Diskret matematik 2018-04-18 #12

Exempelbeskrivningar i PPT på Canvas

Mönster i grupptabellen - Inte ett sammanträffande.

Delgrupper

<u>Def^n</u> Låt $(G, \circ)$ vara en grupp.
En mängd $H \subseteq G$ sägs vara en delgrupp till G om $(H, \circ)$ också är en grupp (dvs uppfyller de 4 gruppaxiomen).

Har en grupp alltid minst en delgrupp?

$H = G$? Ja, en grupp, så en delgrupp.
$H = \{id\}$? Ja, en grupp, så en delgrupp.

Sats Låt $(G, \circ)$ vara en grupp, och låt $H \subset G$. Då är $(H, \circ)$ en delgrupp till $(G, \circ)$ om och endast om

1. H är icke-tom och
2. $a \circ b^{-1} \in H$ för alla $a, b \in H$

Om H är en ändlig mängd, då kan vi istället för (2) kolla att $a \circ b \in H$ för alla $a, b \in H$; dvs, att H är sluten under $\circ$.

<u>Bevis</u> "Om": Varför håller de 4 gruppaxiomen för $(H, \circ)$?

Börja med id-elt: Varför ligger $id \in H$?

Eftersom $H \neq \emptyset$ så finns det ett element $a \in H$. Enligt egenskap (2), med $b = a$, så gäller $\underbrace{a \circ b^{-1}}_{(id)} \in H$

Resten i anteckningar på Canvas ▨

<u>Lagranges sats</u>

Låt $(G, \circ)$ vara en ändlig grupp. Om H är en delgrupp till G, då är $|H|$ en delare i $|G|$, dvs

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

Konsekvens:
Om H är en delgrupp till $(\mathbb{Z}_6, +)$, då är $|H| = 1, 2, 3,$ eller 6. $|\mathbb{Z}_6| = 6$

I $(\mathbb{Z}_7, +)$: Om $H \subseteq \mathbb{Z}_7$ är en delgrupp, då är $|H| = 1$ eller 7.

Det finns INTE alltid en delgrupp för varje delare till $|G|$.

Sidoklasser i $(\mathbb{Z}_6,+)$

Låt $H=\{0,2,4\}$ – en delgrupp till $(\mathbb{Z}_6,+)$.

Då är
$0+H=\{0,2,4\}=H$ | $1+H=\{1,3,5\}$
$2+H=\{2,4,0\}=H$ | $3+H=\{3,5,1\}=1+H$
$4+H=\{4,0,2\}=H$ | $5+H=\{5,1,3\}=1+H$

Två viktiga poänger:

1. Varje element i G står med i något $(k+H)$.

2. Antingen är $k_1+H=k_2+H$ eller så är $(k_1+H)\cap(k_2+H)=\emptyset$.
$(-k_2+k_1\in H$ i exemplet ovan)

Def^{n} (Sidoklasser)

Låt $(G,\circ)$ vara en grupp och låt $H\leq G$ vara en delgrupp.
För varje element $g\in G$ definierar vi den (vänstra) sidoklassen till H (med avseende på g) som mängden

$$g\circ H=\{g\circ h : h\in H\}$$

Skriver oftast bara gH

Låt $(G,\circ)$ vara en grupp och $H<G$ en delgrupp.

Sats (Sidoklasstestet)

För $g_1,g_2\in G$ gäller det att
$g_1H=g_2H$ om och endast om $g_2^{-1}g_1\in H$.

Delgrupper till $(\mathbb{Z},+)$

$H=\{0,\pm 2,\pm 4,\dots\}=2\cdot\mathbb{Z}$
Samma gäller för $n\cdot\mathbb{Z}$, $n\in\mathbb{Z}$

$g_1+3\cdot\mathbb{Z}=g_2+3\cdot\mathbb{Z}$
När?

Då $-g_2+g_1\in 3\cdot\mathbb{Z}$

Bevis av sidoklasstestet

"Om" Anta att $g_2^{-1}g_1\in H$ och visa att $g_1H=g_2H$

Vi visar först att $g_1H\subseteq g_2H$.
Skriv h för $g_2^{-1}g_1$ där $h\in H$. Låt $g_1k\in g_1H$, där $k\in H$.
Då är $g_1k\in g_2H$ för...

Vi vet att $g_1 = g_2 h$.

Så $g_1 k = (g_2 h)k$
$= g_2(hk) \in g_2 H$ för $hk \in H$. ∎

Mer i anteckningar på Canvas

<u>Sats</u> För alla $g \in G$ gäller $|gH| = |H|$

$gH = \{g \circ h : h \in H\}$

Om $g \cdot h_1 = g \cdot h_2$ så är $h_1 = h_2$ enligt vänsterkancellations-lagen.

Sidoklasserna ger en partition av G

<u>Sats</u> Låt H vara en delgrupp till en grupp G.

1. Varje element i G tillhör då någon sidoklass till H.
2. Låt $g_1, g_2 \in G$. Då är sidoklasserna $g_1 H$ och $g_2 H$ antingen disjunkta eller identiska.

<u>Bevis</u> (1) Varför tillhör elementet $g \in G$ någon sidoklass till H? Vilken sidoklass?

Jo $g \in \underbrace{gH}_{\{g \cdot h : h \in H\}}$

Eftersom $id \in H$ så ligger $\underbrace{g \cdot id}_{g} \in gH$

(2) Bevis i anteckningarna

Lagranges sats – fullständiga versionen

Låt $(G, \circ)$ vara en ändlig grupp och låt $H \subset G$ vara en delgrupp. Då är $|G| = (\text{antalet olika sidoklasser till } H) \cdot |H|$.
Alltså är $|H|$ en delare i $|G|$.

Lagrange: $\overset{G = \mathbb{Z}_6}{|G| = 6}$

$H = \{0, 2, 4\}$ $|H| = 3$

Så är

$6 = (\text{antalet sidoklasser}) \cdot 3 = 2 \cdot 3$.

Om $H = \{0, 3\}$ $6 = (\text{antalet sidoklasser}) \cdot 2$

Så antalet sidoklasser $= 3$

Sidoklasser till $H=\{0,3\}$ i $\mathbb{Z}_6$???

$0+H=\{0,3\}$

$1+H=\{1,4\}$

$2+H=\{2,5\}$

$3+H=\{3,0\}=H$

$4+H=\{4,1\}=1+H$

$5+H=\{5,2\}=2+H$

$G=H\cup g_1H\cup g_2H\cup\ldots\cup g_kH$

$|G|=|H|+|g_1H|+|g_2H|+\ldots+|g_kH|$

$=|H|+|H|+|H|+\ldots+|H|$