5.6.6 Beispiel: Es gibt genau 5 Isomorphieklassen von Gruppen der Ordnung p^3. Darunter sind die abelschen die Isomorphieklassen von

$$\mathbb{Z}/p^3\mathbb{Z} \quad \text{und} \quad \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \quad \text{und} \quad (\mathbb{Z}/p\mathbb{Z})^3.$$

Im Fall $p > 2$ sind die nichtabelschen die Isomorphieklassen der semidirekten Produkte

Operation der $(1+pa)(1+pa')$ $\equiv 1+p(a+a')$ mod p^2.

nicht abelsch.

$$\mathbb{Z}/p^2\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z} \quad \text{mit} \quad {}^a b := (1+pa)b \text{ für alle } a \in \mathbb{Z}/p\mathbb{Z} \text{ und } b \in \mathbb{Z}/p^2\mathbb{Z},$$
$$(\mathbb{Z}/p\mathbb{Z})^2 \rtimes \mathbb{Z}/p\mathbb{Z} \quad \text{mit} \quad {}^a(b,c) := (b+ac, c) \text{ für alle } a \in \mathbb{Z}/p\mathbb{Z} \text{ und } (b,c) \in (\mathbb{Z}/p\mathbb{Z})^2.$$

Im Fall $p = 2$ sind die nichtabelschen die Isomorphieklassen der Diedergruppe D_4 sowie der *Quaternionengruppe*

$$Q := \{\pm 1, \pm i, \pm j, \pm k\}$$

mit $i^2 = j^2 = k^2 = -1$ und $ij = k = -ji$ und $jk = i = -kj$ und $ki = j = -ik$.

5.6.7 Bemerkung: Die Quaternionengruppe ist kein semidirektes Produkt von echten Untergruppen.

$$\cong \left\{ \begin{pmatrix} 1 & b & c \\ 0 & 1 & a \\ 0 & 0 & 1 \end{pmatrix} \middle|\, a,b,c \in \mathbb{F}_p \right\}$$

Beh.: Jedes Element hat Ordnung 1 oder p.

Bew.: $g = 1 + n$ mit $n = \begin{pmatrix} 0 & b & c \\ 0 & 0 & a \\ 0 & 0 & 0 \end{pmatrix} \Rightarrow n^3 = 0$

$\Rightarrow g^p = 1 + p \cdot n + \binom{p}{2} \cdot n^2 = 1$

$p > 2 \Rightarrow \binom{p}{2} \equiv 0 \ (p)$ qed

Also sind die beiden Gruppen nicht isomorph.

Sei G nichtabelsch, $|G| = p^3$.

Falls $\exists g \in G$ mit $\operatorname{ord}(g) = p^2$, so $N = \langle g \rangle \lhd G$ da $\operatorname{Nor}_G(N) \supsetneq N$.
und $G/N \cong \mathbb{Z}_p$.

Sei $h \in G \setminus N$. Dann ist $h^p \in N$.

Wäre $\operatorname{ord}(h^p) = p^2$, ist $N = \langle h^p \rangle \Rightarrow G = \langle h \rangle$ zyklisch $\Rightarrow$ abelsch. ↯

Ist $\operatorname{ord}(h^p) = 1$, ist $G = N \rtimes \langle h \rangle$ mit $\langle h \rangle \xrightarrow{\text{nichttrivial}} \operatorname{Aut}(N) \cong (\mathbb{Z}/p^2\mathbb{Z})^\times \supseteq \{[1+pa] \mid a \in \mathbb{Z}\}$.

$\Rightarrow \sim$

$\Rightarrow G \cong \mathbb{Z}/p^2\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$ wie oben.

Sei also $\operatorname{ord}(h^p) = p$. Dann ist $\boxed{h^p = g^{pi}}$ für $i \in \mathbb{Z} \setminus p\mathbb{Z}$.

$\langle h \rangle \xrightarrow{\text{Homo}} \operatorname{Aut}(N) = (\mathbb{Z}/p^2\mathbb{Z})^\times$ nichttrivial $\Rightarrow$ möglich,

Ersetze h durch ein anderes Erzeuger von $\langle h \rangle$ $\Rightarrow$ $\boxed{{}^h g = g^{1+p}}$

Bel.: $\forall a, b \in \mathbb{Z}$: $(g^a h)^b = g^{ab + pa\binom{b}{2}} \cdot h^b$

Induktion über b.

Für $b = p$ folgt $(g^a h)^p = g^{ap + pa\binom{p}{2}} \cdot h^p = g^{ap} \cdot g^{pi} = g^{p(a+i)}$.

$pa\binom{p}{2}$ in $p^2\mathbb{Z}$

Für $a = -i$ ist also $(g^a h)^p = 1 \Rightarrow g^a h \in G \setminus N$ der Ordnung p.

Ersetzen h durch $g^a h$ $\to$ fertig.

Falls $\neg\exists g \in G$: $\operatorname{ord}(g) = p^2$, wähle $g \in G \setminus \{1\}$, dann ist $\operatorname{Nor}_G(\langle g \rangle) \supsetneq \langle g \rangle$. Wähle h $\Rightarrow |\langle g, h \rangle| = p^2$, $N := \langle g, h \rangle$ abelsch $\cong \mathbb{F}_p^2$.

Wähle $k \in G \setminus N$ $\Rightarrow \langle k \rangle \cong \mathbb{Z}_p$ und $G = N \rtimes \langle k \rangle$.

Rest analog.

qed.

5.7 Sylowsätze

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) falls G abelsch.: Schreibe $G \cong \mathbb{Z}_{e_1} \times \dots \times \mathbb{Z}_{e_r}$

Wegen $p \mid |G| = e_1 \cdots e_r$ existiert i mit $p \mid e_i$.

$\Rightarrow \mathbb{Z}_{e_i} \cong \mathbb{Z}/e_i\mathbb{Z} \ni \left[\frac{e_i}{p}\right]$ Element der Ordnung p.

Sei $g \in G$ entsprechend $\left(1, \dots, 1, \left[\frac{e_i}{p}\right], 1, \dots, 1\right) \Rightarrow \mathrm{ord}(g) = p$. qed.

Beweis von $|G|$ durch Induktion über $|G|$. Betrachte die Operation von G auf G durch Konjugation.

Es ist $\underbrace{G = Z(G)}_{\text{Bahnen der Länge 1.}} \,\dot\cup\, (\text{Vereinigung von Bahnen der Länge} > 1.)$

Ist $p \mid |Z(G)|$, wähle $g \in Z(G)$ der Ordnung p. Dann ist $\langle g \rangle =: N \trianglelefteq G$.
mit $|G/N| = p^{k-1} m$. Ist $k = 1$, so ist $N \in Syl_p(G)$.

Ist $k > 1$, so besitzt G/N eine p-Sylowuntergruppe S/N für ein $S < G$ mit $N \trianglelefteq S$.

Also ist $|S/N| = p^{k-1} \Rightarrow |S| = p^{k-1} \cdot p = p^k \Rightarrow S \in Syl_p(G)$.

Ist $p \nmid |Z(G)|$, beachte $p \mid |G|$. Obige Zerlegung $\Rightarrow \exists$ Bahn der Länge $n > 1$, $p \nmid n$.

Sei g in dieser Bahn $\Rightarrow n = [G : Stab_G(g)] \Rightarrow |Stab_G(g)| = p^k \cdot m'$ mit $m' = \frac{m}{n} < m$.

Nach IV besitzt $Stab_G(g)$ eine p-Sylowgruppe S, d.h. mit $|S| = p^k \Rightarrow S \in Syl_p(G)$.

qed