2011-(03)mar-10: dag 15

1) Vilket är identitetselementet?

Jo, $a * c = c$ ger a är identitetselement → ger rad 1 och kolumn 1.

Grupptabellen är en latinsk kvadrat, så $c * f = b$, …

∗	a	b	c	d	f	g
a	a	b	**c**	d	f	g
b	b	a	g	f	**d**	**c**
c	c	**f**	a	**g**	b	a
d	d	g	f	**a**	c	**b**
f	f	**c**	**d**	b	g	a
g	g	d	b	c	**a**	f

a) Gruppen är inte abelsk, ty $b * c = g \neq g = c * b$.

b) $a * c = 1 * c$ ger $a = 1$ som ovan.

c) Inverser: $a^{-1} = a$, $b^{-1} = b$, $c^{-1} = c$, $d^{-1} = d$, $f^{-1} = g$, $g^{-1} = f$

ty till exempel $f * g = a$ $(= 1)$

d) $o(a) = 1$, $o(b) = o(c) = o(d) = 2$, $o(f) = o(g) = 3$

ty $b^2 = a$, men $b^{-1} \neq a$, $f^1 \neq a$, $f^2 = g \neq a$, $f^3 = a$.

Cykliska delgrupper:

$\langle a \rangle = \{a\}$
$\langle b \rangle = \{a, b\}$
$\langle c \rangle = \{a, c\}$
$\langle d \rangle = \{a, d\}$
$\langle f \rangle = \{a, f, g\}$
$\langle g \rangle = \{a, g, f\}$ $\langle f \rangle = \{a, f, g\} = \langle g \rangle$

e) $\underline{a * b} * \underline{c * d} * \underline{f * g} = b * g * a = c * a = c$

2) G en grupp med identitetselement 1, $a, b, c, d \in G$

a) Finn det $x \in G$ som uppfyller (givet att ett sådant finns)

$$\begin{cases} ax^2 = b \\ x^3 = 1 \end{cases}$$

$ax^2 = b \Rightarrow ax^3 = bx \Rightarrow \{x^3 = 1\} \Rightarrow a = bx \Rightarrow x = b^{-1}a$

b) På samma sätt

$$\begin{cases} (xax)^3 = bx & (1) \\ x^2a = (xa)^{-1} & (2) \end{cases}$$

$bx = \{(1)\} = (xax)^3 = xa\underline{x^2a}\underline{x^2a}x = \{(2)\} =$
$= xa(xa)^{-1}(xa)^{-1}x = (xa)^{-1}x$

så $bxa = (xa)^{-1}xa = 1$
så $x = b^{-1}a^{-1}$

d) Visa $(abc)^{-1} = abc \Rightarrow (bca)^{-1} = bca$

Jo, $(abc)^{-1} = abc \Rightarrow bc\underline{a \cdot bc}a = bc(abc)^{-1}a =$
$= \underline{a^{-1}}\underline{abc(abc)^{-1}}a = a^{-1} \cdot 1 \cdot a = 1$

så $bca = (bca)^{-1}$

$bca \cdot bca = 1 = bca \cdot (bca)^{-1}$

f) Visa $b^2ab = a^{-1} \Rightarrow$ det finns $s \in H$ med $a = s^3$

Jo, $b^2ab = a^{-1} \Rightarrow ba = b^{-1}a^{-1}b^{-1}$

$\underline{(ba)^3} = b^{-1}a^{-1}\underline{b^{-1} \cdot b}aba = b^{-1}\underline{a^{-1}a}ba = \underline{b^{-1}b}a = \underline{a}$

3) $G_1 = (\mathbb{Z}_8; +)$, $G_2 = (U(\mathbb{Z}_{15}); \cdot)$

De invertabla elementen i $\mathbb{Z}_{15}$,
det vill säga alla x med sgd(x; 15) = 1

a) Grupptabeller:

G_1:

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

G_2:

·	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

$(U(\mathbb{Z}_m); \cdot)$ är en grupp för alla $m = 1, 2, \ldots$

G1) $\forall\, x, y \in G : x \ast y \in G$

G2) $\forall\, x, y, z \in G : (x \ast y) \ast z = x \ast (y \ast z)$

G3) $\exists\, I \in G : \forall\, x \in G \;:\; I \ast x = x \ast I = x$

G4) $\forall\, x \in G : \exists\, x^{-1} \in G \;:\; x \ast x^{-1} = x^{-1} \ast x = I$

Ty:

G1: $x, y \in U(\mathbb{Z}_m) \Rightarrow (xy)^{-1} = x^{-1}y^{-1}$

$(x\underline{yy^{-1}}x^{-1} = xx^{-1} = 1)$

G2: $\cdot$ associativ i $\mathbb{Z}_m$

G3: $1 \in U(\mathbb{Z}_m)$, identitetselementet

G4: x invertabel ger
$(x^{-1})^{-1} = x$ så
x^{-1} invertabel.

b) Ordningar för elementen:

o(x):	1	2	4	8
$x \in G_1$:	0	4	2, 6	1, 3, 5, 7
$x \in G_2$:	1	4, 11, 14	2, 7, 8, 13	

c) Cykliska delgrupper med sidoklasser
(vänster- = högersidoklass ty abelska grupper)

	Genererande element	delgrupper	sidoklasser
G_1:	0	$\{0\}$	$\{0\}, \{1\}, \{2\}, \ldots, \{7\}$
	4	$\{0, 4\}$	$\{0, 4\}, \{1, 5\}, \{2, 6\}, \{3, 7\}$
	2, 6	$\{0, 2, 4, 6\}$	$\{0, 2, 4, 6\}, \{1, 3, 5, 7\}$
	1	G_1	G_1

Alla singelton-delmängder i G_2

G_2:	1	$\{1\}$	$\{g\}, g \in G_2$
	4	$\{1, 4\}$	$\{1, 4\}, \{2, 8\}, \{7, 13\}, \{1, 14\}$
	11	$\{1, 11\}$	$\{1, 11\}, \{2, 7\}, \ldots$
	14	$\{1, 14\}$	$\{1, 14\}, \{2, 13\}, \ldots$
	2, 8	$\{1, 2, 4, 8\}$	$\{1, 2, 4, 8\}, \{7, 14, 13, 11\}$
	7, 13	$\{1, 7, 4, 13\}$	$\{1, 7, 9, 13\}, \{2, 14, 8, 11\}$

d) Alla delgrupper till G_2?

Del de cykliska enligt ovan, dels:
Ordningen måste vara 1, 2, 4 eller 8 (ty $|H| \backslash 8$)

bara de cykliska

Ordning 4? Elementens ordning måste vara 1 eller 2.
(Ordningen 4 ger en cyklisk delgrupp!)
Ingen i G_1 (ty bara 0, 4 av ordningen 1, 2)
i G_2 kanske $\{1, 4, 11, 14\}$.

Sidoklasser:
$\{1, 4, 11, 14\}, \{2, 7, 8, 13\}$

Ordning 8:
G_1 är cyklisk; $G_1 = \langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle$.
G_2 inte, inget element av ordning 8.

4) Är $G_1 = (U(\mathbb{Z}_8); \cdot)$, $G_2 = (U(\mathbb{Z}_{14}); \cdot)$ cykliska?

G är cyklisk omm $o(g) = |G|$, för något $g \in G$.

$G_1 = U(\mathbb{Z}_8) = \{1, 3, 5, 7\}$
$G_2 = U(\mathbb{Z}_{14}) = \{1, 3, 5, 9, 11, 13\}$

Ordningen för elementen:

G_1:	g^1	g^2	g^3	g^4	ordning för g
	$\underline{1}$				1
	3	$\underline{1}$			2
	5	$\underline{1}$			2
	7	$\underline{1}$			2

Ingen 4 (= $|G_1|$) så G_1 är inte cyklisk.

G_2:	g^1	g^2	g^3	g^4	g^5	g^6	ordning
	$\underline{1}$						1
	3	9	13	11	5	$\underline{1}$	6
	5	11	13	9	3	$\underline{1}$	6
	9	11	$\underline{1}$				3
	11	9	$\underline{1}$				3
	13	$\underline{1}$					2

Så G_2 är cyklisk.
$G_2 = \langle 3 \rangle = \langle 5 \rangle$

5) $G = (\mathbb{Z}_{13} \backslash \{0\}; \cdot)$ $(= (U(\mathbb{Z}_{13}); \cdot))$ är cyklisk. Finn alla generatorer.

$|G| = 12$ så vi söker $g \in G$ med $o(g) = 12$.

Möjliga ordningar: 1, 2, 3, 4, 6, 12, så
$o(g) = 12$ om $g^4, g^6 \neq 1$.

g	1	2	3	4	5	6	7	8	9	10	11	12
g^4	1	3	3	4	1	9	9	1	9	3	3	1
g^6		$\underline{12}$	1	1		$\underline{12}$	$\underline{12}$		1	1	$\underline{12}$	
o												

$o(2) = 12$ $\quad o(3) \neq 12$

Generatorer: 2, 5, 7, 11

Potenser av 2

2^1	2^2	2^3	$2^{\underline{4}}$	2^5	2^6	$2^{\underline{7}}$	2^8	2^9	2^{10}	$2^{\underline{11}}$	
2	4	8	3	6	12	11	9	5	10	7	1
6	10	…									

$3 \cdot 11 = 2^4 \cdot 2p = 2^{11}$ $\qquad$ logaritmer i bas 2.

6) Visa att $g^{32} = 1$ för alla $g \in U(\mathbb{Z}_{64}) = G$.

Jo, $|U(\mathbb{Z}_{64})| = |\{x \in \{0, 1, \ldots, 63\} : \text{sgd}(x; 64) = 1 | =$
$= |\{1, 3, 5, \ldots, 63\}| = 32$

$g^{|G|} = 1$ alla $g \in G$