(Diskret matte SF1688, HT22: F11)

$U(\mathbb{Z}_m)$ är gruppen av alla inverterbara element i $\mathbb{Z}_m$.

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, $\quad G = \langle x \rangle$,
$o(x) = m : \quad C_m = \{1, x, x^2, \dots, x^{m-1}\} \approx (\mathbb{Z}_m, +)$
$o(x) = \infty : \quad C_\infty = \{\dots, x^{-2}, x^{-1}, 1, x, x^2, \dots\} \approx (\mathbb{Z}, +)$

Direkt produkt av grupper Om A, B är grupper, är $(A \times B, *)$ med $(a_1, b_1) * (a_2, b_2) = (a_1a_2, b_1b_2)$ också en grupp, den **direkta produkten** av A och B.

Enligt **kinesiska restsatsen** (nästa vecka) gäller om $sgd(m_i, m_j) = 1$ då $i \neq j$:

$$C_{m_1 \cdot \ldots \cdot m_k} \approx C_{m_1} \times \ldots \times C_{m_k}$$

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

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

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

Exempel: Om G är en grupp är

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

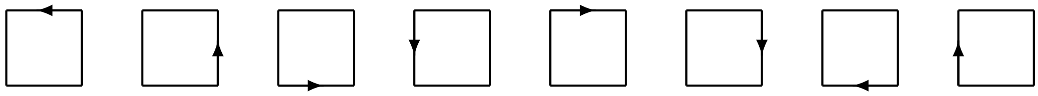
en delgrupp till G. Den kallas ***G*:s centrum**.

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

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

Då är $o(x) = |\langle x \rangle|$.

Ett exempel: Elementen i $G_\square$ är symmetriavbildningar för kvadraten:
Rotationer: speglingar:



$i \quad r \quad r^2 \quad r^3 \quad x \quad rx \quad r^2x \quad r^3x$

(i är identitetsavbildningen. Figurerna visar hur motsvarande avbildning "flyttar" kvadraten från "standardläget", det vid i ovan.)

Gruppen **genereras** av $\{x, r\}$, dvs varje element kan som ovan skrivas som r^jx^i med $i \in \{0, 1\}$, $j \in \{0, 1, 2, 3\}$. Gruppen beskrivs helt av **relationerna**

$$x^2 = r^4 = i, \quad xr = r^3x$$

Grupptabellen blir:

	i	r	r^2	r^3	x	rx	r^2x	r^3x
i	i	r	r^2	r^3	x	rx	r^2x	r^3x
r	r	r^2	r^3	i	rx	r^2x	r^3x	x
r^2	r^2	r^3	i	r	r^2x	r^3x	x	rx
r^3	r^3	i	r	r^2	r^3x	x	rx	r^2x
x	x	r^3x	r^2x	rx	i	r^3	r^2	r
rx	rx	x	r^3x	r^2x	r	i	r^3	r^2
r^2x	r^2x	rx	x	r^3x	r^2	r	i	r^3
r^3x	r^3x	r^2x	rx	x	r^3	r^2	r	i

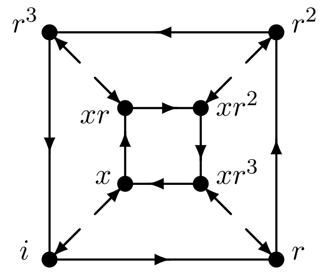
Vi ser att r genererar cyklisk delgrupp $\langle r\rangle = \{i, r, r^2, r^3\}$

Om cayleygrafer (orientering, kommer ej på tentan)

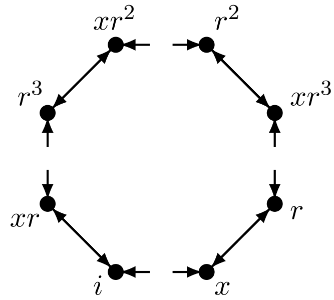
En cayleygraf för en grupp (egentligen för en framställning av gruppen med generatorer) beskriver gruppen fullständigt.

Grafen har ett hörn för varje element i gruppen och om gruppen genereras av a, b, ... (dvs om varje $g \in G$ kan skrivas som en produkt av sådana och deras inverser) har den riktade kanter med olika mörkningar (eller färger), svarande mot a, b, ... En a-kant från hörn g slutar i hörn ag osv. (multiplikationen kan också ske från höger, men vi använder multiplikation från vänster som konvention.)

En cayleygraf för $G_\square$, kvadratens symmetrigrupp: Gruppen genereras ju av r och x med relationerna $\boldsymbol{r^4 = x^2 = i,\ rx = xr^3}$.
Heldragna pilar svarar här mot r, avbrutna mot x.
För att t.ex. finna $r^3 \cdot xr^2$ i grafen: gå från hörnet r^3 längs en pilföljd som leder från i till xr^2, t.ex. x, r, r (eller r, r, x eller r, r, r, x, r), och hamna i resultatet, xr^3.



Samma grupp kan beskrivas med denna graf:
Här används generatorerna x och y (där $y = xr$) med relationerna $\boldsymbol{x^2 = y^2 = (xy)^4 = i}$.
Heldragna pilar svarar nu mot y, avbrutna mot x.



Ett sådant diagram med punkter och pilar är en cayleygraf för en grupp precis om:

1. Både till och från varje punkt går precis en pil av varje typ.
2. Om en pilföljd från en punkt leder tillbaks till startpunkten, gör motsvarande pilföljd från en annan punkt också det (t.ex. r, x, r, r, r, x, r, r i den övre grafen).

Man kan välja vilken punkt man vill som enhetselement och beräkna vilka element som svarar mot övriga punkter.