Mer om abstrakte grupper (fra 7.2)

Def: La $H < G$ være en undergruppe. Den (venstre) restklassen til et element $g \in G$ er definert ved

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

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

enten $g_1 H = g_2 H$

eller $g_1 H \cap g_2 H = \emptyset$ (den tomme mengde)

Bevis: Anta $a \in g_1 H \cap g_2 H$, dvs.

$$a = g_1 h_1 = g_2 h_2, \quad \text{hvor } h_1, h_2 \in H$$

Da er $g_1 = g_2 h_2 h_1^{-1}$. Vi vil vise at $g_1 H \subset g_2 H$. La $h \in H$.

$$g_1 h = (g_2 h_2 h_1^{-1}) h = g_2 (h_2 h_1^{-1} h) \in g_2 H.$$

Tilsvarende er $g_2 H \subset g_1 H$, så $g_1 H = g_2 H$. //

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

<u>Bevis</u>: 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

$$h_i = e \cdot h_i = g^{-1} g h_i = g^{-1} g h_j = e \cdot h_j = h_j.$$

Altså har gH nøyaktig r elementer. //

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

<u>Bevis</u>: 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 $|g_7^5| = 12$.

$|g_7^6| = 2$.

$g_7^{12-i} = g_7^{-i}$, $|g_7^{-i}| = |g_7^i|$.

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

<u>Bevis</u>: 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 $n = p$.

//

<u>Def</u>: La $\phi : G \to H$ være en gruppe-

homomorfi. Vi definerer

* kjernen $\ker(\phi) = \{ g \in G \mid \phi(g) = e \}$
* bildet $\mathrm{im}(\phi) = \{ \phi(g) \mid g \in G \}$.

Prop: (i) $\ker(\phi)$ er en undergruppe av G.

(ii) $\mathrm{im}(\phi)$ er en undergruppe av H.

Bevis: (i) La $K = \ker(\phi)$.

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

La 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 ei undergruppe.

(ii) Som (i). //

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

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

$\Rightarrow$ det er en homom.

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

<u>Prop</u>: La $\phi : G \to H$ vær en gruppe-homomorfi med kjerne K. Da gjelder

$$\phi \text{ injektiv} \iff K = \{e\}.$$

<u>Bevis</u>: (i) Anta ϕ injektiv og $g \in K$.

$$\phi(g) = e = \phi(e) \underset{\phi \text{ inj.}}{\Rightarrow} g = e.$$

Altså er $K = \{e\}$.

(ii) Anta $K = \{e\}$ og $\phi(g_1) = \phi(g_2)$.

$$\phi(g_1 g_2^{-1}) = \phi(g_1) \cdot \phi(g_2)^{-1} = e$$

$$\Rightarrow g_1 g_2^{-1} = e \Rightarrow g_1 = g_2.$$

Altså er ϕ injektiv. //

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

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

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

<u>Bevis</u>: (i) La $a \in \phi^{-1}(h)$, og sett $k = g^{-1}a$.

Da er $\phi(k) = \phi(g)^{-1} \cdot \phi(a) = h^{-1} \cdot h = e$

$\Rightarrow k \in K$, $a = gk \in gK$.

Altså er $\phi^{-1}(h) \subset gK$.

(ii) La $k \in K$. Da er

$$\phi(gk) = \phi(g) \cdot \phi(k) = h \cdot e = h$$

$\Rightarrow gk \in \phi^{-1}(h)$

Altså er $gK \subset \phi^{-1}(h)$. //

<u>Teorem</u> 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

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

Husk En avbildning $f: X \to Y$ mellom to mengder kalles

* <u>injektiv</u> dersom det for hver $y \in Y$ fins høyst en $x \in X$ slik at $f(x) = y$.
* <u>surjektiv</u> dersom det for hver $y \in Y$ fins minst en $x \in X$ slik at $f(x) = y$.
* <u>bijektiv</u> dersom det for hver $y \in Y$ fins nøyaktig en $x \in X$ slik at $f(x) = y$.

Altså: bijektiv = injektiv + surjektiv.

<u>Eks:</u> (1) $\exp: \mathbb{R} \to \mathbb{R}$ er injektiv, men ikke surjektiv:

Inj.: $e^{x_1} = e^{x_2} \Rightarrow e^{x_1 - x_2} = 1 \Rightarrow x_1 = x_2$

Ikke surj: Fordi $e^x > 0$.

② $\cos : \mathbb{R} \to [-1,1]$ er surjektiv,

men ikke injektiv.

<u>Surj</u>: La $y \in [-1,1]$, $x = \arccos(y)$.

Da er $\cos x = y$.

<u>Ikke injektiv</u>: Fordi $\cos(x + 2\pi) = \cos x$

for alle $x \in \mathbb{R}$

<u>Prop</u>: La G være en gruppe og $g \in G$.
Da er avbildningen

$$\ell_g : G \to G, \quad \ell_g(x) = gx$$

bijektiv.

<u>Bevis</u>: La $y \in G$. Da har likningen

$y = gx$ nøyaktig én løsning x,

nemlig $x = g^{-1}y$. Altså er l_g bijektiv.
//.

Husk: For $n > 1$ er

S_n = gruppa av alle bijeksjoner

$\{1, \cdots, n\} \to \{1, \cdots, n\}$,

hvor den binære operasjonen er sammensetning

av avbildninger.

Merk: Elementene i S_n kalles ofte

permutasjoner.

Notasjon: $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$

betegner elementet $\sigma \in S_4$ gitt ved

$\sigma(1) = 3$, $\sigma(2) = 1$, $\sigma(3) = 4$, $\sigma(4) = 2$.