Mer om abstrakte grupper

Def: Dersom en gruppe G har kun endelig mange elementer, definerer vi

ordenen til G ved

$$|G| = \text{antall elementer i } G.$$

Eks: $|\mathbb{Z}_n| = n$, $|S_3| = 6$, $|D_4| = 8$.

Def: La G være en gruppe og $g \in G$.

Ordenen $|g|$ til g er den minste $n \geq 1$ slik at $g^n = e$, hvis en slik n finns.

Ellers sies g å ha <u>uendelig</u> orden.

<u>Eks</u>: $[2) \in \mathbb{Z}_6$ har orden 3, fordi

$2 \cdot [2) = [4) \neq [0)$, ← enhetselementet i $\mathbb{Z}_6$.

$3 \cdot [2) = [6) = [0)$.

<u>Prop</u>: Hvis $g \in G$ har orden n, så har $\langle g \rangle$ nøyaktig n elementer, nemlig

$$\langle g \rangle = \{e, g, g^2, \cdots, g^{n-1}\}.$$

<u>Bevis</u>: (i) La $k \in \mathbb{Z}$. Da finnes det hele tall a, b slik at

$$k = a + bn, \quad 0 \leq a < n.$$

$\Rightarrow$ $g^k = g^a \cdot (g^n)^b = g^a$ fordi $g^n = 1$.

Dette viser at

$$\langle g \rangle = \{e, g, g^2, \cdots, g^{n-1}\}.$$

(ii) La $0 \leq i \leq j < n$ og anta $g^i = g^j$.

Da er $g^{j-i} = e$. Siden $0 \leq j-i < n$,

må $i = j$. Altså er $1, g, g^2, \cdots, g^{n-1}$

parvis forskjellige. //

Prop: I en endelig gruppe G har hvert element endelig orden.

Bevis: La $g \in G$. Elementene

$$e, g, g^2, g^3, g^4, \cdots$$

Kan ikke alle være forskjellige, så det

må finnes hele tall i, j slik at

$$0 \leq i < j \quad \text{og} \quad g^i = g^j.$$

Da er $g^{j-i} = e$, så g har endelig, ordn. $\leq n$.

Def: La $H < G$ være en undergruppe.

Den (venstre) restklassen til et element

$g \in G$ er definert ved

$$gH = \{gh \mid h \in H\}.$$

Eks: $G = \mathbb{Z}$, $n > 1$. $H = \mathbb{Z}n = \{kn \mid k \in \mathbb{Z}\}$

$[k]_n = k + \mathbb{Z}n = k + H$: restklasse.

Eks: $G = S_3 = \{Id, \rho, \rho^2, \mu, \mu\rho, \mu\rho^2\}$

$H = \{Id, \rho, \rho^2\}$: Undergruppe.

$\mu H = \{\mu, \mu\rho, \mu\rho^2\}$: Restklasse.

Prop: La $H \leq G$ være en undergruppe og $g_1, g_2 \in G$. Da gjelder

enten $g_1H = g_2H$

eller $g_1H \cap g_2H = \emptyset$ (den tomme mengde)

Bevis: Anta $a \in g_1H \cap g_2H$, dvs.

$$a = g_1h_1 = g_2h_2, \quad \text{hvor } h_1, h_2 \in H$$

Da er $g_1 = g_2h_2h_1^{-1}$. Vi vil vise at $g_1H \subseteq g_2H$. La $h \in H$.

$$g_1h = (g_2h_2h_1^{-1})h = g_2(h_2h_1^{-1}h) \in g_2H.$$

Tilsvarende er $g_2H \subseteq g_1H$, så $g_1H = g_2H$. //

Lemma Hvis $H < G$ er en endelig undergruppe og $g \in G$, så har H og gH like mange elementer.

Bevis: La H ha orden r, og

$$H = \{h_1, h_2, \dots, h_r\}.$$

Da er $gH = \{gh_1, gh_2, \dots, gh_r\}$.

Hvis $gh_i = gh_j$, må $h_i = h_j$.

Altså har gH nøyaktig r elementer. //

Teorem (Lagrange) La G være en endelig gruppe og $H < G$ en undergruppe. Da vil $|H|$ dele $|G|$.

Bevis: G er en disjunkt union av restklasser:

$$G = g_1 H \amalg g_2 H \amalg \cdots \amalg g_r H$$

hvor $g_1, \ldots, g_r \in G$. Siden hver restklasse inneholder like mange elementer som H, er

$$|G| = r \cdot |H|. \quad //$$

Korollar Hvis G er en endelig gruppe og $g \in G$, så vil $|g|$ dele $|G|$.

Bevis: La $H = \langle g \rangle$ være undergruppa generert av g. Da er $|H| = |g|$, så $|g|$ deler $|G|$. //

Eks: $G = C_{12} = \{1, g, g^2, \dots, g^{11}\}$,

$g = e^{2\pi i/12} = e^{\pi i/6}$.

$|g| = 12$.

$|g^2| = ?$ $\quad (g^2)^i = g^{2i}$, $\quad |g^2| = 6$.

$|g^3| = 4$, $\quad |g^4| = 3$.

$|g^5| = ?$ $\quad (g^5)^i = g^{5i} = 1 \iff 5i = 12k$, $k \in \mathbb{Z}$

$\iff 12 \mid i$.

Altså er $|g^5| = 12$.

$|g^6| = 2$.

$g^{12-i} = g^{-i}$, $|g^{-i}| = |g^i|$.

Prop: La G være en gruppe av orden p, hvor p er et primtall. Da er G syklisk.

Bevis: Siden $p \geq 2$, har G minst ett element $g \neq e$. La n være ordenen til g. Da må $n \geq 2$. Siden undergruppa $\langle g \rangle$ generert av g har orden n, må $n \mid p$. Men p er et primtall, så $n = p$. //

Def: La $\phi : G \to H$ vara en gruppe-homomorfi. Vi definierar

* <u>kärnan</u> $\ker(\phi) = \{ g \in G \mid \phi(g) = e \}$
* <u>bilden</u> $\text{im}(\phi) = \{ \phi(g) \mid g \in G \}$.

ϕ kallas <u>surjektiv</u> om $\text{im}(\phi) = H$.

Prop: (i) $\ker(\phi)$ är en undergrupp av G.
(ii) $\text{im}(\phi)$ är en undergrupp av H.

Bevis: (i) Låt $K = \ker(\phi)$.

$\phi(e) = e \Rightarrow e \in K \Rightarrow K \neq \emptyset$.

Låt nå $g, g' \in K$.

$$\phi(gg') = \phi(g)\cdot\phi(g') = e\cdot e = e$$

$$\Rightarrow gg' \in K.$$

$$\phi(g^{-1}) = \phi(g)^{-1} = e^{-1} = e$$

$$\Rightarrow g^{-1} \in K.$$

$\Rightarrow K$ er en undergruppe.

(iii) Som (i). //

Eks: $\det : O(n) \to C_2 = \{1, -1\}$.

$\det(AB) = \det(A)\cdot\det(B)$

$\Rightarrow \det$ er en homom.

$\ker(\det) = SO(n)$.

Lemma La $\phi: G \to H$ være en gruppe-homomorfi med kjerne K. La $g \in G$ og $h = \phi(g)$. Da er

$$\phi^{-1}(h) = gK.$$

Merk: $\phi^{-1}(h) = \{a \in G \mid \phi(a) = h\}$.

Bevis: La $a \in G$.

$$a \in \phi^{-1}(h) \iff \phi(a) = h \iff \phi(a) = \phi(g)$$

$$\iff \phi(g^{-1}a) = e \iff g^{-1}a \in K$$

$$\iff a \in gK. \quad //$$

Teorem La $\phi: G \to H$ være en surjektiv homomorfi mellom endelige grupper, og la K være kjernen til ϕ. Da er

$$|G| = |K| \cdot |H|.$$

Bevis: La H ha orden r og

$$H = \{h_1, \dots, h_r\}.$$

Da er

$$G = \phi^{-1}(h_1) \amalg \cdots \amalg \phi^{-1}(h_r)$$

Siden ϕ er surjektiv, finnes det for hver h_i en $g_i \in G$ slik at $\phi(g_i) = h_i$.

Da er

$$\phi^{-1}(h_i) = g_i K.$$

$\Rightarrow$ $\phi^{-1}(h_i)$ har like mange elementer som K

$\Rightarrow$ $|G| = r \cdot |K| = |H| \cdot |K|$. //