Forelesning 5. februar

Repetisjon av faktorgrupper (kvosienter)

$H \leq G$

normal undergruppe

Normal betyr $\forall g \in G,\ g^{-1}Hg = H$

$\Updownarrow$

Viktig for at $(g_1H)(g_2H) = g_1g_2H$

Elementene i G/H er restklassene gH

↑ et element

Identitet: $eH = H$

invers: $g^{-1}H$

Eksempler:

- Abelske grupper: $gH = Hg$ eller $g^{-1}Hg = H$

  Normalitet er ikke noe problem

- Eksempel på ikke-normal undergruppe

$$S_3 = \{id, (123), (132), (12), (13)(23)\}$$

(alle permutasjoner av $\{1,2,3\}$)

$H \leq S_3 \quad H = \{id, (12)\}$

undergruppe (ikke normal)

$g = (123) \rightsquigarrow g^{-1} = (132)$

fordi $(123)(132) = (1)(2)(3) = id$

$(132)(12)(123) = (13) \notin H$

- Men $H = \{id, (123), (132)\} \leq S_3$ er normal

$(12)^{-1} = (12)$

$$\left.\begin{aligned} (12)(123)(12) &= (132) \\ (13)(123)(13) &= (132) \\ (23)(123)(23) &= (132) \end{aligned}\right\} \in H$$

Abelske grupper: $\boxed{gh = hg \quad \forall g, h \in G}$

Thm 11.12

Enhver endelig generert abelsk gruppe er isomorf med et direkte produkt av sykliske grupper

$$\underbrace{\mathbb{Z}_{(p_1)^{r_1}} \times \mathbb{Z}_{(p_2)^{r_2}} \times \cdots \times \mathbb{Z}_{(p_n)^{r_n}}}_{T} \times \underbrace{\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}}_{\beta}$$

hvor p_i er primtall, $r_i \in \mathbb{Z}_+$. Primtallen trenger ikke å være forskjellige og β kalles Betti-tallet til gruppa, T kalles torsjonsdelen (eller torsjons-undergruppa) til gruppa og $\underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{\beta}$ den frie abelske undergruppa.

Noen ord:
- Endelig generert
- Direkte produkt
- Fri abelsk gruppe
- Torsjon

For abelske grupper er det vanlig å bruke additiv notasjon, dvs $g_1 + g_2$.

Endelig generert:

$$G = \langle a_1, \ldots, a_m \rangle = \left\{ \sum_{i=1}^{m} r_i a_i \mid r_i \in \mathbb{Z} \right\}$$

Direkte produkt (eller direkte sum)

$$\prod_{i=1}^{k} G_i = G_1 \times G_2 \times \cdots \times G_k$$

- komponentvis addisjon (som for vektorer)

Thm 11.2 Et direkte produkt av grupper er selv en gruppe

Fri abelsk gruppe:
- Ingen relasjoner (m.a.o $\underbrace{a+a+a+\cdots+a}_{n} = 0$ betyr $n=0$)
- $\underbrace{\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}}_{\text{antall kalles rang}}$

Torsjon: Den delen som ikke er $\{0\}$, dvs. alle $g \in G$ så er $\underbrace{g+g+\cdots+g}_{n} = 0$ for en $n \in \mathbb{Z}$.

Oppbygning av beviset:

1. (Thm 38.8) $G = \langle a_1, \ldots, a_n \rangle$ end gen.

$$\varphi : \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{n} \longrightarrow G$$

$$(h_1, \ldots, h_n) \longmapsto h_1 a_1 + \cdots + h_n a_n$$

surjektiv gruppehomomorfi med kjerne $K = \ker \varphi$

2. (Thm 38.11) 1) $K \leq G$, G fri abelsk, $K \neq \{0\}$, $\operatorname{rang} G = n$
$\Rightarrow K$ fri abelsk av rang $s \leq n$

2) $\{x_1, \ldots, x_n\} \Rightarrow \exists\, d_i \in \mathbb{Z}_+$ $d_i \mid d_{i+1}$
basis for G
og $\{d_1 x_1, \ldots, d_s x_s\}$ basis for K

3. (Thm 14.11) $G \simeq F/K \simeq (\mathbb{Z} \times \cdots \times \mathbb{Z}) / (d_1\mathbb{Z} \times \cdots \times d_s\mathbb{Z} \times \{0\} \times \{0\} \times \cdots \times \{0\})$

$\simeq \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_s} \times \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$.
(kan anta $d_1 > 1$)

4 $\mathbb{Z}_m \times \mathbb{Z}_n \simeq \mathbb{Z}_n \times \mathbb{Z}_m$

5 (Thm 11.5) $\gcd(m,n) = 1 \Rightarrow \mathbb{Z}_m \times \mathbb{Z}_n \simeq \mathbb{Z}_{mn}$

6 $\Rightarrow \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_s} \simeq \mathbb{Z}_{(p_1)^{r_1}} \times \cdots \times \mathbb{Z}_{(p_n)^{r_n}}$

7 (Thm 38.6) Betti tall $= \operatorname{rang}(G/T)$ fri abelsk
Rang er entydig gitt.

8 (Ex 14-22) Entydighet av torsjonsdel

Noen anvendelser:

Thm. 11.16 Hvis $m \mid |G|$, G endelig abelsk, så $\exists\, H \leq G$ slik at $|H| = m$.

Bevis $G = \mathbb{Z}_{(p_1)^{r_1}} \times \cdots \times \mathbb{Z}_{(p_n)^{r_n}} \Rightarrow |G| = \prod (p_i)^{r_i}$

$\Rightarrow m = \prod (p_i)^{s_i}$ $0 \leq s_i \leq r_i$

$H_i = \langle (p_i)^{r_i - s_i} \rangle \leq \mathbb{Z}_{(p_i)^{r_i}}$, $|H_i| = \dfrac{(p_i)^{r_i}}{(p_i)^{r_i - s_i}} = (p_i)^{s_i}$

H_i syklush

sett $H = \prod H_i = (p_1)^{s_1} \times \cdots \times (p_n)^{s_n}$, $|H| = m$

$H \leq G$ QED

Thm 11.17 Hvis m er kvadratfri ($\sqrt{m} = m$) så vil enhver abelsk gruppe av orden m være ~~abelsk~~ syklush

Bevis $m = \sqrt{m}$ betyr $G \simeq \mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_n}$ $p_i \neq p_j$

$\simeq \mathbb{Z}_{p_1 \cdots p_n}$

QED

Noen bevis!

Thm 38.6 : Entydig rang for frie abelske grupper

Bevis Reduser til $G/2G \simeq \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$

Alle basiser kan redusers til $\{e_i = (0, \ldots 1 \ldots 0)\}$

Thm 38.11 : $\mathcal{B} = \{y_1, \ldots, y_n\}$ basis for G.

$\Rightarrow g \in K \leq G$; $g = k_1 y_1 + \cdots + k_n y_n$

Siden vi skal vise eksistens kan vi anta at ingen basiser har mindre $|k_i|$-er og at $k_1 = d_1$ er minst, kall denne ω:

$$\omega = d_1 y_1 + k_2 y_2 + \cdots + k_n y_n$$

For hver k_j bruker vi divisjonsalgoritmen

$$k_j = d_1 q_j + r_j \qquad 0 \le r_j < d_1$$

$$\Rightarrow \quad \omega = d_1 \underbrace{(y_1 + q_2 y_2 + \cdots + q_n y_n)}_{x_1} + (r_2 y_2 + \cdots + r_n y_n)$$

$$\Rightarrow \quad \{x_1, y_2, \ldots, y_n\} \text{ basis for } G$$

Koeff til ω i denne basisen er $d_1, r_2, \ldots, r_n$, hvor $r_j < d_1$
Siden d_1 er minst ($\neq 0$) må vi ha $r_2 = \cdots = r_n = 0$

$$\Rightarrow \quad \omega = d_1 x_1 \in K$$

Betrakter basis $\{x_1, y_2, \ldots, y_n\}$, dvs elementa i K kan skrives

$$h_1 x_1 + k_2 y_2 + \cdots + k_n y_n \in K$$
$$- t \cdot d_1 x_1 \qquad\qquad \in K$$
$$\overline{\qquad\qquad\qquad\qquad}$$
$$h_1' x_1 + k_2 y_2 + \cdots + k_n y_n \in K \qquad h_1' < d_1$$
$$\text{dvs } h_1' = 0$$

$$\Rightarrow \quad k_2 y_2 + \cdots + k_n y_n \in K$$

Gjenta prosedyren. Hvis alle $k_i = 0$, så er $K = \langle d_1 x_1 \rangle$.
Hvis ikke,

$$\omega_2 = d_2 y_2 + k_3 y_3 + \cdots + k_n y_n \in K$$

og hvor d_2 er minst. Som over får vi $d_2 x_2 \in K$.
Siden $d_2 \ge d_1$ kan vi skrive $d_2 = q d_1 + r$, $0 \le r < d_1$. Siden

$$\{x_1 + q x_2, x_2, y_3, \ldots, y_n\}$$

er en basis for G og

$$d_1 (x_1 + q x_2) + r x_2 = d_1 x_1 + d_2 x_2 \in K$$

følger det fra minimalitet at $r = 0$ og $d_2 = q d_1$

Gjenta prosessen.

QED

En anvendelse:

$\mathbb{C}^*$ multiplikative gruppe av komplekse tall $\neq 0$

$G \leq \mathbb{C}^*$ endelig $\Rightarrow$ G syklisk

Bevis 1) $\mathbb{C}^*$ er abelsk og derfor er også alle undergrupper abelsk

2) $G \simeq \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \dots \times \mathbb{Z}_{d_r}$ $\quad d_i \mid d_{i+1}$

3) Siden $d_1 \mid d_2$ må $\mathbb{Z}_{d_2}$ inneholde elementer av orden d_1

4) $p \mid d_1 \Rightarrow G$ inneholder $\mathbb{Z}_p \times \mathbb{Z}_p$ som inneholde p^2-1 elementer av orden p
(p prim)

5) p^2-1 komplekse tall som oppfylle $x^p - 1 = 0$
Motsigelse siden denne har p røtter og $p < p^2-1$ for $p \geq 2$ *

$\Rightarrow G \simeq \mathbb{Z}_{d_1}$