(SF1662 Diskret matte, vt15: F17, må 13 april 2015)

## Om **sidoklasser** (eng. cosets)

**Definition**: Om $H$ är en delgrupp till $G$ och $g \in G$ är
$gH = \{gh \mid h \in H\}$ en **vänstersidoklass** till $H$ och
$Hg = \{hg \mid h \in H\}$ en **högersidoklass** till $H$.

Sidoklasserna ger **partitioner av $G$** i **lika stora** mängder
$G = \bigcup_{g \in G} gH$, $\quad g_1H = g_2H$ eller $g_1H \cap g_2H = \varnothing$, $\quad |H| = |gH|$
(och motsvarande för högersidoklasserna).

**Lagranges sats**: För en delgrupp $H$ till en ändlig grupp $G$ gäller $|H| \,\Big|\, |G|$.
$|G : H| = \frac{|G|}{|H|}$ kallas **$H$:s index i $G$**

**Sats**: Om $G$ är en grupp med $|G| = n$ gäller
$o(g) \mid n$, så $g^n = 1$, alla $g \in G$

**Sats**: En grupp av **primtalsordning** är **cyklisk**.
Den genereras av varje element utom identitetselementet.

## Normala delgrupper, kvotgrupper

**Definition**: Delgruppen $N$ till $G$ kallas en **normal delgrupp**
om vänstersidoklasserna = högersidoklasserna, dvs
$\boldsymbol{gN = Ng}$ för alla $g \in G$ (ekvivalent: $gNg^{-1} = N$).
(Speciellt är alla delgrupper till en abelsk grupp normala.)
Då är $\boldsymbol{G/N} = \{gN \mid g \in G\}$ en grupp, **kvotgruppen**,
med operation $g_1Ng_2N = \{h_1h_2 \mid h_1 \in g_1N, h_2 \in g_2N\} = g_1g_2N$.

**Definition:** En funktion $\psi : G_1 \to G_2$ kallas en **homomorfi** mellan grupperna $(G_1, *_1)$ och $(G_2, *_2)$ om:
$\psi(g *_1 g') = \psi(g) *_2 \psi(g')$ för alla $g, g' \in G_1$.
(En isomorfi är alltså precis en bijektiv homomorfi.)
$\psi : G \to G/N$ med $\psi(g) = gN$ är en homomorfi.
(Och för en godtycklig homomorfi $\psi : G_1 \to G_2$ är $\psi(G_1) \approx G_1/N$, där $\psi(G_1) = \{\psi(g) \mid g \in G_1\}$ är en delgrupp till $G_2$ och $N = \psi^{-1}(\{1_2\}) = \{g \in G_1 \mid \psi(g) = 1_2\}$, en normal delgrupp till $G_1$.)

## Två andra **viktiga algebraiska strukturer** (inte så mycket i vår kurs):

$(R, +, \cdot)$ är en **ring** omm
1) $(R, +)$ är en **kommutativ grupp** med **identitetselement** 0
2) $(R, \cdot)$ är **sluten** och **associativ**, med **identitetselement** 1
3) $\cdot$ är **distributiv** m.a.p. $+$,
$a(b + c) = ab + ac$, $(a + b)c = ac + bc$ för alla $a, b, c \in R$

Exempel: $\mathbb{Z}$, $\mathbb{Z}_m$, $R[x]$ (alla polynom med koefficienter i ringen $R$)

**Sats: $\boldsymbol{(U(R), \cdot)}$** är en grupp, där $U(R)$ är de **inverterbara** elementen i $R$.
Exempel: $U(\mathbb{Z}) = \{1, -1\}$, $\quad U(\mathbb{Z}_m) = \{r \in \mathbb{Z}_m \mid \text{sgd}(r, m) = 1\}$

$(F, +, \cdot)$ är en **kropp** (eng. field) omm
1) $(F, +, \cdot)$ är en **ring**
2) $(F \setminus \{0\}, \cdot)$ är en **kommutativ grupp**

Exempel: $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$, $\mathbb{Z}_p$ ($p$ primtal)