a_0 x^n$ är irreducibelt. (2)
 e) Vilka polynom $f(x)$ i $\mathbb{R}[x]$ är sådana att

$$\mathbb{R}[x]/(f(x)) \cong \mathbb{R} \times \mathbb{C}$$

som ringar?

(2)

a). Ett maximalideal I i en ring R är ett äkta ideal som inte är innehållet i något annat äkta ideal.

b). För varje polynom $g(x)$ i $k[x]$ gäller antingen att $f(x)$ delar $g(x)$ eller att $f(x)$ och $g(x)$ saknar gemensamma delare, dvs att 1 är den största gemensamma delaren. Detta innebär att vi kan använda euklides algoritmen för att få fram polynom $\lambda(x)$ och $\mu(x)$ så att

$$1 = \lambda(x)g(x) + \mu(x)f(x)$$

vilket innebär att $\overline{\lambda(x)g(x)} = 1$ i $k[x]/(f(x))$. Alltså har vi visat att alla nollskilda element i $k[x]/(f(x))$ är inverterbara, dvs att $k[x]/(f(x))$ är en kropp. (Observera att vi behöver att k är en kropp för att kunna använda euklides algoritmen. Annars kan vi bara dela med polynom med inverterbar ledande koefficient.)

c). Först visar vi att I är slutet under addition. Om $a \in I$ och $b \in I$ så finns heltal m och n sådana att $a \in I_m$ och $b \in I_n$. Om $\ell = \max\{m, n\}$ så har vi att $a, b \in I_\ell$ och eftersom I_ℓ är ett ideal gäller att $a + b \in I_\ell \subseteq I$.

Vi ser nu på multiplikation av $a \in I$ med ett element $b \in R$. Vi har att $a \in I_m$ för något m och eftersom I_m är ett ideal gäller att $ab \in I_m \subseteq I$.

Påståendet är sant även utan antagandet om att R är kommutativ.

d). Vi kan skriva $f(x) = a_0 + a_1 x + \dots + a_n x^n$ och $g(x) = a_n + a_{n-1} x + \dots + a_0 x^n$ och får att

$$f(x) = x^n g(1/x).$$

Om $g(x) = h(x)\ell(x)$ där $h(x)$ har grad $0 < m < n$ så får vi

$$f(x) = x^n h(1/x)\ell(1/x) = x^m h(1/x) \cdot x^{n-m} \ell(1/x)$$

vilket är en faktorisering av $f(x)$ i två icke-konstanta polynom. Alltså är $f(x)$ irreducibelt om och endast om $g(x)$ är irreducibelt.

e). Vi kan skriva $f(x)$ som en produkt av irreducibla faktorer. De irreducibla faktorerna kan ha grad 1 eller 2 på grund av algebrans fundamentalsats. Om vi skriver $f(x) = p_1(x)^{n_1} p_2(x)^{n_2} \cdots p_m(x)^{n_m}$ där $p_i(x)$ är polynom av grad ett eller två som saknar gemensamma delare får vi enligt kinesiska restsatsen att

$$\mathbb{R}[x]/(f(x)) \cong \mathbb{R}[x]/(p_1(x)^{n_1}) \times \mathbb{R}[x]/(p_2(x)^{n_2}) \times \cdots \times \mathbb{R}[x]/(p_m(x)^{n_m}).$$

Eftersom $\mathbb{R}[x]/(f(x))$ har dimension n som vektorrum över \mathbb{R} om $f(x)$ har grad n ser vi att $f(x)$ måste ha grad tre för att kvoten ska vara isomorf med $\mathbb{R} \times \mathbb{C}$. Om $f(x)$ har någon upprepad faktor skulle finnas nilpotenta element, vilket saknas i $\mathbb{R} \times \mathbb{C}$. Om $f(x)$ har tre olika linjära faktorer blir kvoten isomorf med $\mathbb{R} \times \mathbb{R} \times \mathbb{R}$. Alltså måste $f(x) = g(x)h(x)$ där $g(x)$ är en linjär faktor och $h(x)$ ett irreducibelt polynom. Därmed kan vi skriva

$$f(x) = a(x - b)((x - c)^2 + d^2)$$

där a, b, c och d är reella tal.

Att $\mathbb{R}[x]/(h(x)) \cong \mathbb{C}$ för alla irreducibla andragsgradspolynom $h(x)$ ser man genom att $\mathbb{R}[x]/(f(x))$ är en kropp som innehåller \mathbb{R} och ett komplext icke-reellt tal α . Då kan varje annat komplext tal skrivas som $\lambda + \mu\alpha$ där λ och μ är reella. Alltså innehåller $\mathbb{R}[x]/(h(x))$ \mathbb{C} som en delkropp och på grund av att vektorrumsdimensionen över \mathbb{R} är två måste det vara likhet.

Bedömningskriterier.

- a) Korrekt definition av maximalideal, **1 poäng**.
- b)
 - Korrekt användning av euklides algoritm, **1 poäng**
 - Korrekt slutfört bevis av att ringen är en kropp, **1 poäng**
- c)
 - Korrekt hantering av att I är slutet under addition, **1 poäng**
 - Korrekt slutfört bevis av att I är ett ideal, **1 poäng**
- d)
 - Korrekt relation mellan de båda polynomen, **1 poäng**
 - Korrekt slutfört bevis av påståendet, **1 poäng**
- e)
 - Korrekt användning av kinesiska restsatsen, **1 poäng**
 - Korrekt slutsats om vilka polynom som uppfyller kravet, **1 poäng**