§10. Die Sylow–Sätze

Nachdem wir in (9.3) gesehen haben, daß die Umkehrung des Satzes von Lagrange für endliche **abelsche** Gruppen richtig ist, wollen wir jetzt diese Fragestellung für endliche **nichtabelsche** Gruppen untersuchen: Zu welchen Teilern der Gruppenordnung gibt es auch eine Untergruppe mit diesem Teiler als Ordnung? Antwort darauf geben die sog. **Sylow–Sätze** , die die Existenz gewisser primärer Untergruppen sichern.

L. Sylow , 1832–1918 , norwegischer Mathematiker

Literatur: Fischer/Sacher: "Einführung in die Algebra"

(10.1) SATZ: (1. Sylow–Satz , 1872)

G sei eine endliche Gruppe der Ordnung n , und es gelte $p^k \mid n$ für ein $p \in \mathbb{P}$ und $k \in \mathbb{N}_0$. Dann enthält G eine Untergruppe U der Ordnung p^k .

Bew: Der Beweis wird durch Induktion nach der Gruppenordnung n geführt.

U ist dann eine p–primäre Gruppe.

(10.2) FOLGERUNG: (Lemma von Cauchy)

G sei eine endliche Gruppe und p ein Primteiler von $|G|$. Dann enthält G ein Element der Ordnung p .

(10.3) DEF: G sei eine endliche Gruppe der Ordnung n. Ferner sei p eine Primzahl. Für $m \in \mathbb{N}_0$ gelte $p^m | n$ und $p^{m+1} \nmid n$. Dann heißt eine Untergruppe von G der Ordnung p^m eine ***p*–Sylowuntergruppe von *G*** .

(10.4) B & B: a) Eine p–Sylowuntergruppe von G ist eine p–primäre Untergruppe maximaler Ordnung von G .

b) Nach (10.1) enthält G zu jeder Primzahl p eine p–Sylowuntergruppe, die im Falle $p \nmid |G|$ trivial ist.

c) Die Umkehrung des Satzes von Lagrange gilt also im nichtabelschen Fall zumindest für solche Teiler von $|G|$, die Primzahlpotenzen sind.

d) In S_3 mit $|S_3| = 6 = 2 \cdot 3$ gibt es drei 2–Sylowuntergruppen der Ordnung 2 und genau eine 3–Sylowuntergruppe der Ordnung 3 , nämlich $A_3 \trianglelefteq S_3$.

e) Es ist $|A_4| = 12 = 2^2 \cdot 3$. In A_4 gibt es genau eine 2–Sylowuntergruppe der Ordnung 4 , nämlich $V \trianglelefteq A_4$, und vier 3–Sylowuntergruppen der Ordnung 3 . Es gibt jedoch **keine** Untergruppe in A_4 der Ordnung $6 = 2 \cdot 3$.

f) In S_4 mit $|S_4| = 24 = 2^3 \cdot 3$ gibt es drei 2–Sylowuntergruppen der Ordnung 8 und vier 3–Sylowuntergruppen der Ordnung 3 . Daneben gibt es auch Untergruppen der Ordnung 2^1 und 2^2 , die aber keine Sylowuntergruppen sind.

(10.5) DEF: G sei eine Gruppe. Zwei Untergruppen U und V heißen **konjugiert**, wenn es ein $a \in G$ gibt mit $\tau_a(U) = V$.

BEM: $\tau_a : G \longrightarrow G \;,\; x \longmapsto axa^{-1}$ ist der Gruppenautomorphismus aus Aufgabe 46 . $\tau_a(U) = V$ ist also gleichbedeutend mit $aUa^{-1} = V$. Konjugierte Untergruppen sind insbesondere isomorph.

(10.6) SATZ: (2. Sylow–Satz)

G sei eine endliche Gruppe und $p \in \mathbb{P}$. Dann gilt:

a) Jede Untergruppe von G der Ordnung p^k $(k \in \mathbb{N}_0)$ liegt in einer p–Sylowuntergruppe von G .

b) Je zwei p–Sylowuntergruppen von G sind zueinander konjugiert.

(10.7) BEM: **a)** Eine p–Sylowuntergruppe $U \le G$ ist genau dann ein Normalteiler von G, wenn U die einzige p–Sylowuntergruppe von G ist. Für $N \trianglelefteq G$ gilt nämlich $\tau_a(N) = aNa^{-1} = N \;\; \forall\, a \in G$.

b) In einer endlichen abelschen Gruppe gibt es zu jeder Primzahl p genau eine p–Sylowuntergruppe.

(10.8) SATZ: (3. Sylow–Satz)

G sei eine endliche Gruppe und p eine Primzahl. Es bezeichne $s(p)$ die Anzahl der p–Sylowuntergruppen von G . Dann gilt:

a) $s(p)$ ist ein Teiler von $|G|$

b) $s(p) \equiv 1 \pmod p$.

(10.9) BEISPIELE: **a)** $|S_3| = 6 = 2 \cdot 3$ (s.(10.4d))

$s(p) \in \{1, 2, 3, 6\}$

$s(2) \equiv 1 \pmod 2 \implies s(2)$ ungerade $\implies s(2) \in \{1, \underline{\underline{3}}\}$

$s(3) \equiv 1 \pmod 3 \implies s(3) = 1$.

Da es nur eine 3–Sylowuntergruppe gibt, ist diese nach (10.7a) Normalteiler.

b) $|A_4| = 12 = 2^2 \cdot 3$ (vgl. (10.4e))

$s(p) \in \{1, 2, 3, 4, 6, 12\}$

$s(2) \equiv 1 \pmod 2 \implies s(2)$ ungerade $\implies s(2) \in \{\underline{\underline{1}}, 3\}$

$s(3) \equiv 1 \pmod 3 \implies s(3) \in \{1, \underline{\underline{4}}\}$

c) $|S_4| = 24 = 2^3 \cdot 3$ (vgl. (10.4f))

$s(p) \in \{1, 2, 3, 4, 6, 8, 12, 24\}$

$s(2) \equiv 1 \pmod 2 \implies s(2)$ ungerade $\implies s(2) \in \{1, \underline{\underline{3}}\}$

$s(3) \equiv 1 \pmod 3 \implies s(3) \in \{1, \underline{\underline{4}}\}$.

(10.10) LEMMA: Jede Gruppe der Ordnung 15 ist zyklisch und damit isomorph zu $\mathbb{Z}_{15}$.