Diskret matematik 2018-04-23 #13

Cykliska grupper

Def Om $(G,\circ)$ är en grupp och $g \in G$ så definierar vi

$g^n = \overbrace{g \circ g \circ \dots \circ g}^{n \text{ kopior av } g}$ för $n \in \mathbb{N}$

$g^{-n} = \overbrace{g^{-1} \circ g^{-1} \circ \dots \circ g^{-1}}^{n \text{ kopior av } g^{-1}}$ för $n \in \mathbb{N}$

$g^0 = id$

VARNING: I vissa grupper är $\circ$ faktiskt plus $(+)$

tex. är $1^n = n$ i $(\mathbb{Z},+)$

Sats Låt G vara en grupp och låt $g \in G$. Vi definierar

$\langle g \rangle = \{g^n : n \in \mathbb{Z}\} = \{\dots, g^{-2}, g^{-1}, id, g, g^2, \dots\}$

Detta är en delgrupp till G som kallas gruppen som genereras av g. Elementet g kallas för generator till denna grupp.

Bevis Delgruppstestet säger att $\langle g \rangle$ är en delgrupp om

1) $\langle g \rangle \neq \emptyset$ & 2) $h \circ k^{-1} \in \langle g \rangle$ för alla $h,k \in \langle g \rangle$

1) $\langle g \rangle \neq \emptyset$ för $g \in \langle g \rangle$
2) Om $h \in \langle g \rangle$ då är $h = g^n$ för något $n \in \mathbb{Z}$ och likaså är $k \in \langle g \rangle$ $k = g^m$, $m \in \mathbb{Z}$.

Så $h \circ k^{-1} = g^n \circ (g^m)^{-1} = g^n \circ g^{-m} = g^{n-m} \in \langle g \rangle$ ∎

$G = (\mathbb{Z},+)$ $g = 3$ $\langle g \rangle = \langle 3 \rangle = \{3^n : n \in \mathbb{Z}\}$
$= \{3n : n \in \mathbb{Z}\}$

$G = (\mathbb{R}^*,\cdot)$ $g = 3$ $\langle g \rangle = \langle 3 \rangle = \{3^n : n \in \mathbb{Z}\}$

Def Om G är en grupp och det finns ett element $g \in G$ så att $G = \langle g \rangle$ är G en cyklisk grupp.

Exempel i PPT på Canvas

$(\mathbb{Z},+)$ är cyklisk

$(\mathbb{Z}_n,+)$ är cyklisk

$(\mathbb{Z}_2 \times \mathbb{Z}_2,+)$ är inte cyklisk

$\{id, R_{120}, R_{240}\} \subset Symm_\Delta$ är cyklisk

$\{id, S_1, S_2, S_3\} \subset Symm_\Delta$ är inte cyklisk. Inte ens en delgrupp!

Def Låt G vara en grupp och låt $g \in G$. Ordningen $\text{ord}(g)$ för g definieras som storleken $|\langle g \rangle|$ av gruppen genererad av g. Vi skriver $\text{ord}(g) = \infty$ om $\langle g \rangle$ är oändlig.

I $(\mathbb{Z}_6, +)$ har elementet 2 ordning
$\text{ord}(2) = |\langle 2 \rangle| = |\{0, 2, 4\}| = 3$

$(\mathbb{Z}_{10}, +)$: elementet 2 har ordning

$|\langle 2 \rangle| = |\{0, 2, 4, 6, 8\}| = 5$

Sats Om G är en ändlig grupp och $g \in G$, då är
$\text{ord}(g) =$ det minsta heltalet $m \in \mathbb{N}$ så att $g^m = id$.

Faktiskt är $\langle g \rangle = \{id, g, g^2, \ldots, g^{m-1}\}$.

Vad är det minsta m så att $2^m = 0$ i $(\mathbb{Z}_{10}, +)$?

Eftersom operationen är $+$ så betyder detta $\overbrace{2+2+\ldots+2}^{m}$

$2m = 0$
Detta är $m = 10/2 = 5$

Inversen till g är g^{m-1}:

$g \circ g^{m-1} = g^m = id$
$g^{m-1} \circ g = g^m = id$

Permutationsgrupper

Sats Låt A vara en icke-tom mängd. Då skriver vi

$S_A = \{\text{bijektioner } f: A \to A\}$

för mängden av alla bijektioner från A till sig själv. Under funktionssammansättning är detta en grupp.

När $A = \{1, 2, \ldots, n\}$ skriver vi S_n istället. "Symmetriska gruppen"

$|S_n| = n!$

Def För element $x_1, \ldots, x_n, y_1, \ldots, y_n \in A$

skriver vi

$\begin{bmatrix} x_1 & x_2 & \cdots & x_n \\ y_1 & y_2 & \cdots & y_n \end{bmatrix}$ för funktionen $f: A \to A$ "Tablåform/ Tvårads-form"

med $f(x_1) = y_1$
$\vdots$
$f(x_n) = y_n$

Exempel

$$S_{\{a,b,c\}} = \left\{ \begin{bmatrix} a & b & c \\ a & b & c \end{bmatrix} \begin{bmatrix} a & b & c \\ a & c & b \end{bmatrix} \begin{bmatrix} a & b & c \\ b & c & a \end{bmatrix} \begin{bmatrix} a & b & c \\ b & a & c \end{bmatrix} \begin{bmatrix} a & b & c \\ c & a & b \end{bmatrix} \begin{bmatrix} a & b & c \\ c & b & a \end{bmatrix} \right\}$$

Detta är en grupp, med operationen sammansättning

$$\begin{bmatrix} a & b & c \\ b & c & a \end{bmatrix} \circ \begin{bmatrix} a & b & c \\ c & a & b \end{bmatrix} = \begin{bmatrix} a & b & c \\ a & b & c \end{bmatrix} = id$$

(Alltså är $\begin{bmatrix} a & b & c \\ c & a & b \end{bmatrix}^{-1} = \begin{bmatrix} a & b & c \\ b & c & a \end{bmatrix}$)

OBS! Vi läser permutationsmultiplikationer från HÖGER!

Exempel/metod (Inverser genom 2-radsform)

Vad är $\begin{bmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & \dots & a_n \end{bmatrix}^{-1}$?

$$= \begin{bmatrix} a_1 & a_2 & \dots & a_n \\ 1 & 2 & \dots & n \end{bmatrix}$$

Ordna ev. om kolonnerna så att det står $1, 2, \dots, n$ på övre raden.

Så t.ex. $\begin{bmatrix} a & b & c \\ c & a & b \end{bmatrix}^{-1} = \begin{bmatrix} c & a & b \\ a & b & c \end{bmatrix} = \begin{bmatrix} a & b & c \\ b & c & a \end{bmatrix}$

Def^n (Cykelform)

Med $(a_1\ a_2\ \dots\ a_k)$ menas permutationen (cykel)

$\begin{bmatrix} a_1 & a_2 & \dots & a_{k-1} & a_k \\ a_2 & a_3 & \dots & a_k & a_1 \end{bmatrix}$ (och identitets-funktionen på andra element)

En permutation sägs vara på cykelform om den är en produkt av disjunkta cykler.

Så t.ex. i S_5 betyder

$(1\ 3\ 4) = \begin{bmatrix} 1 & 3 & 4 & 2 & 5 \\ 3 & 4 & 1 & 2 & 5 \end{bmatrix}$ 

Exempel/metod (skriva på cykelform)

Skriv $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 6 & 3 & 1 & 4 \end{bmatrix} = (1\ 5)(2)(3\ 6\ 4)$ ← på cykelform

$(1\ 2\ 3)(3\ 4\ 5)$ ← inte på cykelform, för inte disjunkta.