Sylow-teori

Thm. 17.1. (Burnside)

G ändelig grupp, X ändelig mängd, $G \times X \to X$ verkning

r : antalet banor

$$r \cdot |G| = \sum_{g \in G} |X_g|$$

$$X_g = \{x \in X \mid gx = x\}$$

Bana: $Gx = \{gx \mid g \in G\}$

$$|X| = \sum_{i=1}^{r} |Gx_i|$$

disjunkt union av banor

$$X_G = \{x \in X \mid gx = x \ \forall g \in G\}$$

$$= \bigcap_{g \in G} X_g = \bigcup_{|Gx_i|=1} Gx_i$$

$$|X_G| = s \Rightarrow |X| = |X_G| + \sum_{i=s+1}^{r} |Gx_i|$$

Thm. 36.1

$|G| = p^n$, $G \times X \to X$ ändelig mängd

$$\Rightarrow |X| \equiv |X_G| \pmod{p}$$

Bevis. $|Gx_i| \mid |G| = p^n$ och $|Gx_i| \neq 1$

$\Rightarrow p \mid |Gx_i|$ QED

Defn 36.2

G p-grupp $\overset{\text{def}}{\Leftrightarrow} \forall g \in G,\ |g| = p^m$

Thm 36.2. (Cauchy)

p primtal, $p \mid |G| \Rightarrow \exists g \in G$ sådan att $|g| = p$.

Bevis.

$$X = \{(g_1, \ldots, g_p) \in G^p \mid \prod_{i=1}^{p} g_i = e\}$$

$$\Rightarrow |X| = |G|^{p-1} \Rightarrow p \mid |X|.$$

$\sigma \in S_p$ verkar på X, $|\langle\sigma\rangle| = p$ $\overset{\text{Thm 36.1}}{\Rightarrow} |X| \equiv |X_{\langle\sigma\rangle}| \pmod{p}$

sykel av längd p $\Rightarrow p \mid |X_{\langle\sigma\rangle}|$

$X_{\langle\sigma\rangle} = \{(g_1,\dots,g_p) \mid \sigma(g_1,\dots,g_p) = (g_1,\dots,g_p)\}$

$\Rightarrow g_1 = g_2 = \dots = g_p$

$X_{\langle\sigma\rangle} \neq \emptyset$ siden $(e,\dots,e) \in X_{\langle\sigma\rangle} \Rightarrow |X_{\langle\sigma\rangle}| \geq p$.

$\Rightarrow \exists \underset{\neq e}{a \in G}$ s.a. $(a,\dots,a) \in X_{\langle\sigma\rangle} \Rightarrow \underline{a^p = e}$ QED

Cor 36.4

G endelig gruppe $\quad \forall g \in G,\ |g| = p^m \iff |G| = p^n$.

Bevis $\Leftarrow$ Lagrange

$\Rightarrow$ Anta $q \mid |G|$, $q \neq p$ primtall

Cauchy $\Rightarrow \exists g \in G;\ |g| = q$ Motsigelse QED

G gruppe $\quad \mathcal{S} = \{\text{mengden av undergrupper av } G\} = \{H \mid H \leq G\}$

G virker på $\mathcal{S}$ ved konjugasjon

$g \mapsto g^{-1}Hg$.

$H \leq G_H = \{g \in G \mid g^{-1}Hg = H\} \leq G$

normal undergruppe

G_H er den største undergruppa av G med H som normal undergruppe

Normalisatorgruppe $N[H] = G_H$ alt. $N_G[H]$.

$H \leq G$ endelig $\Rightarrow g \in N[H]$ hviss $g^{-1}Hg \in H\ \forall h \in H$

Bevis $i_g|_H$ er 1-1 $\quad i_g(h_1) = g^{-1}h_1 g = g^{-1}h_2 g = i_g(h_2)$

$\Rightarrow h_1 = h_2$

1-1 og H endelig betyr $i_g : H \to H$ er surjektiv

$i_g(H) = g^{-1}Hg = H$

$\Rightarrow g \in N[H]$. QED

Lemma 36.6

$H \leq G$ p-gruppe endelig $\Rightarrow (N[H] : H) \equiv (G : H) \pmod p$

Bevis $\mathcal{L} = \{xH \mid x \in G\}$ venstre restklasser

$H \times \mathcal{L} \to \mathcal{L}$

$(h, xH) \mapsto (hx)H \quad |\mathcal{L}| = (G : H)$

$N[H] = \{g \in G \mid g^{-1}Hg = H\}$

$\mathcal{L}_H = \{xH \mid hxH = xH \ \forall h \in H\}$ $x \in G$

$hxH = xH \iff H = x^{-1}hx \cdot H$ dvs $x^{-1}hx \in H$

Dette betyr: $hxH = xH \ \forall h \in H \iff x^{-1}hx \in H \ \forall h \in H$

$\iff x^{-1}Hx = H$

$\Rightarrow \mathcal{L}_H = \{xH \mid x \in N[H]\}$ dvs $xH \in N[H]$

$\Rightarrow |\mathcal{L}_H| = (N[H] : H)$

Siden $|\mathcal{L}| \equiv |\mathcal{L}_H| \pmod p$ følger at $(G:H) \equiv (N[H]:H) \pmod p$

Cor 36.7 $H \leq G$, p-undergruppe, $|G| < \infty$ $\quad p \mid (G:H) \Rightarrow N[H] \neq H$

Bevis $p \mid (G:H)$ betyr

$(N[H]:H) \equiv 0 \pmod p$

dvs $p \mid (N[H]:H)$

og $N[H] \neq H$.

Thm 36.8 (Sylows 1. teorem)

$|G| < p^n \cdot m$, $n \geq 1$, $m \not\equiv p^n$

1) $\exists H \leq G$; $|H| = p^i \ \forall 1 \leq i \leq n$

2) $\forall H \leq G$, $|H| = p^i$, normal undergruppe $< K$ hvor $|K| = p^{i+1}$.

Bevis 1) Cauchy $\Rightarrow \exists$ undergruppe av orden p.

Induksjon: Anta $(\forall i < n, \exists H \leq G, |H| = p^i) \Rightarrow \exists H \leq G$ $|H| = p^{i+1}$

Anta $H \leq G$, $|H| = p^i$. Siden $i < n$ har vi $p \mid (G:H) = p^n m / p^i = p^{n-i} m \geq 0$. Det betyr at $p \mid (N[H] : H)$. Siden $H \underset{\text{normal}}{\leq} N[H] \Rightarrow N[H]/H$ gruppe og $p \mid |N[H]/H| \Rightarrow N[H]/H \geq K$, $|K| = p$

$$\gamma : N[H] \longrightarrow N[H]/H$$

$$\gamma^{-1}(K) \longmapsto K, |K| = p$$

$\gamma^{-1}(K)$ undergruppe

$\Rightarrow$ Vi har $H \leq \gamma^{-1}(K) \leq G$

2) Fra 1) har vi

$$H < \gamma^{-1}[K] \leq N[H]$$

hvor $|\gamma^{-1}[K]| = p^{i+1}$, Siden H er normal i $N[H]$ er den også normal i $\gamma^{-1}(K)$

QED

Def 36.9

$P \leq G$: P maximal p-undergruppe av G.

Sylow p-undergruppe

$$|P| = p^n \Rightarrow |g^{-1}Pg| = p^n$$

$\Rightarrow$ Den konjugerte av en Sylow P-undergruppe er selv en Sylow P-undergruppe

Thm 36.10 (Sylows 2. teorem)

Sylow p-undergruppet er konjugerte av hverandre

Bevis

$$\mathcal{L} = \{ aP_1 \mid a \in G \}$$ Venstre restklasser

P_2 virker på $\mathcal{L}$ ved $g(aP_1) = (ga)P_1$

Thm 36.1 $\Rightarrow$ $|\mathcal{L}_{P_1}| \equiv |\mathcal{L}| \pmod p$ og $|\mathcal{L}| = (G : P_1)$

Siden $p \nmid |\mathcal{L}| =$ har vi $|\mathcal{L}_{P_1}|$ ikke deles av p

$xP_1 \in \mathcal{L}_{P_2} \Rightarrow$ dvs $\forall y \in P_2 \; yxP_1 = xP_1 \Leftrightarrow x^{-1}yxP_1 = P_1$

som betyr $x^{-1}yx \in P_1 \quad \forall y \in P_2$

$\Rightarrow x^{-1}P_2x \leq P_1$ dvs $x^{-1}P_2x = P_1$

siden $|P_1| = |P_2|$ QED

Thm 36.11 (Sylows 3 teorem)

$p \mid |G| \Rightarrow$ antall sylow p-undergrupper $\equiv 1 \bmod p$ og deler $|G|$

Bevis $\mathcal{S}$ = mengden av Sylow p-undergrupper, $P \in \mathcal{S}$

$P \times \mathcal{S} \to \mathcal{S}$ ved $(x, T) \mapsto x^{-1} T x$

Vi har $|\mathcal{S}| \equiv |\mathcal{S}_p| \pmod p$

$$\mathcal{S}_p = \{ T \in \mathcal{S} \mid x^{-1} T x = T \ \forall x \in P \}$$

$\Rightarrow T \in \mathcal{S}_p$ gir $P \leq N[T]$

Åpenbart har vi $T \leq N[T]$

$P, T \leq G \Rightarrow P, T \leq N[T]$

Sylow p-ug Sylow p-ug.

$\Downarrow$ Thm 36.10

P, T konjugerte i $N[T]$

Pr. konstruksjon er T normal i $N[T]$

$\Rightarrow P = T$

$\Rightarrow \mathcal{S}_p = \{P\}$; $|\mathcal{S}_p| = 1$

$\Rightarrow |\mathcal{S}| \equiv 1 \pmod p$

La G virke på $\mathcal{S}$ ved konjugasjon. Alle elementa i $\mathcal{S}$ er konjugerte, dvs virkningen har kun én bane

$\Rightarrow |\mathcal{S}| = |G P| = (G : G_P) \mid |G|$

$\Rightarrow |\mathcal{S}| \mid |G|$

Ex. $|G| = pq$, $\exists H \leq G$, $|H| = P$

. antallet slike $N \equiv 1 \pmod p$ og deler pq

$\Rightarrow N = 1, p+1, 2p+1, \ldots (q-1)p+1$

$sp+1 \mid pq \Rightarrow tsp+t = pq$

$s < q \Rightarrow p \mid t$. ($s = 0$)

$\Rightarrow q \mid sp+1$ ella $t = pq$

($0 \leq s < q$) $\Downarrow$ $s = 1$

$\exists$ normal undergr

$p = 3$ $q = 5$:

$N = 1, 4, 9, 13, \not\equiv 15$

$\Rightarrow \exists$ normal undergr

$p = 3$ $q = 7$

$N = 1, 4, 9, 13, 17, 21$

$q = 3$ $p = 7$

$N = 1, 8, 15, 22 \not\equiv 21$

$\exists$ normal undergr

Det er ingen ikke-sykliske simple grupper av orden < 60

Teorem 1. *Det er ingen ikke-sykliske simple grupper av orden* < 60.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	

Teorem 2. *Enhver gruppe av prim orden er syklisk.*

			4		6		8	9	10
	12		14	15	16		18		20
21	22		24	25	26	27	28		30
	32	33	34	35	36		38	39	40
	42		44	45	46		48	49	50
51	52		54	55	56	57	58		

Teorem 3. *Senteret* $Z(G) = \{g \in G \,|\, z^{-1}gz = g \text{ for alle } z \in G\}$ *er en normal undergruppe av* G.

Teorem 4. *Enhver gruppe av orden* p^n *har trivielt senter.*

Bevis. Gruppa G virker på seg selv ved konjugasjon. Klasselikningen gir

$$|G| = |Z(G)| + \sum_{a \in A} [G : G_a]$$

hvor G_a er isotropigruppa til elementet a og hvor A indekserer de ikke-trivielle konjugasjonsklassene. Alle indeksene $[G : G_a]$ deler orden til gruppa og må derfor deles av p. Men det betyr at $|Z(G)|$ også deles av p og er derfor ikke-triviell. □

					6				10
	12		14	15			18		20
21	22		24		26		28		30
		33	34	35			38	39	40
	42		44	45	46		48		50
51	52		54	55	56	57	58		

Teorem 5. *Hvis* $|G| = mp^r$ *hvor* p *er et primtall og* $1 < m < p$, *så er* G *ikke simpel.*

Bevis. Antall Sylow-p-grupper er 1 modulo p og deler $|G| = mp^r$, dvs. det må dele m. Men siden $m < p$ må antallet Sylow-p-grupper være 1, som betyr at den er normal og gruppa er ikke simpel. □

	12								
			24						30
					36				40
				45			48		
					56				