

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

20 december 2017

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 slutenhet behövs inte, eftersom vi förutsatt att $\circ : G \times G \rightarrow G$.)**b)** (1p) $|H|$ delar $|G| = 45$. Antalet sidoklasser till $|H|$ är $\frac{|G|}{|H|}$, så tänkbara är 1, 3, 5, 9, 15, 45. ($\mathbb{Z}_{45}, +$) som G visar att de alla är möjliga.**c)** (1p) Elementen i $G \times H$ är alla ordnade par (g, h) , $g \in G$, $h \in H$ och operationen $\cdot$ ges av $(g_1, h_1) \cdot (g_2, h_2) = (g_1 \circ g_2, h_1 * h_2)$.**2a)** (1p) Stabilisatorn för $x \in X$ då G verkar på X är $G_x = \{g \in G \mid gx = x\}$.**b)** (1p) Antalet banor är ("Burnsides lemma") $\frac{1}{|G|} \sum_{g \in G} |F(g)|$,
där $F(g) = \{x \in X \mid gx = x\} (= X_g)$.**c)** (1p) Varje kropp är en ring, men för att en ring $(R, +, \cdot)$ skall vara en kropp måste $(R \setminus \{0\}, \cdot)$ vara en abelsk grupp.**3a)** (1p) $(F, +)$ är isomorf med en direkt produkt av cykliska grupper, $(C_p)^r$, där p är F 's karakteristisk och $r \in \mathbb{Z}_+$. (Ekvivalent: Ett r -dimensionellt vektorrum över $\mathbb{Z}_p$.)**b)** (1p) $(F \setminus \{0\}, \cdot)$ är en cyklisk grupp av ordning $|F| - 1$.**c)** (1p) Om $f(x) \in F[x]$ är $x - \alpha$ en delare till $f(x)$ omm $f(\alpha) = 0$ i F .**4a)** (1p) H 's kolonner skall alla vara olika och inte **0**-kolonnen.**b)** (1p) Om p, q är primtal och $k \equiv_{(p-1)(q-1)} 1$ är $x^k \equiv_{p \cdot q} x$ för alla $x \in \mathbb{Z}$.**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 g i gruppen G har ordning 60 och söker ordningen för g^{78} .**Lösning:**Ordningen för g^{78} är det minsta $k > 0$ med $(g^{78})^k = g^{78k} = 1$, identitetsselementet i G .Enligt en känd sats är $g^n = 1$ omm $60 \mid n$ (eftersom g 's ordning är 60). $60 \mid 78k \Leftrightarrow 10 \mid 13k$ (ty $60 = 6 \cdot 10$, $78 = 6 \cdot 13$), så det minsta $k > 0$ som uppfyller $g^{78k} = 1$ är 10 (sgd(10, 13) = 1, så $10 \mid k$). Det betyder att g^{78} har ordning 10.**Svar: g^{78} har ordning 10.****6)** $G = A_4$ verkar elementvis på elementen i $\mathcal{P}(\{1, 2, 3, 4\})$. Vi söker banorna $G\{1\}$ och $G\{2, 3\}$ och stabilisatorerna $G_{\{1\}}$ och $G_{\{2, 3\}}$.**Lösning:**Eftersom $\pi\{1\} = \{\pi(1)\}$ har den precis ett element för alla $\pi \in G$. Alla delmängder till $\{1, 2, 3, 4\}$ med precis ett element ligger också i $G\{1\}$, ty $id\{1\} = \{1\}$, $(1\ 2\ 3)\{1\} = \{2\}$, $(1\ 3\ 2)\{1\} = \{3\}$, $(1\ 4\ 2)\{1\} = \{4\}$ (och 3-cykler ligger i A_4) så $G\{1\} = \{\{1\}, \{2\}, \{3\}, \{4\}\}$.P.s.s. $|\pi\{2, 3\}| = |\{\pi(2), \pi(3)\}| = 2$ för alla $\pi \in G$, $id\{2, 3\} = \{2, 3\}$, $(1\ 4\ 2)\{2, 3\} = \{1, 3\}$, $(1\ 3\ 2)\{2, 3\} = \{1, 2\}$, $(1\ 3\ 4)\{2, 3\} = \{2, 4\}$, $(1\ 2\ 4)\{2, 3\} = \{3, 4\}$, $(1\ 2)(3\ 4)\{2, 3\} = \{1, 4\}$ så $G\{2, 3\} = \{\{2, 3\}, \{1, 3\}, \{1, 2\}, \{2, 4\}, \{3, 4\}, \{1, 4\}\}$. $\pi\{1\} = \{1\}$ omm $\pi(1) = 1$, så $G_{\{1\}} = \{id, (2\ 3\ 4), (2\ 4\ 3)\}$. $\pi\{2, 3\} = \{2, 3\}$ omm $\pi(2) = 2$, $\pi(3) = 3$ eller $\pi(2) = 3$, $\pi(3) = 2$, så $G_{\{2, 3\}} = \{id, (1\ 4)(2\ 3)\}$.**Svar: Banorna är $G\{1\} = \{\{1\}, \{2\}, \{3\}, \{4\}\}$ och**

$$G\{2, 3\} = \{\{2, 3\}, \{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 4\}, \{3, 4\}\}.$$

Stabilisatorerna är $G_{\{1\}} = \{id, (2\ 3\ 4), (2\ 4\ 3)\}$ och $G_{\{2, 3\}} = \{id, (1\ 4)(2\ 3)\}$.

7) (3p) Vi söker den moniska största gemensamma delaren i $\mathbb{Z}_5[x]$ till $f(x) = x^4 + x^3 + 3x^2 + x + 1$ och $g(x) = x^5 + 3x^4 + 3x^3 + 3x + 4$.

Lösning:

Vi använder (förstås) Euklides algoritm.

Polynomdivision i $\mathbb{Z}_5[x]$ ger $g(x) = (x+2)f(x) + (3x^3 + 3x^2 + 2) = (x+2)f(x) + h(x)$,

$f(x) = 2x \cdot h(x) + (3x^2 + 2x + 1) = 2x \cdot h(x) + k(x)$ och $h(x) = (x+2)k(x)$.

$k(x) = 3x^2 + 2x + 1$ är alltså en sgd till $f(x)$ och $g(x)$. För att finna den moniska sgd:n multiplicerar vi med (det inverterbara elementet) 2 och får $x^2 + 4x + 2$.

Svar: Den moniska största gemensamma delaren är $x^2 + 4x + 2$.

8) Vi söker i $\mathbb{Z}_{1547}$ ($1547 = 7 \cdot 13 \cdot 17$) potenserna (a, 1p) 55^{1153} , (b, 1p) 10^{100} och (c, 1p) 26^{224} .

Lösning:

Kinesiska restsatsen och Fermats lilla sats för vart och ett av primtalen 7, 13 och 17.

a. $1153 \equiv_6 1, \equiv_{12} 1, \equiv_{16} 1$ och Fermats lilla ($7, 13, 17 \nmid 55$) ger $55^{1153} \equiv_7 55, \equiv_{13} 55, \equiv_{17} 55$, så $55^{1153} = 55$ i $\mathbb{Z}_{1547}$. (Alt. Eulers sats, $\phi(1547) = 6 \cdot 12 \cdot 16 = 1152$.)

b. $100 \equiv_6 4, \equiv_{12} 4, \equiv_{16} 4$ och Fermats lilla ($7, 13, 17 \nmid 10$) ger $10^{100} \equiv_7 10^4, \equiv_{13} 10^4, \equiv_{17} 10^4 = 10\,000$, så $10^{100} \equiv_{1547} 10\,000 \equiv_{1547} 718$.

c. $26 \equiv_7 5, \equiv_{13} 0, \equiv_{17} 9$ och $224 \equiv_6 2, \equiv_{16} 0$ och Fermats lilla ($7, 17 \nmid 26$) ger $26^{224} \equiv_7 5^2 = 25 \equiv_7 4, \equiv_{13} 0, \equiv_{17} 9^0 = 1$.

Med $x = 26^{224}$ har vi alltså $x \equiv_{13} 0, x \equiv_7 4$ och $x \equiv_{17} 1$.

Den första ger $x = 13s$ för något $s \in \mathbb{Z}$. Den andra ger då $13s \equiv_7 4$, så $0 \equiv_7 s + 4$, dvs $s = 7t + 3$ och $x = 13(7t + 3) = 91t + 39$ för något $t \in \mathbb{Z}$. Den tredje ekvationen ger $91t + 39 \equiv_{17} 6t + 5 \equiv_{17} 1$. Eftersom $\text{sgd}(3, 17) = 1$ kan vi multiplicera med 3 och får $18t + 15 \equiv_{17} t - 2 \equiv_{17} 3$, så $t = 17u + 5$ för något $u \in \mathbb{Z}$ och för varje $u \in \mathbb{Z}$ fås en lösning $x = 91(17u + 5) + 39 = 1547u + 455 + 39 \equiv_{1547} 494$.

Svar: Potenserna är a: 55, b: 718, c: 494 i $\mathbb{Z}_{1547}$.

9) (4p) Gruppen G har delgrupperna H och N , varav N är en normal delgrupp.

Vi skall visa att HN är en delgrupp till G .

Lösning:

Enligt en känd sats är $M \subseteq G$, $M \neq \emptyset$, en delgrupp till G om $x, y \in M \Rightarrow xy, x^{-1} \in M$.
 $x, y \in HN \Rightarrow x = h_1 n_1, y = h_2 n_2$ (några $h_i \in H, n_i \in N$) så $xy = h_1 n_1 h_2 n_2 = h_1 h_2 n_3 n_2 \in HN$,
 $x^{-1} = n_1^{-1} h_1^{-1} = h_1^{-1} n_4 \in HN$ (ty $N h_2 = h_2 N$ ger att $n_1 h_2 = h_2 n_3$ för något $n_3 \in N$ och motsvarande $n_1^{-1} h_1^{-1} = h_1^{-1} n_4$ för något $n_4 \in N$). $HN \neq \emptyset$, ty $1 \in H, N$ ger $1 = 1 \cdot 1 \in HN$, så HN är en delgrupp.

Saken är klar.

10) (4p) Vi skall visa att $(\text{End}(G), +, \circ)$ (o sammansättning) är en ring (med etta) om $(G, +)$ är en abelsk grupp. $\text{End}(G)$ är mängden av endomorfier av G , dvs homomorfier $f: G \rightarrow G$ (dvs $f(x+y) = f(x) + f(y)$, alla $x, y \in G$) och för $f, g \in \text{End}(G)$ är $(f+g)(x) = f(x) + g(x)$, alla $x \in G$.

Lösning:

Låt $R = \text{End}(G)$. Vi har att visa 1, 2, 3 nedan för $(R, +, \circ)$ (enligt definitionen av en ring).

1. $(R, +)$ är en **abelsk grupp**, ty om $f, g, h \in R, x, y \in G$ är $(f+g)(x+y) \stackrel{\text{def}}{=} f(x+y) + g(x+y) \stackrel{f, g \in R}{=} f(x) + f(y) + g(x) + g(y) \stackrel{G \text{ abelsk}}{=} f(x) + g(x) + f(y) + g(y) \stackrel{\text{def}}{=} (f+g)(x) + (f+g)(y)$, så $f+g \in R$ (slutenhet); $(f+(g+h))(x) = f(x) + (g+h)(x) = f(x) + (g(x) + h(x)) = (f(x) + g(x)) + h(x) = ((f+g)+h)(x)$, så $f+(g+h) = (f+g)+h$ (associativitet); med $0_R(x) = 0 \in G$, alla $x \in G$, är $0_R \in R$ och $f+0_R = 0_R+f = f$ (identitetsselement) och med $-f$, given av $(-f)(x) = -f(x)$, alla $x \in G$, är $-f \in R$ och $f+(-f) = (-f)+f = 0_R$ (invers).

2. $(R, \circ)$ är **sluten** (ty $(f \circ g)(x+y) = f(g(x+y)) = f(g(x)+g(y)) = (f \circ g)(x) + (f \circ g)(y)$), **associativ** (ty sammansättning av funktioner) och har **identitetsselementet** $\text{id}_G \in R$.

3. **Distributivitet**, ty för alla $x \in G, (f \circ (g+h))(x) = f(g(x)+h(x)) = ((f \circ g) + (f \circ h))(x), ((f+g) \circ h)(x) = (f+g)(h(x)) = ((f \circ h) + (g \circ h))(x)$.

Saken är klar.

11) G är mängden av bijektioner $f: X \rightarrow X$ på mängden X och vi skall (a, 2p) visa att $(G, \circ)$ är en grupp och (b, 2p) avgöra om $H = \{f \in G \mid f(y) \in Y \text{ för alla } y \in Y\}$ säkert är en delgrupp till G om $Y \subseteq X$.

Lösning:

a. $(G, \circ)$ är en grupp, ty sammansättningen av två bijektioner är en bijektion (känd sats) (slutenhet), sammansättning av funktioner är associativ (associativitet), id_X är en bijektion med $id_x \circ f = f \circ id_X = f$, alla $f \in G$, (identitetselement) och $f^{-1} \in G$ för alla $f \in G$ (känd sats) och $f \circ f^{-1} = f^{-1} \circ f = id_X$ (invers). **Saken är klar.**

b. H behöver inte vara en delgrupp till G , ty med $X = \mathbb{Z}$, $Y = \mathbb{N}$ är $f \in H$ då $f(x) = x + 1$, alla $x \in X$, men dess invers $f^{-1} \notin H$, eftersom $0 \in Y$, $f^{-1}(0) = -1 \notin Y$.

Svar a: Visat ovan, b: H är inte säkert en delgrupp till G .

12) Vi söker (a, 1p) $|R|$ och (b, 4p) alla lösningar till ekvationen $t^2 + 3t + 3 = 0$ i ringen $R = \mathbb{Z}_{11}[x]/(x^2 + 1)$. Vi kallar restklassen som innehåller x för α .

Lösning:

a. Varje restklass i R innehåller precis ett polynom av grad ≤ 1 (och alla sådana ligger förstås i sin restklass), så elementen i R kan skrivas $a + b\alpha$, där olika $a, b \in \mathbb{Z}_{11}$ ger olika element. Det ger att $|R| = 11^2 = 121$.

b. $t^2 + 3t + 3 = t^2 + 14t + 5 + 9 = (t + 7)^2 + 9 = 0$, så ekvationen kan skrivas $(t + 7)^2 + 9 = 0$. $t + 7$ måste alltså vara ett element i R med kvadraten $-9 = 2$. Kvadraterna av elementen i $\mathbb{Z}_{11} = \{0, 1, 2, 3, \dots, 10\}$ är $0, 1, 4, 9, 5, 3, 3, 5, 9, 4, 1$, alla skilda från 2, men eftersom $x^2 = (x^2 + 1) - 1$ är $\alpha^2 = -1$ och $(3\alpha)^2 = (8\alpha)^2 = 9(-1) = -9 = 2$, så $t + 7 = 3\alpha$, 8α ger lösningar till ekvationen: $t = -7 + 3\alpha$, $-7 + 8\alpha = 4 \pm 3\alpha$.

Det finns inget element i $\mathbb{Z}_{11}$ med kvadrat $-1 = 10$, så $x^2 + 1$ är irreducibelt (andragradspolynom utan nollställe) och R alltså en kropp. Det följer (från faktorsatsen) att ett andragradspolynom kan ha högst två nollställen i R , så vi har funnit alla lösningar.

Svar a: $|R| = 121$, b: Alla lösningar är $t = 4 \pm 3\alpha$.

13) (5p) Vi söker antalet väsentligt olika sätt att färga en kubs kanter med hälften av kanterna röda eller blå och hälften gula eller gröna.

Lösning:

Vi använder Burnsidess lemma och behöver $|F(g)|$ för varje (typ av) symmetrirotation g .

typ av g	g :s permutation av kubens kanter	antal g	$ F(g) $
id	$[1^{12}]$	1	$\binom{12}{6} \cdot 2^{12}$
rot $hh \pm \frac{2\pi}{3}$	$[3^4]$	8	$\binom{4}{2} \cdot 2^4$
rot $kk \pi$	$[1^2 2^5]$	6	$(\binom{5}{2} + \binom{5}{3}) \cdot 2^7$
rot $ss \pm \frac{\pi}{2}$	$[4^3]$	6	0
rot $ss \pi$	$[2^6]$	3	$\binom{6}{3} \cdot 2^6$

("rot xxv ": rotation vinkeln v kring en axel genom kubens och sidors(s), kanters(k) eller hörns(h) medelpunkter.)

$|F(g)|$: antalet g -invarianta (dvs samma färg på alla kanter i samma cykel i g :s permutation) färgningar.

$|F(id)|$: vilka 6 kanter röd/blå?, varje kant kan sedan ha en av två färger,

på övriga rader fördelas cyklerna på motsvarande sätt.

Lemmat ger antalet färgningar: $\frac{1}{|G|} \sum_{g \in G} |F(g)| = \frac{1}{24} (\binom{12}{6} \cdot 2^{12} + 8 \cdot \binom{4}{2} \cdot 2^4 + 6 \cdot (\binom{5}{2} + \binom{5}{3}) \cdot 2^7 + 6 \cdot 0 + 3 \cdot \binom{6}{3} \cdot 2^6) = \frac{1}{24} (\frac{12!}{6!^2} \cdot 2^{12} + 8 \cdot 6 \cdot 2^4 + 6 \cdot 20 \cdot 2^7 + 3 \cdot 20 \cdot 2^6) = 308 \cdot 2^9 + 2^5 + 5 \cdot 2^7 + 5 \cdot 2^5 = 77 \cdot 2^{11} + 13 \cdot 2^6 = 158\,528$.

Svar: Det sökta antalet är $77 \cdot 2^{11} + 13 \cdot 2^6 = 158\,528$.