Forelesning 22. januar 2024

Generatorer for grupper:

G gruppe — $\{g_1, \dots, g_k\}$ kalles en GENERATORMENGDE for G dersom ethvert element $g \in G$ kan skrives som et produkt av potenser av g_i-ene

$$g = g_{i_1}^{n_1} \cdots g_{i_m}^{n_m}$$

Syklisk gruppe $\longleftrightarrow$ Gruppe generert av ett element

$$G = \langle a \rangle = \{e, a, a^2, \dots\}$$

Hvis $|G| = n < \infty$ så må vi ha $a^n = a^m$ for en $m < n$.

$$\Rightarrow a^{n-m} = e$$

Den minste k slik at $a^k = e$ kalles ORDEN til a.

Thm 10.10 (Lagrange)

G endelig gruppe, Orden til $g \in G$ må dele $|G|$

Bevis g definerer undergruppe $\langle g \rangle \leq G$.

$$\langle g \rangle = \{e, g, \dots, g^m\}$$

For $h \in G$ kan vi lage $h\langle g \rangle = \{h, hg, \dots, hg^m\}$

Merk: $hg^i = hg^j \overset{h^{-1}}{\Rightarrow} g^i = g^j \Rightarrow i = j$

$$\Rightarrow |h\langle g \rangle| = |\langle g \rangle|$$

Anta $h_1\langle g \rangle \cap h_2\langle g \rangle \neq \emptyset$

$$\Rightarrow h_1 g^i = h_2 g^j$$

$$\Rightarrow h_1 = h_2 g^{j-i}, \quad h_2 = h_1 g^{i-j}$$

$$\Rightarrow h_1 \in h_2\langle g \rangle \quad h_2 \in h_1\langle g \rangle$$

$$\Rightarrow h_1\langle g \rangle \subseteq h_2\langle g \rangle\langle g \rangle \subseteq h_2\langle g \rangle$$

$$h_2\langle g \rangle \quad \cdots \quad \subseteq h_1\langle g \rangle$$

$$\Rightarrow h_1\langle g \rangle = h_2\langle g \rangle$$

Det betyr

$$h_1\langle g\rangle = h_2\langle g\rangle \quad \text{eller} \quad h_1\langle g\rangle \cap h_2\langle g\rangle = \emptyset$$

I tillegg har vi

$$G = \langle g\rangle \cup h_1\langle g\rangle \cup \dots \cup h_k\langle g\rangle$$

disjunkt union

$$\Rightarrow \quad |G| = (k+1)\,|\langle g\rangle| \qquad \text{Q.E.D.}$$

Undergrupper av syklisk grupper er sykliske

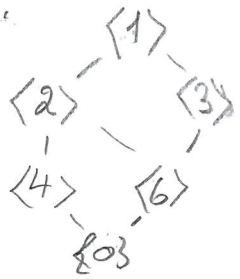
$$H \leq \langle g\rangle$$

$$\Rightarrow \quad H = \{e, g^{i_1}, \dots, g^{i_k}\}$$

$$\Rightarrow \quad H = \langle g^s\rangle \quad \text{hvor } s \text{ er største felles faktor av } i_1, \dots, i_k, \langle g\rangle$$

Eksempler: $\mathbb{Z}_{12} = \{0, 1, \dots, 11\}$ $(12 \equiv 0)$ $\Rightarrow |\mathbb{Z}_{12}| = 12$

Undergrupper generert av $2, 3, 4, 6, 8, 9, 10$ (samme)



Uendelige sykliske grupper $G = \{\dots, g^{-2}, g^{-1}, e, g, g^2, \dots\} \simeq (\mathbb{Z}, +)$

Def 15.14 En gruppe G er SIMPEL dersom den ikke har noen ekte, ikke-trivielle normale undergrupper

Hva er en normal undergruppe?

- $H \leq G$
- $\forall g \in G \; ; \; g^{-1}Hg = H$

  Alt. $Hg = gH$

Merk: G abelsk $\Rightarrow$ Alle undergrupper er normale (siden $hg = gh \; \forall h \in G$, og derfor $h \in H$)

Thm: Sykliske grupper av primorden er simple

Bevis Anta $H \leq G$ og la $h \in H$. Da har vi

- $\langle h \rangle \leq G$
- orden til h deler $|G|$ = prim

$\Rightarrow$ orden til h er 1 $\Rightarrow \langle h \rangle = \{e\}$

elle

orden til h er $|G|$ $\Rightarrow \langle h \rangle = G$

QED

Thm 6.1 Sykliske grupper er abelske

Bevis $G = \langle g \rangle$. To vilkårlige elemente g^i, g^j

$$g^i g^j = g^{i+j} = g^j g^i$$

QED

Resultat som vi skal vise senere:

Den minste ikke-sykliske simple gruppa har orden 60. (A_5: Den alternerende gruppe)

$\Rightarrow$ Det finnes ingen generell formel for løsningene til en 5. grads likning

Thm En gruppe av prim orden er syklisk

Bevis La $h \in G$ og betrakt $\langle h \rangle \leq G$. Vi har sett $|\langle h \rangle|$ deler $|G|$. Siden $|G|$ er prim betyr det at $|\langle h \rangle| = 1$ eller $|\langle h \rangle| = |G|$.

Vi kan anta $h \neq e$, dvs at

$$\langle h \rangle \leq G$$
$$|\langle h \rangle| = |G|$$

$\Rightarrow G = \langle h \rangle$

QED.

Klassifikasjon av grupper av lav orden

$|G| = 1, 2,$ primtall ok.

$|G| = 4$.
1) G inneholder et element av orden 4 $\Rightarrow G = \mathbb{Z}_4$
2) Ingen elementer i G har orden 4
$\Rightarrow$ Alle (unntatt e) har orden 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

Sudoku-prinsippet gir resten!

$G \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$

$e = (0,0)$
$a = (1,0)$
$b = (0,1)$
$c = (1,1)$

$|G| = 6$.
1) $\exists h \in G$ orden til h er 6 $\Rightarrow G = \mathbb{Z}_6$
2) $\nexists h \in G$ av orden 6,
$\exists h \in G$ av orden 3 $(|h| = 3)$ $h^3 = e$

La $g \in G$, $g \neq e, h, h^2$
$\Rightarrow gh \neq e, h, h^2$, $gh^2 \neq e, h, h^2$

$\Rightarrow G = \{e, h, h^2, g, gh, gh^2\}$ (g^4, g^2, g^3)

Hva gjenstår? Vi vet ikke hva hg er, eller g^2

	e	h	h^2	g	gh	gh^2
$hg = \Rightarrow$	$g = h^{-1}$	$g = e$	$g = h$	$h = e$		
	Nei	Nei	Nei	Nei	ok	ok
$g^2 = \Rightarrow$		$\mathbb{Z}_6$		$g = e$	$g = h$	$g = h^2$
	ok	ok	ok	Nei	Nei	Nei

	$hg = gh$	$hg = gh^2$
$g^2 = e$	$\mathbb{Z}_6 = \langle gh \rangle$	ok
$g^2 = h^2$	$\mathbb{Z}_6 = \langle g \rangle$	$g = h^{-1}$ Nei

To grupper
$\mathbb{Z}_6$ (abelsk)
S_3 (symmetrisk)

3) Alle elementer har orden ≤ 2

Thm. En gruppe G der alle elementene har orden ≤ 2 er abelsk

Bevis $g,h \in G \setminus \{e\}$ Pr. antagelse $g^2 = h^2 = e$, og $(gh)^2 = (hg)^2 = e$

$$e = (gh)^2 = ghgh \Rightarrow g \cdot e = g(ghgh) = hgh$$

$$\Rightarrow h \cdot g = h(hgh) = h^2 gh = egh = gh$$

QED

$G = \{e, g_1, g_2, g_3, g_4, g_5\}$ $g_i^2 = e$ $g_i g_j = g_j g_i$

Hva med g_1g_2, g_1g_3 g_1g_4 g_1g_5 g_2g_3 g_2g_4 g_2g_5
g_3g_4 g_3g_5, g_4g_5 (10 elementer)

Anta (uten tap av generalitet) at $g_1g_2 = g_3$

$$\Rightarrow g_1g_2g_3 = g_3^2 = e$$

$$\Rightarrow g_1g_3 = g_2 \text{ , } g_2g_3 = g_1$$

	e	g_1	g_1g_3	g_3	g_4	g_5
$g_1g_4 =$	$g_4 = g_1$	$g_4 = e$	$g_3 = g_4$	$g_2 = g_4$	$g_1 = e$	ok

$g_5 = g_1g_4$

$G = \{e, g_1, g_3, g_1g_3, g_4, g_1g_4\}$

Hva med g_3g_4

	e	g_1	g_1g_3	g_3	g_4	g_1g_4
$g_3g_4 =$	$g_3 = g_4$	$g_4 = g_1g_3$	$g_1 = g_4$	$g_4 = e$	$g_3 = e$	$g_1 = g_3$
	Nei	Nei	Nei	Nei	Nei	Nei