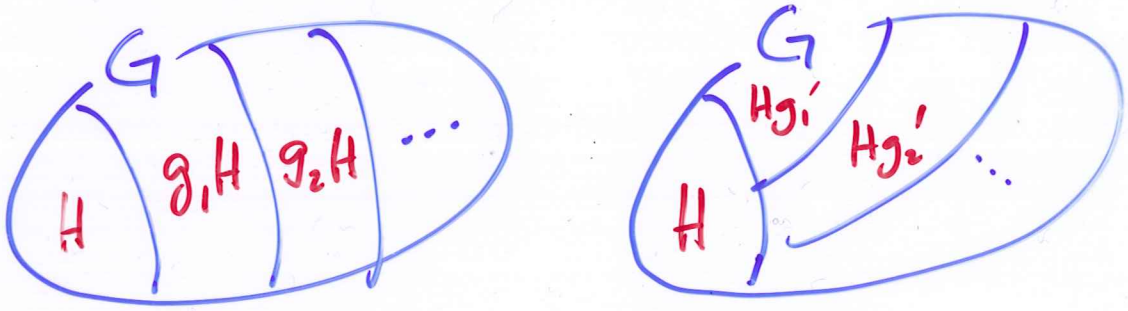
Sist
F17

Om H är en delgrupp till G och $g \in G$
är gH en vänstersidoklass till H
och Hg en högersidoklass
($gH = \{gh \mid h \in H\}$, $Hg = \{hg \mid h \in H\}$)

$$|H| = |gH| = |Hg|$$

Sidoklasserna ger partitioner av G
i lika stora mängder



Lagranges sats:

Om G är ändlig och H en delgrupp till G,

$$|H| \mid |G|$$

$|G:H| = \frac{|G|}{|H|}$, H:s **index** i G

(= antalet H-sidoklasser i G)

Sats: Om G är en grupp, $|G| = n$ och $g \in G$,

$o(g) \mid n$, så $g^n = 1$

Sats: En grupp G med $|G| = p$, primtal,
är **cyklisk** och genereras
av varje element utom 1

Direkt produkt av grupper:

$$(G_1, *_1) \times (G_2, *_2) = (G_1 \times G_2, \circ)$$

med $(g_1, g_2) \circ (h_1, h_2) = (g_1 *_1 h_1, g_2 *_2 h_2)$

Def. En normal delgrp N till G:

$$gN = Ng \text{, alla } g \in G$$

$$(\, gNg^{-1} = N \,)$$

$G/N = \{ gN \mid g \in G \}$ är då en grupp,

kvotgruppen, med $g_1 N g_2 N = g_1 g_2 N$

ex $(\mathbb{Z}, +)/(m\mathbb{Z}, +) = (\mathbb{Z}_m, +)$

Def. En homomorfi mellan $(G_1, *_1)$ och $(G_2, *_2)$

$$\psi : G_1 \to G_2$$

så att $\psi(g *_1 h) = \psi(g) *_2 \psi(h)$

för alla $g, h \in G_1$

ex $\psi : G \to G/N$

$g \mapsto gN$ N en normal delgrp

Ex $G_{\square}$:

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

så $G_{\square}/\{i, r^2\}$:

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$(R, +, \cdot)$ är en ring om

1) $(R, +)$ är en kommutativ grupp, ident. el. 0

2) $(R, \cdot)$ sluten, associativ, identitetselement 1

3) distributiva lagar $a(b+c) = ab + ac$

$(a+b)c = ac + bc$

ex. $\mathbb{Z}$, $\mathbb{Z}_m$, $\mathbb{Z}[i]$, $R[x]$

$U(R)$: de inverterbara elementen i R

$(U(R), \cdot)$ är en grupp

ex. $U(\mathbb{Z}) = \{1, -1\}$

$U(\mathbb{Z}_m) = \{r \in \mathbb{Z}_m \mid \text{sgd}(r, m) = 1\}$

$(F, +, \cdot)$ är en kropp om

1) $(F, +, \cdot)$ är en ring

2) $(F \setminus \{0\}, \cdot)$ är en kommutativ grupp

ex. $\mathbb{R}, \mathbb{C}, \mathbb{Q}, \mathbb{Z}_p$, $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$

↑ primtal