Forelesning, 17. januar 2024

Husk: Binær struktur $(S, *)$, $S \times S \xrightarrow{*} S$.

Assosiativ $a*(b*c) = (a*b)*c$

Kommutativ $a*b = b*a$

Isomorfi $S \cong T$: $\varphi: (S,*) \to (T,\circ)$
- bijeksjon (injektiv og surjektiv)
- $\varphi(a*b) = \varphi(a) \circ \varphi(b)$

Identitetselement $e*a = a*e = a$.

Eksempler: $(\mathbb{Z},+)$, $(\mathbb{Z},\cdot)$, $(\mathbb{Q},+)$ $(\mathbb{Q},\cdot)$, $M_2(\mathbb{R})$, S_n.

Def. Venstreinvers til $a \in S$: a' slik at $a'*a = e$
Høgreinvers $a*a' = e$

Def. 4.1 $(G,*)$ binær struktur kalles en GRUPPE dersom
- lukket under $*$: $g*h \in G \ \forall \ g,h \in G$
- assosiativ: $g*(h*k) = (g*h)*k$
- $\exists$ identitetselement $e \in G$: $e*g = g*e = g$
- $\forall g \in G \ \exists$ invers (høgre og venstre): $a*a' = a'*a = e$

Notasjon: Hvis G er endelig mengde
$|G|$ = antall elementer
$\overset{\text{def}}{=}$ ORDEN til G.

Eksempler:

Mengde	operasjon	identitet	invers
$\mathbb{Z}$	$+$	0	$-a$
$\mathbb{Q}\setminus\{0\}$	$\cdot$	1	$\frac{1}{a}$
$M_2(\mathbb{R})$	$+$	$\begin{pmatrix}0&0\\0&0\end{pmatrix}$	$-M$
Invertible 2×2-matriser $\to$ $GL_2(\mathbb{R})$	$\cdot$	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$	M^{-1}
S_n	komposisjon	id	

$$\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 1 & 5 & 2 & 4 \end{array}$$

$$\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 5 & 3 \end{array}$$

Def 4.3 Kommutativ gruppe kalles ABELSK GRUPPE

Litt mer om $GL_n(\mathbb{R})$: $M \cdot N$ matrisemultiplikasjon

Husk: $\det(M) \neq 0$

- $\det(M \cdot N) = \det(M) \cdot \det(N)$

$\det(M), \det(N) \neq 0 \Rightarrow \det(MN) \neq 0$

$\Rightarrow$ lukket under multiplikasjon

- $M \cdot \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & & \\ \vdots & & \ddots & \\ 0 & & & 1 \end{pmatrix} = M$

- Invertible matriser har invers.

Eksempel $(\mathbb{R}_+, \cdot) \simeq (\mathbb{R}, +)$

Bijektiv avbildning $\varphi: \mathbb{R} \to \mathbb{R}_+$

$x \longmapsto e^x$

$\varphi^{-1}: \mathbb{R}_+ \to \mathbb{R}$

$y \longmapsto \ln y$

$\varphi(x+y) = e^{x+y} = e^x \cdot e^y = \varphi(x) \cdot \varphi(y)$

$\varphi(0) = e^0 = 1$

$\varphi(-x) = e^{-x} = \frac{1}{e^x}$

Eksempel $(\mathbb{Q}_+, *)$ $a * b = \frac{ab}{2} \in \mathbb{Q}_+$

Assosiativ $a*(b*c) = a * \frac{bc}{2} = \frac{abc}{4}$

$(a*b)*c = \frac{ab}{2} * c = \frac{abc}{4}$

Identitet $a * 2 = \frac{a \cdot 2}{2} = a$

Invers $a * b = \frac{ab}{2} = 2 \Rightarrow b = \frac{4}{a}$

Eksempel $a * b = ab + a + b = (a+1)(b+1) - 1$

Assosiativt: $a*(b*c) = a*((b+1)(c+1)-1) = (a+1)(b+1)(c+1) - 1$

$(a*b)*c = ((a+1)(b+1)-1)*c = (a+1)(b+1)(c+1) - 1$

identitet $a * 0 = (a+1)(0+1) - 1 = a + 1 - 1 = a$

Invers $a * \left(\frac{-a}{1+a}\right) = (a+1)\left(\frac{-a}{1+a} + 1\right) - 1 = -a + a + 1 - 1 = 0$

Noen resultater:

Thm. 4.15 Forkortningsregel $gx = hx \Rightarrow g = h$

Bevis $\exists\, y$ slik at $xy = e$

$$(gx)y = (hx)y$$
$$g(xy) \quad h(xy)$$
$$ge \quad he$$
$$g \quad h$$

QED

Eks. $(\mathbb{Z}, +)$ gruppe
$x+5 = x+y \Rightarrow y = 5$
$(\mathbb{Z}, \cdot)$ ikke gruppe
$x \cdot 5 = x \cdot y$ gir ikke $y = 5$ siden vi kunne ha $x = 0$.

Thm 4.17 Entydige inverser. Anta $xy = xz = e$
$\Rightarrow y = z$

skriver x^{-1}

Bevis Forkortningsregel.

Cor 4.18 $(gh)^{-1} = h^{-1}g^{-1}$

Bevis $(gh)(gh)^{-1} = e$

$(gh)(h^{-1}g^{-1}) = g(hh^{-1})g^{-1} = geg^{-1} = gg^{-1} = e$

QED

Eksempler:

Gruppe med ett element

	e
e	e

Gruppe med to elementer

	e	a
e	e	a
a	a	

Hvis $aa = a^2 = a$, så er $a = e$.
Det betyr $a^2 = e$.

Gruppe med tre elementer

	e	a	b
e	e	a	b
a	a		
b	b		

$a^2 = a$ gir $a^2 = ea \Rightarrow a = e$

$a^2 = e$ betyr $a(ab) = a^2 b = eb = b$

Så $ab = e$ gir $a = b$

$ab = b$ gir $a = e$

$ab = a$ gir $b = e$

Det betyr $a^2 = b$ og derfor $ab = e$ siden

$ab = a$ gir $b = e$

$ab = b$ gir $a = e$

Tilsvarende for ba

Til slutt: $b^2 = bb = a^2 b = a(ab) = ae = a$

Noen spørsmål:

- Hvorfor må hver rad/søyle i gruppetabellen inneholde bare ulike elementer?
- Grupper med 4 elementer må være abelsk?
- $(ab)^2 = a^2 b^2 \Rightarrow ab = ba$ Vis!

Undergrupper

$H \subseteq G$: $\Leftrightarrow$ H er gruppe med samme operasjon

UNDERGRUPPE $\Leftrightarrow H \subseteq G$.

}

$H \leq G$

Noen begreper: Ekte undergruppe $H < G$, dvs $H \neq G$

Triviell undergruppe $\{e\} \leq G$.

Eksempel: $\mathbb{Z}_6 = \{0,1,2,3,4,5\}$ Gruppe.

$*$: addisjon modulo 6.

$\{0,2,4\}$ $\quad$ $\{0,3\}$

$\{0\}$

Hvordan kjenne igjen en undergruppe?

Thm. 5.14 $H \subseteq G$ er undergruppe hvis og bare hvis

i) H lukket under operasjon i G

ii) $e \in H$

iii) $\forall g \in H$; $g^{-1} \in H$.

Bevis. Den ene veien er oppfylt etter def av gruppe

Anta $H \subseteq G$ og i), ii) og iii) er oppfylt

- Associativitet arves fra G.
- $e \in H$ er ii)
- Inverser er iii)

De enkleste gruppene: Sykliske

Thm. 5.17 $g \in G$ $\quad H := \{g^n \mid n \in \mathbb{Z}\}$ gruppe

Minste undergruppe av G som inneholder g.

Syklisk gruppe

Bevis i) Lukket $g^n \cdot g^m = g^{n+m}$

ii) $e = g^0 \in H$

iii) $(g^n)^{-1} = g^{-n}$

Vi skriver $H = \langle g \rangle$ $\quad g$: generator for H.

$g^n \neq e$ for alle $n \neq 0$ UENDELIG SYKLISK

$g^n = e$ for en $n \in \mathbb{Z}$ ENDELIG SYKLISK

Hvis n er det minste positive tallet slik at $g^n = e$

$$H = \langle g \rangle \simeq \mathbb{Z}_n = \{0, 1, \ldots, n-1\}.$$

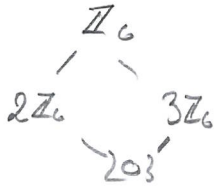
addisjon modulo n

Eksempel $H = \{0,1,2,3,4,5\}$ addisjon modulo 6.

$$\Rightarrow H \simeq \mathbb{Z}_6 = \langle 1 \rangle = \langle 5 \rangle$$

Undergrupper: $\{0,2,4\}$ (= $\{0,4,2\}$), $\{0,3\}$, $\{0\}$

$2H \trianglelefteq \mathbb{Z}_3$, $3H \trianglelefteq \mathbb{Z}_2$



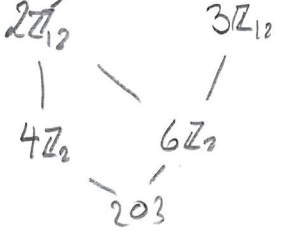
$2\mathbb{Z}_6 = \{0\cdot 2, 1\cdot 2, 2\cdot 2, 3\cdot 2, 4\cdot 2, 5\cdot 2\}$

$= \{0, 2, 4, 0, 2, 4\}$

$= \{0, 2, 4\}$

$H = \{0,1,2,3,4,5,6,7,8,9,10,11\}$ modulo 12

$\simeq \mathbb{Z}_{12}$



svarer til (oppned)



Addisjonstabell for $\mathbb{Z}_6$:

	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Tabell for gruppe operasjon har SUDOKU-egenskapen:
Alle elementene i hver rad/søyle er forskjellige

Bevis Anta $a*b = a*c$ hvor $b \neq c$
Forkortning gir $b = c$ Motsigelse.

Grupper med 4 elementer:

*	e	a	b	c
e	e	a	b	c
a	a			
b	b			
c	c			

Rute $a*b = \begin{cases} e \\ c \end{cases}$

*	e	a	b	c
e	e	a	b	c
a	a	(c)	e	(b)
b	b	(e)	(c)	(a)
c	c	(b)	(a)	(e)

$a*c = c \Rightarrow a = e$
dus $\begin{cases} a*c = b \\ a*a = c \end{cases}$

$b*a = b \Rightarrow a = e$
dus $\begin{cases} b*a = a \\ c*a = b \end{cases}$

$b*c = c \Rightarrow b = e$
dus $\begin{cases} b*c = a \\ b*b = c \end{cases}$

$\Rightarrow \begin{matrix} c*b = a \\ c*c = e \end{matrix}$

*	e	a	b	c
e	e	a	b	c
a	a	(e)	c	b
b	b	(c)		
c	c	(b)		

$a*c = b$
$a*a = e$

Tilsv. argument som for $a*b = e$

$b*b = (c*a)*b$
$= c*(a*b)$
$= c*c$

$b*c = (c*a)*b$
$= c*(a*b)$
$= c*b$

	e	a	b	c
e	e	a	b	c
a	a	(b)	c	e
b	b	(c)	(e)	(a)
c	c	(e)	(a)	(b)

c a c a
c b a

4 muligheter

1)

	e	a	b	c
e	e	a	b	c
a	a	c	e	b
b	b	e	c	a
c	c	b	a	e

$a \mapsto b$, $b \mapsto c$, $c \mapsto a$

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

Isomorfe

$a \mapsto b$, $b \mapsto c$, $c \mapsto a$

	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

2)

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

	e	a	b	c
e	e	a	b	c
a	a	c	e	b
b	b	e	c	a
c	c	b	a	e

$a \mapsto b$, $b \mapsto c$, $c \mapsto a$

	e	b	c	a
e	e	b	c	a
b	b	a	e	c
c	c	e	a	b
a	a	c	b	e

=

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

To grupper 1) $\mathbb{Z}_4 = \{0,1,2,3\}$

$e = 0$
$a = 1$
$b = 3$
$c = 2$

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	1	0
3	3	1	2	0

2) $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0), (0,1), (1,0), (1,1)\}$

	(0,0)	(0,1)	(1,0)	(1,1)	
(0,0)	(0,0)	(0,1)	(1,0)	(1,1)	(e)
(0,1)	(0,1)	(0,0)	(1,1)	(1,0)	(a)
(1,0)	(1,0)	(1,1)	(0,0)	(0,1)	(b)
(1,1)	(1,1)	(1,0)	(0,1)	(0,0)	(c)

struktur:

$a+a = b+b = c+c = e$

$a+b = c \quad a+c = b \quad b+c = a$