Erinnerung: Sei G eine endliche Gruppe und p ein Primteiler der Gruppenordnung $|G|$. Schreibe

$$|G| = p^k m \quad \text{für} \quad k, m \geqslant 1 \text{ mit } p \nmid m.$$

5.7.1 Definition: Jede Untergruppe von G der Ordnung p^k heisst eine *p-Sylowuntergruppe* oder *p-Sylowgruppe von G*. Sei $\mathrm{Syl}_p(G)$ die Menge aller p-Sylowgruppen von G.

5.7.2 Satz: *(Sylowsätze)*

(a) Es existiert eine p-Sylowgruppe von G.

(b) Jede p-Untergruppe von G ist in einer p-Sylowgruppe von G enthalten.

(c) Alle p-Sylowgruppen von G sind zueinander konjugiert.

(d) Die Anzahl der p-Sylowgruppen von G ist $\equiv 1 \bmod p$ und ein Teiler von m.

5.7.3 Folge: (e) Die Gruppe G besitzt ein Element der Ordnung p.

Beweis (e): G abelsch ✓.

G beliebig $\Rightarrow$ Wähle $P \in \mathrm{Syl}_p(G) \Rightarrow |P| = p^k$, $k \geq 1$. $\Rightarrow Z(P) \neq 1$.

$Z(P)$ abelsch, $|Z(P)| = p^l$ für ein $l \geq 1$. Fertig! qed.

(b) Sei $H < G$ eine p-Gruppe, sei $P \in Syl_p(G)$.

Betrachte die Linksoperation von H auf G/P durch Translation.

$\Rightarrow$ Jede Bahn hat Länge p^l für ein $l \geq 0$.
$|G/P| = m \not\equiv 0 \ (p)$.
$\Bigg\} \Rightarrow \exists$ Bahn der Länge 1, d.h. ein Fixpunkt.

Also $\exists\, g \in G : \forall\, h \in H,\ hgP = gP. \Rightarrow hg \in gP \Rightarrow h \in gPg^{-1} = {}^gP$

Also $H < {}^gP \in Syl_p(G)$.

(c) $H, P \in Syl_p(G) \xrightarrow{\text{oben}} \exists\, g \in G;\ H < {}^gP$
und $|H| = p^k = |P| = |{}^gP|$
$\Big\} \Rightarrow H = {}^gP$.

(d) Betrachte die Operation von G auf $Syl_p(G)$ durch Konjugation.

Nach (c) ist sie transitiv. Wähle $P \in Syl_p(G)$ und setze $N := Norm_G(P)$

$\Rightarrow \boxed{G/N \xrightarrow{\text{bij}} Syl_p(G)},\ gN \longmapsto {}^gP$

$P \lhd N \Rightarrow |N| = \underbrace{|P|}_{p^k} \cdot [N:P]$

$\Rightarrow |Syl_p(G)| = |G/N| = \dfrac{|G|}{|N|} = \dfrac{p^k m}{p^k \cdot [N:P]} =$ Teiler von m.

Betrachte die Operation von P durch Linksmultiplikation auf G/N.

$\Rightarrow$ Jede Bahn der Länge > 1 hat Länge $\equiv 0$ mod p.

Sei gN eine Bahn der Länge 1, d.h. Fixpunkt,

$\Rightarrow \forall\, p \in P:\ pgN = gN. \Rightarrow p \in {}^gN,$

$\Rightarrow P < {}^gN. \Rightarrow {}^{g^{-1}}P < N \rhd P$

$\Rightarrow \exists!$ Bahn der Länge 1.

Betrachte den Homo: ${}^{g^{-1}}P \xrightarrow{\varphi} N/P$.
Ist der nichttrivial, so ist Bild(φ) eine nichttriviale p-Gruppe.
Dies widerspricht $|N/P|$ teilt m.
Also ist φ trivial, daher ${}^{g^{-1}}P < P$.
$\Rightarrow {}^{g^{-1}}P = P \Rightarrow g^{-1} \in N \Rightarrow g \in N \Rightarrow gN = N$.

Also ist $|G/N| = 1 + \sum(\text{Bahnenlängen} \equiv 0\,(p)) \equiv 1\,(p)$. qed

5.8 Kleine endliche Gruppen

5.8.1 Proposition: Jede Gruppe der Ordnung pq oder p^2q oder pqr für Primzahlen p, q, r ist auflösbar.

$p \neq q \neq r$.

Bew.: Sei $|G| = pq$ mit $p < q$.

$\Rightarrow \#Syl_q(G) \equiv 1 \bmod (q)$ und teilt p.

$\Rightarrow \;= 1$.

$\Rightarrow$ Die einzige q-Sylowgruppe $Q \lhd G$.

$\left.\begin{array}{l}\Rightarrow |Q| = q \Rightarrow Q \text{ zyklisch.}\\ |G/Q| = p \Rightarrow G/Q \text{ zyklisch}\end{array}\right\} \Rightarrow G$ auflösbar.

Weiter: Sei P eine p-Sylowgruppe $\Rightarrow P \simeq G/Q$

$\Rightarrow P \cap Q = 1$ und $P \cdot Q = G$.

$\Rightarrow G = Q \rtimes P$ via $P \to Aut(Q)$

$$\begin{array}{ccc} P & & Aut(Q) \\ \| & & \| \\ \mathbb{Z}_p & & Aut(\mathbb{Z}_q) \\ & \searrow & \wr\| \\ & & \mathbb{F}_q^\times \\ & & \| \\ & & \text{zyklisch der} \\ & & \text{Ordnung } q-1 \end{array}$$

Ist $p \nmid q-1$, so folgt G abelsch.

Ist $p \mid q-1$, kann G nicht abelsch sein.

Sei $|G| = p^2q$.

Ist $|Syl_p(G)| = 1$, hat G eine normale p-Sylowgruppe P und $|P| = p^2 \Rightarrow P$ abelsch und $|G/P| = q$

$\Rightarrow G/P$ zyklisch $\Rightarrow G$ auflösbar.

Ist $|Syl_q(G)| = 1$, hat G eine normale q-Sylowgruppe Q und $|Q| = q \Rightarrow Q$ zyklisch und $|G/Q| = p^2$

$\Rightarrow G/Q$ abelsch $\Rightarrow G$ auflösbar.

Bsp.: $A_4 \cong K \rtimes \mathbb{Z}_3 \cong \mathbb{Z}_2^2 \rtimes \mathbb{Z}_3$

Bsp.: $\mathbb{F}_5 \rtimes \mathbb{F}_5^\times \cong \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix} < Gl_2(\mathbb{F}_5)$.

Sei also $|Syl_p(G)| > 1$ und $|Syl_q(G)| > 1$.

$\left.\begin{array}{l}\Rightarrow |Syl_p(G)| = q \equiv 1 \bmod (p) \Rightarrow q > p. \\ \text{und } |Syl_q(G)| = \left\{\begin{array}{l} p \\ p^2 \end{array}\right\} \equiv 1 \bmod (q).\end{array}\right\} \Rightarrow |Syl_q(G)| = p^2$.

Zähle die Elemente der Ordnung q.

Jedes $Q \in Syl_q(G)$ ist zyklisch der Ordnung q.

$\Rightarrow$ Jedes Element der Ordnung q liegt in einer eindeutigen q-Sylowgruppe.

$\Rightarrow$ (Anzahl der Elemente von G der Ordnung q)

$= |\mathrm{Syl}_q(G)| \cdot$ (Anzahl der Elemente der Ordnung q in einer q-Sylowgruppe)

$= p^2 \cdot (q-1)$.

$\Rightarrow$ (Anzahl der Elemente der Ordnung $\neq q$) $= p^2$.

Ordnung jeder p-Sylowgruppe P ist p^2.

$\Rightarrow P = \{g \in G \mid \mathrm{ord}(g) \neq q\} \lhd G$.

Widerspruch! $\underline{\text{qed.}}$

5.8.2 Satz: *(Burnside)* Jede Gruppe der Ordnung $p^a q^b$ für Primzahlen p, q ist auflösbar.
(ohne Beweis)

5.8.3 Lemma: Eine nichtabelsche einfache Gruppe besitzt keine Untergruppe vom Index 2, 3, oder 4.

Beweis: Sei $H < G$ mit $[G:H] =: n \in \{2,3,4\}$.
$\Rightarrow$ Linksoperation von G auf G/H transitiv.
$\Rightarrow$ Homo $G \xrightarrow{\varphi} S_n$; nichttrivial. $n \le 4 \Rightarrow S_n$ auflösbar!
$\Rightarrow$ Bild(φ) nichttrivial, auflösbar.

G einfach, φ nichttrivial
$\Rightarrow \mathrm{Ke}(\varphi) = 1$
$\Rightarrow G \cong \mathrm{Bild}(\varphi)$ ↯. qed

5.8.4 Proposition: Jede Gruppe der Ordnung < 60 ist auflösbar.

Beweis: $|G| = 1, p^i, pq, pqr, p^2q \Rightarrow$ fertig. Bleiben übrig: 24, 36, 40, 48, 54, 56.

Genügt zu zeigen: Es existiert keine nichtabelsche einfache Gruppe der Ordnung < 60.

Sei also G nichtabelsch einfach.

Für jeden Primteiler $p \,|\, |G|$ ist dann $|Syl_p(G)| > 4$
denn $|Syl_p(G)| = 1 \Rightarrow p$-Sylowgruppe normal ↯
$n = |Syl_p(G)| \in \{2,3,4\} \Rightarrow n = [G : N_G(P)]$ ↯ zu Lemma.

$|G| = 24 = 2^3 \cdot 3 \Rightarrow |Syl_2| \in \{1, 3\}$.

$|G| = 36 = 2^2 \cdot 3^2 \Rightarrow |Syl_3| \in \{1, 2, 4\}$

$|G| = 40 = 2^3 \cdot 5 \Rightarrow |Syl_5|$ teilt 2^3, $\equiv 1\ (5)$
$\Rightarrow |Syl_5| = 1$.

$|G| = 48 = 2^4 \cdot 3 \Rightarrow |Syl_2| \in \{1, 3\}$

$|G| = 54 = 2 \cdot 3^3 \Rightarrow |Syl_3| \in \{1, 2\}$

$|G| = 56 = 2^3 \cdot 7 \Rightarrow |Syl_7(G)|$ teilt 2^3, $\equiv 1$ mod 7
$\Rightarrow |Syl_7(G)| \in \{1, 8\}$ fertig. Sei jetzt $|Syl_7| = 8$.
Jede 7-Sylowgruppe ist zyklisch der Ordnung 7.
$\Rightarrow \#(\text{Elemente der Ordnung 7 in } G) = |Syl_7(G)| \cdot (7-1) = 8 \cdot 6$
$\Rightarrow \#(\text{ " \quad " } \neq 7) = 8 \cdot 7 - 8 \cdot 6 = 8 = |\text{2-Sylowgruppe}|$

$\Rightarrow \{g \in G \mid \mathrm{ord}(g) \neq 7\}$ ist eine 2-Sylowgruppe
$\Rightarrow |Syl_2(G)| = 1$
qed.

5.8.5 Lemma: Jede nichtabelsche einfache Gruppe mit einer Untergruppe vom Index 5 ist isomorph zur A_5.

Bew.: $H < G$, $[G:H]=5$ $\Rightarrow$ Operation von G auf G/H ergibt einen nichttrivialen Hom. $G \xrightarrow{\varphi} S_5$. Wieder ist dieser injektiv.

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & S_5 \\ & \searrow^{\text{trivial}} & \downarrow \text{sgn} \\ & & \{\pm 1\} \end{array}$$

$\Rightarrow G \xhookrightarrow{\varphi} A_5$. Wäre φ kein Iso, wäre $|G| < |A_5| = \frac{5!}{2} = \frac{120}{2} = 60$.

$\Rightarrow$ wäre G auflösbar! $\Rightarrow$ φ Iso. qed.

5.8.6 Proposition: Jede einfache Gruppe der Ordnung 60 ist isomorph zu A_5.