Matematik, KTH
B.Ek

Lösningar tenta TENB SF1630(/1631) DISKRET MATEMATIK, D3
20 augusti 2014
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 $x \in G$ (identitetselement) 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 $\circ : G \times G \to G$.)
b) (1p) Gruppen $(G, \circ)$ är abelsk omm $a \circ b = b \circ a$ för alla $a, b \in G$.
c) (1p) Antalet delgrupper av ordning m är 1 om $m \mid n$, annars 0.

2a) (1p) Stabilisatorn för $x \in X$ då G verkar på X är $G_x = \{g \in G \mid gx = x\}$.
b) (1p) Om $x \in X$ har banan Gx och stabilisatorn G_x gäller $|G| = |Gx| \cdot |G_x|$.
c) (1p) Operationen $\cdot$ skall vara kommutativ och alla $x \in R$ utom 0 skall ha en invers $x^{-1} \in R$ (dvs $x \cdot x^{-1} = 1$). R skall förstås ha en etta.

3a) (1p) Möjliga värden för karakteristiken är alla primtal och 0.
b) (1p) $f(x) \in F[x]$ är irreducibelt omm $f(x) = g(x)h(x)$, $g(x), h(x) \in F[x]$, medför att precis en av $g(x)$ och $h(x)$ är konstant (dvs av grad 0).
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 $n = p \cdot q$ (p, q primtal) bestäms d av $e \cdot d \equiv_m 1$, där $m = (p-1)(q-1)$.
c) (1p) Om p, q är primtal och $k \equiv_{(p-1)(q-1)} 1$ är $x^k \equiv_{p \cdot q} x$ för alla $x \in \mathbb{Z}$.

---

5) (3p) Vi söker x då $ax^2 = b$ och $x^5 = c$, där $a, b, c, x \in G$, en grupp.

Lösning:
T.ex. $ac = ax^5 = ax^2x^3 = bx^3$, så $b^{-1}ac = x^3$ och $ab^{-1}ac = ax^3 = ax^2x = bx$, så

Svar: $x = b^{-1}ab^{-1}ac$.

---

6) Delgruppen H till gruppen $(G, *)$ verkar på mängden G enligt $h(g) = h * g$.
Vi söker för $g \in G$ (a, 1p) stabilisatorn H_g och (b, 2p) banan $H(g)$.

Lösning:
a. Enligt definition är $H_g = \{h \in H \mid h(g) = g\}$. Men $h(g) = h * g = g$ ger $h = 1$, identitetselementet (multiplicera från höger med g^{-1}), så $H_g = \{1\}$.
b. Enligt definition är $H(g) = \{h(g) \mid h \in H\} = \{h * g \mid h \in H\}$, dvs banan $H(g)$ är högersidoklassen Hg.

Svar a: Stabilisatorn H_g är $\{1\}$, b: Banan $H(g)$ är högersidoklassen Hg.

---

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

Lösning:
Vi undersöker först om (det är så lyckligt att) $f(x)$ har någon förstagradsfaktor, dvs om det har något nollställe i $\mathbb{Z}_5$. Vi finner $f(0) = 4$, $f(1) = 1 + 1 + 1 + 4 = 2$, $f(2) = 1 + 3 + 2 + 4 = 0$, så $f(x)$ har enligt faktorsatsen en faktor $x - 2 = x + 3$. Polynomdivision ger $f(x) = (x+3)(x^3 + 3x^2 + x + 3) = (x+3)g(x)$. $x+3$ är irreducibelt. Om $g(x)$ är reducibelt har det en förstagradsfaktor. $g(0), g(1) \neq 0$ (ty $f(0), f(1) \neq 0$), $g(2) = 3 + 2 + 2 + 3 = 0$, så $g(x)$ har en faktor $x + 3$. Polynomdivision ger $g(x) = (x + 3)(x^2 + 1) = (x + 3)h(x)$. $h(0), h(1) \neq 0$ och $h(2) = 4 + 1 = 0$, så $h(x)$ har en faktor $x + 3$. Polynomdivision ger $h(x) = (x + 3)(x + 2)$, med irreducibla faktorer.

Svar: $f(x) = (x + 2)(x + 3)^3$, där faktorerna är irreducibla.

---

8) Vi söker dels det minsta $e \geq 10$ sådant att $(391, e)$ kan användas som krypteringsnyckel i ett RSA-system, dels ett d, sådant att $(391, d)$ är en motsvarande dekrypteringsnyckel.

Lösning:
$n = 391 = 17 \cdot 23$ ger $m = 16 \cdot 22 = 2^5 \cdot 11 = 352$. Villkoret på e är då $\text{sgd}(m, e) = \text{sgd}(2^5 \cdot 11, e) = 1$, med minsta lösning ≥ 10 : $e = 13$.
Det skall gälla $e \cdot d \equiv_{352} 1$. Vi använder Euklides algoritm:
$352 = 27 \cdot 13 + 1$, så $1 = 1 \cdot 352 - 27 \cdot 13 = 1 \cdot 352 - 13 \cdot 352 + 352 \cdot 13 - 27 \cdot 13 = 325 \cdot 13 - 12 \cdot 352$ och vi kan välja $d = 325$.

Svar: $e = 13$, $d = 325$.

---

9) Vi skall (a, 1p) finna alla element i U_{21} (de inverterbara elementen i $\mathbb{Z}_{21}$) och (b, 3p) avgöra om gruppen $(U_{21}, \cdot)$ är cyklisk.

Lösning:
a. $x \in U_{21}$ omm $x \in \mathbb{Z}_{21}$ och $\text{sgd}(x, 21) = 1$, så $U_{21} = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$.
b. Eftersom $\mathbb{Z}_{21} \approx \mathbb{Z}_3 \times \mathbb{Z}_7$ är $U_{21} \approx U_3 \times U_7$. Alla $y \in U_3$ och alla $z \in U_7$ uppfyller $y^6 = 1$, $z^6 = 1$. Det ger att $x^6 = 1$ för alla $x \in U_{21}$, så $(U_{21}, \cdot)$ är inte cyklisk.
(Man kan förstås också beräkna ordningarna för elementen i U_{21}. Eftersom ordningen måste vara en delare till 12 ($= |U_{21}|$) har $x \in U_{21}$ ordning 12 (dvs genererar gruppen) omm $x^4 \neq 1$, $x^6 \neq 1$. Använd också $x^{4,6} = (-x)^{4,6}$.)

Svar a: $U_{21} = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$, b: $(U_{21}, \cdot)$ är inte cyklisk.

---

10) Vi har ringen $F = \mathbb{Z}_3[x]/(f(x))$, där $f(x) = x^2 + 2x + 2$, och kallar x:s ekvivalensklass för α. Vi skall (a, 1p) visa att F är en kropp, (b, 1p) uttrycka α^2 som en linjärkombination av 1 och α och (c, 2p) faktorisera $g(x) = x^2 + x + 2 \in F[x]$ i irreducibla faktorer.

Lösning:
a. F är en kropp omm $f(x)$ är irreducibelt i $\mathbb{Z}_3[x]$, dvs omm det saknar nollställen i $\mathbb{Z}_3$ (om det vore reducibelt skulle det ha förstagradsfaktorer). $f(0) = 0 + 0 + 2 = 2$, $f(1) = 1 + 2 + 2 = 2$, $f(2) = 1 + 1 + 2 = 1$, så saken är klar.
b. Eftersom $x^2 + 2x + 2 \equiv_{(f(x))} 0$ är $\alpha^2 + 2\alpha + 2 = 0$, så $\alpha^2 = -2\alpha - 2 = \alpha + 1$ i F.
c. $g(x)$ är reducibelt i $F[x]$ omm det har något nollställe i F (ty det är av grad 2). Prövning (använd t.ex. att $\alpha^2 = (2\alpha)^2 = \alpha + 1$, $(\alpha+1)^2 = (2\alpha+2)^2 = 2$, $(2\alpha+1)^2 = (\alpha+2)^2 = 2\alpha+2$) ger att $g(2\alpha) = 0$, så det har en faktor $x - 2\alpha = x + \alpha$. Polynomdivision i $F[x]$ ger $g(x) = (x + \alpha)(x + 2\alpha + 1)$, med irreducibla faktorer (ty av grad 1).

Svar a: Visat ovan, b: $\alpha^2 = \alpha + 1$ i F, c: $g(x) = (x + \alpha)(x + 2\alpha + 1)$.

---

11) $S_{\mathbb{Z}}$ är mängden av bijektioner av $\mathbb{Z}$. $(S_{\mathbb{Z}}, \circ)$ är en grupp och vi skall (a, 1p) finna identitetselement och invers till $f \in S_{\mathbb{Z}}$ och (b, 3p) avgöra om $K_A = \{f \in S_{\mathbb{Z}} \mid f(x) \in A \text{ för alla } x \in A\}$ är en delgrupp till $S_{\mathbb{Z}}$ för alla $A \subseteq \mathbb{Z}$.

Lösning:
a. $id \in S_{\mathbb{Z}}$, där $id(x) = x$ för alla $x \in \mathbb{Z}$, är identitetselement, ty $(f \circ id)(x) = f(id(x)) = f(x)$ och $(id \circ f)(x) = id(f(x)) = f(x)$ för alla $x \in \mathbb{Z}$, $f \in S_{\mathbb{Z}}$. Inversfunktionen f^{-1} (finns, ty f är en bijektion) är inverselement till $f \in S_{\mathbb{Z}}$: $f \circ f^{-1} = f^{-1} \circ f = id$.
b. Om A är oändlig är K_A inte en delgrupp till $S_{\mathbb{Z}}$.
För $A = \mathbb{N}$ ger t.ex. $f(x) = x + 1$ att $f \in K_{\mathbb{N}}$ (f är ju en bijektion av $\mathbb{Z}$ och $x \in \mathbb{N}$ medför att $x + 1 \in \mathbb{N}$), men dess invers $f^{-1} \notin K_{\mathbb{N}}$, ty $f^{-1}(x) = x - 1$, så $0 \in \mathbb{N}$ men $f^{-1}(0) = -1 \notin \mathbb{N}$.

Svar a: id är identitetselement, funktionsinversen f^{-1} är inverselement till f,
b: Nej, K_A är inte säkert en delgrupp till $S_{\mathbb{Z}}$.

---

12) (5p) Vi söker antalet väsentligt olika armband av 5 svarta, 2 röda och 2 vita pärlor uppträdda på en ögla av snöre.

Lösning:
Vi använder Burnsides lemma. Om armbandet placeras med pärlorna i hörnen av en reguljär 9-hörning, ser man att gruppen G som verkar på mängden av konfigurationer består av identitetsavbildningen id, elementen $r, r^2, \ldots, r^8$ (där r är rotation $\frac{2\pi}{9}$ kring en axel genom 9-hörningens mittpunkt och vinkelrät mot dess plan) och $s, rs, r^2s, \ldots, r^8s$ (där s är rotation kring en axel i 9-hörningens plan, genom dess medelpunkt och en av pärlorna. $|F(g)|$, antalet konfigurationer som inte ändras av g ses vara som i tabellen:

g:s typ	antal sådana g	$\lvert F(g)\rvert$	
id	1	$\binom{9}{5,2,2} = 756$	alla konfigurationer
$r, r^2, \ldots, r^8$	8	0	de två vita kan inte roteras till varandra
$s, rs, \ldots, r^8s$	9	$4 \cdot 3 = 12$	8 pärlor paras ihop 2 och 2, ett par skall vara vitt, ett rött

Så antalet väsentligt olika armband = antalet banor under G:s verkan $= \frac{1}{|G|}\sum_{g\in G}|F(g)| = \frac{1}{18}(1\cdot 756 + 8\cdot 0 + 9\cdot 12) = \frac{1}{18}864 = 48$.

Svar: Antalet olika sådana armband är 48.

---

13) Vi skall visa (a, 1p) att $\mathrm{Aut}(G)$, mängden av G:s automorfier, är en grupp, (b, 1p) att $\phi_a \in \mathrm{Aut}(G)$ om $a \in G$ och $\phi_a(g) = aga^{-1}$ och (c, 3p) att $\mathrm{I}(G) = \{\phi_a \mid a \in G\}$ är en normal delgrupp till $\mathrm{Aut}(G)$.

Lösning:
a. Eftersom $\mathrm{Aut}(G) \subseteq S_G$ (gruppen av bijektioner av G), räcker det att visa att $\mathrm{Aut}(G)$ är en delgrupp till S_G.
$id \in \mathrm{Aut}(G)$, så $\mathrm{Aut}(G) \neq \varnothing$.
Låt $\psi_1, \psi_2 \in \mathrm{Aut}(G)$. $\psi_1\psi_2$ är en bijektion (en sammansättning av bijektioner) och för $g, h \in G$ gäller $(\psi_1\psi_2)(gh) = \psi_1(\psi_2(gh)) = \psi_1(\psi_2(g)\psi_2(h)) = \psi_1(\psi_2(g))\psi_1(\psi_2(h)) =$
$= (\psi_1\psi_2)(g)(\psi_1\psi_2)(h)$, så $\psi_1\psi_2 \in \mathrm{Aut}(G)$.
Om $\psi \in \mathrm{Aut}(G)$ är ψ^{-1} en bijektion och $\psi(gh) = \psi(g)\psi(h)$ ger (ersätt g, h med $\psi^{-1}(g), \psi^{-1}(h)$ och tag ψ^{-1} av båda leden) att $\psi^{-1}(gh) = \psi^{-1}(g)\psi^{-1}(h)$, så $\psi^{-1} \in \mathrm{Aut}(G)$.
Enligt en känd sats är $\mathrm{Aut}(G)$ en delgrupp till S_G, så en grupp.
b. $aga^{-1} = h$ omm $g = a^{-1}ha$, så ϕ_a är en bijektion (med $(\phi_a)^{-1} = \phi_{a^{-1}}$).
Eftersom också $\phi_a(gh) = agha^{-1} = aga^{-1}aha^{-1} = \phi_a(g)\phi_a(h)$ fås $\phi_a \in \mathrm{Aut}(G)$.
c. Vi visar först att $\mathrm{I}(G)$ är en delgrupp till $\mathrm{Aut}(G)$.
Enligt b) är $\mathrm{I}(G) \subseteq \mathrm{Aut}(G)$. $\mathrm{I}(G) \neq \varnothing$ (ty $G \neq \varnothing$).
Om $a, b \in G$: $(\phi_a\phi_b)(g) = \phi_a(\phi_b(g)) = \phi_a(bgb^{-1}) = a(bgb^{-1})a^{-1} = (ab)g(ab)^{-1} = \phi_{ab}(g)$, så $\phi_a\phi_b = \phi_{ab} \in \mathrm{I}(G)$.
Enligt ovan $(\phi_a)^{-1} = \phi_{a^{-1}} \in \mathrm{I}(G)$.
Enligt satsen som användes i a) är $\mathrm{I}(G)$ en delgrupp till $\mathrm{Aut}(G)$.
Den är en normal delgrupp precis om $\psi\,\mathrm{I}(G) = \mathrm{I}(G)\psi$ för varje $\psi \in \mathrm{Aut}(G)$.
$(\psi\phi_a)(g) = \psi(\phi_a(g)) = \psi(aga^{-1}) = \psi(a)\psi(g)\psi(a^{-1}) = \psi(a)\psi(g)\psi(a)^{-1} = \phi_{\psi(a)}(\psi(g)) = (\phi_{\psi(a)}\psi)(g)$, där vi använt att $\psi \in \mathrm{Aut}(G)$ och definitionen av ϕ_a. Det betyder att $\psi\phi_a = \phi_{\psi(a)}\psi$ och därmed $\phi_a\psi = \psi\phi_{\psi^{-1}(a)}$, så $\psi\,\mathrm{I}(G) \subseteq \mathrm{I}(G)\psi$ och $\mathrm{I}(G)\psi \subseteq \psi\,\mathrm{I}(G)$. Saken är klar.

Svar a, b, c: Visade ovan.
