(Diskret matte D, ht13: F19, må 4 nov 2013)

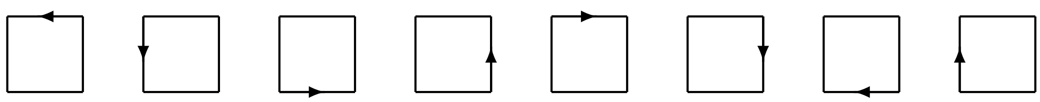
Algebradelen av kursen börjar med begreppet **grupp**, definierat **axiomatiskt**:
$(G, *)$ är en **grupp** om G1–G4 är uppfyllda (G en mängd, $*$ en binär operation),

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

($\forall x \in G \ldots$ betyder här ”för alla x i G gäller …”,
$\exists x \in G \ldots$ betyder ”det finns (minst) ett x i G så att …”.)
(Vi skriver ofta $\cdot$, $+$ (eller inget) för $*$ och 1, 0 eller I för e i en grupp.)

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

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 $\quad r$ $\quad r^2$ $\quad r^3$ $\quad x$ $\quad xr$ $\quad xr^2$ $\quad xr^3$

(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** $\beta : G_1 \to G_2$ så att

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

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

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

$$o(g) = \begin{cases} \text{om } g^n = 1, \text{ något } n > 0 : \; \textbf{minsta} \text{ sådana } n \\ \text{annars} : \; \infty \end{cases}$$

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