Matematiska Institutionen
KTH

Lösningar till tentamensskrivning på kursen Diskret Matematik, moment B, för D2 och F, SF1631 och SF1630, den 21 maj 2008.

DEL I

1. (3p) Betrakta gruppen $G = (Z_{30}, +)$. Är mängden

$$H = \{0, 3, 7, 17, 10, 27, 2, 5, 29\},$$

en delgrupp till G?

(**OBS:** Glöm ej att motivera!)

Lösning: Antal element i H är nio och talet nio delar inte antalet element i gruppen G. Enligt Lagranges sats kan inte H då vara en delgrupp till G.

2. (3p) Avgör om polynomet $x^2 + x + 1$ är irreducibelt i polynomringen $Z_5[x]$.

Lösning: Om polynomet $p(x) = x^2 + x + 1$ vore irreducibelt skulle det, eftersom dess grad är två, med nödvändighet ha två faktorer av grad 1, och därmed nollställen i Z_5. Vi testar nu om polynomet har nollställen:

$$\begin{aligned}
&p(0) = 0^2 + 0 + 1 = 1 \neq 0,\\
&p(1) = 1^2 + 1 + 1 = 3 \neq 0,\\
&p(2) = 2^2 + 2 + 1 = 2 \neq 0,\\
&p(3) = p(-2) = (-2)^2 + (-2) + 1 = -2 \neq 0,\\
&p(4) = p(-1) = (-1)^2 + (-1) + 1 = 1 \neq 0.
\end{aligned}$$

Vi fann just att nollställen saknas till $p(x)$ i ringen Z_5 och därmed är polynomet irreducibelt.

SVAR: Polynomet är irreducibelt.

3. (3p) Mängden av enheter (eng: units) i ringen Z_{18} bildar en grupp G. Avgör om G är en cyklisk grupp.

Lösning: Ett element a i Z_{18} är en enhet om och endast om $sgd(a, 18) = 1$. Detta ger att enheterna i Z_{18} är elementen

$$G = U(Z_{18}) = \{1, 5, 7, 11, 13\}.$$

Antalet element i gruppen G är sex och då är G cyklisk om och endast om G har ett element av ordning sex, dvs det finns $g \in G$ sådant att $\sigma(g) = 6$, där $\sigma(g)$ betecknar ordningen av elementet g.

Vi vet att allmänt gäller i alla grupper G och för alla element $g \in G$ att $\sigma(g) \mid |G|$. Vi finner att för elementet $5 \in U(Z_{18})$ så gäller

$$5^2 = 7 \neq 1, \qquad 5^3 = 5 \cdot 5^2 = 5 \cdot 7 = 17 \neq 1.$$

Eftersom elementet 5 varken har ordning 2 eller 3 så måste dess ordning vara 6. Vår slutsats blir alltså

SVAR: Gruppen G är cyklisk.

4. (3p) Den e-felsrättande koden C har kontrollmatrisen (eng: (parity) check matrix)

$$H = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

   (a) Bestäm e. (**OBS:** Glöm ej att ge en kortfattad motivering!)

   Lösning: Kodens minimiavstånd är tre eftersom, dels kolonnerna är olika och dels både nollordet 000000 och ordet 000111 (se nedan) tillhör koden C. Koden kan då rätta högst ett fel och därmed är $e = 1$.
   SVAR: $e = 1$.

   (b) Bestäm ett ord $\bar{c} \in C$ sådant att $\bar{c} \neq \bar{0}$.

   Lösning: Ordet $\bar{c} = 000111$ tillhör koden eftersom summan av de tre sista kolonnerna i H är lika med nollkolonnen, eller ekvivalent:

$$H \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

   (c) Går ordet 111001 att rätta.

   Lösning: Då

$$H \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix},$$

   vilket är den första kolonnen i matrisen H så gäller att om ändrar vi ettan i ordets första position till en nolla får vi ordet 011001 och

$$H \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix},$$

   dvs ordet 011001 tillhör C och ligger på avståndet ett från det givna ordet.
   SVAR: Ordet 111001 kunde rättas till ordet 011001.

5. (3p) Bestäm antalet olika sätt att färga kanterna i en regelbunden 6-hörning med högst k olika färger. Man kan vrida och vända på 6-hörningen, men inte flytta om kanterna genom att ha sönder 6-hörningen.

   Lösning: Vi numrerar kanterna med siffrorna 1, 2, 3, 4, 5, 6. Låt G beteckna mängden, och gruppen, av alla vridningar och vändningar av sexhörningen. Vi tillämpar den sk Burnsides lemma som säger att antalet banor, vilket är det vi söker, ges av formeln

$$|\mathcal{O}| = \frac{1}{|G|} \sum g \in G|Fix(g)|,$$

där $Fix(g)$ är mängden av färläggningar som fixeras vid vridningen (vändningen) $g \in G$.

Gruppen G består av 12 element. Vi bestämmer nu dessa: Sidan 1 vrids till någon sida, sidan k, och det finns då två möjligheter för grannsidan till sidan 1, dvs sidan 2, antingen blir den sidan $k+1$ eller sidan $k-1$, dvs med nödvändighet någon av sidan k:s grannar. Den första av dessa vridningar kallar vi för φ_k och den andra för ψ_k.

Vi gör en tabell över elementen $g \in G$ och motsvarande tal $|Fix(g)|$:

$g \in G$	$\lvert Fix(g)\rvert$
$\varphi_1 = (1)(2)(3)(4)(5)(6)$	k^6
$\varphi_2 = (1\ 2\ 3\ 4\ 5\ 6)$	k
$\varphi_3 = (1\ 3\ 5)(2\ 4\ 6)$	k^2
$\varphi_4 = (1\ 4)(2\ 5)(3\ 6)$	k^3
$\varphi_5 = (1\ 5\ 3)(2\ 6\ 4)$	k^2
$\varphi_6 = (1\ 6\ 5\ 4\ 3\ 2)$	k
$\psi_1 = (1)(2\ 6)(3\ 5)(4)$	k^4
$\psi_2 = (1\ 2)(3\ 6)(4\ 5)$	k^3
$\psi_3 = (1\ 3)(2)(4\ 6)(5)$	k^4
$\psi_4 = (1\ 4)(2\ 3)(5\ 6)$	k^3
$\psi_5 = (1\ 5)(2\ 4)(3)(6)$	k^4
$\psi_6 = (1\ 6)(2\ 5)(3\ 4)$	k^3

Observera att sidor i samma cykel måst ges samma färg om färgläggningen skall fixeras av motsvarande vridning och eventuell vändning. Burnsides lemma ger nu direkt

SVAR: Antal olika färgläggningar är

$$\frac{1}{12}(k^6 + 3k^4 + 4k^3 + 2k^2 + 2k).$$

DEL II

6. (3p) Låt F beteckna den minsta ändlig kroppen med q element där $q > 3$:

$$F = \{\alpha_1, \alpha_2, \ldots, \alpha_q\}.$$

Skriv upp additions- och multiplikationstabeller för F.

Lösning: I detta fall blir q lika med 4 eftersom 4 är det minsta tal större än tre som antingen är en potens av ett primtal eller ett primtal. Följande mängd blir en kropp med fyra element

$$F_4 = \{a + bx \mid a, b \in Z_2\},$$

där man räknar som om $x^2 + x + 1 = 0$, eller $x^2 = x + 1$, eftersom polynomet $x^2 + x + 1$ är irreducibelt.

Vi låter nu

$$\alpha_1 = 0, \quad \alpha_2 = 1, \quad \alpha_3 = x, \quad \alpha_4 = 1 + x,$$

och får tabellerna

$+$	α_1	α_2	α_3	α_4
α_1	α_1	α_2	α_3	α_4
α_2	α_2	α_1	α_4	α_3
α_3	α_3	α_4	α_1	α_2
α_4	α_4	α_3	α_2	α_1

$\cdot$	α_1	α_2	α_3	α_4
α_1	α_1	α_1	α_1	α_1
α_2	α_1	α_2	α_3	α_4
α_3	α_1	α_3	α_4	α_2
α_4	α_1	α_4	α_2	α_3

7. (4p) Låt G beteckna gruppen

$$G = (Z_2, +) \times (Z_3, +) \times (Z_4, +).$$

Bestäm samtliga delgrupper med fyra element till G och avgör vilka av dessa som är isomorfa med varandra.

Lösning: Ett element (a, b, c) där $b \neq 0$ kommer att ha en ordning som delas av 3 eftersom om $b \neq 0$ så har b en ordning i $(Z_3, +)$ som är 3. Eftersom inget element i en grupp H med fyra element har en ordning som delas av talet tre så vet vi nu att om $(a, b, c) \in H$, där H är en delgrupp till G, så gäller att $b = 0$. Elementen i en grupp med fyra element har antingen ordning ett, två eller fyra. Vi undersöker nu ordningarna hos de element (a, b, c) i G där $b = 0$:

$$\begin{aligned}
\sigma((1,0,0)) &= 2\\
\sigma((1,0,1)) &= 4\\
\sigma((1,0,2)) &= 2\\
\sigma((1,0,3)) &= 4\\
\sigma((0,0,1)) &= 4\\
\sigma((0,0,2)) &= 2\\
\sigma((0,0,3)) &= 4\\
\sigma((0,0,0)) &= 1.
\end{aligned}$$

Element av ordning fyra genererar cykliska delgrupper med fyra element. Vi får två stycken:

$$H_1 = \{(0,0,0), (1,0,1), (0,0,2), (1,0,3)\} \quad \text{och} \quad H_2 = \{(0,0,0), (0,0,1), (0,0,2), (0,0,3)\}.$$

I dessa grupper finns nu samtliga element av ordning fyra med, så inga fler cykliska delgrupper med fyra element finns.

En grupp med fyra element varav inget har ordning fyra består av identitetselementet och tre element av ordning två. Enda möjligheten till en sådan grupp är i vårt fall

$$H_3 = \{(0,0,0), (1,0,0), (1,0,2), (0,0,2)\},$$

och det är lätt att verifiera att denna mängd är en delgrupp till G. Lika stora cykliska grupper är alltid isomorfa, och grupper med samma antal element men med en inte iöverensstämmande uppsättning ordningar av elementen kan aldrig vara isomorfa. Nu har vi

SVAR: Grupperna H_1, H_2 och H_3 enligt ovan varav H_1 och H_2 är isomorfa.

8. (4p) Låt $\mathcal{S}_5$ beteckna mängden av permutationer på en mängd med fem element. Bestäm en delgrupp med 12 element till $\mathcal{S}_5$.

Lösning: Vi använder att mängden av jämna permutationer i gruppen $\mathcal{S}_4$ bildar en delgrupp $\mathcal{A}_4$ till $\mathcal{S}_4$ och att denna delgrupp $\mathcal{A}_4$ innehåller precis 12 element. Vidare kan vi uppfatta $\mathcal{S}_4$ some en delgrupp till $\mathcal{S}_5$, nämlgen de permutationer φ i $\mathcal{S}_5$ för vilka elementet 5 fixeras, dvs $\varphi(5) = 5$.

SVAR De permutationer $\varphi \in \mathcal{S}_4$ som är jämna och sådana att $\varphi(5) = 5$.

Anm. Det finns givetvis många andra delgrupper till $\mathcal{S}_5$ som har 12 element.

DEL III

Om du i denna del använder eller hänvisar till satser från läroboken skall dessa citeras, ej nödvändigvis ordagrant, där de används i lösningen.

9. (a) (2p) Betrakta gruppen $G = (Z_{20}, +)$. Bestäm två olika delgrupper H och K till G med sidoklasser $a + H$ och $b + K$, där $a \notin H$ och $b \notin K$, sådana att

$$|(a + H) \cap (b + K)| = 2.$$

Lösning: Låt

$$H = \{0, 5, 10, 15\} \qquad \text{och} \qquad K = \{0, 10\},$$

och låt $a = b = 7$. Då har vi

$$7 + H = \{7, 12, 17, 22\} \qquad \text{och} \qquad 7 + K = \{7, 17\}.$$

(b) (3p) Betrakta nu en abelsk grupp G, vilken som helst. Gäller det generellt att om H_1 och K_1 är sidoklasser till delgrupper H och K till G så måste antalet element i $H_1 \cap K_1$ antingen vara noll eller dela antalet element i G, dvs

$$|H_1 \cap K_1| = m \quad \text{och} \quad |G| = n \qquad \Longrightarrow \qquad m = 0 \quad \text{eller} \quad m \mid n.$$

(Givetvis skall svaret motiveras på ett lämpligt sätt.)

Lösning: Vi tillåter oss skriva gruppoperationen som $+$ eftersom gruppen förutsättes vara abelsk. Det gäller allmänt att om c och d båda tillhör samma sidoklass L_1 till en delgrupp L till en grupp G så är

$$L_1 = c + L = d + L.$$

Detta ger att för varje $d \in L_1$ så gäller att $(-d) + L_1 = L$, eftersom

$$(-d) + L_1 = (-d) + d + L = \{(-d) + (d + h) \mid h \in L\} =$$

$$\{(-d + d) + h \mid h \in L\} = \{h \mid h \in L\} = L.$$

Antag nu att $H_1 \cap K_1 \neq \emptyset$ och låt $a \in H_1 \cap K_1$. Då a tillhör både sidoklassen H_1 till H och sidoklassen K_1 till K så har vi alltså att

$$(-a) + H_1 = H \qquad \text{och} \qquad (-a) + K_1 = K,$$

och

$$x \in H_1 \cap K_1 \quad \Longrightarrow \quad (-a) + x \in H \cap K.$$

Dessutom gäller att $x_1 \neq x_2 \Rightarrow (-a) + x_1 \neq (-a) + x_2$ och därmed

$$|H_1 \cap K_1| \leq |H \cap K|.$$

Vidare om $h_1 \neq h_2$ är element i $H \cap K$ så måste $a + h_1 \neq a + h_2$ och alltså, eftersom $H_1 = a + H$ och $K_1 = a + K$ har vi att

$$|H_1 \cap K_1| \geq |H \cap K|.$$

Nu vet vi att

$$|H_1 \cap K_1| = |H \cap K|.$$

Eftersom H och K är delgrupper till G så är också $H \cap K$ en delgrupp till G och därmed enligt Lagranges sats har vi att antalet element i $H \cap K$ delar antalet element i G. Så

SVAR: Ja, antingen är $|H_1 \cap K_1| = 0$ eller så delar antalet element i $H_1 \cap K_1$ antalet element i G.

10. (a) (2p) Undersök om det existerar något element α i kroppen F_{1024} med 1024 element sådant att polynomet $z^3 + \alpha$ är irreducibelt i polynomringen $F_{1024}[z]$.

Lösning: Multiplikativa gruppen i kroppen F_{1024} består av 1023 element och genereras av ett element γ, dvs

$$(F_{1024} \setminus \{0\}, \cdot) =< \gamma >= \{\gamma, \gamma^2, \gamma^3, \ldots, \gamma^{1023} = (\gamma^3)^{341} = 1\}.$$

Om $-\alpha$ inte är någon trepotens i $< \gamma >$ så saknar det givna polynomet nollställen och kommer att vara irreducibelt. Så vilka är trepotenerna i $< \gamma >$? De är

$$\{(\gamma^k)^3 \mid k = 1, 2, 3, \ldots, 1023\} = \{(\gamma^3)^k \mid k = 1, 2, 3, \ldots, 1023\} =$$

$$\{(\gamma^3)^k \mid k = 1, 2, 3, \ldots, 341\},$$

eftersom $1023 = 3 \cdot 341$. Precis en tredjedel av de nollskilda elementen i F_{1024} är trepotenser och två tredjedelar av elementen duger som kanditater till elementet α.

(b) (3p) En kropp med p^3 stycken element skall konstrueras där p är ett stort primtal. Så du behöver ett irreducibelt polynom $p(x)$ av grad 3 i polynomringen $Z_p[x]$. Emellertid har du bara några minuter på dig så du är tvungen att gissa på ett polynom $p(x)$. Är sannolikheten för alla typer av polynom av grad tre att vara irreducibla lika stor eller beror sannolikheten för ett polynom av grad tre och av viss typ att vara irreducibelt på primtalet p?
(**Anm.** Frågan är kanske lite luddigt formulerad och kanske det inte finns något rätt svar på denna deluppgift, men antagligen mer eller mindre kloka och mer eller mindre väl motiverade strategier för att gissa på ett polynom $p(x)$.)

Lösning: Först kontrollerar vi lätt om $p - 1$ är delbart med tre med hjälp av egenskapen att ett tal är delbart med tre precis då dess siffersumma är delbar med tre. Om $p - 1$ är delbart med tre så är vart tredje element en trepotens, jfr lösningen till deluppgift a), och en gissning på ett polynom av typen $z^3 + a$ har sannolikheten 0.66 att ge ett irreducibelt polynom.
Låt nu γ vara en generator till den multiplikativa gruppen med $p - 1$ element till kroppen med p element. Om $3 \not| (p - 1)$ så finns i ringen Z_{p-1} en invers till elementet 3, och ekvationen $3x = m$ är lösbar för varje element m i denna ring. Detta ger att till varje element $a = \gamma^m$ så finns ett element $\alpha = \gamma^x$ sådant att

$$a = \gamma^{3x} = (\gamma^x)^3 = \alpha^3,$$

och vi sluter att inget polynom $z^3 - a$ kommer att vara irreducibelt.
Betrakta nu ett allmänt tredjegradspolynom $q(z) = z^3 + az^2 + bz + c$. Med hjälp av substitutionen $z = (w - \frac{a}{3})$ kan $q(z)$ omformas till ett polynom av typen

$$q(w - a) = w^3 + rw + s.$$

(**Anm.** Denna omformning är ej nödvändig att genomföra för att man skall få full poäng på uppgiften.)
Om $s = 0$ är detta polynom ej irreducibelt, ty $w^3 + rw = w(w^2 + r)$. Om $r = 0$ och $3 \not| (p-1)$ så är polynomet ej heller irreducibelt, enligt vårt resonemang ovan. Vår slutsats blir alltså
SVAR: Om $3 \mid (p - 1)$ chansar vi med ett polynom $z^3 + a$, där $a \neq 1$. Om $3 \not| (p - 1)$ chansar vi på ett polynom $z^3 + sz + r$ med $s \neq 0$ och $r \neq 0$. Mer kommer ej heller att gå att säga generellt eftersom hur elementen 1,2,3,4, ... uppför sig i kropparna Z_p är helt beroende av talet p.