# Elementär gruppteori, v.39

# Generering av grupper

**Definition.** *Om* $G = \langle M \rangle$ *och* $M$ *är en ändlig mängd, dvs.* $M = \{a_1, ..., a_n\}$, *så kallas* $G$ *en ändligt genererad grupp,* $G = \langle \{a_1, ..., a_n\} \rangle$.

En cyklisk grupp är då ändligt genererad (av ett element), men en ändligt genererad grupp behöver inte vara cyklisk, jämför $Z \times Z$ i ovanstående exempel, (eller diedergruppen $D_n = \langle \{R, S\} \rangle$)

**Exempel.** Några ändligt genererade grupper. (Se föreläsningsanteckningar).

# Generering av grupper

**Sats 21.** *Låt $\langle G, * \rangle$ vara en ändlig grupp och antag att $e \neq a \in G$. Vi definierar ordningen för elementet $a$ som det minsta positiva heltal $n$ för vilket det gäller att $a^n = e$. Då är $n = |\langle a \rangle|$.*

**Bevis:** (Klart att satsen gäller även för $a = e$, $n = 1$ och $\langle a \rangle = \{e\}$). Lemma 19 ger att det finns ett $n$ med $a^n = e$, $a^k \neq e$, $k = 1, ..., n-1$, och elementen $a^1, ..., a^n = e$ är alla olika. Alltså $\{a, a^2, ..., a^n = e\} = \langle a \rangle$, (Sats 20), och $|\langle a \rangle| = n$. $\square$



(*) Ibland ord(a) eller o(a)

## Sidoklasser och Lagranges sats

I exempelvis $\langle Z_6, +_6 \rangle$ gäller det att $|\langle 2 \rangle| = 3$ och $|\langle 3 \rangle| = 2$. Båda dessa tal är faktorer i $|Z_6| = 6$. Detta är ingen tillfällighet, vilket inses såsnart vi har bevisat Lagranges sats!

**Definition.** *Antag att $G$ är en grupp och att $H$ är en undergrupp till $G$. Då definieras för varje $a \in G$ (vänster)sidoklassen $aH$ och (höger)sidoklassen $Ha$ genom*

$$aH = \{a\,h : h \in H\} \text{ och } Ha = \{h\,a : h \in H\}.$$

# Sidoklasser och Lagranges sats

**Påstående:**

$(i)$ $G = \bigcup_{a \in G} aH$;

$(ii)$ *Sidoklasserna är disjunkta,* $aH \cap bH \neq \emptyset \Rightarrow aH = bH$ .

**Bevis:** (i) Klart att

$$\bigcup_{a \in G} aH \subseteq G\,.$$

Tag godtyckligt $a \in G$. För $e \in H$ gäller $a = a\,e$, vilket medför att $a \in aH$. Alltså har vi att

$$G \subseteq \bigcup_{a \in G} aH$$

och därmed gäller påståendet (i).

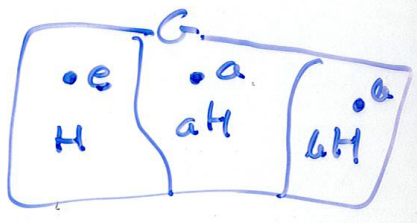
# Sidoklasser och Lagranges sats

(ii) Om $aH \cap bH \neq \emptyset$, så finns det $h_1, h_2 \in H$ sådana att $a\,h_1 = b\,h_2$. Då är $a = b\,h_2\,h_1^{-1}$ och för varje $h \in H$ är $a\,h = b\,h_2\,h_1^{-1}\,h \in bH$, så $aH \subseteq bH$. Vidare är $b = a\,h_1\,h_2^{-1}$, så för varje $h \in H$ gäller att $b\,h = a\,h_1\,h_2^{-1}\,h \in aH$, vilket ger att $bH \subseteq aH$. Alltså $aH = bH$ om $aH \cap bH \neq \emptyset$. $\square$

# Sidoklasser och Lagranges sats

Med stöd av $(i)$ och $(ii)$ är då mängden av sidoklasser $\{aH : a \in G\}$ en **partition** av $G$. Denna partition betecknas $G/H$,

$$G/H = \{aH : a \in G\}.$$



# Sidoklasser och Lagranges sats

**Sats 22.** *Om $H$ är en undergrupp till $G$, så är $G/H$ en partition av $G$ med $|H| = |aH|$ för alla $a \in G$.*

**Bevis:** Tag godtyckligt $a \in G$. Definiera $\varphi : H \to aH$ genom $\varphi(h) = a\,h$ för alla $h \in H$.

(i) Funktionen $\varphi$ är **surjektiv**, ty för godtyckligt $a\,h \in aH$ gäller att $\varphi(h) = a\,h$.

(ii) Funktionen $\varphi$ är **injektiv**, ty $\varphi(h_1) = \varphi(h_2) \Rightarrow a\,h_1 = a\,h_2 \Rightarrow h_1 = h_2$.

Därmed är $\varphi$ en bijektion och $|H| = |aH|$. $\square$

# Sidoklasser och Lagranges sats

Partitionen $G/H$ av $G$ i delmängder som alla har lika många element ger att (G ändlig)

$$|G| = |H|\,|G/H|\,.$$

$|G/H|$ brukar kallas **index** för undergruppen $H$ i $G$. Nu kan vi formulera Lagranges viktiga sats. (Joseph-Louis Lagrange (1736-1813)).

# Sidoklasser och Lagranges sats

**Sats 23. (Lagrange).** *Om $H$ är en undergrupp till en ändlig grupp $G$, så är $|G|$ delbar med $|H|$.*

Satserna 23 och 21 ger att ordningen för ett element i en ändlig grupp $G$ alltid delar $|G|$:

# Sidoklasser och Lagranges sats

**Sats 24.** *För varje $a \in G$ i en ändlig grupp $G$ är $|G|$ delbar med ordningen för $a$. Speciellt gäller $a^{|G|} = e$.*

minsta pos. heltal så att $a^n = e$.

**Bevis:** Sats 23 ger att $|\langle a \rangle|$ delar $|G|$. Ordningen för $a$ ges av $n = |\langle a \rangle|$, (Sats 21). Då finns det ett heltal $m > 0$ sådant att $|G| = m \cdot n$, vilket medför att $a^{|G|} = a^{m\,n} = (a^n)^m = e^m = e$. $\square$

# Sidoklasser och Lagranges sats

Varje grupp av primtalsordning är cyklisk:

**Sats 25.** *Antag att $G$ är en ändlig grupp och att $|G|$ är ett primtal. Då är $G$ cyklisk med $G = \langle a \rangle$ för alla $a \in G$ med $a \neq e$, och vidare gäller:*

$$G = \{a, a^2, ..., a^{n-1}, e\}.$$

# Sidoklasser och Lagranges sats

**Bevis:** Antag att $|G| = p$, där $p$ är ett primtal. Låt $a \in G$ och antag att $a \neq e$. Då är $a^1 \neq e$, så $|\langle a \rangle| > 1$. Sats 24 ger att $a : s$ ordning $n = |\langle a \rangle|$ delar $|G|$. Därmed gäller det att $|\langle a \rangle| = |G| = p$. Lemma 19 ger att elementen $a^1, a^2, ..., a^p = e$ är alla olika. Då gäller det att

$$G = \{a, a^2, ..., a^{|G|-1}, a^{|G|} = e\},$$

så $G$ är cyklisk med $G = \langle a \rangle$. $\square$

# Sidoklasser och Lagranges sats

Det finns väsentligen en grupp av primtalsordning:

**Sats 26.** *Om gruppen $G$ är av primtalsordning $p$, så är är $G \cong Z_p$.*

# Sidoklasser och Lagranges sats

**Bevis:** Antag att $|G| = p$, där $p$ är ett primtal. Tag $a \in G$ sådant att $a \neq e$. Definiera $\varphi : Z_p \to G$ genom

$$\varphi(k) = a^k, \quad \text{för } k \in \{0, 1, ..., p-1\}.$$

Då är $\varphi$ en bijektion, ty $G = \langle a \rangle$ (Sats 25) och $a, a^2, ..., a^p = e$ är alla olika (Lemma 19). Vidare gäller

$$\varphi(k_1 +_p k_2) = a^{k_1 +_p k_2} = a^{k_1}\, a^{k_2},$$

ty (i) Om $k_1 + k_2 \leq p - 1$, så gäller det att $a^{k_1 +_p k_2} = a^{k_1 + k_2} = a^{k_1}\, a^{k_2}$. (ii) Om $k_1 + k_2 \geq p$, så gäller det att $a^{k_1 +_p k_2} = a^{k_1 + k_2 - p} = a^{k_1}\, a^{k_2}\, a^{-p} = a^{k_1}\, a^{k_2}\, (a^p)^{-1} = a^{k_1}\, a^{k_2}\, e^{-1} = a^{k_1}\, a^{k_2}$. Alltså har vi att

$$\varphi(k_1 +_p k_2) = a^{k_1}\, a^{k_2} = \varphi(k_1)\, \varphi(k_2),$$

och således gäller det att $Z_p \cong G$. $\square$

# Sidoklasser och Lagranges sats

Vi avslutar detta avsnitt med ett hjälpresultat.

**Lemma 27.** *Om $H$ är en undergrupp av $G$ så gäller det att*

$$aH = \{b \in G : aH = bH\}$$

$(b \in aH \Leftrightarrow aH = bH)$

*för alla $a \in G$.*

**Bevis:** Visar att $b \in aH \Leftrightarrow aH = bH$.

# Sidoklasser och Lagranges sats

(i) ($\Rightarrow$). Antag att $b \in aH$. Då $b = be \in bH$, gäller det att $b \in aH \cap bH$. Alltså $aH = bH$, ty $\{aH : a \in G\}$ är en partition av $G$.

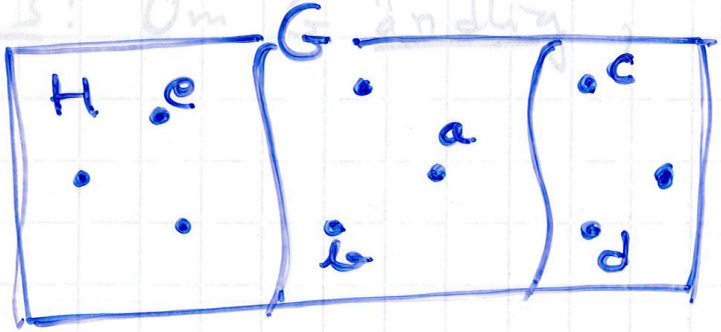
(ii) ($\Leftarrow$). Antag att $aH = bH$. Då har vi att $b \in bH \Rightarrow b \in aH$. $\square$

# Sidoklasser och Lagranges sats

**Ex** **Schematisk repetition:**

$G$ grupp, $H$ undergrupp.

$\forall a \in G: \quad aH = \{ah : h \in H\}$




$H = eH$
$aH = bH$
$cH = dH$

$G/H = \{aH : a \in G\} = \{H, aH, cH\}$

$\forall a \in G: |H| = |aH|$ (Sats 22)

**Sats 23:** Om $G$ ändlig, $|G| = |G/H| \cdot |H|$.

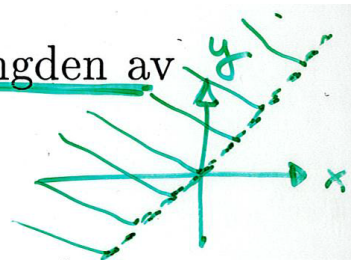
## Ekvivalensklasser

Genom att dela in elementen i en mängd $X$ i mängder bestående av "ekvivalenta" element erhåller vi en partition av $X$ i ekvivalensklasser. För att kunna göra detta bör vi införa en generalisering av begreppet likhet, nämligen en ekvivalensrelation på $X$. Först definierar vi begreppet relation.

**Definition.** *Givet en mängd $X$. En relation $R$ på $X$ är en delmängd av $X \times X$. Om $(x, y) \in R$ så säger vi att $x$ står i relationen $R$ till $y$ och betecknar detta med $x\,R\,y$.*

# Ekvivalensklasser

**Exempel.** Att $x \leq y$ för $x, y$ reella är en relation på mängden av reella tal.



# Ekvivalensklasser

**Definition.** *En relation $R$ på en mängd $X$ är en ekvivalensrelation om för alla $x, y, z \in X$ gäller:*

1. $x\,R\,x$ *(den reflexiva egenskapen);*
2. $x\,R\,y \Leftrightarrow y\,R\,x$ *(den symmetriska egenskapen);*
3. $x\,R\,y$ *och* $y\,R\,z \Rightarrow x\,R\,z$ *(den transitiva egenskapen).*

**Exempel.** a) Relationen $x \leq y$ på de reella talens mängd är reflexiv och transitiv, men inte symmetrisk, så "$\leq$" är inte en ekvivalensrelation.

b) Exempel på en ekvivalensrelation, se föreläsningarna.

# Ekvivalensklasser

**Definition.** *Låt $R$ vara en ekvivalensrelation på en mängd $X$. För varje $x \in X$ bildar vi mängden $[x]$ bestående av alla element som är relaterade till $x$,*

$$[x] = \{y : x\,R\,y\},$$

*som kallas en ekvivalensklass med avseende på $R$. Alltså $y \in [x] \Leftrightarrow x\,R\,y$.* ($\Leftrightarrow y\,R\,x \Leftrightarrow x \in [y]$)

(*) den till $x$ hörande ekvivalensklassen

**Exempel.** (Se föreläsningsanteckningar).