Matematik, KTH
B.Ek

Lösningar tentan TENB SF1630(/1631) DISKRET MATEMATIK för D
31 maj 2013
Tryckfel kan förekomma.

1) (3p) H är en delgrupp till G. Vi skall visa att H är en delgrupp till K som är en delgrupp till G om $K = \{g \in G \mid gH = Hg\}$.

Lösning: Eftersom $hH = Hh = H$ för alla $h \in H$ är $H \subseteq K \subseteq G$ och det räcker att visa att K är en grupp. Enligt känd sats är det tillräckligt att visa att $a, b \in K \Rightarrow ab, a^{-1} \in K$. $aH = Ha$, $bH = Hb$ betyder att för varje $h \in H$ finns $h_1, h_2 \in H$ med $bh = h_1 b$, $ah_1 = h_2 a$, så $(ab)h = a(bh) = a(h_1 b) = (ah_1)b = (h_2 a)b = h_2(ab)$, så $abH \subseteq Hab$ och "p.s.s." visas $Hab \subseteq abH$, så $a, b \in K \Rightarrow ab \in K$. $ha = ah_3 \Leftrightarrow a^{-1}h = h_3 a^{-1}$, så $Ha = aH \Rightarrow a^{-1}H \subseteq Ha^{-1}$ och "p.s.s." $Ha^{-1} \subseteq a^{-1}H$, så $a \in K \Rightarrow a^{-1} \in K$. **Saken är klar.**

---

2) (3p) Gruppen G verkar på mängden X, där $|G| = 77$ och $|X| = 24$.
Vi skall visa att G:s verkan har minst två fixpunkter.

Lösning: X är en disjunkt union av banor $Gx = \{g(x) \mid g \in G\}$ för G:s verkan. Varje bana har ett antal element som delar $|G| = 77$ (elementen i banan motsvarar sidoklasser till stabilisatorn $G_x = \{g \in G \mid g(x) = x\}$), så de har 1, 7, 11 eller 77 element. 77 är förstås uteslutet. X är inte en disjunkt union av 7- och 11-mängder ($24 = 2 \cdot 11 + 2 \cdot 1 = 11 + 7 + 6 \cdot 1 = 3 \cdot 7 + 3 \cdot 1 = \dots$), minst två blir "över". Antalet 1-banor (=fixpunkter) är alltså minst två. **Saken är klar.**

---

3) (3p) Vi skall korrigera ett element i $H' = \begin{bmatrix} 1&1&0&0&1&0 \\ 0&0&1&1&1&0 \\ 1&0&1&0&1&1 \end{bmatrix}$, så att den blir kontrollmatrisen H för en linjär, binär 1-felsrättande kod med ett kodord (110110).

Lösning: Eftersom $H'[110110]^T = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$ finns felet i första raden och i en position där ordet har en 1:a. Positionerna 1, 2, 5 går inte, ty om de ändras fås två lika kolonner eller en 0-kolonn i matrisen (så koden vore inte 1-felsrättande), men position 4 går bra.

Svar: Den riktiga kontrollmatrisen är $\boldsymbol{H = \begin{bmatrix} 1&1&0&1&1&0 \\ 0&0&1&1&1&0 \\ 1&0&1&0&1&1 \end{bmatrix}}$.

---

4) Vi skall (a, 1p) visa att $f(x) = x^2 + x + 2 \in \mathbb{Z}_5[x]$ är irreducibelt, (b, 1p) finna antalet element i kroppen F som konstrueras med $\mathbb{Z}_5[x]$ och $f(x)$ och (c, 1p) beskriva elementen, addition och multiplikation i F.

Lösning: Eftersom $f(x)$ har grad 2, är det reducibelt omm det har något nollställe. Man finner $f(0) = f(4) = 2$, $f(1) = f(3) = 4$, $f(2) = 3$, så **a)-saken är klar**. Då $f(x)$ är av grad 2, svarar elementen i F precis mot förstagradspolynomen i $\mathbb{Z}_5[x]$. De är alltså $5 \cdot 5 = 25$ st. Elementen i F ges (med α motsvarande x) som $a + b\alpha$, $a, b \in \mathbb{Z}_5$. Räkning i F sker (mod $f(x)$), så $\alpha^2 + \alpha + 2 = 0$ och man räknar med vanliga (kropps-)räkneregler och regeln $\alpha^2 = 4\alpha + 3$.

Svar a: Visat ovan, b: F har 25 element,
c: $F = \{a + b\alpha \mid a, b \in \mathbb{Z}_5\}$, räkning i F "som vanligt" plus $\alpha^2 = 4\alpha + 3$.

---

5) (3p) Vi söker alla lösningar till $x^2 = x$ i $\mathbb{Z}_{341}$ och i $\mathbb{Z}_{431}$.

Lösning: $x^2 = x \Leftrightarrow x(x-1) = 0$. Eftersom 431 är ett primtal är $\mathbb{Z}_{431}$ en kropp och de enda lösningarna där är $x = 0$ och $x = 1$ ($431 \mid x(x-1) \Leftrightarrow 431 \mid x$ eller $431 \mid (x-1)$).
$341 = 11 \cdot 31$, så $341 \mid x(x-1) \Leftrightarrow 11 \mid x(x-1)$ och $31 \mid x(x-1)$, dvs $x \equiv_{11} 0, 1$ och $x \equiv_{31} 0, 1$.
Om $x \equiv_{11} 0$ är $x = 11k$ för något $k \in \mathbb{Z}$ och $x \equiv_{31} 0$ ger $k \equiv_{31} 0$, så $x \equiv_{341} 0$, medan $x \equiv_{31} 1$ ger $11k \equiv_{31} 1 \Leftrightarrow 33k \equiv_{31} 3$ (ty $\text{sgd}(3, 31) = 1$) $\Leftrightarrow 2k \equiv_{31} 3 \Leftrightarrow 32k \equiv_{31} 48$ (ty $\text{sgd}(16, 31) = 1$) $\Leftrightarrow k \equiv_{31} 17$, så $x \equiv_{341} 11 \cdot 17 = 187$.
Om $x \equiv_{11} 1$ är $x = 11k + 1$ för något $k \in \mathbb{Z}$ och $x \equiv_{31} 1$ ger $k \equiv_{31} 0$, så $x \equiv_{341} 1$, medan $x \equiv_{31} 0$ ger $11k \equiv_{31} -1 \Leftrightarrow 33k \equiv_{31} -3$ (ty $\text{sgd}(3, 31) = 1$) $\Leftrightarrow 2k \equiv_{31} -3 \Leftrightarrow 32k \equiv_{31} -48$ (ty $\text{sgd}(16, 31) = 1$) $\Leftrightarrow k \equiv_{31} 14$, så $x \equiv_{341} 11 \cdot 14 + 1 = 155$.

Svar: Alla lösningar är $x = 0, 1, 155, 187$ i $\mathbb{Z}_{341}$ och $x = 0, 1$ i $\mathbb{Z}_{431}$.

---

6) (4p) $a \oplus b = a + b + 1$, $a \odot b = ab + a + b$ för $a, b \in \mathbb{Q}$.
Vi skall visa att $(\mathbb{Q}, \oplus, \odot)$ är en kropp och ange motsvarande identitetselement.

Lösning: Vi noterar att $a \oplus b + 1 = (a+1) + (b+1)$ och $a \odot b + 1 = (a+1)(b+1)$, så funktionen $\phi : \mathbb{Q} \to \mathbb{Q}$, $\phi(x) = x + 1$ bevarar strukturen, som funktion från $(\mathbb{Q}, \oplus, \odot)$ till $(\mathbb{Q}, +, \cdot)$. Eftersom ϕ är en bijektion (med $\phi^{-1}(y) = y - 1$) är den en isomorfi mellan $(\mathbb{Q}, \oplus, \odot)$ och $(\mathbb{Q}, +, \cdot)$. Eftersom $(\mathbb{Q}, +, \cdot)$ är en kropp är $(\mathbb{Q}, \oplus, \odot)$ också det. Identitetselementet till $\oplus$ är $\phi^{-1}(0) = -1$ och det till $\odot$ är $\phi^{-1}(1) = 0$.

Svar: $(\mathbb{Q}, \oplus, \odot)$ är en kropp enligt ovan. Identitetselementen är -1, 0.

---

7) (4p) $(G, \cdot)$ är en ändlig grupp och p ett primtal.
Vi skall visa att antalet element av ordning p i G är en multipel av $p - 1$

Lösning: Om $g \in G$ har ordning p är dess cykliska delgrupp $\langle g \rangle$ av primtalsordning (p), så den genereras av varje element utom identitetselementet 1. $\langle g \rangle^* = \langle g \rangle \setminus \{1\}$ har alltså $p - 1$ element, alla av ordning p och $h \in \langle g \rangle^* \Rightarrow \langle h \rangle^* = \langle g \rangle^*$. Det betyder att olika $\langle g \rangle^*$ är disjunkta och eftersom deras union är mängden av alla element i G som har ordning p följer påståendet. **Saken är klar.**

---

8) (4p) Vi söker antalet väsentligt olika fördelningar av 6 vita och 6 svarta kanter på en kub.

Lösning: Vi använder Burnsides lemma (Thm 21.4 i Biggs). Symmetrigruppen G har 24 element ($|Gx||G_x| = 8 \cdot 3 = 24$ om x är ett av kubens hörn):
identitets"rotationen" id,
8 rotationer $\frac{2\pi}{3}$ kring axlar genom motsatta hörn rot_{hh},
6 rotationer π kring axlar genom mittpunkter av motsatta kanter rot_{kk},
3 rotationer π kring axlar genom mittpunkter av motsatta sidor $\text{rot}_{ss\pi}$ och
6 rotationer $\frac{\pi}{2}$ kring axlar genom mittpunkter av motsatta sidor $\text{rot}_{ss\frac{\pi}{2}}$.
$|F(g)|$, antalet konfigurationer som inte ändras av g för de olika $g \in G$ blir:

g	antal element	$\lvert F(g)\rvert$
id	1	$\binom{12}{6} = \cdots = 924$ (vilka 6 kanter vita?)
rot_{hh}	8	$\binom{4}{2} = 6$ (kanterna samma färg 3,3,3,3; vilka trippler vita?)
rot_{kk}	6	$\binom{6}{3} = 20$ (kanterna samma färg 1,1,2,2,2,2; vilka par vita?)
$\text{rot}_{ss\pi}$	3	$\binom{6}{3} = 20$ (kanterna samma färg parvis; vilka par vita?)
$\text{rot}_{ss\frac{\pi}{2}}$	6	0 (kanterna samma färg 4,4,4; går inte)

Antalet olika fördelningar av kantfärger = antalet banor då G verkar på färgningarna =
$= \frac{1}{|G|} \sum_{g \in G} |F(g)| = \frac{1}{24}(1 \cdot 924 + 8 \cdot 6 + 6 \cdot 20 + 3 \cdot 20 + 6 \cdot 0) = \frac{1}{24} \cdot 1152 = 48$.
Svar: Det finns 48 väsentligt olika sådana färgningar.

---

9) (5p) $(F,+,\cdot)$ är en ändlig kropp av karakteristik p, ett primtal.
Vi skall visa att varje element i F har en entydig p:e rot.

Lösning: Att för varje $a \in F$ finns precis ett $b \in F$ med $a = b^p$ är detsamma som att funktionen $f : F \to F$, $f(x) = x^p$ är en bijektion. Eftersom F är ändlig är f en bijektion omm det är en injektion. Det räcker alltså att visa att för godtyckliga $x, y \in F$ gäller att $x^p = y^p \Rightarrow x = y$, men $x^p = y^p \Leftrightarrow 0 = x^p - y^p = (x-y)^p$ (ty $(x-y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k (-y)^{p-k} = x^p + (-y)^p$, ty $p \mid \binom{p}{k}$ för $k = 1, 2, \ldots, p-1$ och $p \cdot 1 = 0$ i F, och $(-y)^p = -y^p$ i karakteristik p ($+ = -$ om $p = 2$)). Eftersom F är en kropp gäller $(x-y)^p = 0 \Leftrightarrow x - y = 0$, dvs $x = y$. **Saken är klar.**
(Man kan alternativt utnyttja att $(F \setminus \{0\}, \cdot)$ är en abelsk grupp av ordning $p^k - 1$, relativt primt med p. $x^p = y^p \neq 0 \Rightarrow (xy^{-1})^p = 1$, så $o(xy^{-1}) \mid p, p^k - 1$, så $o(xy^{-1}) = 1 \Rightarrow xy^{-1} = 1$.
Eller, eftersom $(F \setminus \{0\}, \cdot)$ är cyklisk, med generator g säg, kan man skriva ett godtyckligt $a \in F \setminus \{0\}$ som $a = g^m$ för något $m \in \mathbb{Z}$. Med $b = g^n$ gäller $a = b^p \Leftrightarrow m \equiv pn \pmod{p^k - 1}$, vilken har en lösning som är entydig $\pmod{p^k - 1}$ eftersom $\text{sgd}(p, p^k - 1) = 1$. Det betyder att b är entydigt bestämt av a. Om $a = 0$ är $b = 0$ förstås det enda b som uppfyller $a = b^p$.)

---

10) Vi skall visa att (a, 2p) om $g(x), h(x) \in \mathbb{Z}[x]$ och alla koefficienter i $g(x)h(x)$ är delbara med primtalet p, är alla koefficienterna i minst en av $g(x)$ och $h(x)$ också det och (b, 3p) att om $f(x) \in \mathbb{Z}[x]$ är reducibel i $\mathbb{Q}[x]$ så är den reducibel i $\mathbb{Z}[x]$.

Lösning: a) Låt $g(x) = a_m x^m + \cdots + a_1 x + a_0$, $h(x) = b_n x^n + \cdots + b_1 x + b_0$ och antag att p varken delar alla a_i:na eller alla b_j:na. Om r är minst så att $p \nmid a_r$, men $p \mid a_i$ för alla $i < r$ och s är minst så att $p \nmid b_s$, men $p \mid b_j$ för alla $j < s$, gäller att p inte delar koefficienten för x^{r+s} i $g(x)h(x)$, $a_0 b_{r+s} + a_1 b_{r+s-1} + \cdots + a_{r+s} b_0$, ($p$ delar ju alla termer i summan utom $a_r b_s$). Det ger påståendet. **a)-saken är klar.**
b) Låt $f(x) \in \mathbb{Z}[x]$ och $f(x) = \varphi(x)\psi(x)$, där $\varphi(x), \psi(x) \in \mathbb{Q}[x]$. Om k är en gemensam multipel till alla nämnarna i $\varphi(x)$:s koefficienter gäller att $k\varphi(x) \in \mathbb{Z}[x]$. Vi kallar den $g(x)$ och p.s.s. låter vi $h(x) = l\psi(x) \in \mathbb{Z}[x]$. Då är $kl \cdot f(x) = g(x)h(x)$ en faktorisering i $\mathbb{Z}[x]$ och vi kan, enligt a), förkorta med en primfaktor i kl i taget, tills vi får en faktorisering av $f(x)$ i $\mathbb{Z}[x]$. Faktorerna i den har samma grader som $\varphi(x)$, $\psi(x)$, så om $f(x)$ är reducibel i $\mathbb{Q}[x]$ är den det också i $\mathbb{Z}[x]$. **b)-saken är också klar.**
