

Lösningar tenta TENB SF1630(/1631) DISKRET MATEMATIK, D3 m.fl.

13 januari 2016

Tryckfel kan förekomma.

- 1a) (1p) $(G, \circ)$ är en grupp omm 1. $(x \circ y) \circ z = x \circ (y \circ z)$ för alla $x, y, z \in G$ (associativitet),
 2. Det finns $e \in G$ sådant att $e \circ x = x \circ e = x$ för alla $x \in G$ (identitetsselement) och
 3. För varje $x \in G$ finns $x^{-1} \in G$ med $x \circ x^{-1} = x^{-1} \circ x = e$ (inverselement).
 (Villkoret om slutenhets behövs inte, eftersom vi förutsatt att $\circ : G \times G \rightarrow G$.)
 b) (1p) Gruppen $(G, \circ)$ är abelsk omm $a \circ b = b \circ a$ för alla $a, b \in G$.
 c) (1p) En delmängd till en grupp $(G, *)$ är en högersidoklass till delgruppen H i G omm den är av form $H * g = \{h * g \mid h \in H\}$ för något $g \in G$.

- 2a) (1p) Banan för $x \in X$ är $Gx = \{gx \mid g \in G\}$ (gx är resultatet av g 's verkan på x).
 b) (1p) Om $x \in X$ har banan Gx och stabilisatorn G_x gäller $|G| = |Gx| \cdot |G_x|$.
 c) (1p) Nej. $1, -1 \in \mathbb{Q} \setminus \{0\}$ och $1 + (-1) = 0 \notin \mathbb{Q} \setminus \{0\}$, så $(\mathbb{Q} \setminus \{0\}, +, \cdot)$ är inte en ring.

- 3a) (1p) Av $k \in \{5, 6, \dots, 30\}$ finns en kropp F med $|F| = k$ omm
 $k \in \{5, 7, 8, 9, 11, 13, 16, 17, 19, 23, 25, 27, 29\}$ (alla $k = p^n$, p primtal, $n \in \mathbb{Z}_+$).
 b) (1p) Karakteristiken för $(F, +, \cdot)$ är ordningen för den additiva delgruppen $\langle 1 \rangle$ som genereras av 1 (om, i oändlig F , $|\langle 1 \rangle| = \infty$, sägs karakteristiken vara 0).
 c) (1p) $f \in F$ är ett primitivt element i kroppen $(F, +, \cdot)$ omm f är en generator för gruppen $(F \setminus \{0\}, \cdot)$.

- 4a) (1p) Kontrollmatrisen H ger en linjär kod som rättar minst ett fel omm alla H 's kolonner är olika och skilda från $\mathbf{0}$ (kolonnen med alla element 0).
 b) (1p) Om $n = p \cdot q$ (p, q primtal) bestäms d av $e \cdot d \equiv_m 1$, där $m = (p-1)(q-1)$.
 c) (1p) Fermattestet med bas b ($b \in \mathbb{Z}_+$, $b < N$) för att avgöra om $N \in \mathbb{Z}_+$ är ett primtal: Är $b^{N-1} \equiv 1 \pmod{N}$? Om svaret är "nej" är N inte ett primtal.

- 5) (3p) Vi vet att $x^2a = bxc^{-1}$ och $acx = xac$, där $a, b, c, x \in G$, en grupp. Vi skall uttrycka x i a, b, c .

Lösning:

$$x^2a = bxc^{-1} \stackrel{\cdot c}{\Rightarrow} x^2ac = bx \stackrel{acx = xac}{\Rightarrow} xacx = bx \stackrel{\cdot x^{-1}}{\Rightarrow} xac = b \stackrel{\cdot (ac)^{-1}}{\Rightarrow} x = b(ac)^{-1}.$$

Svar: $x = b(ac)^{-1} (= bc^{-1}a^{-1})$.

- 6) G är gruppen av rotationssymmetrier för en ikosaeder. Vi söker (a, 1p) $|G|$ och (b, 2p) alla storlekar på banor för G 's verkan på punkter i rummet.

Lösning:

Varje hörn i ikosaedern kan tas till varje hörn av element i G och hörnet hålls fixt av fem symmetrirotationer kring axeln genom medelpunkten och hörnet och bara av dem, så om x är ett hörn fås $|G| = |Gx| \cdot |G_x| = 12 \cdot 5 = 60$.

Om x är ikosaederns medelpunkt m är $|Gx| = 1$ (den ligger på alla rotationsaxlarna).

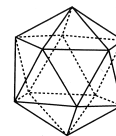
Om x är någon annan punkt på en axel genom ett hörn har den $|G_x| = 5$ och $|Gx| = \frac{|G|}{|G_x|} = 12$.

$x \neq m$ på en axel genom en kants mittpunkt har $|G_x| = 2$, så $|Gx| = 30$.

$x \neq m$ på en axel genom mittpunkten av en sida har $|G_x| = 3$, så $|Gx| = 20$.

övriga punkter fixeras inte av något $g \in G \setminus \{id\}$, så $|G_x| = 1$ och $|Gx| = 60$.

Svar a: $|G| = 60$, b: Banorna har storlekarna 1, 12, 20, 30 och 60.



En ikosaeder

7) (3p) Vi skall faktorisera $f(x) = x^5 + x^3 + 2x^2 + x + 4 \in \mathbb{Z}_5[x]$ i irreducibla faktorer.

Lösning:

Vi söker först linjära faktorer. Enligt faktorsatsen motsvarar de precis nollställena till $f(x)$. Man finner $f(0) = f(1) = f(2) = 4$, men $f(3) = 0$. Så $x - 3 = x + 2$ är en faktor i $f(x)$.

Division ger $f(x) = (x + 2)g(x)$, där $g(x) = x^4 + 3x^3 + 2x + 2$.

$x + 2$ är irreducibelt, men vi försöker faktorisera $g(x)$. $g(0), g(1), g(2) \neq 0$ (ty $f(0), f(1), f(2) \neq 0$), men $g(3) = 0$ och vi finner $g(x) = (x + 2)h(x)$, där $h(x) = x^3 + x^2 + 3x + 1$.

$h(3) = 1, h(4) = 3$, så $h(x)$ irreducibelt ($\deg h(x) = 3$, så varje icke-trivial faktorisering måste ha en förstgradsfaktor).

Svar: $f(x) = (x + 2)^2(x^3 + x^2 + 3x + 1)$, där faktorerna är irreducibla i $\mathbb{Z}_5[x]$.

8) $H = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix}$ är kontrollmatrisen för en linjär, binär kod. Vi söker (a, 2p) antalet ord i koden och (b, 1p) antalet ord som inte kan fås med högst ett fel i ett kodord.

Lösning:

a. H :s tre rader är linjärt oberoende (ses t.ex. av de tre först kolonnerna), så kodens dimension är $k = n - \text{rank } H = 5 - 3 = 2$ och antalet ord $2^k = 4$.

b. Eftersom alla kolonner i H är olika och nollskilda rättar koden ett fel. Till varje kodord hör sex ord (kodordet själv och de fem ord som fås ur det med ett fel) och inget ord hör så till två olika kodord (eftersom koden rättar ett fel). Totala antalet ord som fås ur kodord med högst ett fel är alltså $4 \cdot 6$ och de sökta är resten, $2^5 - 4 \cdot 6 = 8$ st.

(Alt: De som innehåller mer än ett fel är precis de som löser $H\mathbf{x} = \mathbf{c}$, där $\mathbf{c}$ är en av de två nollskilda kolonner som inte ingår i H . Fyra lösningar för varje $\mathbf{c}$.)

Svar a: Koden innehåller 4 ord, b: Det finns 8 sådana ord.

9) $\pi, \sigma \in S_8$ är $\pi = (17568)(234)$ och $\sigma = (1478653)$. H är mängden av produkter av π :n och σ :n och vi skall visa (a, 2p) att H är en delgrupp till S_8 och (b, 2p) att $|H| \geq 420$.

Lösning:

a. För att visa att H är en delgrupp räcker det (enligt känd sats, H är ju ändlig ($H \subseteq S_8$ och $|S_8| = 8!$)) att visa S0. $H \neq \emptyset$ och S1. $a, b \in H \Rightarrow ab \in H$.

S0: $id \in H$, S1: om a och b båda är ändliga produkter av π :n och σ :n är ab också det.

b. Ordningen för en permutation är mgm av dess cykellängder, så $o(\pi) = \text{mgm}(5, 3) = 15$ och $o(\sigma) = 7$. Det räcker inte för den önskade slutsatsen, men $\pi\sigma = (17568)(234)(1478653) = (1237)(45) \in H$ har ordningen $o(\pi\sigma) = \text{mgm}(4, 2) = 4$.

Ordningen för ett element i en grupp delar alltid gruppens ordning, så $15, 7, 4 \mid |H|$, vilket medför $\text{mgm}(15, 7, 4) = 15 \cdot 7 \cdot 4 = 420 \mid |H|$, så ($|H| \geq 1 \Rightarrow |H| \geq 420$). **Sakerna är klara.**

10) Vi skall avgöra om varje vänstersidoklass A till en delgrupp H till gruppen G måste vara högersidoklass till någon delgrupp H' till G .

Lösning:

Låt $A = gH = \{gh \mid h \in H\}$ och $H' = gHg^{-1} = \{ghg^{-1} \mid h \in H\}$.

Då är $H'g = \{h'g \mid h' \in H'\} = \{ghg^{-1}g \mid h \in H\} = gH$ och eftersom H' är en delgrupp till G (S0. $1 = g1g^{-1} \in H'$, S1. $h_1, h_2 \in H \Rightarrow (gh_1g^{-1})(gh_2g^{-1}) = gh_1h_2g^{-1} \in H'$,

S2. $h \in H \Rightarrow (ghg^{-1})^{-1} = (g^{-1})^{-1}h^{-1}g^{-1} = gh^{-1}g^{-1} \in H'$) är svaret på frågan "ja".

Svar a: Ja, $gH = H'g$ om $H' = gHg^{-1}$, en delgrupp till G .

11) Vi ska (a, 2p) visa att $k(x) = x^5 + x^2 + 1 \in \mathbb{Z}_2[x]$ är irreducibelt och (b, 2p) finna $(\alpha^2 + 1)^{-1}$ i F då $F = \mathbb{Z}_2[x]/(k(x))$ och α är restklassen som innehåller polynomet x .

Lösning:

a. Om $k(x)$ vore reducibelt (dvs vore en produkt av två icke-konstanta polynom) skulle det ha en förstgradsfaktor eller en irreducibel andragradsfaktor.

$k(x)$ har inget nollställe ($k(0) = k(1) = 1$), så enligt faktorsatsen ingen förstgradsfaktor.

Det enda irreducibla andragradspolynomet i $\mathbb{Z}_2[x]$ är $x^2 + x + 1$ (andragrad ger $x^2 \neq 0$ då $x = 0$ ger 1 och $x^2 + 1 = (x + 1)^2$). Polynomdivision ger $k(x) = (x^2 + x + 1)(x^3 + x^2) + 1$, så inget irreducibelt andragradspolynom delar $k(x)$. **a-Saken är klar.**

b. Eftersom $k(x)$ är irreducibelt är $\text{sgd}(k(x), x^2 + 1) = 1$ och $(\alpha^2 + 1)^{-1}$ existerar i F .

Euklides algoritim: $k(x) = (x^2 + 1)(x^3 + x + 1) + x$, $x^2 + 1 = x \cdot x + 1$, så $1 = (x^2 + 1) + x(k(x) + (x^3 + x + 1)(x^2 + 1)) = x \cdot k(x) + (x^4 + x^2 + x + 1)(x^2 + 1)$. ($+ = -$ i $\mathbb{Z}_2[x]$.)

Det betyder att $(\alpha^2 + 1)^{-1} = \alpha^4 + \alpha^2 + \alpha + 1$ i F .

Svar b: $(\alpha^2 + 1)^{-1} = \alpha^4 + \alpha^2 + \alpha + 1$ i F .

12) Vi skall visa att (a, 2p) om p är ett primtal med $p \equiv_4 3$, så gäller $p \nmid (x^2 + 1)$ för alla $x \in \mathbb{Z}$ och (b, 3p) om p är ett primtal med $p \equiv_4 1$, så finns ett heltal x , sådant att $p \mid (x^2 + 1)$.

Lösning:

a. $p \nmid (x^2 + 1)$ innebär precis att $x^2 + 1 \neq 0$ i $\mathbb{Z}_p$. Det gäller alltså att visa att det inte finns x med $x^2 = -1$ i $\mathbb{Z}_p$ om p är ett primtal av form $4k + 3$.

I gruppen $(\mathbb{Z}_p \setminus \{0\}, \cdot)$ skulle ett sådant x ha ordning 4 (ty $x^4 = 1$, men $x^2 \neq 1$), men $4 \nmid (p - 1) = 4k + 2$, gruppens ordning. Ett sådant x finns alltså inte. **Saken är klar.**

b. Nu är p ett primtal av form $4k + 1$ och det gäller att visa att det finns ett x sådant att $x^2 = -1$ i $\mathbb{Z}_p$.

Eftersom $\mathbb{Z}_p$ är en ändlig kropp är $(\mathbb{Z}_p \setminus \{0\}, \cdot)$ en cyklisk grupp av ordning $p - 1 = 4k$ (känd sats). Låt g vara en generator för denna grupp och betrakta $x = g^k$. $x^4 = g^{4k} = 1$, men $x^2 = g^{2k} \neq 1$, eftersom g har ordning $4k$. Då är $x^2 = -1$, ty i en kropp har ekvationen $y^2 = 1$ bara lösningarna $y = 1$ och $y = -1$ (ty $y^2 - 1 = (y - 1)(y + 1)$ och i en kropp kan en produkt bara vara 0 om en faktor är det) och $y = x^2 \neq 1$ är en lösning. **Saken är klar.**

13) Två binära relationer $\mathcal{R}, \mathcal{R}'$ på en mängd X kallas **isomorfa** omm för någon bijektion $f: X \rightarrow X$ gäller att $a\mathcal{R}b \Leftrightarrow f(a)\mathcal{R}'f(b)$ för alla $a, b \in X$.

Vi söker antalet icke-isomorfa binära relationer på X , då (a, 3p) $|X| = 3$ och (b, 2p) $|X| = 4$.

Lösning:

a. En binär relation på X med $|X| = 3$ ges precis av en 0/1-matris (varje element antingen 0 eller 1) av format 3×3 och två sådana matriser beskriver isomorfa relationer omm den ena fås från den andra genom att permutera rader och kolonner med samma permutation i S_3 . Vi söker alltså antalet banor (motsvarande isomorfiklasserna av relationer) då S_3 verkar genom att permutera rader och kolonner samtidigt i 0/1-matriser av format 3×3 .

Vi använder Burnsidess lemma (Thm 21.4 i Biggs) och behöver $|F(\pi)|$ för alla $\pi \in S_3$.

$|S_3| = (3!) = 6$ och elementen har tre cykelstrukturer: $[1^3]$ (bara id), $[12]$ (3 st) och $[3]$ (2 st).

Konjugerade $\pi \in S_3$ (sådana med samma cykelstruktur) har samma $|F(\pi)|$ och vi finner för en permutation av varje typ: id fixerar varje matris, så $|F(id)| = 2^9$,

(12) fixerar en matris omm element med samma bokstav har samma värde i $\begin{bmatrix} a & b & c \\ b & a & c \\ d & d & e \end{bmatrix}$, så $|F((12))| = 2^5$ och (123) fixerar dem enligt $\begin{bmatrix} a & b & c \\ c & a & b \\ b & c & a \end{bmatrix}$, så $|F((123))| = 2^3$.

Antalet banor blir $\frac{1}{|S_3|} \sum_{\pi \in S_3} |F(\pi)| = \frac{1}{6}(2^9 + 3 \cdot 2^5 + 2 \cdot 2^3) = \frac{8}{3}(32 + 6 + 1) = 104$.

b. Som i a, men med S_4 i stället för S_3 . Vi ställer upp en tabell:

Cykelstruktur:	$[1^4]$	$[1^22]$	$[13]$	$[2^2]$	$[4]$
Antal sådana:	1	6	8	3	6
Ett sådant π :	id	(12)	(123)	$(12)(34)$	(1234)
π fixerar:	$\begin{bmatrix} a & b & c & d \\ e & f & g & h \\ i & j & k & l \\ m & n & o & p \end{bmatrix}$	$\begin{bmatrix} a & b & c & d \\ b & a & c & d \\ e & e & f & g \\ h & h & i & j \end{bmatrix}$	$\begin{bmatrix} a & b & c & d \\ c & a & b & d \\ b & c & a & d \\ e & e & e & f \end{bmatrix}$	$\begin{bmatrix} a & b & c & d \\ b & a & d & c \\ e & f & g & h \\ f & e & h & g \end{bmatrix}$	$\begin{bmatrix} a & b & c & d \\ d & a & b & c \\ c & d & a & b \\ b & c & d & a \end{bmatrix}$
$ F(\pi) $	2^{16}	2^{10}	2^6	2^8	2^4

Det ger det sökta antalet: $\frac{1}{|S_4|} \sum_{\pi \in S_4} |F(\pi)| = \frac{1}{24}(2^{16} + 6 \cdot 2^{10} + 8 \cdot 2^6 + 3 \cdot 2^8 + 6 \cdot 2^4) = 3044$.

Svar a: 104 st, b: $\frac{1}{24}(2^{16} + 6 \cdot 2^{10} + 8 \cdot 2^6 + 3 \cdot 2^8 + 6 \cdot 2^4) = 3044$ st.

(Exponenten för 2 i termen som motsvarar en viss cykelstruktur kan fås utan att betrakta matriserna "för hand".

De är antalet banor då π verkar på positionerna i matrisen enligt $(i, j) \mapsto (\pi(i), \pi(j))$. Antalet element i en sådan bana är ordningen för denna verkan, $\text{mgm}(\ell_i, \ell_j)$, där $\ell_{i,j}$ är längden av den cykel i π som i, j ingår i. Antalet banor (den sökta exponenten) är då $\sum_{i,j} \frac{1}{\text{mgm}(\ell_i, \ell_j)} = \sum \frac{\ell \cdot \ell'}{\text{mgm}(\ell, \ell')} = \sum \text{sgd}(\ell, \ell')$, där de två sista summorna tas över alla ordnade par av π -cykler och ℓ, ℓ' är längderna för de två cyklerna i paret.

T.ex. med π av typ $[1^223]$ (så $|X| = 7$) fås 16 termer, en 3:a, en 2:a, och resten 1:or, så exponenten blir 19.)