15. Die Sylowsätze

Bemerkung: In Satz 105 haben wir die Umkehrung des Satzes von Lagrange für endliche abelsche Gruppen G bewiesen (d.h. hat $n \in \mathbb{N} \setminus \{0\}$ die Eigenschaft $n \,\big|\, |G|$, so gibt es eine Untergruppe $H \leq G$ der Ordnung $|H| = n$). Im folgenden werden wir uns der analogen Frage für beliebige endliche Gruppen G widmen, wenn n eine Primzahlpotenz ist.

Definition: Ist G eine Gruppe und $H \leq G$, $H \neq G$, so schreiben wir kurz $H < G$.

Satz 111 (Cauchy): Es sei G eine endliche Gruppe und p eine Primzahl mit der Eigenschaft $p \,\big|\, |G|$. Dann gibt es ein $a \in G$ mit der Eigenschaft $\operatorname{ord}(a) = p$ (d.h. $|\langle a \rangle| = p$).

Beweis: Induktion nach $|G|$. Für $|G| = 1$ ist die Behauptung trivial erfüllt (und natürlich auch für $|G| = 2$). Sei nun $|G| > 1$ und $p \,\big|\, |G|$.

1. Fall: Es gibt ein $H < G$ mit der Eigenschaft $p \,\big|\, |H|$. Dann gibt es nach IV ein $a \in H$ mit der Eigenschaft $\operatorname{ord}(a) = p$.

2. Fall: Es gibt kein $H < G$ mit der Eigenschaft $p \,\big|\, |H|$. Ist $x \in G \setminus Z(G)$, so ist $C_G(x) < G$ und daher nach Voraussetzung $p \nmid |C_G(x)|$. Da $p \,\big|\, |G|$ und

$$|G| = \big[G : C_G(x)\big] \cdot |C_G(x)|$$

(wegen Korollar 19 (i)) muss $p \,\big|\, \big[G : C_G(x)\big]$ gelten. Ist $x_1, \ldots, x_n \in G$ ein Repräsentantensystem für die Konjugationsklassen von G, so gilt folglich

$$\big[G : C_G(x_i)\big] \equiv 0 \pmod{p} \text{ wenn } x_i \notin Z(G).$$

Mittels Korollar 110 folgt

$$|Z(G)| \equiv |Z(G)| + \sum_{\substack{1 \leq i \leq n \\ x_i \notin Z(G)}} \big[G : C_G(x_i)\big] = |G| \equiv 0 \pmod{p},$$

d.h. $p \,\big|\, |Z(G)|$. Wegen der Voraussetzung für den 2. Fall kann nicht $Z(G) < G$ gelten. Daher ist $Z(G) = G$, d.h. G ist abelsch. Für abelsche Gruppen folgt die Behauptung aber bereits aus Satz 105.

Definition: Es sei p eine Primzahl. Eine Gruppe G heißt p-Gruppe, wenn die Ordnung jedes Elements von G eine Potenz von p ist (d.h. $\forall a \in G \; \exists n \in \mathbb{N} \cup \{0\} : \operatorname{ord}(a) = p^n$).

Definition: Es sei p eine Primzahl und G eine Gruppe. Eine Untergruppe H von G heißt p-Untergruppe von G, wenn H eine p-Gruppe ist.

Bemerkung: Wegen $\operatorname{ord}(e) = 1 = p^0$ ist $\{e\}$ eine p-Untergruppe der Gruppe G für jede Primzahl p.

Korollar 112: Es sei p eine Primzahl und G eine endliche Gruppe. Dann sind äquivalent:

(i) G ist eine p-Gruppe,
(ii) $|G|$ ist eine Potenz von p, d.h. $\exists n \in \mathbb{N} \cup \{0\} : |G| = p^n$.

Beweis: (i) $\Rightarrow$ (ii) Ist $|G|$ keine Potenz von p, so gibt es eine Primzahl $q(\neq p)$ mit der Eigenschaft $q \,\big|\, |G|$. Nach Satz 111 existiert dann ein $a \in G$ mit der Eigenschaft $\operatorname{ord}(a) = q$ und G ist daher keine p-Gruppe.
(ii) $\Rightarrow$ (i) Folgt aus Korollar 19 (iii), d.h. $\forall a \in G : \operatorname{ord}(a) \,\big|\, |G|$.

Satz 113: Es sei p eine Primzahl und G eine endliche p-Gruppe. Operiert G auf einer endlichen Menge M, so gilt $|M^G| \equiv |M| \pmod{p}$.

Bemerkungen: Ist $x \in M \setminus M^G$, so $\exists a \in G : ax \neq x$ und daher $G_x < G$. Ist $n \in \mathbb{N} \cup \{0\}$, derart dass $|G| = p^n$, so $\exists m \in \{0, 1, \dots, n-1\} : |G_x| = p^m$. Aus

$$p^n = |G| = |G_x| \cdot [G : G_x] = p^m \cdot [G : G_x]$$

folgt $p \mid [G : G_x]$. Ist $x_1, \dots, x_n \in M$ ein Repräsentantensystem für die Bahnen der Operation von G auf M, so gilt daher $\left[G : G_{x_i}\right] \equiv 0 \pmod{p}$ falls $x_i \notin M^G$. Aus Satz 109 folgt

$$|M^G| \equiv |M^G| + \sum_{\substack{1 \leq i \leq n \\ x_i \notin M^G}} \left[G : G_{x_i}\right] = |M| \pmod{p}.$$

Korollar 114: Ist p eine Primzahl und $G \neq \{e\}$ eine endliche p-Gruppe, so gilt $p \,\big|\, |Z(G)|$. Insbesondere ist $Z(G) \neq \{e\}$.

Beweis: Wendet man Satz 113 auf die Operation der Gruppe G auf sich selbst durch Konjugation an, so erhält man $|Z(G)| \equiv |G| \equiv 0 \pmod{p}$.

Satz 115 (Erster Sylowsatz): Es sei G eine endliche Gruppe und p eine Primzahl. Ist $n \in \mathbb{N} \cup \{0\}$, derart dass $p^n \,\big|\, |G|$, so existiert für jedes $i \in \{0, 1, \dots, n\}$ eine Untergruppe $H \leq G$ mit der Ordnung $|H| = p^i$.

Beweis: Der Fall $n = 0$ ist trivial erfüllt und wir können ab sofort $n \geq 1$ voraussetzen. Wir verwenden Induktion nach $|G|$. Für $|G| = 1$ ist die Behauptung trivial erfüllt (und natürlich auch für $|G| = 2$).

1. Fall: $p \,\big|\, |Z(G)|$. Nach Satz 111 gibt es ein $a \in Z(G)$ mit $\operatorname{ord}(a) = p$. Da $a \in Z(G)$ ist $\langle a \rangle \trianglelefteq G$. (Trivialerweise ist $\langle a \rangle \leq G$ und $xa^k x^{-1} = a^k x x^{-1} = a^k \in \langle a \rangle \ \forall k \in \mathbb{Z} \ \forall x \in G$.) Es ist

$$\left|G \Big/ \langle a \rangle\right| = \frac{|G|}{|\langle a \rangle|} = \frac{|G|}{p} < |G|.$$

Da

$$p^{n-1} \Big| \Big| G \Big/ \langle a \rangle \Big|$$

enthält $G/\langle a\rangle$ nach IV für jedes $i \in \{1, \dots, n\}$ ein $\overline{H}_i \leq G/\langle a\rangle$ mit $|\overline{H}_i| = p^{i-1}$. Nach Satz 31 (ii) gibt es für jedes $i \in \{1, \dots, n\}$ eine Untergruppe H_i mit $\langle a\rangle \leq H_i \leq G$ und der Eigenschaft $H_i/\langle a\rangle = \overline{H}_i$. Diese hat Ordnung

$$|H_i| = \big|\langle a\rangle\big| \cdot \Big|H_i \Big/ \langle a\rangle\Big| = \big|\langle a\rangle\big| \cdot \big|\overline{H}_i\big| = p \cdot p^{i-1} = p^i.$$

(Der nicht bewiesene Fall $i = 0$ ist trivial.)

2. Fall: $p \nmid |Z(G)|$. Bezeichnet $x_1, \dots, x_n$ ein Repräsentantensystem für die Konjugationsklassen von G, so ist nach Korollar 110

$$|G| = |Z(G)| + \sum_{\substack{1 \leq j \leq n \\ x_j \notin Z(G)}} \big[G : C_G(x_j)\big].$$

Daher muss es ein $j \in \{1, \dots, n\}$ geben, für das $x_j \notin Z(G)$ und $p \nmid [G : C_G(x_j)]$ gelten. Da $|G| = |C_G(x_j)| \cdot [G : C_G(x_j)]$ folgt $p^n \,\big|\, |C_G(x_j)|$. Aus $x_j \notin Z(G)$ folgt $C_G(x_j) < G$ und daher $|C_G(x_j)| < |G|$. Nach IV gibt es für jedes $i \in \{0, 1, \dots, n\}$ eine Untergruppe $H_i \leq C_G(x_j)$ mit Ordnung $|H_i| = p^i$. Da dann auch $H_i \leq G$, ist die Behauptung auch im 2. Fall bewiesen.

Definition: Es sei G eine endliche Gruppe und p eine Primzahl. Ist $|G| = p^n \cdot m$ (mit $n \in \mathbb{N} \cup \{0\}$, $m \in \mathbb{N} \setminus \{0\}$ und $p \nmid m$), so wird eine Untergruppe $P \leq G$ mit Ordnung $|P| = p^n$ eine p-Sylowgruppe von G genannt.

Korollar 116: Es sei G eine endliche Gruppe und p eine Primzahl. Dann enthält G eine p-Sylowgruppe P.

Beweis: Folgt sofort aus Satz 115.

Beispiele: 1) Betrachte die symmetrische Gruppe S_3. Da $|S_3| = 3! = 6 = 2 \cdot 3$, sind $\{\varepsilon, (1\ 2)\}$, $\{\varepsilon, (1\ 3)\}$ und $\{\varepsilon, (2\ 3)\}$ drei 2-Sylowgruppen von S_3 und $\{\varepsilon, (1\ 2\ 3), (1\ 3\ 2)\}$ ist eine 3-Sylowgruppe von S_3.
2) Betrachte die alternierende Gruppe A_4. Da $|A_4| = 4!/2 = 12 = 2^2 \cdot 3$, ist

$$\{\varepsilon, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

eine 2-Sylowgruppe von A_4 und

$$\{\varepsilon, (1\ 2\ 3), (1\ 3\ 2)\},\ \{\varepsilon, (1\ 2\ 4), (1\ 4\ 2)\},\ \{\varepsilon, (1\ 3\ 4), (1\ 4\ 3)\} \text{ und } \{\varepsilon, (2\ 3\ 4), (2\ 4\ 3)\}$$

sind vier 3-Sylowgruppen von A_4.

Lemma 117: Es sei G eine endliche Gruppe, p eine Primzahl und P eine p-Sylowgruppe von G.

(i) Ist $Q \leq G$ zu P konjugiert, so ist Q ebenfalls eine p-Sylowgruppe von G.

(ii) Ist P die einzige p-Sylowgruppe von G, so ist $P \trianglelefteq G$.

Beweis: (i) Da Q zu P konjugiert ist, gibt es ein $a \in G$, sodass $Q = aPa^{-1}$. D.h. Q ist das Bild von P unter dem inneren Automorphismus $\varphi_a : G \to G$, $x \mapsto axa^{-1}$ und daher $|Q| = |aPa^{-1}| = |P|$.
(ii) Nach (i) ist aPa^{-1} eine p-Sylowgruppe von G für jedes $a \in G$. Nach Voraussetzung muss daher $aPa^{-1} = P \ \forall a \in G$ gelten und P ist ein Normalteiler.

Satz 118 (Zweiter Sylowsatz): Es sei G eine endliche Gruppe, p eine Primzahl und P eine p-Sylowgruppe von G. Ist H eine p-Untergruppe von G, so $\exists a \in G : H \leq aPa^{-1}$.

Beweis: Die Gruppe H operiert auf der Menge $M = \{aP \mid a \in G\}$ der Linksnebenklassen von P in G mittels $(h, aP) \mapsto haP$. (Diese Abbildung ist wohldefiniert, denn ist $aP = bP$, so ist $a^{-1}b \in P$ und daher $(ha)^{-1}(hb) = a^{-1}h^{-1}hb = a^{-1}b \in P$. Die Gruppe H operiert auf M weil $eaP = aP \ \forall a \in G$ und $(h_1h_2)aP = h_1(h_2a)P \ \forall h_1, h_2 \in H \ \forall a \in G$.) Es ist $|M| = [G : P] = |G|/|P|$ und folglich $p \nmid |M|$. Nach Satz 113 gilt $|M^H| \equiv |M| \pmod{p}$ und daher auch $p \nmid |M^H|$. Also ist $|M^H| \neq 0$ und somit $M^H \neq \varnothing$, d.h. $\exists a \in G : aP \in M^H$. Das besagt aber gerade $haP = aP$ oder $a^{-1}h^{-1}a = (ha)^{-1}a \in P \ \forall h \in H$. Also ist $a^{-1}Ha \leq P$ und daher $H \leq aPa^{-1}$.

Bemerkung: Nach Satz 118 sind die p-Sylowgruppen einer endlichen Gruppe G genau die (bezüglich der Mengeninklusion) maximalen p-Untergruppen von G. Man kann diese Eigenschaft als Definition verwenden, um den Begriff der p-Sylowgruppe für beliebige (d.h. auch unendliche) Gruppen zu definieren.

Korollar 119: Es sei G eine endliche Gruppe und p eine Primzahl.
(i) Die p-Sylowgruppen von G bilden eine Konjugationsklasse von Untergruppen von G.
(ii) Ist P eine p-Sylowgruppe von G so gilt:

$$P \text{ ist die einzige } p\text{-Sylowgruppe von } G \iff P \trianglelefteq G.$$

Beweis: (i) Sind P und Q zwei p-Sylowgruppen von G, so gibt es nach Satz 118 ein $a \in G$, sodass $Q \leq aPa^{-1}$. Da $|Q| = |P| = |aPa^{-1}|$, muss $Q = aPa^{-1}$ gelten, d.h. P und Q sind konjugiert. Die Behauptung folgt nun mit Hilfe von Lemma 117 (i).
(ii) ($\Rightarrow$) Wurde schon in Lemma 117 (ii) bewiesen.
($\Leftarrow$) Es sei Q eine p-Sylowgruppe von G. Nach (i) ist Q zu P konjugiert, d.h. es gibt ein $a \in G$, sodass $Q = aPa^{-1} = P$.

Satz 120 (Dritter Sylowsatz): Es sei G eine endliche Gruppe und p eine Primzahl. Bezeichnet s die Anzahl der p-Sylowgruppen von G, so gelten $s \,\big|\, |G|$ und $s \equiv 1 \pmod{p}$.

Beweis: Ist P eine p-Sylowgruppe, so ist $\{aPa^{-1} \mid a \in G\}$ wegen Korollar 119 (i) die Menge aller p-Sylowgruppen von G. Wir betrachten die Operation von G auf der Menge der $\mathcal{U}_G$ aller Untergruppen von G durch Konjugation. Die Menge $\{aPa^{-1} \mid a \in G\}$ der p-Sylowgruppen ist dann die Bahn und der Normalisator $N_G(P)$ die Isotropiegruppe von P bezüglich dieser Operation. Durch Anwenden von Satz 108 erhält man

$$s = |\{aPa^{-1} \mid a \in G\}| = [G : N_G(P)] = |G|/|N_G(P)|.$$

Daher ist $s \cdot |N_G(P)| = |G|$ und folglich $s \,\big|\, |G|$.
Wir betrachten nun eine andere Gruppenoperation, nämlich die von P auf der Menge $M = \{aPa^{-1} \mid a \in G\}$ aller p-Sylowgruppen durch Konjugation. Offenbar ist $P \in M$ Fixpunkt dieser Operation (denn $xPx^{-1} = P \ \forall x \in P$). Wir behaupten, dass es keine weiteren Fixpunkte gibt. Offenbar gilt:

$$Q \text{ ist Fixpunkt} \Leftrightarrow xQx^{-1} = Q \ \forall x \in P \Leftrightarrow P \leq N_G(Q)$$

Nach Definition des Normalisators ist $Q \trianglelefteq N_G(Q)$. Daher ist auch $PQ \leq N_G(Q)$ (wegen Satz 29 (iii)). Man kann nun den 1. Isomorphiesatz (Korollar 30) anwenden und erhält $PQ/Q \cong P/(P \cap Q)$. Daraus folgt sofort $|PQ/Q| = |P/(P \cap Q)|$ und da P eine p-Gruppe ist, sind auch $P/(P \cap Q)$ und folglich PQ/Q beides p-Gruppen. Würde $p \,\big|\, |PQ/Q|$ gelten, so wäre

$$0 \not\equiv [G : Q] = [G : PQ] \cdot [PQ : Q] \equiv 0 \pmod{p},$$

ein Widerspruch. Also ist $|PQ/Q| = 1$ und $PQ = Q$, woraus $P \subseteq Q$ folgt. Da $|P| = |Q|$, muss $P = Q$ gelten (und P ist tatsächlich der einzige Fixpunkt). Aus Satz 113 folgt $s = |M| \equiv |M^P| = 1 \pmod{p}$.

Bemerkung: Ist G eine endliche Gruppe der Ordnung $|G| = p^n m$ (mit p eine Primzahl, $n, m \in \mathbb{N} \setminus \{0\}$ und $p \nmid m$) und bezeichnet s die Anzahl der p-Sylowgruppen von G, so gilt nach Satz 120 $s \mid p^n m$. Da auch $s \equiv 1 \pmod{p}$ muss $p \nmid s$ und daher $\mathrm{ggT}(s, p^n) = 1$ gelten. Also muss sogar $s \mid m$ gelten.

Beispiele: 1) Wir betrachten wieder die symmetrische Gruppe S_3 mit $|S_3| = 6 = 2 \cdot 3$. Die Anzahl s_2 der 2-Sylowgruppen muss $s_2 \mid 3$ und $s_2 \equiv 1 \pmod{2}$ erfüllen. Nach der ersten Bedingung muss $s_2 \in \{1, 3\}$ gelten. Daher haben wir oben mit $\{\varepsilon, (1\ 2)\}$, $\{\varepsilon, (1\ 3)\}$ und $\{\varepsilon, (2\ 3)\}$ bereits alle 2-Sylowgruppen von S_3 gefunden und $s_2 = 3$. Die Anzahl s_3 der 3-Sylowgruppen muss $s_3 \mid 2$ und $s_3 \equiv 1 \pmod{3}$ erfüllen. Daher ist $s_3 = 1$ und $A_3 = \{\varepsilon, (1\ 2\ 3), (1\ 3\ 2)\}$ ist die einzige 3-Sylowgruppe von S_3. Nach Korollar 119 (ii) ist $A_3 \trianglelefteq S_3$. (Das wurde allerdings schon in Satz 46 (i) bewiesen, woraus mit Hilfe von

Korollar 119 (ii) ebenfalls $s_3 = 1$ folgt.)
2) Wir betrachten wieder die alternierende Gruppe A_4 mit $|A_4| = 12 = 2^2 \cdot 3$. Die Anzahl s_2 der 2-Sylowgruppen muss wieder $s_2 \mid 3$ und $s_2 \equiv 1 \pmod 2$ erfüllen. Es folgt wieder $s_2 \in \{1, 3\}$. Nun ist $V := \{\varepsilon, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \trianglelefteq A_4$. (Es wurde bereits gezeigt, dass es sich um eine Untergruppe handelt. Ist $\{a, b, c, d\} = \{1, 2, 3, 4\}$, so ist $\sigma \circ (a\ b)(c\ d) \circ \sigma^{-1} = \big(\sigma(a)\ \sigma(b)\big)\big(\sigma(c)\ \sigma(d)\big) \in V\ \forall \sigma \in A_4$ und daher $V \trianglelefteq A_4$.) Wegen Korollar 119 (ii) ist V die einzige 2-Sylowgruppe von A_4 und $s_2 = 1$. Die Anzahl s_3 der 3-Sylowgruppen muss $s_3 \mid 4$ und $s_3 \equiv 1 \pmod 3$ erfüllen. Daher ist $s_3 \in \{1, 4\}$. Daher haben wir oben mit

$$\{\varepsilon, (1\ 2\ 3), (1\ 3\ 2)\},\ \{\varepsilon, (1\ 2\ 4), (1\ 4\ 2)\},\ \{\varepsilon, (1\ 3\ 4), (1\ 4\ 3)\} \text{ und } \{\varepsilon, (2\ 3\ 4), (2\ 4\ 3)\}$$

bereits alle 3-Sylowgruppen von A_4 gefunden und $s_3 = 4$.

Bemerkung: Man kann sich fragen, ob man die Sylowsätze (zumindest teilweise) auf folgende Situation verallgemeinern kann: Es sei G eine endliche Gruppe und $|G| = mn$ mit $m, n \in \mathbb{N} \setminus \{0\}$ und $\mathrm{ggT}(m, n) = 1$. Gibt es dann z.B. stets eine Untergruppe $H \leq G$ mit Ordnung $|H| = m$? Das ist im allgemeinen nicht richtig. Z.B. ist $|A_5| = 60 = 4 \cdot 15$ aber A_5 besitzt keine Untergruppe der Ordnung 15. Man kann einen entsprechenden Satz allerdings beweisen, wenn es sich bei G um eine sogenannte auflösbare Gruppe handelt.