

(Diskret matte D, ht16: F20, on 2 nov 2016)

Cykliska grupper

En grupp G är **cyklisk** om för något $x \in G$ varje $g \in G$ är x^n för något $n \in \mathbb{Z}$.
(Om $n < 0$ skall x^n förstås som $(x^{-1})^{-n}$.)

x **genererar** G , $G = \langle x \rangle$,

$o(x) = m$: $C_m = \{1, x, x^2, \dots, x^{m-1}\} \approx (\mathbb{Z}_m, +)$

$o(x) = \infty$: $C_\infty = \{\dots, x^{-2}, x^{-1}, 1, x, x^2, \dots\} \approx (\mathbb{Z}, +)$

(Om $g = x^i$ låter man $i = \log_x g \in \mathbb{Z}_m$ ($\in \mathbb{Z}$ om $o(x) = \infty$). Då gäller $\log_x(gh) = \log_x g + \log_x h$.)

Direkt produkt av grupper

Om A, B är grupper, är $(A \times B, *)$ med $(a_1, b_1) * (a_2, b_2) = (a_1 a_2, b_1 b_2)$ också en grupp, den **direkta produkten** av A och B .

Enligt kinesiska restsatsen gäller om $\text{sgd}(m_i, m_j) = 1$ då $i \neq j$:

$$C_{m_1 \dots m_k} \approx C_{m_1} \times \dots \times C_{m_k}$$

Delgrupper

H är en **delgrupp** till $(G, *)$ om $H \subseteq G$ och $(H, *)$ är en grupp.

Sats: Om G är en grupp och $H \subseteq G$ gäller att

$$H \text{ är en delgrupp till } G \Leftrightarrow \begin{cases} S0 & H \neq \emptyset \\ S1 & x, y \in H \Rightarrow xy \in H \\ S2 & x \in H \Rightarrow x^{-1} \in H \end{cases}$$

Om H är **ändlig**, räcker $S0$ och $S1$.

Exempel: Om G är en grupp är

$$Z(G) = \{z \in G \mid zg = gz \text{ för alla } g \in G\}$$

en delgrupp till G . Den kallas **G 's centrum**.

Varje $x \in G$ (G en grupp) genererar en **cyklisk delgrupp**,

$$\langle x \rangle = \{x^i \mid i \in \mathbb{Z}\}.$$

Då är $o(x) = |\langle x \rangle|$.