2011-(03)mar-21: dag 16

Mer algebra

- Direkta produkter av grupper
- Normala grupper
- Ringar och kroppar
- Permutationsgrupper

Direkta produkter av grupper

Från förra övningen

7) Definiera den direkta produkten $(G_1, *_1) \times (G_2, *_2) = (G_1 \times G_2, \circ)$ av $(g_1, g_2) \circ (h_1, h_2) = (g_1 *_1 h_1, g_2 *_2 h_2)$.
$g_1, h_1 \in G_1$; $g_2, h_2 \in G_2$

a) Verifiera att detta är en grupp.

G1, Sluten:

Gäller eftersom det gäller för G_1 och G_2.

$g_1 *_1 h_1 \in G_1$
$g_2 *_2 h_2 \in G_2$

G2, Associativ:

Gäller eftersom det gäller för G_1 och G_2.

Vänsterelementet: $g_1 *_1 h_1 \in G_1$
Högerelementet: $g_2 *_2 h_2 \in G_2$

G3, Identietselement:

$1 = (1_1, 1_2)$

1_1 är identietselementet i G_1.
1_2 är identietselementet i G_2.

$(g_1, g_2) \circ (1_1, 1_2) = (g_1 *_1 1_1, g_2 *_2 1_2) = (g_1, g_2)$

G4, Inverser:

$(g, h)^{-1} = (g^{-1}, h^{-1})$

$(g, h) \circ (g^{-1}, h^{-1}) = (g *_1 g^{-1}, h *_2 h^{-1}) = (1_1, 1_2) = 1$

$(\mathbb{R}, +) \times (\mathbb{R}, +) = (\mathbb{R}^2, +)$

b) Visa att $(\mathbb{Z}_2, +) \times (\mathbb{Z}_3, +) \cong (\mathbb{Z}_6, +)$
(Vi ska alltså visa isomorfi.)

Båda grupperna $[\mathbb{Z}_2 \times \mathbb{Z}_3$ och $\mathbb{Z}_6]$ är cykliska av ordningen 6.

En isomorfi: $\mathbb{Z}_2 \quad \mathbb{Z}_3 \quad \mathbb{Z}_6$

$\phi(0, 0) = 0$
$\phi(1, 1) = 1$
$\phi(0, 2) = 2$
$\phi(1, 0) = 3$
$\phi(0, 1) = 4$
$\phi(1, 2) = 5$
$\phi(0, 0) = 0$

Detta är en isomorfi på grund av att båda är cykliska. Beror på additionen.

Däremot $(\mathbb{Z}_3, +) \times (\mathbb{Z}_3, +) \not\cong (\mathbb{Z}_9, +)$ eftersom alla element har ordning 1 eller 3 i $\mathbb{Z}_3$, $(\mathbb{Z}_3, +) \times (\mathbb{Z}_3, +)$ är alltså inte cyklisk; det är dock $\mathbb{Z}_9$.

Normala delgrupper

Definition: En delgrupp, N, till en grupp, G, är en normal delgrupp $(N \trianglelefteq G)$ om vänstersidoklasser = högersidoklasser.

Det vill säga:

$$gN = Ng \ \forall \ g \in G$$

Exempel: Alla delgrupper för abelska (kommutativa) grupper.

För $G_\square$: $\{i, r^2\}$, $\{i, r, r^2, r^3\}$

Om N är en normal degrupp så bildas

$G/N = \{gN \mid g \in G\} = \{\text{normal}\} = \{Ng \mid g \in G\}$, kvotgruppen som är en grupp.

Motivieringen till namnet är: $|G| = |G/N| \cdot |N|$

$g_1N \cdot g_2N = \{g_1n_1g_2n_2 \mid n_1, n_2 \in N\} = \{\text{normal}\} = \{g_1g_2n_3n_2 \mid n_3, n_2 \in N\} =$
$= g_1g_2N$ och $g_1g_2N \leq g_1Ng_2N$ så $g_1Ng_2N = g_1g_2N$.

G/N med operationen $g_1Ng_2N = g_1g_2N$ är en grupp:

G1, Sluten: $g_1g_2N \in G/N \Rightarrow \{g_1g_2 = h\} \Rightarrow hN \in G/N$

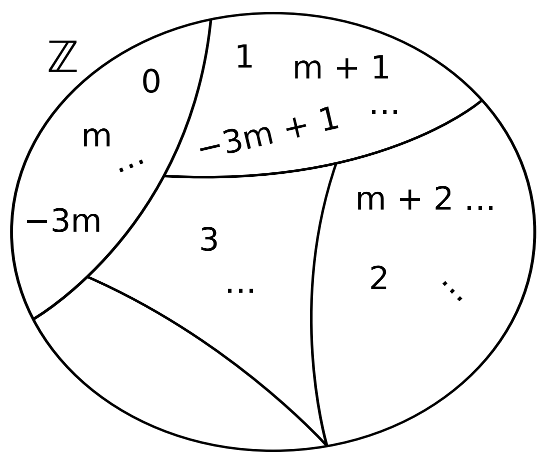
G2, Associativ: $(g_1Ng_2N)g_3N = (g_1g_2)g_3N = g_1(g_2g_3)N = g_1N(g_2Ng_3N\ )$

G3, Identietselement: $N = 1N$

G4, Inverser: $gN)^{-1} = g^{-1}N$

Exempel: $(\mathbb{Z}, +)$ (abelsk, så sidoklasserna är normala)

$(\mathbb{Z}, +) / (m\mathbb{Z}, +) = (\mathbb{Z}_m, +)$



G grupp
N normal delgrupp

$G/N = \{gN \mid g \in G\}$

Exempel: $N = \{i, r^2\}$

$G_{\square}/N = \{\{i, r^2\} = e, \{r, r^3\} = a, \{x, xr^2\} = b, \{xr, xr^3\} = c\}$

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

$N = iN = r^2N$ $xN = Nx = xr^2N =$
$N = Ni = Nr^2$ $= Nxr^2$

Till exempel:

$ab = \{r, r^3\}\{x, xr^2\} =$
$= \{rx, rxr^2, r^3x, r^3xr^2\} =$
$= \{xr^3, xr^2r^3, r^3x, r^3xr^2\} =$
$= \{xr^3, xr, xr, xr^2r\} =$
$= \{xr^3, xr\}$

Gruppisomorfi: $\psi : G_1 \to G_2$ $((G_1, \ast), (G_2, \circ))$
sådan att
$\psi(g \ast h) = \psi(g) \circ \psi(h)$

Då är $G \cong G/N$
Varje homomorfi ges så (av någon normal delgrupp)

Ringar är mängder med 2 operationer.
En ring (R, med addition och multiplikation) betecknas $(R, +, \cdot)$,
och definieras av: (Ringar liknar $\mathbb{Z}$.)

(1) $(R, +)$ är en abelsk grupp, med identitetselement 0.

(2) $(R, \cdot)$ är sluten, associativ, med identietselement 1.

(3) Multiplikation $(\cdot)$ är distributiv över addition $(+)$:

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) = ab + ac$$
$$(a + b) \cdot c = (a \cdot c) + (b \cdot c) = ac + bc$$

Exempel på ringar:

$\mathbb{Z}$, $\mathbb{Z}_m$, $M_n(R)$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$, $\mathbb{R}[x]$

$M_n(R)$ = $n \times n$-matriser med element i ringen R.
$\mathbb{R}[x]$ = Polynom med koefficienter i $\mathbb{R}$. (Polynom över $\mathbb{R}$)

$(F, +, \cdot)$ (F skrivs ofta $\mathbb{F}$) är en kropp (en. field) om det är en ring sådan att
$(F \setminus \{0\}, \cdot)$ är en abelsk grupp.

Exempel (p primtal):

$$\mathbb{R}, \mathbb{Q}, \mathbb{C}, \mathbb{Z}_p, F(x) = \left\{ \frac{p(x)}{q(x)} \;\middle|\; \begin{array}{l} p, q \in F[x] \\ q(x) \neq 0 \end{array} \right\}$$

I en ring R: $x \in R$ kallas invertibel i R omm det finns $u \in R$ sådant att
$ux = xu = 1$; då är $u = x^{-1}$

$U(R) = \{x \in R : x \text{ invertibelt}\}$

Sats: $(U(R), \cdot)$ är en grupp för varje ring R.

Exempel: $U(\mathbb{Z}) = \{-1, 1\}$
$U(\mathbb{Z}_m) = \{x \in \mathbb{Z}_m : \text{sgd}(x, m) = 1\}$

En permutation är en bijektiv funktion med samma domän som kodomän (från en mängd till sig själv):

$\pi : X \to X$, π bijektiv

S_n = mängden av alla permutationer av $[n] = \{1, 2, 3, \ldots, n\}$

$|S_n| = n!$ (Antelet permutationer)

$(S_n, \circ)$ är en grupp:

G1: En sammansättning av bijektioner är också en bijektion.
G2: Associativitet gäller alltid för sammasättning av funktioner.
G3: Identietspermutationen $id(x) = x$ är identietselement.

$\{1, 2, 3, \ldots\} \to \{1, 2, 3, \ldots\}$

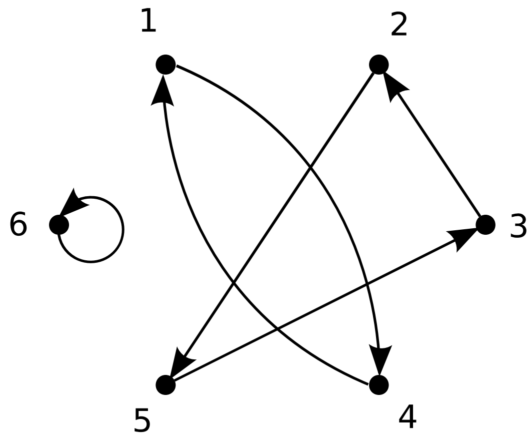
G4: Inversen som funktion är inverselement.
Inversen av en bijektion är en bijektion.

Varje $g \in G$ (G grupp) ger en permutation av g.

$\pi_g(h) = gh$ $\pi_g \in S_G$ (G är isomorf med en delgrupp av S_G)

För att beskriva permutationer

Till exempel $\pi \in S_6$:



Tvåradsnotation som beskriver bijektionen:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 2 & 1 & 3 & 6 \end{pmatrix}$$

Enradsnotation:

[4 5 2 1 3 6]

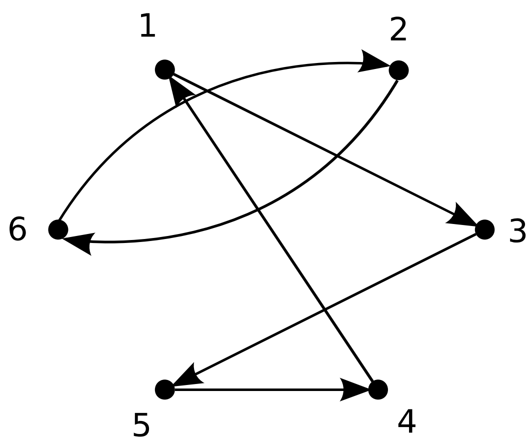
Det vill säga nedra raden i tvåradsnotation och övre raden är underförstådd.

Cykelnotation:

(1 4 1)(2 5 3 2)(6 6)
alltså:
(1 4)(2 5 3)(6)

Cykelnotation, börja någonstans och följ “avbildningspilarna” till man kommer tillbaka. Upprepa tills alla element har tagits med.

$\sigma \in S_6$



Tvåradsnotation:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 5 & 1 & 4 & 2 \end{pmatrix}$$

Enradsnotation:

[3 6 5 1 4 2]

Cykelnotation:

(1 3 5 4)(2 6)

Produkten i S_6: (först σ sedan π)

$$\pi\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 5 & 1 & 4 & 2 \\ 2 & 6 & 3 & 4 & 1 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 3 & 4 & 1 & 5 \end{pmatrix} = (1\ 2\ 6\ 5)(3)(4)$$

(id→σ i först–andra raden, σ→π i andra–tredje raden)