KAPITEL 6

Sylowuntergruppen

1. Die Sylowsätze

Wir wiederholen nochmals die Definition von Sylowgruppen:

DEFINITION. *Ist G eine endliche Gruppe und p ein Primteiler der Gruppenordnung $|G|$, zerlegt man*

$$|G| = p^\ell m \quad \textit{mit} \quad p \nmid m,$$

so heißt eine Untergruppe P eine p**-Sylowgruppe** *(oder* p**-Sylowuntergruppe***) von G, falls*

$$|P| = p^\ell$$

gilt.

Die Aussagen des folgenden Satzes werden oft auch als **Sylowsätze**[1] bezeichnet.

SATZ (Sylowsätze). *Sei G eine endliche Gruppe und p ein Primteiler von $|G|$. Wir zerlegen $|G| = p^\ell m$ mit $p \nmid m$. Sei s_p die Anzahl der p-Sylowuntergruppen von G.*

(1) *Es gilt*
$$s_p \equiv 1 \bmod p \quad \textit{und} \quad s_p \mid m.$$
(2) *Alle p-Sylowuntergruppen sind konjugiert.*
(3) *Eine p-Sylowuntergruppe P ist genau dann ein Normalteiler in G, wenn P die einzige p-Sylowuntergruppe von G ist, d.h. wenn gilt $s_p = 1$.*
(4) *Ist H eine p-Untergruppe von G, so gibt es eine p-Sylowuntergruppe P mit $H \subseteq P$. (Jede p-Untergruppe von G ist in einer p-Sylowuntergruppe enthalten.)*

Beispiele:

(1) In der symmetrischen Gruppe S_3 mit $6 = 2 \cdot 3$ Elementen
   - sind $\langle(12)\rangle = \{(1), (12)\}$, $\langle(13)\rangle = \{(1), (13)\}$, $\langle(23)\rangle = \{(1), (23)\}$ die 2-Sylowgruppen,
   - ist $\langle(123)\rangle = \{(1), (123), (132)\}$ die einzige 3-Sylowgruppe.

   Hier ist also $s_2 = 3$ und $s_3 = 1$.
(2) In der alternierenden Gruppe A_4 mit $12 = 2^2 \cdot 3$ Elementen
   - ist $V_4 = \{(1), (12)(34), (13)(24), (14)(23)\}$ die einzige 2-Sylowgruppe,
   - sind $\langle(123)\rangle$, $\langle(124)\rangle$, $\langle(134)\rangle$, $\langle(234)\rangle$ die 3-Sylowuntergruppen.

   Hier ist also $s_2 = 1$ und $s_3 = 4$.

2. Beweis der Sylowsätze

Vorbemerkungen:

(1) In diesem Abschnitt werden die Sylowsätze bewiesen. Um die Aussagen anzuwenden, muss man die Beweise nicht kennen.
(2) Wir haben im letzten Kapitel bereits gezeigt, dass es zu jedem Primteiler p der Gruppenordnung $|G|$ mindestens eine p-Sylowgruppe gibt.
(3) Wir beweisen die Sylowsätze, indem wir Gruppen geeignet auf Mengen operieren lassen.

Datei: alg_sylow.tex. Version vom 18.12.2023

[1] Die „Sylowsätze“ gehen auf die Arbeit *Théorèmes sur les groupes de substitutions“ (Mathematische Annalen* **5** *(1872), 584-594)* von M. L. Sylow zurück.

LEMMA (A). *Sei G eine endliche Gruppe, P eine p-Sylowuntergruppe von G und H eine p-Untergruppe von G. Dann ist H in einer zu P konjugierten Untergruppe enthalten, d.h. es gibt ein $a \in G$ mit*

$$H \subseteq aPa^{-1}.$$

Beweis:

- $|G| = p^\ell m$ mit $\ell \geq 1$ und $p \nmid m$. Dann gilt
$$|P| = p^\ell \quad \text{und} \quad |H| = p^k \text{ für ein } k \in \{1, \dots, \ell\}.$$
- Wir betrachten die Linksnebenklassen von P in G:
$$G/P = \{aP : a \in G\} \quad \text{mit} \quad |G/P| = [G : P] = m.$$
Wir lassen H auf G/P durch Linksmultiplikation operieren:
$$H \times G/P \to G/P, \quad (h, aP) \mapsto haP.$$
Unter dieser Operation zerfällt G/P in H-Bahnen. Sei $a_1P, \dots, a_rP$ ein Repräsentantensystem der Bahnen. Die i-te Bahn ist $\{ha_iP : h \in H\}$. Sei $H_i \subseteq H$ die Fixgruppe von a_iP, d.h. $H_i = \{h \in H : ha_iP = a_iP\}$. Dann gilt:
$$|H| = |H_i| \cdot |\{ha_iP : h \in H\}|.$$
Wegen $|H| = p^k$ folgt für die Bahnlängen
$$|\{ha_iP : h \in H\}| \in \{1, p, p^2, p^3, \dots\}.$$
- G/P zerfällt in H-Bahnen, also
$$G/P = \{aP : a \in G\} = \bigcup_{i=1}^{r} \{ha_iP : h \in H\} \quad \text{und} \quad m = |G/P| = \sum_{i=1}^{r} |\{ha_iP : h \in H\}|.$$
Da $|G/P| = m$ teilerfremd zu p ist, können nicht alle Bahnlängen durch p teilbar sein, es gibt also mindestens eine Bahn der Länge 1.
- Sei i ein Index mit $|\{ha_iP : h \in H\}| = 1$. Dann gilt
$$ha_iP = a_iP \text{ für alle } h \in H,$$
und wegen $e \in P$
$$ha_i \in a_iP, \quad \text{also} \quad h \in a_iPa_i^{-1} \text{ für alle } h \in H,$$
und damit
$$H \subseteq a_iPa_i^{-1}.$$
Dies ist die Aussage, die wir beweisen wollten. ■

Bemerkungen:

(1) Aus dem Lemma folgt direkt Teil (4) der Sylowsätze: Ist H eine p-Untergruppe von G, gibt es ein ein a mit $H \subseteq aPa^{-1}$. Da aber mit P auch aPa^{-1} eine p-Sylowuntergruppe ist, folgt die Aussage.
(2) Aus dem Lemma folgt direkt Teil (2) der Sylowsätze: Ist P' irgendeine p-Sylowuntergruppe von G, so gibt es ein a mit $P' \subseteq aPa^{-1}$. Da aber P' und aPa^{-1} gleichmächtig sind, folgt schon $P' = aPa^{-1}$, d.h. P' und P sind konjugiert.
(3) Teil (3) der Sylowsätze folgt sofort aus Teil (2) der Sylowsätze.

Lässt man eine Gruppe G auf Teilmengen von G durch Konjugation operieren, so tritt als Fixgruppe eine Untergruppe auf, die als Normalisator bezeichnet wird:

DEFINITION. *Ist G eine Gruppe und $H \subseteq G$ eine Untergruppe, so heißt*

$$\mathrm{N}_G(H) = \{g \in G : gHg^{-1} = H\}$$

der **Normalisator von H in G.**

Bemerkungen: Sei H Untergruppe einer Gruppe G.

(1) Der Normalisator $\mathrm{N}_G(H)$ ist eine Untergruppe, die H enthält.
(2) H ist ein Normalteiler der Gruppe $\mathrm{N}_G(H)$.
(3) Genau dann ist H ein Normalteiler in G, wenn $\mathrm{N}_G(H) = G$ gilt.

LEMMA (B). *Sei G eine endliche Gruppe und p ein Primteiler der Gruppenordnung. Sei $\mathcal{P}$ die Menge der p-Sylowuntergruppen von G.*

(1) *G operiert durch Konjugation auf $\mathcal{P}$ transitiv:*
$$G \times \mathcal{P} \to \mathcal{P}, \quad (g, P) \mapsto gPg^{-1}.$$
(2) *Die Fixgruppe von $P \in \mathcal{P}$ ist $\mathrm{N}_G(P)$.*
(3) *Es gilt*
$$|\mathcal{P}| = \frac{|G|}{|\mathrm{N}_G(P)|}.$$
(4) *Zerlegt man $|G| = p^\ell m$ mit $p \nmid m$, so gilt*
$$|\mathcal{P}| \mid m.$$

Beweis:

(1) Da mit P auch gPg^{-1} eine p-Sylowuntergruppe ist, wird durch
$$G \times \mathcal{P} \to \mathcal{P}, \quad (g, P) \mapsto gPg^{-1}$$
eine Operation definiert. Sind P, P' zwei p-Sylowuntergruppen von G, so folgt aus Lemma (A) die Inklusion $P' \subseteq aPa^{-1}$, die aus Mächtigkeitsgründen zu $P' = aPa^{-1}$ wird. Daher ist die Operation transitiv, $\mathcal{P}$ besteht aus einer G-Bahn.
(2) Sei $P \in \mathcal{P}$. Dann ist $\mathcal{P} = \{gPg^{-1} : g \in G\}$. Die Fixgruppe von P ist
$$\{g \in G : gPg^{-1} = P\} = \mathrm{N}_G(P),$$
also der Normalisator von P in G.
(3) Die Bahngleichung für P liefert
$$|G| = |\{g \in G : gPg^{-1} = P\}| \cdot |\{gPg^{-1} : g \in G\}|,$$
also
$$|G| = |\mathcal{P}| \cdot |\mathrm{N}_G(P)|,$$
da es nur eine Bahn gibt.
(4) Es ist $|P| = p^\ell$. Aus $P \subseteq \mathrm{N}_G(P)$ folgt dann $|\mathrm{N}_G(P) = p^\ell n$ mit $n \in \mathbb{N}$. Aus (3) ergibt sich
$$|\mathcal{P}| = \frac{p^\ell m}{p^\ell n} = \frac{m}{n}, \quad \text{und damit} \quad |\mathcal{P}| \mid m,$$
wie behauptet. ■

Bemerkung: Teil (4) von Lemma (B) zeigt den zweiten Teil der Aussage (1) der Sylowsätze.

LEMMA (C). *Seien P und Q zwei p-Sylowgruppen einer endlichen Gruppe G, sodass gilt*
$$P \subseteq \mathrm{N}_G(Q), \quad \textit{also} \quad gQg^{-1} = Q \textit{ für alle } g \in P.$$
Dann gilt
$$P = Q.$$

Beweis: Sei $|P| = |Q| = p^\ell$.

- Wir betrachten
$$PQ = \{xy : x \in P, y \in Q\}.$$
Für $x_i \in P$ und $y_i \in Q$ gilt
$$(x_1y_1)(x_2y_2) = x_1x_2x_2^{-1}y_1x_2y_2 = (x_1x_2) \cdot ((x_2^{-1}y_1x_2)y_2) \in PQ \text{ wegen } x_2^{-1}y_1x_2 \in Q.$$
Da G endlich ist, folgt daraus bereits, dass PQ eine Untergruppe von Q ist. Da p^ℓ die größte p-Potenz ist, die in $|G|$ aufgeht, folgt aus $P \subseteq PQ \subseteq G$
$$|PQ| = p^\ell n \text{ mit } p \nmid n.$$
- Mit $x \in P$, $y \in Q$ sieht man aus
$$(xy)Q(xy)^{-1} = xyQy^{-1}x^{-1} = x(yQy^{-1})x^{-1} = xQx^{-1} = Q,$$
dass Q ein Normalteiler in PQ ist. Die Faktorgruppe PQ/Q hat Ordnung
$$|PQ/Q| = \frac{|PQ|}{|P|} = n.$$
Da wegen $P \subseteq PQ$ folgt dann:
$$x \in P \quad \Longrightarrow \quad x^n \in Q.$$
- Sei nun $x \in P$ ein beliebiges Element. Mit $|P| = p^\ell$ folgt
$$x^{p^\ell} = e.$$
Wegen $\mathrm{ggT}(p^\ell, n) = 1$ finden wir mit dem erweiterten euklidischen Algorithmus $u, v \in \mathbb{Z}$ mit
$$1 = u \cdot p^\ell + v \cdot n.$$
Damit folgt
$$x = x^{u \cdot p^\ell + v \cdot n} = \left(x^{p^\ell}\right)^u \cdot (x^n)^v = (x^n)^v \in Q.$$
Also gilt $P \subseteq Q$. Da aber P und Q gleiche Ordnung haben, ergibt sich
$$P = Q,$$
wie behauptet. ■

LEMMA (D). *Sei G eine endliche Gruppe, p ein Primteiler von $|G|$, $\mathcal{P}$ die Menge der p-Sylowuntergruppen von G und $P \in \mathcal{P}$.*

(1) *P operiert auf $\mathcal{P}$ durch Konjugation:*
$$P \times \mathcal{P} \to \mathcal{P}, \quad (g, Q) \mapsto gQg^{-1}.$$
Ist $P_1, \dots, P_r$ ein Repräsentantensystem der Bahnen und o.E. $P_1 = P$, so gilt für die Bahnlängen:
$$|\{gPg^{-1} : g \in P\}| = 1 \quad \text{und} \quad p \mid |\{gP_ig^{-1} : g \in P\}| \text{ für } i = 2, \dots, r.$$

(2) *Es gilt*
$$|\mathcal{P}| \equiv 1 \bmod p.$$

Beweis:

(1)
- Wir haben die Zerlegung in Bahnen:
$$\mathcal{P} = \bigcup_{i=1}^{r} \{gP_ig^{-1} : g \in P\}$$
und
$$|\mathcal{P}| = \sum_{i=1}^{r} |\{gP_ig^{-1} : g \in P\}|.$$
Die Bahnlängen sind Teiler der Gruppenordnung $|P| = p^\ell$, also
$$|\{gP_ig^{-1} : g \in P\}| \in \{1, p, p^2, p^3, \dots\}.$$

- Wann ist die Bahnlänge 1? Es gilt:

$$\begin{aligned} |\{gP_ig^{-1} : g \in P\}| = 1 \quad &\Longleftrightarrow \quad \{gP_ig^{-1} : g \in P\} = \{P_i\} \quad \Longleftrightarrow \\ &\Longleftrightarrow \quad gP_ig^{-1} = P_i \text{ für alle } g \in P \quad \Longleftrightarrow \\ &\overset{\text{Lemma (C)}}{\Longleftrightarrow} \quad P_i = P_1. \end{aligned}$$

  Daher folgt

$$|\{gPg^{-1} : g \in P\}| = 1 \quad \text{und} \quad p \mid |\{gP_ig^{-1} : g \in P\}| \text{ für } i = 2, \ldots, r.$$

(2) Aus

$$|\mathcal{P}| = |\{gPg^{-1} : g \in P\}| + \sum_{i=2}^{r} |\{gP_ig^{-1} : g \in P_1\}| = 1 + \sum_{i=2}^{r} |\{gP_ig^{-1} : g \in P\}|$$

folgt mit (1)

$$|\mathcal{P}| = 1 + p \cdot k \text{ mit einer Zahl } k \in \mathbb{N}_0,$$

und damit

$$|\mathcal{P}| \equiv 1 \bmod p,$$

wie behauptet. ■

Bemerkung: Aussage (2) in Lemma (D) liefert den ersten Teil der Aussage (1) in den Sylowsätzen.

3. Anwendungen der Sylowsätze

Beispiel: Ist G eine zyklische Gruppe, so gibt es zu jedem Teiler der Gruppenordnung genau eine Untergruppe dieser Ordnung. Daher gibt es für jeden Primteiler p der Gruppenordnung genau eine p-Sylowgruppe, d.h. $s_p = 1$.

Beispiel: Ist G eine p-Gruppe, so ist natürlich G selbst die einzige p-Sylowuntergruppe von G. Die Sylowsätze bringen hier nichts.

Beispiel: Sei D_p eine Diedergruppe der Ordnung $2p$, wobei $p \geq 3$ eine Primzahl ist. Dann gilt für die Anzahl der Sylowgruppen

$$s_2 \equiv 1 \bmod 2, \quad s_2 \mid p \quad \text{und} \quad s_p \equiv 1 \bmod p, \quad s_p \mid 2.$$

Daraus ergibt sich zunächst

$$s_2 \in \{1, p\} \quad \text{und} \quad s_p = 1.$$

Wir kennen aber die Sylowuntergruppen bereits: Schreibt man $D_p = \langle \delta, \sigma \rangle$ mit $\operatorname{ord}(\delta) = p$, $\operatorname{ord}(\sigma) = 2$ und $\sigma\delta\sigma^{-1} = \delta^{-1}$, so ist

$$\langle \delta \rangle$$

die (einzige) p-Sylowuntergruppe, die auch ein Normalteiler ist, und

$$\langle \sigma \rangle, \quad \langle \delta\sigma \rangle, \quad \langle \delta^2\sigma \rangle, \quad \ldots \langle \delta^{p-1}\sigma \rangle$$

sind die p 2-Sylowuntergruppen von D_p.

Bemerkung: Kennt man die Gruppenordnung $|G|$, betrachtet man einen Primteiler p der Gruppenordnung, so erhält man aus der Zerlegung $|G| = p^\ell m$ für die Anzahl s_p der p-Sylowuntergruppen

$$s_p \equiv 1 \bmod p \quad \text{und} \quad s_p \mid m.$$

Damit kann man leicht alle Möglichkeiten für s_p bestimmen. In der folgenden Tabelle finden sich alle Möglichkeiten für die Gruppenordnung zwischen 2 und 50:

$\lvert G\rvert$	Faktorisierung von $\lvert G\rvert$	Möglichkeiten für s_p für $p \mid \lvert G\rvert$
2	2	$s_2 = 1$
3	3	$s_3 = 1$
4	2^2	$s_2 = 1$
5	5	$s_5 = 1$
6	$2 \cdot 3$	$s_2 \in \{1, 3\}$, $s_3 = 1$
7	7	$s_7 = 1$
8	2^3	$s_2 = 1$
9	3^2	$s_3 = 1$
10	$2 \cdot 5$	$s_2 \in \{1, 5\}$, $s_5 = 1$
11	11	$s_{11} = 1$
12	$2^2 \cdot 3$	$s_2 \in \{1, 3\}$, $s_3 \in \{1, 4\}$
13	13	$s_{13} = 1$
14	$2 \cdot 7$	$s_2 \in \{1, 7\}$, $s_7 = 1$
15	$3 \cdot 5$	$s_3 = 1$, $s_5 = 1$
16	2^4	$s_2 = 1$
17	17	$s_{17} = 1$
18	$2 \cdot 3^2$	$s_2 \in \{1, 3, 9\}$, $s_3 = 1$
19	19	$s_{19} = 1$
20	$2^2 \cdot 5$	$s_2 \in \{1, 5\}$, $s_5 = 1$
21	$3 \cdot 7$	$s_3 \in \{1, 7\}$, $s_7 = 1$
22	$2 \cdot 11$	$s_2 \in \{1, 11\}$, $s_{11} = 1$
23	23	$s_{23} = 1$
24	$2^3 \cdot 3$	$s_2 \in \{1, 3\}$, $s_3 \in \{1, 4\}$
25	5^2	$s_5 = 1$
26	$2 \cdot 13$	$s_2 \in \{1, 13\}$, $s_{13} = 1$
27	3^3	$s_3 = 1$
28	$2^2 \cdot 7$	$s_2 \in \{1, 7\}$, $s_7 = 1$
29	29	$s_{29} = 1$
30	$2 \cdot 3 \cdot 5$	$s_2 \in \{1, 3, 5, 15\}$, $s_3 \in \{1, 10\}$, $s_5 \in \{1, 6\}$
31	31	$s_{31} = 1$
32	2^5	$s_2 = 1$
33	$3 \cdot 11$	$s_3 = 1$, $s_{11} = 1$
34	$2 \cdot 17$	$s_2 \in \{1, 17\}$, $s_{17} = 1$
35	$5 \cdot 7$	$s_5 = 1$, $s_7 = 1$
36	$2^2 \cdot 3^2$	$s_2 \in \{1, 3, 9\}$, $s_3 \in \{1, 4\}$
37	37	$s_{37} = 1$
38	$2 \cdot 19$	$s_2 \in \{1, 19\}$, $s_{19} = 1$
39	$3 \cdot 13$	$s_3 \in \{1, 13\}$, $s_{13} = 1$
40	$2^3 \cdot 5$	$s_2 \in \{1, 5\}$, $s_5 = 1$
41	41	$s_{41} = 1$
42	$2 \cdot 3 \cdot 7$	$s_2 \in \{1, 3, 7, 21\}$, $s_3 \in \{1, 7\}$, $s_7 = 1$
43	43	$s_{43} = 1$
44	$2^2 \cdot 11$	$s_2 \in \{1, 11\}$, $s_{11} = 1$
45	$3^2 \cdot 5$	$s_3 = 1$, $s_5 = 1$
46	$2 \cdot 23$	$s_2 \in \{1, 23\}$, $s_{23} = 1$
47	47	$s_{47} = 1$
48	$2^4 \cdot 3$	$s_2 \in \{1, 3\}$, $s_3 \in \{1, 4, 16\}$
49	7^2	$s_7 = 1$
50	$2 \cdot 5^2$	$s_2 \in \{1, 5, 25\}$, $s_5 = 1$

Bemerkung: Wir haben schon gezeigt:

- Ist die Gruppenordnung eine Primzahl p, so ist die Gruppe isomorph zu $\mathbb{Z}_p$.
- Ist die Gruppenordnung das Quadrat einer Primzahl, also p^2, so ist die Gruppe isomorph zu $\mathbb{Z}_{p^2}$ oder $\mathbb{Z}_p \times \mathbb{Z}_p$.
- Ist die Gruppenordnung von der Form $2p$ mit einer Primzahl $p \geq 3$, so ist die Gruppe isomorph zu $\mathbb{Z}_{2p}$ oder D_p (Diedergruppe der Ordnung $2p$).

Dies haben wir in folgende Liste eingetragen für Gruppenordnung zwischen 2 und 20.

$\lvert G\rvert$	$\lvert G\rvert$	s_p für $p \mid \lvert G\rvert$	Gruppen
2	2	$s_2 = 1$	$\mathbb{Z}_2$
3	3	$s_3 = 1$	$\mathbb{Z}_3$
4	2^2	$s_2 = 1$	$\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2$
5	5	$s_5 = 1$	$\mathbb{Z}_5$
6	$2 \cdot 3$	$s_2 \in \{1,3\}$, $s_3 = 1$	$\mathbb{Z}_6$, D_3
7	7	$s_7 = 1$	$\mathbb{Z}_7$
8	2^3	$s_2 = 1$	
9	3^2	$s_3 = 1$	$\mathbb{Z}_9$, $\mathbb{Z}_3 \times \mathbb{Z}_3$
10	$2 \cdot 5$	$s_2 \in \{1,5\}$, $s_5 = 1$	$\mathbb{Z}_{10}$, D_5
11	11	$s_{11} = 1$	$\mathbb{Z}_{11}$
12	$2^2 \cdot 3$	$s_2 \in \{1,3\}$, $s_3 \in \{1,4\}$	
13	13	$s_{13} = 1$	$\mathbb{Z}_{13}$
14	$2 \cdot 7$	$s_2 \in \{1,7\}$, $s_7 = 1$	$\mathbb{Z}_{14}$, D_7
15	$3 \cdot 5$	$s_3 = 1$, $s_5 = 1$	
16	2^4	$s_2 = 1$	
17	17	$s_{17} = 1$ $\mathbb{Z}_{17}$	$\mathbb{Z}_{17}$
18	$2 \cdot 3^2$	$s_2 \in \{1,3,9\}$, $s_3 = 1$	
19	19	$s_{19} = 1$	$\mathbb{Z}_{19}$
20	$2^2 \cdot 5$	$s_2 \in \{1,5\}$, $s_5 = 1$	

Das folgende Lemma ist hilfreich bei der Klassifikation von Gruppen.

LEMMA. *Sei G eine endliche Gruppe und seien $N_1, \ldots, N_r$ Normalteiler in G mit paarweise teilerfremden Ordnungen, d.h.* $\mathrm{ggT}(|N_i|, |N_j|) = 1$ *für $i \neq j$. Dann gilt:*

(1) *Für $i \neq j$ gilt $N_i \cap N_j = \{e\}$ und*
$$n_i n_j = n_j n_i \text{ für alle } n_i \in N_i, n_j \in N_j.$$
(2) $N_1 \ldots N_r = \{n_1 \ldots n_r : n_1 \in N_1, \ldots, n_r \in N_r\}$ *ist eine Untergruppe von G. ($N_1 \ldots N_r$ ist sogar ein Normalteiler in G.)*
(3) *Die Abbildung*
$$\phi : N_1 \times \cdots \times N_r \to N_1 \ldots N_r, \quad (n_1, \ldots, n_r) \mapsto n_1 \ldots n_r$$
ist ein Gruppenisomorphismus.
(4) *Gilt $|G| = |N_1| \ldots |N_r|$, so ist G isomorph zum Produkt $N_1 \times \cdots \times N_r$, also*
$$G \simeq N_1 \times \cdots \times N_r.$$

Beweis:

(1)
- Wir zeigen zunächst $N_i \cap N_j = \{e\}$. Ist $n \in N_i \cap N_j$ mit $i \neq j$, so gilt $\mathrm{ord}\,(n) \mid |N_i|$ und $\mathrm{ord}\,(n) \mid |N_j|$, damit $\mathrm{ord}\,(n) \mid \mathrm{ggT}(|N_i|, |N_j|)$, also $\mathrm{ord}\,(n) = 1$ und damit $n = e$ folgt.
- Für $i \neq j$ und $n_i \in N_i$, $n_j \in N_j$ gilt wegen der Normalteilereigenschaft
$$n_i n_j n_i^{-1} n_j^{-1} = n_i (n_j n_i^{-1} n_j^{-1}) \in N_i \quad \text{und} \quad n_i n_j n_i^{-1} n_j^{-1} = (n_i n_j n_i^{-1}) n_j \in N_j,$$
also
$$n_i n_j n_i^{-1} n_j^{-1} \in N_i \cap N_j = \{e\}, \quad \text{und damit} \quad n_i n_j n_i^{-1} n_j^{-1} = e,$$

also

$$n_i n_j = n_j n_i.$$

(2) Wir überprüfen die Untergruppeneigenschaften:
- Für $n_1, n_1' \in N_1, \ldots, n_r, n_r' \in N_r$ erhält man durch wiederholte Anwendung von (1)
$$(n_1 \ldots n_r)(n_1' \ldots n_r') = (n_1 n_1') \ldots (n_r n_r') \in N_1 \ldots N_r.$$
- Für $n_1 \in N_1, \ldots, n_r \in N_r$ erhält man durch wiederholte Anwendung von (1)
$$(n_1 \ldots n_r)^{-1} = n_r^{-1} \ldots n_1^{-1} = n_1^{-1} \ldots n_r^{-1} \in N_1 \ldots N_r.$$
- Natürlich gilt $e \in N_1 \ldots N_r$.

Damit ist $N_1 \ldots N_r$ eine Untergruppe. Dass $N_1 \ldots N_r$ ein Normalteiler ist, sieht man aus

$$g(n_1 \ldots n_r)g^{-1} = (gn_1g^{-1}) \ldots (gn_rg^{-1}) \in N_1 \ldots N_r.$$

(3)
- Es gilt für $n_1, n_1' \in N_1, \ldots, n_r, n_r' \in N_r$ durch wiederholte Anwendung von (1)
$$\begin{aligned} \phi((n_1, \ldots, n_r) \cdot (n_1', \ldots, n_r')) &= \phi((n_1 n_1', \ldots, n_r n_r')) = (n_1 n_1') \ldots (n_r n_r') = \\ &= (n_1 \ldots n_r)(n_1' \ldots n_r') = \\ &= \phi((n_1, \ldots, n_r))\phi((n_1', \ldots, n_r')). \end{aligned}$$
Also ist ϕ ein Homomorphismus.
- Da die Elemente aus N_i und N_j für $i \neq j$ vertauschbar sind, sieht man, dass für $d \in \mathbb{N}$
$$(n_1 n_2 \ldots n_r)^d = n_1^d n_2^d \ldots n_r^d$$
gilt. Ist $n_1 \ldots n_r \in \mathrm{Kern}(\phi)$ und $d = |N_2| \ldots |N_r|$, so folgt aus
$$n_1 \ldots n_r = e$$
$$n_1^d = e.$$
Mit $\mathrm{ggT}(|N_1|, d) = 1$ folgt $n_1 = e$. So macht man weiter und erhält schließlich, dass der Kern trivial ist. Also ist ϕ injektiv. Da ϕ nach Konstruktion surjektiv ist, ist ϕ ein Isomorphismus.

(4) Dies ist klar. ■

Damit erhalten wir folgenden Satz:

SATZ. *Ist G eine endliche Gruppe mit Gruppenordnung $|G| = p_1^{e_1} \ldots p_r^{e_r}$ und gibt es für jeden Primteiler p_i genau eine p-Sylowgruppe P_{p_i}, d.h. $s_{p_i} = 1$, so ist G isomorph zum direkten Produkt seiner Sylowgruppen:*

$$G \simeq P_{p_1} \times \cdots \times P_{p_r}.$$

Beweis: Da es nur eine p_i-Sylowgruppe P_{p_i} gibt, ist diese ein Normalteiler. Wir können also das vorangegangene Lemma anwenden. Wegen $|G| = p_1^{e_1} \ldots p_r^{e_r} = |P_{p_1}| \ldots |P_{p_r}|$ folgt dann sofort

$$G \simeq P_{p_1} \times \cdots \times P_{p_r},$$

wie behauptet. ■

Beispiel: Ist G eine Gruppe der Ordnung 15, so gilt nach unserer Tabelle $s_3 = 1$ und $s_5 = 1$, es ist also

$$G \simeq P_3 \times P_5.$$

Wegen $|P_3| = 3$ und $|P_5| = 5$ sind die Sylowgruppen aber zyklische Gruppen, sodass wir erhalten

$$G \simeq P_3 \times P_5 \simeq \mathbb{Z}_3 \times \mathbb{Z}_5 \simeq \mathbb{Z}_{15}.$$

Jede Gruppe der Ordnung 15 ist also zyklisch.

4. Abelsche p-Gruppen

In einer abelschen Gruppe sind alle Untergruppen Normalteiler. Daher ist eine endliche abelsche Gruppe A isomorph zum Produkt ihrer Sylowuntergruppen: Ist $|A| = p_1^{e_1} \dots p_r^{e_r}$, so gibt es Untergruppen P_{p_i} mit $|P_{p_i}| = p_i^{e_i}$ und

$$A \simeq P_{p_1} \times \cdots \times P_{p_r}.$$

Wir müssen daher untersuchen, wie abelsche p-Gruppen aussehen. Im Folgenden schreiben wir die Verknüpfung bei abelschen Gruppen als Addition und das neutrale Element als 0.

Satz. *Jede abelsche p-Gruppe A ist isomorph zu einem Produkt*

$$\mathbb{Z}_{p^{e_1}} \times \mathbb{Z}_{p^{e_2}} \times \cdots \times \mathbb{Z}_{p^{e_n}}$$

zyklischer Gruppen mit $e_1 \geq e_2 \geq \cdots \geq e_n \geq 1$. Das n-Tupel $(e_1, \dots, e_n)$ ist durch A eindeutig bestimmt.

Lemma. *Sei A eine abelsche p-Gruppe und $a \in A$ ein Element maximaler Ordnung p^e, d.h.* $\operatorname{ord}(a) = p^e$ *und* $\operatorname{ord}(x) \mid p^e$ *für alle $x \in A$. Weiter werde vorausgesetzt, dass alle Elemente der Ordnung p schon in $\langle a \rangle$ enthalten sind, d.h.*

$$x \in A \text{ mit } \operatorname{ord}(x) = p \quad \Longrightarrow \quad x \in \langle a \rangle.$$

Dann gilt schon

$$A = \langle a \rangle.$$

Beweis: Wir zeigen durch Induktion nach i (für $0 \leq i \leq e$), dass alle Elemente $x \in A$ mit $\operatorname{ord}(x) = p^i$ in $\langle a \rangle$ enthalten sind.

- Ist $\operatorname{ord}(x) = 1$, so ist $x = 0 \in A$.
- Ist $\operatorname{ord}(x) = p$, so ist $x \in A$ nach Voraussetzung.
- Sei nun $\operatorname{ord}(x) = p^i$ mit $i \geq 2$ und die Aussage bereits für alle Elemente kleinerer Ordnung gezeigt. Es gilt
$$\operatorname{ord}(px) = p^{i-1}.$$
Nach Induktionsvoraussetzung existiert ein $j \in \mathbb{Z}$ mit $px = ja$. Multiplikation mit p^{i-1} liefert
$$0 = p^i x = p^{i-1}(px) = p^{i-1}(ja), \quad \text{also} \quad \operatorname{ord}(a) \mid p^{i-1}j, \text{ d.h. } p^e \mid p^{i-1}j.$$
Wegen $i \leq e$ gilt $p \mid j$, wir können also schreiben $j = pk$ mit $k \in \mathbb{Z}$. Dann ist $px = ja = pka$, also
$$p(x - ka) = 0.$$
Wegen $\operatorname{ord}(x - ka) \in \{1, p\}$ gilt $x - ka \in \langle a \rangle$, d.h. es gibt ein $l \in \mathbb{Z}$ mit $x - ka = la$, und damit
$$x = ka + la = (k + l)a \in \langle a \rangle.$$
Damit ist die Behauptung durch Induktion bewiesen. ■

Lemma. *Sei A eine abelsche p-Gruppe und $a \in A$ ein Element maximaler Ordnung p^e, d.h.* $\operatorname{ord}(a) = p^e$ *und* $\operatorname{ord}(x) \mid p^e$ *für alle $x \in A$. Dann existiert eine Untergruppe B von A mit*

$$A = \langle a \rangle + B \quad \text{und} \quad \langle a \rangle \cap B = \{0\},$$

was insbesondere

$$A \simeq \langle a \rangle \times B$$

zeigt.

Beweis: Wir beweisen die Aussage durch Induktion nach $\frac{|A|}{p^e}$. Im Fall $\frac{|A|}{p^e} = 1$ gilt $A = \langle a \rangle$, die Aussage ist also richtig mit $B = \{0\}$. Sei nun $\frac{|A|}{p^e} > 1$.

- Nach dem vorangegangenen Lemma gibt es ein $c \in A$ mit
$$\operatorname{ord}(c) = p \quad \text{und} \quad c \notin \langle a \rangle,$$
da andernfalls schon $A = \langle a \rangle$ folgen würde. Wegen $\operatorname{ord}(c) = p$ gilt dann auch
$$\langle a \rangle \cap \langle c \rangle = \{0\}.$$

- Wir betrachten die Faktorgruppe $\overline{A} = A/\langle c\rangle$ mit der kanonischen Abbildung $\pi : A \to \overline{A}$.
- Wir zeigen, dass $\operatorname{ord}(\overline{a}) = p^e$ gilt. Natürlich gilt $p^e \cdot \overline{a} = \overline{0}$. Wäre $\operatorname{ord}(\overline{a}) < p^e$, so würde
$$p^{e-1} \cdot \overline{a} = \overline{0}$$
gelten, also
$$p^{e-1} \cdot a \equiv 0 \bmod \langle c\rangle, \quad \text{und damit} \quad p^{e-1} \cdot a \in \langle c\rangle.$$
Dies widerspricht wegen $p^{e-1} \cdot a \neq 0$ der Aussage $\langle a\rangle \cap \langle c\rangle = \{0\}$.
- Wegen $|\overline{A}| = |A/\langle c\rangle| = \frac{|A|}{p}$ und $\operatorname{ord}(\overline{a}) = p^e$ können wir die Induktionsvoraussetzung auf $\overline{A}$ und $\overline{a}$ anwenden. Wir finden eine Untergruppe $\overline{B} \subseteq \overline{A}$ mit
$$\overline{A} = \langle \overline{a}\rangle + \overline{B} \quad \text{und} \quad \langle \overline{a}\rangle \cap \overline{B} = \{\overline{0}\}.$$
Sei
$$B = \pi^{-1}(\overline{B}).$$
Wir beweisen, dass
$$A = \langle a\rangle + B \quad \text{und} \quad \langle a\rangle \cap B = \{0\}$$
gilt.
- Sei $x \in A$. Dann ist $\overline{x} \in \overline{A} = \langle \overline{a}\rangle + \overline{B}$, es gibt also ein $i \in \mathbb{Z}$ und ein $\overline{b} \in \overline{B}$ mit
$$\overline{x} = i\overline{a} + \overline{b}.$$
Wir wählen nun $b \in B$ mit $\pi(b) = \overline{b}$. Dann gilt
$$x \equiv ia + b \bmod \langle c\rangle.$$
Es gibt also ein $j \in \mathbb{Z}$ mit
$$x = ia + b + jc.$$
Wegen $\operatorname{Kern}(\pi) = \langle c\rangle$ ist $c \in B$, also $b + jc \in B$, und damit
$$x = ia + (b + jc) \in \langle a\rangle + B.$$
Dies beweist $A = \langle a\rangle + B$.
- Sei nun $x \in \langle a\rangle \cap B$. Dann ist $\overline{x} \in \langle \overline{a}\rangle \cap \overline{B} = \{\overline{0}\}$, also $x \in \operatorname{Kern}(\pi) = \langle c\rangle$. Dann ist $x \in \langle a\rangle \cap \langle c\rangle = \{0\}$, also $x = 0$. Damit folgt
$$\langle a\rangle \cap B = \{0\},$$
was noch zu zeigen war.

Damit ist die Behauptung durch Induktion bewiesen. ■

Durch Induktion ergibt sich dann sofort die Existenzaussage im zuvor angegebenen Satz. (Die Eindeutigkeit müssen wir noch beweisen.)

Bemerkung: Wir können jetzt leicht angeben, welche abelsche p-Gruppen es zu einer bestimmten Ordnung (bis auf Isomorphie) gibt.

Ordnung	Abelsche Gruppen dieser Ordnung
p	$\mathbb{Z}_p$
p^2	$\mathbb{Z}_{p^2}$, $\mathbb{Z}_p \times \mathbb{Z}_p$
p^3	$\mathbb{Z}_{p^3}$, $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$, $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$
p^4	$\mathbb{Z}_{p^4}$, $\mathbb{Z}_{p^3} \times \mathbb{Z}_p$, $\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$, $\mathbb{Z}_{p^2} \times \mathbb{Z}_p \times \mathbb{Z}_p$, $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$

Bemerkung: Wir haben zuvor die Regel
$$\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n \text{ für } m, n \in \mathbb{N} \text{ mit } \operatorname{ggT}(m, n) = 1$$
kennengelernt. Damit können wir nun eine andere Zerlegung endlicher abelscher Gruppen angeben. Sei A eine endliche abelsche Gruppe mit Gruppenordnung $|G| = p_1^{e_1} \dots p_r^{e_r}$. Dann ist
$$P_i = \{x \in G : p_i^{e_i} x = 0\}$$
die p_i-Sylowgruppe von A. Wir zerlegen:
$$P_i = \prod_{j \geq 1} \mathbb{Z}_{p_i^{e_{ij}}} \text{ mit } e_{i1} \geq e_{i2} \geq e_{i3} \geq \dots$$

Wir definieren

$$m_j = \prod_{i=1}^{r} p_i^{e_{ij}}.$$

Dann gilt

$$\mathbb{Z}_{p_1^{e_{1j}}} \times \cdots \times \mathbb{Z}_{p_r^{e_{rj}}} \simeq \mathbb{Z}_{m_j}$$

und

$$A \simeq \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \mathbb{Z}_{m_3} \times \dots$$

mit

$$m_2 \mid m_1, \quad m_3 \mid m_2, \quad m_4 \mid m_3, \quad \dots,$$

was man auch in der Form

$$\cdots \mid m_5 \mid m_4 \mid m_3 \mid m_2 \mid m_1$$

schreiben kann. Wir formulieren dies als Satz:

SATZ. *Ist A eine endliche abelsche Gruppe mit $|A| \geq 2$, so gibt es natürliche Zahlen $m_1, m_2, \dots, m_r$ mit*

$$m_r \mid m_{r-1} \mid m_{r-2} \mid \cdots \mid m_2 \mid m_1, \quad m_r \geq 2$$

und

$$A \simeq \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \mathbb{Z}_{m_3} \times \dots$$

Die Zahlen $m_1, m_2, \dots, m_r$ sind dabei eindeutig bestimmt.

Wir erwähnen noch ohne Beweis folgenden Satz, der auch als **Hauptsatz über endlich erzeugte abelsche Gruppen** bezeichnet wird.

SATZ. *Sei A eine endlich erzeugte abelsche Gruppe.*

(1) *Dann ist (die* **Torsionsuntergruppe***)*

$$A_{\text{torsion}} = \{x \in A : \operatorname{ord}(x) < \infty\}$$

eine endliche abelsche Gruppe, also gibt es natürliche Zahlen $m_1, \dots, m_s$ mit

$$m_s \mid m_{s-1} \mid \cdots \mid m_2 \mid m_1, \quad m_s > 1 \quad \text{und} \quad A_{\text{torsion}} \simeq \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r}.$$

(2) *Die Faktorgruppe A/A_{torsion} ist isomorph zu einem Produkt*

$$\mathbb{Z}^r = \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{r \text{ Faktoren}} \quad \text{mit} \quad r \geq 0.$$

r heißt der **Rang** *der abelschen Gruppe A.*

(3) *Es gibt eine Untergruppe B von A mit*

$$A = A_{\text{torsion}} + B, \quad A_{\text{torsion}} \cap B = \{0\}, \quad B \simeq \mathbb{Z}^r.$$

(4) *Es ist*

$$A \simeq \mathbb{Z}_{m_s} \times \dots \mathbb{Z}_{m_1} \times \mathbb{Z}^r.$$

Die Größen r und m_i mit $m_s \mid m_{s-1} \mid \cdots \mid m_2 \mid m_1$ sind durch A eindeutig bestimmt.

5. Semidirekte Produkte

DEFINITION. *Für zwei (multiplikativ geschriebene) Gruppen N und H und einen Gruppenhomomorphismus $\tau : H \to \mathrm{Aut}(N)$ definieren wir auf $N \times H = \{(n,h) : n \in N, h \in H\}$ eine Verknüpfung durch*

$$(n,h) \cdot_\tau (n',h') = (n \cdot \tau(h)(n'), h \cdot h').$$

Wir schreiben dafür auch

$$N \rtimes_\tau H \quad \text{oder} \quad N \rtimes H$$

und nennen dies das **semidirekte Produkt** *der Gruppen N und H bezüglich $\tau : H \to \mathrm{Aut}(N)$.*

LEMMA. *Sei $N \rtimes_\tau H$ das semidirekte Produkt der Gruppen N und H bezüglich $\tau : H \to \mathrm{Aut}(N)$.*

(1) *$N \rtimes_\tau H$ ist eine Gruppe. Neutrales Element ist (e_N, e_H). Für die Inversenbildung gilt*

$$(n,h)^{-1} = (\tau(h^{-1})(n^{-1}), h^{-1}).$$

(2) *$\widetilde{N} = \{(n, e_H) : n \in N\}$ ist eine Untergruppe von $N \rtimes H$ und*

$$N \to \widetilde{N}, \quad n \mapsto (n, e_H)$$

ein Gruppenisomorphismus.

(3) *$\widetilde{H} = \{(e_N, h) : h \in H\}$ ist eine Untergruppe von $N \rtimes H$ und*

$$H \to \widetilde{H}, \quad h \mapsto (e_N, h)$$

ein Isomorphismus.

(4) *Für $n \in N$ und $h \in H$ gilt*

$$(n,h) = (n, e_H) \cdot_\tau (e_G, h),$$

also

$$N \rtimes_\tau H = \widetilde{N}\widetilde{H} \quad \text{und} \quad \widetilde{N} \cap \widetilde{H} = \{(e_N, e_H)\}.$$

(5) *Es ist*

$$(e_N, h) \cdot_\tau (n, e_H) \cdot_\tau (e_N, h)^{-1} = (\tau(h)(n), e_H).$$

Der Beweis fehlt noch.

Beispiel: Wir wollen ein semidirektes Produkt $\mathbb{Z}_3 \rtimes_\phi \mathbb{Z}_4$ konstruieren, wobei wir die abelschen Gruppen $\mathbb{Z}_3$ und $\mathbb{Z}_4$ additiv schreiben.

- Wir brauchen einen Homomorphismus

  $$\phi : \mathbb{Z}_4 \to \mathrm{Aut}(\mathbb{Z}_3).$$

  Wir kennen die Automorphismengruppen der zyklischen Gruppen $\mathbb{Z}_n$, denn

  $$\mathbb{Z}_n^* \to \mathrm{Aut}(\mathbb{Z}_n), \quad a \mapsto (x \mapsto ax \bmod n)$$

  ist ein Isomorphismus. (Dabei wird $\mathbb{Z}_n^*$ multiplikativ geschrieben.) In unserem Fall haben wir

  $$\mathbb{Z}_3^* \to \mathrm{Aut}(\mathbb{Z}_3), \quad a \mapsto (x \mapsto ax \bmod 3) \quad \text{und} \quad \mathbb{Z}_3^* = \{1, 2\}.$$

- Nun brauchen wir einen Homomorphismus

  $$\mu : \mathbb{Z}_4 \to \mathbb{Z}_3^*.$$

  Da wir keinen trivialen Homomorphismus haben wollen, bilden wir den Erzeuger 1 (von $\mathbb{Z}_4$) auf den Erzeuger 2 (von $\mathbb{Z}_3^*$) ab: $\mu(1) = 2$. Es folgt dann

  $$\mu(i) = 2^i \bmod 3.$$

  Man prüft nach, dass μ durch diese Definition tatsächlich ein (surjektiver) Gruppenhomomorphismus ist.
- Insgesamt erhalten wir damit

  $$\phi : \mathbb{Z}_4 \to \mathrm{Aut}(\mathbb{Z}_3) \quad \text{mit} \quad \phi(i)(x) = 2^i x \bmod 3.$$

- Damit können wir jetzt die Verknüpfung auf $\mathbb{Z}_3 \rtimes_\phi \mathbb{Z}_4$ bestimmen:

$$\begin{aligned}(i_1, j_1) \cdot_\phi (i_2, j_2) &= (i_1 + \phi(j_1)(i_2) \bmod 3, j_1 + j_2 \bmod 4) = \\ &= (i_1 + 2^{j_1} i_2 \bmod 3, j_1 + j_2 \bmod 4).\end{aligned}$$

  Hier ist eine Verknüpfungstabelle:

$x \cdot_\phi y$	$(0,0)$	$(0,1)$	$(0,2)$	$(0,3)$	$(1,0)$	$(1,1)$	$(1,2)$	$(1,3)$	$(2,0)$	$(2,1)$	$(2,2)$	$(2,3)$
$(0,0)$	$(0,0)$	$(0,1)$	$(0,2)$	$(0,3)$	$(1,0)$	$(1,1)$	$(1,2)$	$(1,3)$	$(2,0)$	$(2,1)$	$(2,2)$	$(2,3)$
$(0,1)$	$(0,1)$	$(0,2)$	$(0,3)$	$(0,0)$	$(2,1)$	$(2,2)$	$(2,3)$	$(2,0)$	$(1,1)$	$(1,2)$	$(1,3)$	$(1,0)$
$(0,2)$	$(0,2)$	$(0,3)$	$(0,0)$	$(0,1)$	$(1,2)$	$(1,3)$	$(1,0)$	$(1,1)$	$(2,2)$	$(2,3)$	$(2,0)$	$(2,1)$
$(0,3)$	$(0,3)$	$(0,0)$	$(0,1)$	$(0,2)$	$(2,3)$	$(2,0)$	$(2,1)$	$(2,2)$	$(1,3)$	$(1,0)$	$(1,1)$	$(1,2)$
$(1,0)$	$(1,0)$	$(1,1)$	$(1,2)$	$(1,3)$	$(2,0)$	$(2,1)$	$(2,2)$	$(2,3)$	$(0,0)$	$(0,1)$	$(0,2)$	$(0,3)$
$(1,1)$	$(1,1)$	$(1,2)$	$(1,3)$	$(1,0)$	$(0,1)$	$(0,2)$	$(0,3)$	$(0,0)$	$(2,1)$	$(2,2)$	$(2,3)$	$(2,0)$
$(1,2)$	$(1,2)$	$(1,3)$	$(1,0)$	$(1,1)$	$(2,2)$	$(2,3)$	$(2,0)$	$(2,1)$	$(0,2)$	$(0,3)$	$(0,0)$	$(0,1)$
$(1,3)$	$(1,3)$	$(1,0)$	$(1,1)$	$(1,2)$	$(0,3)$	$(0,0)$	$(0,1)$	$(0,2)$	$(2,3)$	$(2,0)$	$(2,1)$	$(2,2)$
$(2,0)$	$(2,0)$	$(2,1)$	$(2,2)$	$(2,3)$	$(0,0)$	$(0,1)$	$(0,2)$	$(0,3)$	$(1,0)$	$(1,1)$	$(1,2)$	$(1,3)$
$(2,1)$	$(2,1)$	$(2,2)$	$(2,3)$	$(2,0)$	$(1,1)$	$(1,2)$	$(1,3)$	$(1,0)$	$(0,1)$	$(0,2)$	$(0,3)$	$(0,0)$
$(2,2)$	$(2,2)$	$(2,3)$	$(2,0)$	$(2,1)$	$(0,2)$	$(0,3)$	$(0,0)$	$(0,1)$	$(1,2)$	$(1,3)$	$(1,0)$	$(1,1)$
$(2,3)$	$(2,3)$	$(2,0)$	$(2,1)$	$(2,2)$	$(1,3)$	$(1,0)$	$(1,1)$	$(1,2)$	$(0,3)$	$(0,0)$	$(0,1)$	$(0,2)$

- Die folgende Tabelle gibt zu x die Ordnung $\operatorname{ord}(x)$ und die erzeugte Untergruppe $\langle x \rangle$ an.

x	$\operatorname{ord}(x)$	$\langle x \rangle$
$(0,0)$	1	$\{(0,0)\}$
$(0,1)$	4	$\{(0,0),(0,1),(0,2),(0,3)\}$
$(0,2)$	2	$\{(0,0),(0,2)\}$
$(0,3)$	4	$\{(0,0),(0,3),(0,2),(0,1)\}$
$(1,0)$	3	$\{(0,0),(1,0),(2,0)\}$
$(1,1)$	4	$\{(0,0),(1,1),(0,2),(1,3)\}$
$(1,2)$	6	$\{(0,0),(1,2),(2,0),(0,2),(1,0),(2,2)\}$
$(1,3)$	4	$\{(0,0),(1,3),(0,2),(1,1)\}$
$(2,0)$	3	$\{(0,0),(2,0),(1,0)\}$
$(2,1)$	4	$\{(0,0),(2,1),(0,2),(2,3)\}$
$(2,2)$	6	$\{(0,0),(2,2),(1,0),(0,2),(2,0),(1,2)\}$
$(2,3)$	4	$\{(0,0),(2,3),(0,2),(2,1)\}$

Der folgende Satz zeigt, wie man ein semidirektes Produkt erkennen kann.

SATZ. *Sei G eine Gruppe, N ein Normalteiler und H eine Untergruppe von G. Es gelte*

$$G = NH = \{nh : n \in N, h \in H\} \quad \text{und} \quad N \cap H = \{e\}.$$

Wir definieren für $h \in H$ eine Abbildung $\tau(h) : N \to N$ durch

$$\tau(h)(n) = hnh^{-1}.$$

Dann gilt:

(1) *τ ist ein Gruppenhomomorphismus $H \to \operatorname{Aut}(N)$.*
(2)

$$\phi : N \rtimes_\tau H \to G, \quad (n,h) \mapsto hk$$

ist ein Gruppenisomorphismus.

Beweis:

(1) Dies rechnet man einfach nach.
(2)
- Wir zeigen, dass ϕ ein Gruppenhomomorphismus ist:

$$\begin{aligned}\phi((n,h) \cdot_\tau (n',h')) &= \phi((n \cdot \tau(h)(n'), h \cdot h')) = \phi((n \cdot hn'h^{-1}, h \cdot h')) = \\ &= n \cdot hn'h^{-1} \cdot h \cdot h' = n \cdot h \cdot n' \cdot h' = \phi((n,h)) \cdot \phi((n',h')).\end{aligned}$$

- Wegen der Voraussetzung $G = NH$ ist ϕ surjektiv.

- Ist $(n, h) \in \mathrm{Kern}(\phi)$, so gilt $nh = e$, also
$$n = h^{-1} \in N \cap H = \{e\}, \quad \text{und damit} \quad (n, h) = (e, e).$$
Damit ist ϕ injektiv. Daher folgt insgesamt, dass ϕ ein Isomorphismus ist. ■