(Diskret matte F, ht17: L14, ti 21 nov 2017)

Begreppet **grupp** definieras **axiomatiskt**:

$(G, *)$ är en **grupp** omm G1–G4 är uppfyllda (G en mängd, $*$ en binär operation på G),

G1.	$\forall\, x, y \in G$	$x * y \in G$	slutenhet
G2.	$\forall\, x, y, z \in G$	$(x * y) * z = x * (y * z)$	associativitet
G3.	$\exists\, e \in G\ \forall\, x \in G$	$e * x = x * e = x$	identitet
G4.	$\forall\, x \in G\ \exists\, x^{-1} \in G$	$x * x^{-1} = x^{-1} * x = e$	invers

($\forall x \in G \ldots$ står för "för alla x i G : $\ldots$", $\exists x \in G \ldots$ för "det finns (minst) ett x i G så att : $\ldots$".)

(G1 behövs egentligen inte, det ingår i begreppet "binär operation på G".)

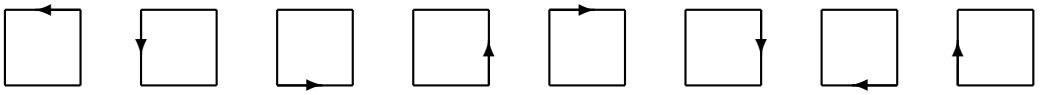
(e i G4 skall vara samma som i G3, vilket det strängt taget inte står.)

(Vi skriver ofta $\cdot$ (eller inget) för $*$ och 1 eller I för e i en grupp.
För abelska grupper skrivs ofta $+$ för $*$ och 0 för e.)

Exempel: Symmetrigrupper, $\{n \times n$-matriser med determinant $\neq 0\}$,
$(\mathbb{Z}, +)$, $(\mathbb{Z}_m, +)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$, S_n, $(\mathbb{Z}_p \setminus \{0\}, \cdot)$ (p primtal) , $(U(\mathbb{Z}_m), \cdot), \ldots$

Som exempel visades **grupptabellerna** ("multiplikationstabellerna") för $G_\triangle$ och $G_\square$, **symmetrigrupperna** för en **liksidig triangel** och för en **kvadrat**.

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



i r r^2 r^3 x xr xr^2 xr^3

(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 $x^i r^j$ med $i \in \{0, 1\},\ j \in \{0, 1, 2, 3\}$. Gruppen beskrivs helt av **relationerna**

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

Grupptabellen blir:

	i	r	r^2	r^3	x	xr	xr^2	xr^3
i	i	r	r^2	r^3	x	xr	xr^2	xr^3
r	r	r^2	r^3	i	xr^3	x	xr	xr^2
r^2	r^2	r^3	i	r	xr^2	xr^3	x	xr
r^3	r^3	i	r	r^2	xr	xr^2	xr^3	x
x	x	xr	xr^2	xr^3	i	r	r^2	r^3
xr	xr	xr^2	xr^3	x	r^3	i	r	r^2
xr^2	xr^2	xr^3	x	xr	r^2	r^3	i	r
xr^3	xr^3	x	xr	xr^2	r	r^2	r^3	i

Slut på exemplet.

Om $ab = ba$ för alla $a, b \in G$ kallas G **abelsk** (eller **kommutativ**)

Sats: Om a, b är element i gruppen G har ekvationerna $\boldsymbol{ax = b}$ och $\boldsymbol{ya = b}$ **entydiga lösningar** $x = a^{-1}b,\ y = ba^{-1}$ i G.
Grupptabellen är alltså en **latinsk kvadrat**.

En **isomorfi** mellan $(G_1, *)$ och $(G_2, \circ)$: en **bijektion** $\beta\colon G_1 \rightleftarrows G_2$ så att

$$\beta(g * g') = \beta(g) \circ \beta(g') \qquad \text{för alla } g, g' \in G_1.$$

Vi skriver $(G_1, *) \cong (G_2, \circ)$ (eller oftast bara $G_1 \cong G_2$) då G_1 och G_2 är isomorfa.
Isomorfi är en **ekvivalensrelation** mellan grupper.

Ordningen $\begin{cases} \text{för en grupp } G \ : \ |G| \\ \text{för ett element } g \in G \ : \ o(g) \end{cases}$

$$o(g) = \begin{cases} \text{om } g^n = 1, \text{ något } n \in \mathbb{Z}_+ : \ \textbf{minsta} \text{ sådana } n \\ \text{annars} : \ \infty \end{cases}$$

Sats : Om $o(g) = m$: $\quad g^s = 1 \Leftrightarrow m \mid s$

Om $(G_1, *_1)$, $(G_2, *_2)$ är grupper, är den **direkta produkten** av G_1 och G_2, $(G_1 \times G_2, *)$ med $(g_1, g_2) * (h_1, h_2) = (g_1 *_1 h_1, g_2 *_2 h_2)$ också en grupp.
Enligt kinesiska restsatsen ("+-delen") gäller om $\text{sgd}(m_i, m_j) = 1$ då $i \neq j$:

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

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

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