6. Die Sylow-Theoreme

Einleitung: In diesem Kapitel geht es darum, die Existenz von Untergruppen einer endl. Gruppe mit speziellen Ordnungen zu zeigen. Für die Untersuchung von endlichen Gruppen sind die Sylow-Theoreme von zentraler Bedeutung.

Erinnerung: Im Beweis werden wir folgende beiden Gruppenwirkungen benutzen (siehe Bsp. (1) & (2) Kap. 3):

(1) $G \curvearrowright G: \quad G \times G \longrightarrow G$

$$(a, x) \longmapsto axa^{-1}$$

$\underbrace{[x]}$ $\underbrace{G\text{-Bahnen}}_{\text{Konj.-Klassen}}$; $|[x]| = [G : \underbrace{Z_G(x)}_{\text{Zentralisator}}]$

(2) $G \curvearrowright UGr(G): \quad G \times UGr(G) \longrightarrow UGr(G)$

$$(a, H) \longmapsto aHa^{-1}$$

$[H]$ Konj.-Klasse ; $|[H]| = [G : \underbrace{N(H)}_{\text{Normalisator}}]$

Lemma 6.1 Sei G eine endliche Gruppe mit $|G| = p^m \cdot n$, wobei p prim ist, $m, n > 0$ und $p \nmid n$. Sind $P, Q \leq G$ mit $|P| = |Q| = p^m$, dann gilt:

$$Q \leq N(P) \iff Q = P$$

$$\left[\ N(P) = \{x \in G : xPx^{-1} = P\}\ \right]$$

Beweis: ($\Leftarrow$) Ist $P=Q$ so gilt $Q \trianglelefteq N(P)=N(Q)$.

($\Rightarrow$) Ist $Q \leq N(P)$, dann ist, weil $P \trianglelefteq N(P)$, mit Thm. 2.14

$$PQ \leq N(P).$$

Also gilt mit Prop. 2.13:

$$|PQ| = \frac{|P|\cdot|Q|}{|P\cap Q|} = \frac{p^m\cdot p^m}{\underbrace{|P\cap Q|}_{=p^t\leq p^m}} = p^k \ (\text{für } \underset{(*)}{k\geq m}).$$

Weil $p^k / p^m\cdot n$ (denn $|PQ|\,\big|\,|G|$) und $p\nmid n$, muss gelten $\underset{(**)}{k\leq m}$, also $\underset{\text{mit } (*) \,\&\, (**)}{k=m}$. D.h. $|P\cap Q|=p^m$, also $P=Q$. $\dashv$

Def. Sei G eine endliche Gruppe mit $|G|=p^m\cdot n$, wobei p prim und $p\nmid n$. Dann heisst eine UG von G der Ordnung p^m Sylow p-Untergruppe von G; die Menge aller Sylow p-UG von G wird mit $\mathrm{Syl}_p(G)$ bezeichnet.

Theorem 6.2 (Sylow) Sei $|G|=p^m\cdot n$, p prim, $p\nmid n$. Dann gilt:

(a) Es gibt mind. eine Sylow p-Untergruppe $P\leq G$.

(b) Die Sylow p-UG in $\mathrm{Syl}_p(G)$ sind paarweise konjugiert.

(c) $|\mathrm{Syl}_p(G)| \equiv 1 \bmod p$. [kongruent 1 modulo p, d.h. $k\cdot p+1$]

(d) $|\mathrm{Syl}_p(G)| \,\big|\, n$.

Beweis: (a) Mit Induktion über $|G|$. Ist $|G|=1$, so ist nichts zu beweisen. Sei $|G|>1$ und (a) bewiesen für G' mit $|G'|<|G|$. Mit Faktum 3.4 gilt [Gruppenwirkung $G \curvearrowright G$ Konj.]

$$|G| = |Z(G)| + \sum_{j=1}^{s}[G:Z_G(x_j)] \quad \text{für } |[x_j]|\geq 2,$$

d.h. $Z_G(x_j)<G$ (echte Untergruppe). [beinhaltet Fall $s=0$]

Fall 1: $p\,\big|\,[G:Z_G(x_j)]$ für jedes j mit $1\leq j\leq s$ für $s\geq 1$, bzw. $p\,\big|\,|G|$ für $s=0$.

Dann haben wir $p\,\big|\,|Z(G)|$, also $|Z(G)|>1$.
(auch für $s=0$)

Weil $Z(G)$ abelsch ist, ist mit Korollar 5.5
$Z(G) \cong C_{n_1} \times \cdots \times C_{n_s}$ mit $n_i \mid n_{i+1}$ und $p \mid n_s$.
Somit ex. ein $a \in Z(G)$ mit $\mathrm{ord}(a) = p$, und weil
$\langle a \rangle \leq Z(G)$ ist $\langle a \rangle \trianglelefteq G$. Sei $\pi: G \to G/\langle a \rangle$
der natürliche Homomorphismus. Weil $|G/\langle a\rangle| = p^{m-1} \cdot n < |G|$,
ist $\langle a \rangle$ eine Sylow p-UG (falls $m=1$) oder es ex. mit Ind.-Voraus. in
$G/\langle a \rangle$ eine Sylow p-UG P' der Ordnung p^{m-1} (falls $m>1$).
Das Urbild $P \leq G$ von P' unter π ist dann eine Sylow p-UG
von G (der Ordnung p^m).

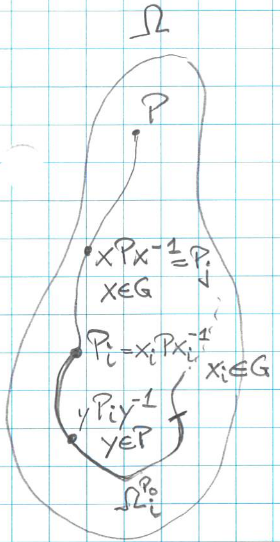
Bem: Ist $N \trianglelefteq G$ und $\bar{K} \leq G/N$, so ist
$N \leq K = \{x \in G : xN \in \bar{K}\} \leq G$ (Lem. 2.4(e))

Fall 2: Es ex. ein $1 \leq j_0 \leq s$ mit $p \nmid [G : Z_G(x_{j_0})]$
[weil $|[x_{j_0}]| \geq 2$, $Z_G(x_{j_0}) < G$]
Dann ist $|Z_G(x_{j_0})| = p^m \cdot k$ für ein $k < n$ mit $k \mid n$.
D.h. $|Z_G(x_{j_0})| < |G|$ und somit hat $Z_G(x_{j_0})$ nach Induktions-
voraussetzung eine Sylow p-UG P der Ordnung p^m,
und weil $P \leq G$ hat G eine Sylow p-Untergruppe.

Für (b) & (c) sei P_0 eine Sylow p-UG von G. $G \curvearrowright \{xP_0x^{-1} : x \in G\} = M_P$

Sei $\Omega_0 := \{xP_0x^{-1} : x \in G\}$ die Menge aller G-konj. von P_0.
Mit Bsp. (2) von Kap. 3 ist $|\Omega_0| = [G : N(P_0)]$. Für $P_i \in \Omega_0$
sei $\Omega_i^{P_0} := \{yP_iy^{-1} : y \in P_0\}$ die Menge aller P_0-konj. von P_i.
Dann ist Ω_0 die disjunkte Vereinigung von $\Omega_i^{P_0}$'s, also

$$|\Omega_0| = \sum_i |\Omega_i^{P_0}|.$$



Wieder mit Bsp. (2) von Kap. 3 haben wir

$$|\Omega_i^{P_0}| = [P_0 : N(P_i) \cap P_0].$$

$P_0 \curvearrowright M_P$

D.h. $|\Omega_i^{P_0}| = p^{k_i}$ (für $0 \leq k_i \leq m$) wobei $|\Omega_i^{P_0}| = 1 \Leftrightarrow P_i = P_0$:
denn $|\Omega_i^{P_0}| = 1 \iff P_0 \leq N(P_i)$ und $|P_0| = |P_i| = p^m \overset{\text{Lem. 6.1.}}{\iff} P_0 = P_i$.
Von allen Konj.-Klassen hat also genau eine nur ein Element,
alle anderen haben eine Grösse, welche durch p teilbar ist.
Somit ist $|\Omega_0| = \sum_i |\Omega_i^{P_i}| \equiv 1 \mod p$.
Es bleibt zu zeigen: $\Omega_0 = \mathrm{Syl}_p(G)$. [D.h. Sylow p-UG sind paarweise konj.]
[$\subseteq$ ist klar]

Für einen Widerspruch nehmen wir an $\Omega_0 \subsetneq \mathrm{Syl}_p(G)$,
d.h. es ex. eine Sylow p-UG $Q \leq G$ mit $Q \notin \Omega_0$,
also Q ist nicht konj. zu P_0. Alle Q-konj.

$$\Omega_i^Q := \{ y P_i y^{-1} : y \in Q \} \quad \text{wobei } P_i \in \Omega,$$

haben eine Grösse welche durch p teilbar ist, weil
sonst $Q \leq N(P_i)$ (für ein i) gelten würde, was mit
Lem. 6.1. $Q = P_i$ impliziert, also $Q \in \Omega_0$ $\lightning$ zur Annahme $Q \notin \Omega_0$
Weil nun $\Omega_0 = \dot{\bigcup_i} \Omega_i^Q$ und $p \mid |\Omega_i^Q|$ folgt, dass $p \mid |\Omega_0|$,
also $|\Omega_0| \equiv 0 \mod p$ im Widerspruch zu $|\Omega_0| \equiv 1 \mod p$.
Somit gilt $\Omega_0 = \mathrm{Syl}_p(G)$ (d.h. die Sylow p-UG sind
paarweise konj.) $\underset{\text{Teil (b)}}{}$ und $|\mathrm{Syl}_p(G)| \equiv 1 \mod p$. $\underset{\text{Teil (c)}}{}$

Für (d) sei $P_0 \in \mathrm{Syl}_p(G)$. Mit (b) ist $\mathrm{Syl}_p(G) = \{ x P_0 x^{-1} : x \in G \}$
und wieder ist $|\mathrm{Syl}_p(G)| = [G : N(P_0)]$. Weil $P_0 \leq N(P_0) \leq G$
folgt $p^m \mid |N(P_0)|$, also $|N(P_0)| = p^m \cdot k$ $(k \geq 1)$ und
weil $N(P_0) \leq G$, gilt $k \mid n$ und $[G : N(P_0)] = \underbrace{\frac{n}{k}}_{\in \mathbb{N}}$, d.h., weil $\frac{n}{k} \mid n$,
$|\mathrm{Syl}_p(G)| = [G : N(P_0)] \mid n$.

$\dashv$

Aus (b) folgt direkt

<u>Korollar 6.3</u> $\quad \mathrm{Syl}_p(G) = \{P\} \iff P \trianglelefteq G$

d.h. es ex. genau dann nur eine Sylow p-UG von G
wenn diese ein Normalteiler von G ist. [zwei Sylow p-UG sind immer konjugiert]

<u>Beispiel:</u> Sylow p-Untergruppen der Dodekaedergruppe D.

- $|D| = 60 = 2^2 \cdot 3 \cdot 5$; 30 Kanten, 20 Ecken, 12 Flächen
- $|\mathrm{Syl}_2(D)| \in \{1, 3, \underline{\underline{5}}, 15\}$ $\quad n = 15 \quad C_2 \times C_2 \quad$ Kantenmitten

  $|\mathrm{Syl}_3(D)| \in \{1, 4, \underline{\underline{10}}\}$ $\quad n = 20 \quad C_3 \quad$ Ecken

  $|\mathrm{Syl}_5(D)| \in \{1, \underline{\underline{6}}\}$ $\quad n = 12 \quad$ Flächenmitten

$\Rightarrow$ keine der Sylow p-UG von D ist ein Normalteiler.