2011-(03)mar-02: dag 13

Algebra

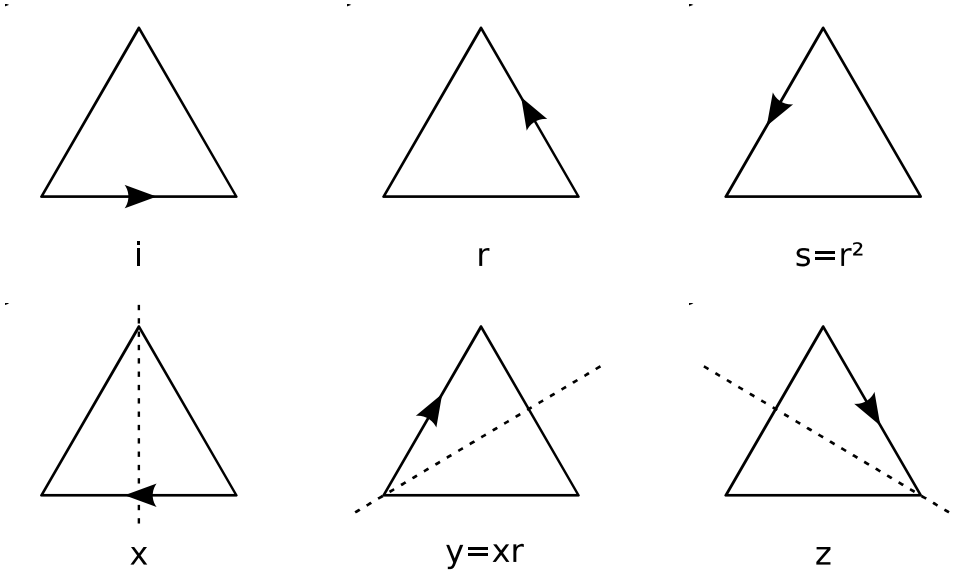
- Grupper
  - Gruppdefinitionen
    Ändliga grupper, grupptabeller
- Abelska grupper
- Ekvationslösning i grupper
  - Grupptabeller är en latinsk kvadrat
- Ordning
  - Ordningen för en grupp, $|G|$
  - Ordningen för ett gruppelement, $o(g)$
- Cyklisk grupper, $G = \langle g \rangle$
  - Generatorer, genererande element
- Övnings-KS 2

Vi börjar med “abstrakt algebra”, mest om grupper.

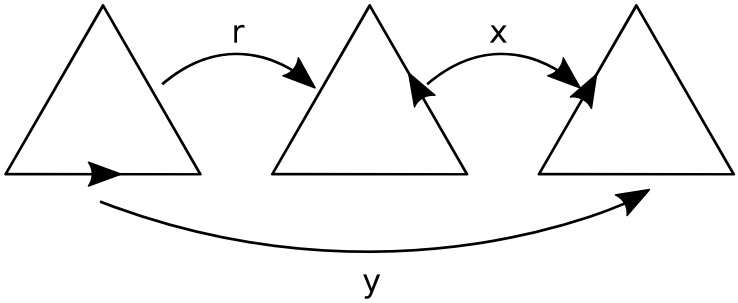
Exempel:

Symmetrier för en liksidig triangel
(det vill säga stela avbildningar som för över $\triangle_i$ sig själv).

Alla symmetrier $G_\triangle = \{i, r, s, x, y, z\}$



y = xr “först r, sedan x”



ix = xi = x

Definition:

$(G; *)$ är en grupp om

G1) $\forall\, x, y \in G : x * y \in G$
“slutenhet”

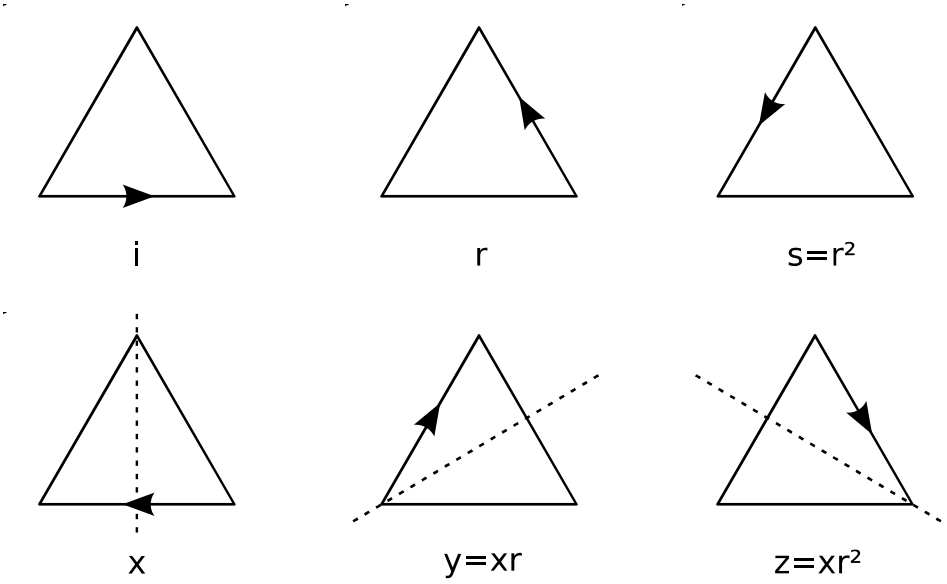
G2) $\forall\, x, y, z \in G : (x * y) * z = x * (y * z)$
“associativitet”

G3) $\exists\, I \in G : \forall\, x \in G \;:\; I * x = x * I = x$
“identitetselement”

G4) $\forall\, x \in G : \exists\, x^{-1} \in G \;:\; x * x^{-1} = x^{-1} * x = I$
“invers”

$(G_{\triangle}; \cdot)$ är en grupp ty axiomen G1, ..., G4 är uppfyllda.

Symmetrigrupper för en liksidig triangel, $G_{\triangle}$



	i	r	s	x	y	z
i	i	r	s	x	y	z
r	r	s	i	z	x	y
s	s	i	r	y	z	x
x	x	y	z	i	r	s
y	y	z	x	s	i	r
z	z	x	y	r	s	i

	i	r	r^2	x	xr	xr^2
i	i	r	r^2	x	xr	xr^2
r	r	r^2	i	xr^2	x	xr
r^2	r^2	i	r	xr	xr^2	x
x	x	xr	xr^2	i	r	r^2
r	xr	xr^2	x	r^2	i	r
xr^2	xr^2	x	xr	r	r^2	i

$r^3 = x^2 = i$

$rx = xr^2$

Andra exempel på grupper:

Oändliga: $(\mathbb{Z}; +)$, $(\mathbb{Q}\backslash\{0\}; \cdot)$, $(GL(n; \mathbb{R}); \cdot)$

reella n×n-matriser med det ≠ 0

Ändliga: $G_{\triangle}$, S_n, $(\mathbb{Z}_m; +)$, $(\mathbb{Z}_p\backslash\{0\}; \cdot)$, $\left(\{x \in \mathbb{R} \mid -1 < x\ 1\}, x*y = \frac{x+y}{xy+1}\right)$

p, primtal

En grupps struktur bestäms helt av grupptabellen.

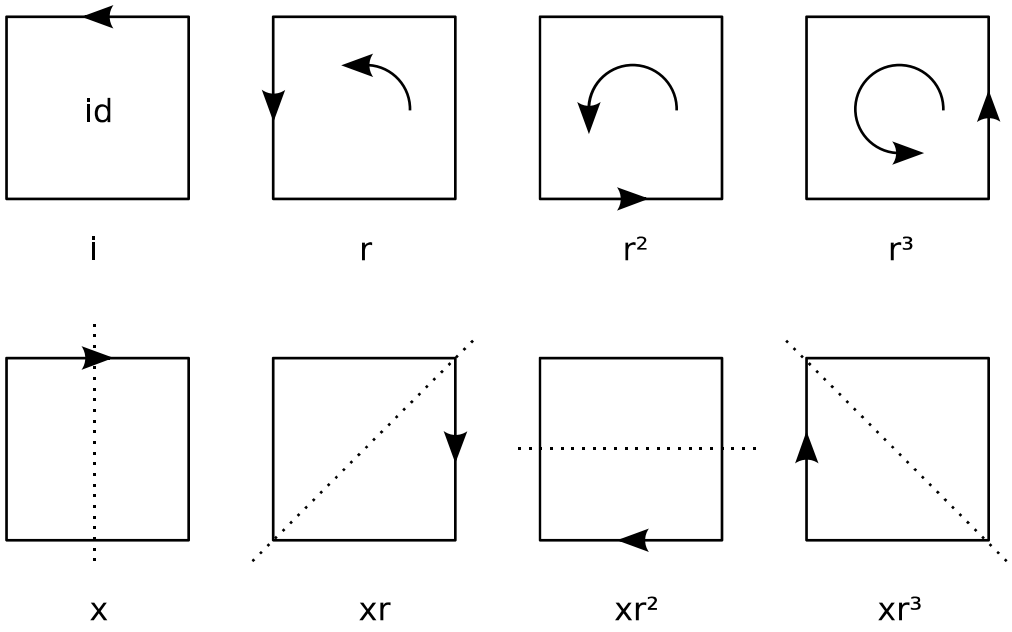
Exempel:

$(\mathbb{Z}_5; +)$:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

I = 0 här. Inversen (under +) till 3: $-3 = 2$ ty $2+3 = 3+2 = 0$.

Symmetrigruppen för en kvadrat, $G_{\square}$



$r^4 = x^2 = i$

$rx = xr^3$

	i	r	r^2	r^3	x	xr	xr^2	xr^3
i	i	r	r^2	r^3	x	xr	xr^2	xr^3
r	r	r^2	r^3	i	xr^3	x	xr	xr^2
r^2	r^2	r^3	i	r	xr^2	xr^3	x	xr
r^3	r^3	i	r	r^2	xr	xr^2	xr^3	x
x	x	xr	xr^2	xr^3	i	r	r^2	r^3
xr	xr	xr^2	xr^3	x	r^3	i	r	r^2
xr^2	xr^2	xr^3	x	xr	r^2	r^3	i	r
xr^3	xr^3	x	xr	xr^2	r	r^2	r^3	i

Om det i en grupp $(G; *)$ gäller att

$$a * b = b * a$$

för alla $a, b \in G$, kallas G abelsk eller kommutativ.

Exempel:

Abelska:

$(\mathbb{Z}_m; +)$, $(\mathbb{R}_+; \cdot)$, $(\mathbb{Z}_p \backslash \{0\}; \cdot)$, $(\{e\}; *)$, $(\mathbb{R}^n; +)$, $(\mathbb{Z}; +)$

Icke-abelska:

$G_\triangle$, $G_\square$, $(GL(n; \mathbb{R}); \cdot)$ $\quad n \geq 2$

Exempel på allmän sats för grupper:

Om $a, b \in G$, G är grupp så har $ax = b$ och $ya = b$ entydig lösning, x, y.

Ty: Existens:

$x = a^{-1}b$ är en lösning:

$$ax = a(a^{-1}b) \underset{G2}{=} (aa^{-1})b \underset{G4}{=} Ib \underset{G3}{=} b$$

Entydighet:

Om x är en lösning:

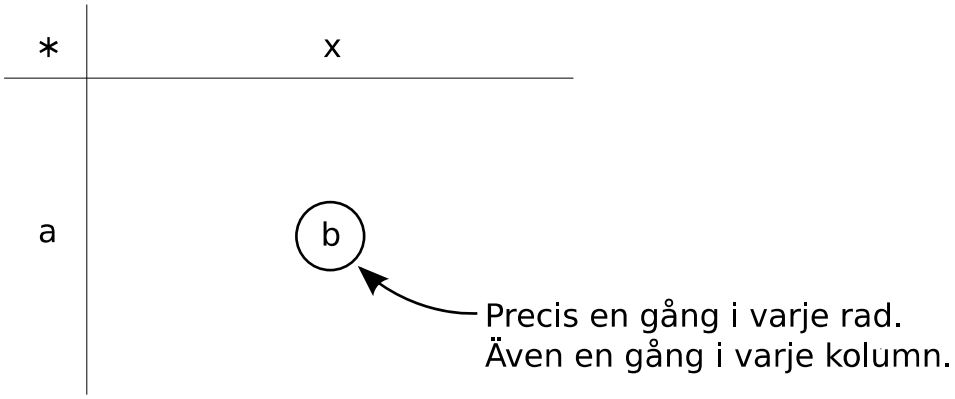
$ax = b \Rightarrow a^{-1}(ax) = a^{-1}b \Rightarrow \{G2\} \Rightarrow (a^{-1}a)x = a^{-1}b \Rightarrow \{G4\} \Rightarrow$

$\Rightarrow Ix = a^{-1}b \Rightarrow \{G3\} \Rightarrow x = a^{-1}b$

Andra ekvationen på samma sätt:

$y = ba^{-1}$

Så grupptabeller är latinska kvadrater.



Satsen ger också att man alltid kan förkorta:

$ax = ay \Rightarrow x = y \Leftarrow xa = ya$

Exempel:

$G = \{e, a, b, c\}$ är en grupp (med $\cdot$) och $x^2 = e$ för alla $x \in G$.
4 olika

Finn dess grupptabell!

Identitetselement? $e^2 = e = eI \Rightarrow e = I$ Identitetselement.

·	e	a	b	c	
e	**e**	**a**	**b**	**c**	← x = e
a	**a**	**e**	c	b	
b	**b**	c	**e**	a	Inte a, −e (rad) eller b (kolumn)
c	**c**	b	a	**e**	

↑ ex = x

↖ $x^2 = e$

G är abelsk

Allmän sats:

Om $|G| = p^2$ (p, primtal) så är G abelsk.

Ordningen för en grupp G: |G|

Ordningen för ett element $g \in G$: o(g),

det minsta > 0 sådant att $g^n = 1$ (1 identitetselement),
∞ om inget sådant finns.

Exempel:

$|G_\triangle| = 6$, o(x) = 2, o(r) = 3, o(i) = 1

y, z $\in G_\triangle$

s $\in G_\triangle$

Sats:

Om $g \in G$, en grupp, och o(g) = m, $g^s = 1$ (identitetselement) ⇔ m|s.

Ty:

⇒: Låt $g^s = 1$ och $s = qm+r$, $0 \leq r < m$.

så $1 = g^s = (g^m)^q \cdot g^r = 1^q \cdot g^r = g^r$

så $r = 0$ enligt defintionen av $o(g)$.

⇐: Klart.

Defintion:

En grupp, G, är cyklisk om det finns ett element $g \in G$ sådant att varje element i G är av formen g^n, något $n \in \mathbb{Z}$.

Ett sådant g kallas en generator, ett genererande element för G.

$G = \langle g \rangle$

Om $o(g) = m$:

$G = \{1, g, g^2, g^3, \ldots, g^{m-1}\}$ ser ut som $(\mathbb{Z}_m; +)$.
alla olika

Om $G = \langle g \rangle$ gäller $|G| = o(g)$

$o(g) = \infty$:

$G = \{\ldots, g^{-2}, g^{-1}, 1, g, g^2, \ldots\}$ ser ut som $(\mathbb{Z}; +)$.

Exempel:

$(\mathbb{Z}_{12}; +) = \langle 5 \rangle$ ty

n	0	1	2	3	4	5	6	7	8	9	10	11	(12)
ng	0	5	10	3	8	1	6	11	4	9	2	7	(0)