Gruppentheorie

michael.gerhaeuser@gmx.de benedikt.ahrens@web.de

10. August 2007

Zusammenfassung

Gruppentheorie nach Dr. Harald Meyer, Sommersemester 2007

Inhaltsverzeichnis

0 Einführung

Folgendes wird als bekannt vorausgesetzt:

- Definitionen: Gruppe, Untergruppe, Normalteiler, Faktorgruppe, Ordnung
- Untergruppenkriterien
- Homomorphiesatz und Isomorphiesätze:

  0.1 Satz Homomorphiesatz
  G, H Gruppen, $\varphi : G \to H$ Homomorphismus. Dann gilt:

  $$G/\operatorname{Ker} H \cong \operatorname{Im} \varphi.$$

  0.2 Satz 1. Isomorphiesatz
  Sei $H \leq G, N \lhd G$. Dann gilt:

  1. *$HN \leq G$.*
  2. *$N \lhd HN$.*
  3. *$H \cap N \lhd H$.*

4. *Der kanonische Homomorphismus*

$$H/H \cap N \to HN/N, \quad h\,(H \cap N) \mapsto hN$$

ist ein Isomorphismus.

0.3 Satz 2. Isomorphiesatz
Seien $M, N \lhd G, M \leq N$. Dann gilt:

1. *$N/M \lhd G/M$.*
2. *Der kanonische Homomorphismus*

$$(G/M)\,/\,(N/M) \to G/N, \quad (gM)\,(N/M) \mapsto gN$$

ist ein Isomorphismus.

- Der Satz von Lagrange:

  0.4 Satz Satz von Lagrange
  Die Ordnung der Untergruppe teilt stets die Ordnung der Gruppe.

- Definition von zyklischen Gruppen, die Gruppen $\mathbb{Z}_n$.

- Hauptsatz über endliche abelsche Gruppen:

  0.5 Satz Hauptsatz über endliche abelsche Gruppen
  Jede endliche abelsche Gruppe ist direktes Produkt von Gruppen von Primzahlpotenzordnung, das heißt es gibt (nicht notwendig verschiedene) Primzahlen $p_1, \ldots, p_k$, so dass

$$G \cong \mathbb{Z}_{p_1^{a_1}} \times \ldots \mathbb{Z}_{p_k^{a_k}}.$$

- Eigenschaften zyklischer Gruppen, zum Beispiel:

$$\mathbb{Z}_{nm} \cong \mathbb{Z}_n \times \mathbb{Z}_m \Leftrightarrow \mathrm{ggT}\,(n, m) = 1.$$

- Definition des direkten Produkts von Gruppen.

- Definition der symmetrischen Gruppe S_n, alternierenden Gruppe A_n.

$$\mathrm{sign} : \mathrm{S}_n \to \{1, -1\}.$$

- Rechnen mit Zykeln in S_n, Zerlegung in elementfremde Zykeln.

1 Grundlagen

Im ersten Kapitel werden wir verschiedene Sätze besprechen, die evtl. auch schon bekannt sind.

Generalvoraussetzung: G sei eine endliche Gruppe.

1.1 Lemma
Seien $A, B \subset G$ (nicht notwendig Untergruppen) mit $A^{-1} = A, \quad B^{-1} = B$. Dann gilt:

1. $$|AB| = \frac{|A| \cdot |B|}{|A \cap B|},$$
   wobei AB die Menge aller Produkte der Form $a \cdot b$ mit $a \in A$ und $b \in B$ ist.

2. *Seien jetzt $A, B \leq G$ Untergruppen von G. Dann gilt: AB ist Untergruppe von G genau dann, wenn $AB = BA$.*

Beweis:

1. Seien a_1, a_2 aus A, b_1, b_2 aus B. Dann gilt:
   $$\begin{aligned} a_1 b_1 = a_2 b_2 &\Leftrightarrow a_2^{-1} a_1 = b_2 b_1^{-1} =: d \in A \cap B \\ &\Leftrightarrow \exists d \text{ in } A \cap B \text{ mit } a_1 = a_2 d, b = d^{-1} b_2. \end{aligned}$$
   Zu einem festen Produkt $a_2 b_2$ gibt es genau $|A \cap B|$ Möglichkeiten, Elemente a_1 in A, b_1 in B zu wählen derart, dass $a_2 b_2 = a_1 b_1$. Damit ist $|AB| = \frac{|A| \cdot |B|}{|A \cap B|}$.

2. Sei zunächst AB Untergruppe von G. Dann ist $AB = (AB)^{-1} = B^{-1} A^{-1} \overset{A,B \leq G}{=} BA$.
   Ist umgekehrt $AB = BA$, so folgt $(AB)(AB) = A(BA)B \overset{Vor.}{=} A(AB)B = (AA)(BB) = AB$. Nach dem Untergruppenkriterium für endliche Gruppen (setze REF!) ist damit AB Untergruppe von G.

1.2 Definition und Satz

1. Die Menge *Aut(G)* aller Automorphismen $\alpha : G \to G$ bildet mit der Verknüfpung über Komposition eine Gruppe, die sog. *Automorphismengruppe von G.*

2. Für jedes g in G ist die Abbildung $\varphi_g : G \to G, x \mapsto g^{-1} x g$, die sog. *Konjugation mit g*, ein Automorphismus von G. Automorphismen von diesem Typ heißen *innere Automorphismen*, andere heißen *äußere Automorphismen.*

3. Die Menge *Inn(G)* der inneren Automorphismen bildet eine Untergruppe von $\mathrm{Aut}(G)$. Es gilt: $\mathrm{Inn}(G) \lhd \mathrm{Aut}(G)$.

4. Eine Untergruppe U von G heißt *charakteristisch* (schreibe $U \operatorname{char} G$), wenn U invariant ist unter Automorphismen von G, d.h. wenn $\alpha(U) = U$ für alle α aus $\mathrm{Aut}(G)$.

Bemerkung
Es gilt $U \lhd G \iff g^{-1}Ug = U$ für alle $g \in G \iff \alpha(U) = U$ für alle $\alpha \in \mathrm{Inn}(G)$. Daher gilt $U \operatorname{char} G \Longrightarrow U \lhd G$.

Beweis von 1.2:

1. trivial

2. $g^{-1}xg = 1 \Leftrightarrow x = gg^{-1}$. Also ist φ_x injektiv und, da $|G| < \infty$, auch surjektiv. Weite ist $\varphi_g(xy) = g^{-1}xyg = g^{-1}xgg^{-1}yg = \varphi_g(x)\varphi_g(y)$. Also ist φ_g ein Homomorphismus.

3. Seien $h_1, h_2 \in G$. Wir zeigen
   $\varphi_{h_2} \circ \varphi_{h_1} =$
   $\varphi_{h_1h_2} \in \mathrm{Inn}(G)$:
   $\varphi_{h_2} \circ \varphi_{h_1}(x) = \varphi_{h_2}(h_1^{-1}xh_1) = h_2^{-1}h_1^{-1}xh_1h_2 = (h_1h_2)^{-1}x(h_1h_2) = \varphi_{h_1h_2}(x)$ Also ist $\varphi_{h_2} \circ \varphi_{h_1} = \varphi_{h_1h_2} \in \mathrm{Inn}(G)$ und damit $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$.
   Sei nun $\psi \in \mathrm{Aut}(G), g \in G$. Dann gilt: $(\psi^{-1}\varphi_g\psi)(x) = \psi^{-1}(g^{-1}\psi(x)g) = \psi^{-1}(g)^{-1}x\psi^{-1}(g) = \varphi_{\psi^{-1}(g)}(x)$. Also ist $\psi^{-1}\varphi_g\psi = \varphi_{\psi^{-1}(g)} \in \mathrm{Inn}(G)$ und damit $\mathrm{Inn}(G) \lhd \mathrm{Aut}(G)$.

1.3 Bemerkung
Die Formel $\varphi_{h_2} \circ \varphi_{h_1} = \varphi_{h_1h_2}$ im letzten Beweis ist nicht nur unschön, sondern verursacht häufig technische Schwierigkeiten: Die Komposition von Abbildungen ist für die Gruppentheorie "verkehrt herum". Z.B. sollte bei einem Homomorphismus $\varphi : G \to \mathrm{Aut}(H)$ mit $\varphi(g) = \alpha, \varphi(h) = \beta$ auch $\varphi(gh) = \alpha\beta$ gelten.
Als Abhilfe vereinbart man folgende Konvention: Abbildungen, Homomorphismen werden rechts von Elementen als Exponent geschrieben, also g^α statt $\alpha(g)$ und entsprechend $g^{\alpha\beta}$ statt $\beta(\alpha(g))$.
In der symmetrischen Gruppe lesen wir Zykel von links nach rechts und multiplizieren sie auch von links, also $(1\quad 2)(1\quad 3) = (1\quad 2\quad 3)$.

1.4 Satz Korrespondenzsatz
Sei N Normalteiler in G. Der natürliche Epimorphismus $v : G \to G/N$ induziert eine Bijektion

$$\tilde{v} : \{U | N \leq U \leq G\} \to \{V | V \leq G/N\}, \quad U \longmapsto v(U)$$

zwischen der Menge der Zwischengruppen von N und G und der Menge der Untergruppen von G/N. Dabei entsprechen Normalteiler einander, es gilt also $N \leq U \lhd G$ genau dann, wenn $v(U) \lhd G/N$.

Beweis:
Ist $U \lhd G$, so ist $v(U) \leq G/N$ wieder Untergruppe, denn Homomorphismen bilden Untergruppen wieder auf Untergruppen ab. Also ist $\tilde{v}$ wohldefiniert.
Die Umkehrabbildung ist $\tilde{v}^{-1} : V \to v^{-1}(V)$. Weil v surjektiv ist, gilt $v(v^{-1}(V)) = V$. Ist $N \leq U$, so gilt $v^{-1}(\underbrace{v(U)}_{UN/N}) = UN = U$. Damit ist $\tilde{v}$ bijektiv.
Sei jetzt $N \leq U \lhd G$. Dann ist $x^{-1}Ux = U$ für alle $x \in G$. Hierauf v angewandt liefert $v(U) = v(x^{-1}Ux) = v(x)^{-1}v(U)v(x)$. Durchläuft x ganz G, so durchläuft $v(x)$ ganz G/N, also folgt $v(U) \lhd G/N$. Sei $V \lhd G/N$ und $U \leq G$ mit $N \leq U$ eine Untergruppe mit $v(U) = V$. Wir zeigen, dass U und $x^{-1}Ux$ für jedes $x \in G$ durch $\tilde{v}$ auf V abgebildet werden: es gilt $\tilde{v}(x^{-1}Ux) = v(x^{-1}Ux) = v(x)^{-1}v(U)v(x) = v(x)^{-1}Vv(x) \overset{V \lhd G/N}{=} V = v(U) = \tilde{v}(U)$. Nach dem ersten Teil folgt $x^{-1}Ux = U$‘. Da dies für alle $x \in G$ gilt, ist $U \lhd G$. □

1.5 Definition

1. G heißt *einfach*, wenn G außer $\langle 1 \rangle$ und G keine Normalteiler besitzt.

2. Ein Normalteiler $N \lhd G$ heißt *maximal*, wenn es keinen Normalteiler $M \lhd G$ gibt mit $N < M < G$. Nach dem Korrespondenzsatz 1.4 ist dies genau dann der Fall, wenn G/N einfach ist.

3. Ein Normalteiler $N \lhd G$ heißt *minimal*, wenn es keinen Normalteiler $M \lhd G$ gibt mit $\langle 1 \rangle < M < N$.
   Beachte: N muss hier nicht einfach sein, da $M \lhd N \lhd G \overset{\text{i.A.}}{\nRightarrow} M \lhd G$.

1.6 Satz Cayley
Jede Gruppe der Ordnung n ist isomorph zu einer Untergruppe der S_n.

Beweis:
Sei $|G| = n$ und für jedes $g \in G$ sei $r_g : G \to G, x \mapsto xg$ die *Rechtstranslation um g*.
Die Abbildung $r : G \to \mathrm{S}_G, g \mapsto r_g$ ist ein injektiver Gruppenhomomorphismus:

$$x^{r(gh)} = x \cdot (gh) = (xg)h = xg^{r(h)} = (x^{r_g})^{r_h} = x^{r(g)r(h)}$$

liefert $r(gh) = r(g)r(h)$. Weil

$$\mathrm{Ker}(r) = \{g | x \cdot g = x \forall x \in G\} = \langle 1 \rangle$$

ist r injektiv.
Mit dem Homomorphiesatz folgt

$$G \cong G/\operatorname{Ker}(r) \cong \operatorname{Inn}(r) \leq \mathrm{S}_G \cong \mathrm{S}_n\,.$$

1.7 Satz
Sei G eine Gruppe mit $|G| = 2n$, n ungerade. Dann besitzt G einen Normalteiler der Ordnung n.

Beweis:
Wir zeigen zunächst, dass G ein Element g der Ordnung 2 enthält. Sei $A := \{g \in G | g = g^{-1}\}$ und $B := \{g \in G | g \neq g^{-1}\}$. Dann ist $G = A \amalg B$.$|B|$ ist gerade, da mit $g \in B$ auch $g^{-1} \in B, g^{-1} \neq g$. Also ist auch $|A| = 2n - |B|$ gerade. Da $1 \in A$ folgt $|A| \geq 2$, d.h. es gibt $g \neq 1$ mit $g = g^{-1}$, also $g^2 = 1$. Sei $r : G \to \mathrm{S}_G$ die Einbettung von G wie im Beweis von 1.6. Dann ist $r(G) =: h$ ein Element der Ordnung 2. Wegen $\operatorname{ord}(h) = 2$ kommen in der Zerlegung von h in disjunkte Zykel nur Zykel der Länge 2 vor. Nach 1.6 gilt $h(x) = x \cdot g$ für alle x in G. Da $g \neq 1$, ist $x \cdot g \neq x$ für alle x in G, d.h. die Permutation h hat keine Fixpunkte. Also ist h das Produkt von n Zykeln der Länge 2. Damit ist $\operatorname{sign}(h) = (-1)^n = -1$. Also ist $\operatorname{sign} \circ r : G \to (-1, 1)$ ein surjektiver Gruppenhomomorphismus und $\operatorname{Ker}(\operatorname{sign} \circ r) \lhd G$. Nach dem Homomorphiesatz gilt $|\operatorname{Ker}(\operatorname{sign} \circ r)| = \frac{|G|}{2} = n$. □

Bemerkung
Ist G eine einfache Gruppe mit $2 \mid |G|$, so gilt $4 \mid |G|$ (für $|G| > 2$).

1.8 Satz Konstruktion
Sei $U \leq G$ eine Untergruppe von Index $[G : U] = k$ und $\{U_{g_1}, \ldots, U_{g_k}\} = \{N_1, \ldots, N_k\}$ die Menge der rechten Nebenklassen von U. Dann wird durch

$$\varphi : G \to \mathrm{S}_n, g \longmapsto \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}$$

mit $N_1 g = N_{i_1}, \ldots, N_k g = N_{i_k}$ ein Gruppenhomomorphismus definiert.
Es gilt $\operatorname{Ker}(\varphi) = \bigcap_{g \in G} g^{-1} U g \leq U$. Für $k \geq 2$ ist φ nicht trivial.

Beweis:
φ ist wohldefiniert:

$$\begin{aligned} N_i g = N_j g &\iff U g_i g = U g_j g \iff g_i g \in U g_j g \\ &\iff \exists u \in U : g_i g = u g_j g \iff \exists u \in U : g_i = u g_j \\ &\iff g_i \in U g_j \iff U g_i = U g_j \\ &\iff N_i = N_j. \end{aligned}$$

Das bedeutet, $\varphi(g)$ ist tatsächlich Permutation. φ ist ein Homomorphismus: Sei $\varphi(gh) = \pi$. Sei $N_i g = N_j und N_j h = N_m$. Dann ist $N_i gh = N_m$. Also ist π eine Permutation mit $i^\pi = m$. Gleichzeitig ist $\varphi(g) = \sigma$ mit $i^\sigma = j$ und $\varphi(h) = \tau$ mit $j^\tau = m$. Daher ist $i^{\sigma\tau} = j^\tau = m = i^\pi$, also $\pi = \sigma\tau$ und damit $\varphi(gh) = \varphi(g)\varphi(h)$. Es gilt: $\mathrm{Ker}(\varphi) = \{g \in G | Ug_i g = Ug_i, i = 1, \ldots, n\} = \{g \in G | g_i g g_i^{-1} \in U, i = 1, \ldots, n\} = \{g \in G | g \in g_i^{-1} U g_i, i = 1, \ldots, n\} = \bigcap_{g \in G} g^{-1} U g$. Sei $k \geq 2$. Sei $Ug_1 \neq Ug_2$. Setze $g := g_1^{-1} g_2$, dann ist $Ug_1 g = Ug_1 g_1^{-1} = Ug_2 \neq Ug_1$. Also ist $\varphi(g) \neq 1 \in \mathrm{S}_N$.

Bemerkung

1. Setzen wir $U = \langle 1 \rangle$, so erhalten wir wieder den Satz von Cayley mit genau dem dortigen Beweis.

2. Die Rechtsmultiplikation auf den Rechtsnebenklassen ist eine sogenannte *Gruppenoperation*. Zu jeder Gruppenoperation gehört ein Homomorphismus in eine geeignete symmetrische Gruppe - in diesem Fall genau der oben konstruierte.

1.9 Definition *inneres und äußeres Produkt*

1. Seien G_1, G_2 Gruppen. Das kartesische Produkt $G_1 \times G_2$ wird mit der komponentenweisen Verknüpfung zu einer Gruppe, dem sogenannten *äußeren direkten Produkt* von G_1 und G_2.

2. Seien $N_1, \ldots, N_k$ Normalteiler von G mit:

   (a) $G = N_1 N_2 \cdots N_k$

   (b) $N_i \cap N_1 \cdots N_{i-1} N_{i+1} \cdots N_k = \langle 1 \rangle$ für $i = 1, \ldots, k$.

   Dann heißt G *inneres direktes Produkt* von $N_1, \ldots, N_k$.

1.10 Satz
Sei $G = N_1 \cdot \ldots \cdot N_k$ ein inneres direktes Produkt der Normalteiler $N_1, \ldots, N_k$. Dann gilt:

1. *Für $i \neq j$ kommutieren Elemente von N_i und N_j, d.h. für $a \in N_i, b \in N_j$ gilt $ab = ba$.*

2. *Jedes $a \in G$ besitzt eine (bis auf Reihenfolge) eindeutige Darstellung $a = a_1 \cdot a_2 \cdot \ldots \cdot a_k$ mit $a_i \in N_i$.*

Beweis:

1. $N_i, N_j \lhd G$, daher gilt $\underbrace{a^{-1}b^{-1}a}_{\in N_i}\underbrace{b}_{\in N_j} = \underbrace{a^{-1}}_{\in N_i}\underbrace{b^{-1}ab}_{\in N_i} \in N_i \cap N_j \leq N_i \cap (N_1 \cdot \ldots \cdot N_{i-1}N_{i+1} \cdot \ldots \cdot N_k) = \langle 1 \rangle$. Also folgt $a^{-1}b^{-1}ab = 1 \Longleftrightarrow ab = ba$.

2. Wegen $G = N_1 \cdot \ldots \cdot N_k$ gibt es eine Darstellung $a = a_1 \cdot \ldots \cdot a_k$ mit $a_i \in N_i$.
   Zur Eindeutigkeit: Sei zunächst $a = 1 = a_1 \cdot \ldots \cdot a_k$. Nach 1 gilt: $N_i \ni a_i^{-1} = a_1 a_2 \ldots a_{i-1}a_{i+1} \ldots a_k \in N_1 \ldots N_{i-1}N_{i+1} \ldots N_k$. Damit ist $a_i^{-1} \in N_i \cap (N_1 \ldots N_{i-1}N_{i+1} \ldots N_k) = \langle 1 \rangle$, also ist $a_i = 1$.
   Sei nun $a = a_1 \ldots a_k = b_1 \ldots b_k$ mit $a_i, b_i \in N_i$. Dann gilt nach 1: $1 = (a_1^{-1}b_1)(a_2^{-1}b_2) \cdot \ldots \cdot (a_k^{-1}b_k)$. Wie oben gezeigt gilt dann $a_i^{-1}b_i = 1 \Longleftrightarrow a_i = b_i$ für $i = 1, \ldots, k$.

1.11 Satz
Sei $G = N_1 \cdot \ldots \cdot N_k$ das innere direkte Produkt der Normalteiler $N_1, ldots, N_k$. Dann ist G isomorph zum äußeren direkten Produkt $G \cong N_1 \times \ldots \times N_k$.

Beweis:
Nach 1.10 besitzt jedes $g \in G$ eine eindeutige Darstellung $g = a_1 \cdot \ldots \cdot a_k$ mit $a_i \in N_i$. Wir definieren

$$\varphi : G \to N_1 \times \ldots \times N_k, g \longmapsto (a_1, \ldots, a_k).$$

Wegen der Eindeutigkeit der Darstellung ist φ wohldefiniert und bijektiv. Sei $h = b_1 \cdot \ldots \cdot b_k$ mit $b_i \in N_i$. Dann ist $gh = (a_1 \cdot \ldots \cdot a_k)(b_1 \cdot \ldots \cdot b_k) \overset{1.10.1}{=} a_1 b_1 a_2 b_2 \ldots a_k b_k$ und $\varphi(gh) = (a_1 b_1, a_2 b_2, \ldots, a_k b_k) = (a_1, \ldots, a_k) \cdot (b_1, \ldots b_k) = \varphi(g)\varphi(h)$. Damit ist φ ein Homomorphismus.

1.12 Bemerkung
Das äußere Produkt $G_1 \times \ldots \times G_k$ ist das innere Produkt der Normalteiler $\langle 1 \rangle \times \ldots \times \langle 1 \rangle \times G_i \times \langle 1 \rangle \times \ldots \times \langle 1 \rangle$. Wegen 1.11 unterscheiden wir im Folgenden nicht mehr zwischen äußerem und innerem direkten Produkt, denn isomorphe Gruppen sind vom Standpunkt der Gruppentheorie nicht unterscheidbar. Der Unterschied zwischen beiden besteht in der Sichtweise. Beim äußeren direkten Produkt haben wir mehrere "kleine" Gruppen gegeben und setzen daraus eine "große" Gruppe zusammen. Beim inneren direkten Produkt stehen wir vor dem umgekehrten Problem. Eine große Gruppe ist gegeben und wir suchen ihre "Bestandteile", d.h. ihre direkten Faktoren. Das gleiche Problem werden wir beim semidirekten Produkt haben.

1.13 Definition
Sei $U \leq G_1 \times G_2$ und seien $\pi_i : G_1 \times G_2 \to G_i$ die Projektionen. U heißt *diagonal*, wenn $U \subsetneqq \pi_1(U) \times \pi_2(U)$.

Beispiel
In $\mathbb{Z}_2 \times \mathbb{Z}_2$ ist $U := \{(0,0),(1,1)\}$ diagonal, denn $U < \pi_1(U) \times \pi_2(U) = \mathbb{Z}_2 \times \mathbb{Z}_2$.

1.14 Satz
Seien $G_1, \ldots, G_r \lhd G$ und $|G_1|, \ldots, |G_r|$ paarweise teilerfremd. Gilt dann $|G| = |G_1| \cdot \ldots \cdot |G_r|$, so ist $G = G_1 \times \ldots \times G_r$ und jede Untergruppe U von G hat die Form $U = U_1 \times \ldots \times U_r$ mit $U_i \leq G_i$, d.h. es gibt keine diagonalen Untergruppen in G.

Beweis:
Wir zeigen durch Induktion über i: $G_1 \cdot \ldots \cdot G_i$ ist Untergruppe von G und es gilt $|G_1 \cdot \ldots \cdot G_i| = |G_1| \cdot \ldots \cdot |G_i|$ und $G_1 \cdot \ldots \cdot G_i \cong G_1 \times \ldots \times G_i$.
Nach Induktionsvoraussetzung (IV) ist $G_1 \cdot \ldots \cdot G_{i-1} \leq G$. Wegen $G_i \lhd G$ folgt aus dem 1. Isomorphiesatz, dass auch $G_1 \cdot \ldots \cdot G_{i-1} \cdot G_i \leq G$. Weiter gilt $|G_1 \cdot \ldots \cdot G_{i-1} = |G_1| \cdot \ldots \cdot |G_{i-1}|$ nach Induktionsvoraussetzung, und diese Zahl ist teilerfremd zu $|G_i|$. Mit 1.1 folgt

$$|G_1 \cdot \ldots \cdot G_i| = \frac{|G_1 \cdot \ldots \cdot G_{i-1}| \cdot |G_i|}{|(G_1 \cdot \ldots \cdot G_{i-1}) \cap G_i|} = |G_1 \cdot \ldots \cdot G_{i-1}| \cdot |G_i| = |G_1| \cdot \ldots \cdot |G_i|,$$

da nach dem Satz von Lagrange gilt $(G_1 \cdot \ldots \cdot G_{i-1}) \cap G_i = \langle 1 \rangle$. Nach dem Satz 1.11 folgt $G_1 \cdot \ldots \cdot G_i \cong (G_1 \cdot \ldots \cdot G_{i-1}) \times G_i \overset{\text{IV}}{\cong} G_1 \times \ldots \times G_{i-1} \times G_i$.

Sei nun $U \leq G$ und $u \in U$. Nach 1.10 gibt es eindeutig bestimmte $u_i \in G_i$ derart, dass $u = u_1 \cdot \ldots \cdot u_r$. Sei $\sigma_i := \text{ord}(u_i)$ und sei $n_i := \frac{\sigma_1 \cdot \ldots \cdot \sigma_r}{\sigma_i}$. Weil die $|G_i|$ paarweise teilerfremd sind, folgt $\text{ggT}(\sigma_i, n_i) = 1$. Deshalb gibt es $x, y \in \mathbb{Z}$ derart, dass $x\sigma_i + yn_i = 1$. Nach 1.10 kommutieren die u_i, also ist wegen $u_i^{\sigma_i} = 1$

$$u^{yn_i} = (u_1 \cdot \ldots \cdot u_r)^{yn_i} = u_1^{yn_i} \cdot \ldots \cdot u_r^{yn_i} = u_i^{yn_i} = u_i^{yn_i + x\sigma_i} = u_i^1 = u_i.$$

Es gilt

$$\pi_i(U) = \{u_i \in U_i | \forall j \in \{1, \ldots, r\} - \{i\} \exists u_j \in G_j : u = u_1 \cdot \ldots \cdot u_r \in U\}.$$

Ist aber $u = u_1 \cdot \ldots \cdot u_r \in U$, so ist auch $u_i \in U$, d.h. $\pi_i(U) \subset U$ für alle i. Daher ist $\pi_1(U) \cdot \ldots \cdot \pi_r(U) \subset U$, also $U = \pi_1(U) \times \ldots \times \pi_r(U)$.

1.15 Definition *inneres semidirektes Produkt*
Sei $N \lhd G$. Gibt es eine Untergruppe $U \leq G$ derart, dass $UN = G$ und $U \cap N = \langle 1 \rangle$, so heißt U *Komplement* zu N in G und G heißt *inneres semidirektes Produkt von N und U.*

1.16 Bemerkung
Sei $G = NU$ inneres semidirektes Produkt des Normalteilers N mit U. Dann ist auch $G = NU$.
Die Abbildung $\psi : U \to \mathrm{Aut}(N), u \longmapsto (n \mapsto n^u)$ ist ein Gruppenhomomorphismus und es gilt

$$(u_1 n_1)(u_2 n_2) = (u_1 u_2)(n_1^{u^\psi} n_2)$$

für $u_1, u_2 \in U, n_1, n_2 \in N$.

Beweis:
Wegen $N \lhd G$ ist $UN = NU$. ψ ist wohldefiniert, denn für $u \in U$ ist

$$\varphi_u : G \to G, x \longmapsto u^{-1} x u$$

ein Automorphismus. Wegen $N \lhd G$ ist $\varphi_u(n) \in N$ für $n \in N$, also ist $\varphi_u|_N \in \mathrm{Aut}(N)$.
Die Homomorphieeigenschaft von ψ ist klar.
Für $u_1, u_2 \in U, n_1, n_2 \in N$ ist

$$(u_1 n_1)(u_2 n_2) = u_1 u_2 u_2^{-1} n_1 u_2 n_2 = u_1 u_2 n_1^{u_2} n_2 = u_1 u_2 n_1^{u_2^\psi} n_2.$$

1.17 Definition und Satz
Seien U, N Gruppen und sei $\varphi : U \to \mathrm{Aut}(N)$ ein Gruppenhomomorphismus. Dann wird das kartesische Produkt $U \times N$ mit der Multiplikation

$$(u_1, n_1)(u_2, n_2) := (u_1 u_2, n_1^{(u_2^\varphi)} n_2)$$

zu einer Gruppe, dem sogenannten *äußeren semidirekten Produkt von U mit N bezüglich φ*.
Schreibweise:$U \overset{\varphi}{\ltimes} N$ (Spitze zum Normalteiler).

Beweis:
Das Einselement ist $(1_U, 1_N)$, Inverses zu (u, n) ist $(u^{-1}, (n^{-1})^{(u^{-1})^\varphi})$:

$$\begin{aligned}(u, n)(u^{-1}, (n^{-1})^{(u^{-1})^\varphi}) &= (uu^{-1}, n^{(u^{-1})^\varphi}(n^{-1})^{(u^{-1})^\varphi}) = \\ &= (1_U, n^{(u^{-1})^\varphi}(n^{(u^{-1})^\varphi})^{-1}) = (1_U, 1_N).\end{aligned}$$

Zur Assoziativität:

$$\begin{aligned}[(u_1, n_1)(u_2, n_2)](u_3, n_3) &= (u_1 u_2, n_1^{u_2^\varphi} n_2)(u_3, n_3) \\ &= (u_1 u_2 u_3, (n_1^{u_2^\varphi} n_2)^{u_3^\varphi}) n_3) \\ &= (u_1 u_2 u_3, (n_1^{u_2^\varphi})^{u_3^\varphi} n_2^{u_3^\varphi} n_3) \\ &= (u_1 u_2 u_3, n_1^{(u_2 u_3)^\varphi} n_2^{u_3^\varphi} n_3) \\ &= (u_1, n_1)(u_2 u_3, n_2^{u_3^\varphi} n_3) \\ &= (u_1, n_1)[(u_2, n_2)(u_3, n_3)].\end{aligned}$$

1.18 Bemerkung

- Ist φ der triviale Homomorphismus, der alles auf id_N abbildet, so ist $U \overset{\varphi}{\ltimes} N \cong U \times N$.
- $U \overset{\varphi}{\ltimes} N$ kann auch als inneres semidirektes Produkt von $U \times \langle 1 \rangle$ und $\langle 1 \rangle \times N$ gesehen werden. Die Unterscheidung zwischen inneren und äußerem semidirekten Produkt ist also wieder unnötig, Bemerkung 1.12 gilt entsprechend.
- Ein wichtiges Problem der Gruppentheorie ist die Frage "Wann gibt es zu einem Normalteiler $N \lhd G$ ein Komplement?" Eine relativ allgemeine Antwort liefert der

  Satz von Zassenhaus
  Sind $|N|$ und $|G/N|$ teilerfremd, so besitzt N ein Komplement in G.

1.19 Beispiel
Seien $\langle d \rangle \cong \mathbb{Z}_n$ und $\langle s \rangle \cong \mathbb{Z}_2$ zyklisch. Durch

$$\begin{aligned} \varphi : \langle s \rangle \to \mathrm{Aut}(\langle d \rangle), s &\longmapsto (x \mapsto x^{-1} \\ 1 &\longmapsto \mathrm{id}_{\langle d \rangle} \end{aligned}$$

wird ein Homomorphismus gegeben. Das semidirekte Produkt $\mathrm{D}_n := \langle d \rangle \overset{\varphi}{\rtimes} \langle s \rangle$ der Ordnung $2n$ heißt *Diedergruppe*.

Bemerke: D_n ist isomorph zur Symmetriegruppe des regelmäßigen n-Ecks. Das Element d entspricht der Drehung um $\frac{360^\circ}{n}$, s einer Spiegelung an einer Symmetrieachse.

1.20 Definition *Kranzprodukt*

1. Seien G, H Gruppen. Sei $|H| = n$, $H = \{h_1, \ldots, h_n\}$. Dann wird für $h \in H$ durch $h_i \cdot h = h_{\pi_h(i)}$ eine Permutation $\pi_h \in \mathrm{S}_n$ definiert. Die Abbildung

   $$\vartheta_h : G^n \to G^n, (g_1, \ldots, g_n) \longmapsto (g_{\pi_h(1)}, \ldots, g_{\pi_h(n)})$$

   ist ein Automorphismus von G^n, dem n-fachen direkten Produkt von G mit sich selbst. Durch

   $$\varphi : H \to \mathrm{Aut}(G^n), h \longmapsto \vartheta_n$$

   wird ein Gruppenhomomorphismus definiert. Das semidirekte Produkt

   $$G \wr_r H := (G^n) \overset{\varphi}{\rtimes} N$$

   heißt *reguläres Kranzprodukt von G mit H.*

2. Sei G Gruppe, $H \leq \mathrm{S}_n$. Sei $h \in H$. Durch

$$\vartheta_h : G^n \to G^n, (g_1, \ldots, g_n) \longmapsto (g_{h(1)}, \ldots, g_{h(n)})$$

wird ein Automorphismus von G^n definiert. Die Abbildung

$$\varphi : H \to \mathrm{Aut}(G^n), h \longmapsto \vartheta_h$$

ist ein Gruppenhomomorphismus. Das semidirekte Produkt

$$G \wr_p H := (G^n) \overset{\varphi}{\rtimes} H$$

heißt *Permutations-Kranzprodukt*. Elemente von $G \wr_p H$ werden meistens in der Form (f, h) geschrieben. Dabei ist $h \in H \leq \mathrm{S}_n$ und $f : \{1, \ldots, n\} \to G$ eine Abbildung, die $(g_1, \ldots, g_n) \in G^n$ angibt

Bemerkung 1. $|G \wr_r H| = |G|^{|H|} \cdot |H|$ und $|G \wr_p H| = |G|^n |H|$, wobei $H \leq \mathrm{S}_n$.

2. $G \wr_r H$ ist ein Spezialfall von $G \wr_p H$ (Satz von Cayley).

3. $G \wr_r H$ und $G \wr_p H$ können durchaus verschieden sein. Fr $G \cong \mathbb{Z}_2$ und $H \cong \mathrm{S}_3$ ist $|G \wr_r H| = 2^6 \cdot 6$ und $|G \wr_p H| = 2^3 \cdot 6$, wenn wir H als Permutationsgruppe auf drei Ziffern auffassen. In der Literatur wird meistens $G \wr H$ geschrieben.

2 Zentralisator, Normalisator und Kommutator

2.1 Definition *Zentralisator, Normalisator und Zentrum*
Sei $H \leq G$ und $X \subset G$.

1. $\mathrm{C}_H(X) = \{h \in H \mid h^{-1}xh = x \quad \forall x \in X\}$ (Vertauschung elementweise) heißt *Zentralisator von X in H*. Ist $|X| = 1$, so schreiben wir $\mathrm{C}_H(x)$.

2. $\mathrm{N}_H(X) = \{h \in H \mid h^{-1}Xh = X\}$ (Vertauschung als Menge, d.h. $h^{-1}xh = y \in X$) heißt *Normalisator von X in H*.

3. $\mathrm{Z}(G) := \mathrm{C}_G(G) = \{g \in G \mid g^{-1}xg = x \quad \forall x \in G\}$ (Die Elemente, die mit allen vertauschen) heißt *Zentrum von G*.

2.2 Satz
Sei G Gruppe, $X \subset G$ Teilmenge und $H, U \leq G$. Dann gilt:

1. $\mathrm{C}_H(X)$ *und* $\mathrm{N}_H(X)$ *sind Untergruppen von* H *und* G.
2. $U \lhd G \Leftrightarrow \mathrm{N}_G(U) = G$.
3. $\mathrm{N}_G(U)$ *ist die größte Untergruppe von* G*, in der* U *Normalteiler ist, d.h.:*
   - $U \lhd \mathrm{N}_G(U)$.
   - $U \lhd V \Rightarrow V \leq \mathrm{N}_G(U)$.
4. $\mathrm{Z}(G)$ *ist abelsch.*
5. *Für alle* $X \subset G$ *ist* $\mathrm{Z}(G) \leq \mathrm{C}_G(X) \leq \mathrm{N}_G(X)$.
6. $\mathrm{Z}(G) \operatorname{char} G$.
7. $U \leq \mathrm{Z}(G) \Rightarrow U \lhd G$.
8. $\mathrm{Z}(G) = G \Leftrightarrow G$ *abelsch.*
9. G *abelsch* $\Leftrightarrow G/\mathrm{Z}(G)$ *zyklisch.*
10. $\mathrm{Z}(G_1 \times G_2) = \mathrm{Z}(G_1) \times \mathrm{Z}(G_2)$.

Beweis:
Wir beweisen hier nur die Aussagen 1) und 9), 2) bis 8) und 10) sind trivial und werden dem geneigten Leser überlassen.

1. Seien $u, v \in \mathrm{C}_H(X)$, d.h. $u^{-1}xu = x, v^{-1}xv = x$ für alle $x \in X$. Dann:

   $$(uv)^{-1} x (uv) = v^{-1} \left(u^{-1}xu\right) v = v^{-1}xv = x.$$

   Also ist $uv \in \mathrm{C}_H(X)$. Damit ist $\mathrm{C}_H(X)$ eine Untergruppe. Analog für $\mathrm{N}_H(X)$ (X statt x).

9. Sei zunächst G abelsch. Dann ist $G = \mathrm{Z}(G)$ und daher $|G/\mathrm{Z}(G)| = 1$, also $G/\mathrm{Z}(G)$ zyklisch.

   Sei nun umgekehrt $x \in G$, so dass $G/\mathrm{Z}(G) = \langle x\,\mathrm{Z}(G)\rangle$. Seien $a, b \in G$. Dann existiert $i, j \in \mathbb{N}_0 : a\,\mathrm{Z}(b) = x^i\,\mathrm{Z}(G), b\,\mathrm{Z}(G) = x^j\,\mathrm{Z}(G)$. Also gibt es $w, z \in \mathrm{Z}(G)$, so dass $a = x^i w, b = x^j z$. Damit ist $ab = x^i w x^j z = x^{i+j} zw = x^j z x^i w = ba$, denn w, z vertauschen mit allen Elementen. Also ist G abelsch.

□

2.3 Satz
$G/\operatorname{Z}(G) \cong \operatorname{Inn} G$.

Beweis:
Durch $\psi : G \to \operatorname{Inn} G, g \mapsto .^g$ wird ein Gruppenhomomorphismus definiert, denn es gilt

$$\psi(gh) = .^{gh} = (.^g)^h = \psi(g)\,\psi(h).$$

Weiter gilt:

$$\ker\psi = \{g \in G \mid .^g = \mathrm{id}\} = \left\{g \in G \mid g^{-1}xg = x \quad \forall x \in G\right\} = \operatorname{Z}(G).$$

Weil ψ surjektiv ist, folgt mit dem Homomorphiesatz 0.1

$$G/\operatorname{Z}(G) \cong \operatorname{Inn} G$$

und mit dem vorangegangenen Satz folgt: $\operatorname{Inn} G$ zyklisch $\Rightarrow \operatorname{Inn} G = \{id\}$.
□

2.4 Satz
Sei $U \leq G$. Dann ist

$$\operatorname{C}_G(U) \lhd \operatorname{N}_G(U).$$

und $\operatorname{N}_G(U)/\operatorname{C}_g(U)$ ist isomorph zu einer Untergruppe von $\operatorname{Aut} U$. Ist insbesondere $U \lhd G$, so gilt

$$\operatorname{C}_G(U) \lhd G.$$

Beweis:
Die Abbildung

$$\psi : \operatorname{N}_G(U) \to \operatorname{Aut}(U), a \mapsto (u \mapsto u^a)$$

ist ein Gruppenhomomorphismus. Wegen $U \lhd \operatorname{N}_G(U)$ ist die Abbildung $(u \mapsto u^a) \in \operatorname{Aut} U$. ψ ist ein Homomorphismus, da

$$\psi(ab) = \left(u \mapsto u^{ab}\right) = \left(u \mapsto (u^a)^b\right) = \psi(a)\,\psi(b).$$

Es gilt:

$$\begin{aligned}\ker\psi &= \{a \in \operatorname{N}_G(U) \mid u^a = a \quad \forall a \in U\} = \\ &= \left\{a \in \operatorname{N}_G(U) \mid a^{-1}ua = u \quad \forall u \in U\right\} = \\ &= \operatorname{C}_G(U),\end{aligned}$$

wobei die letzte Gleichung aus $\operatorname{C}_G(U) \leq \operatorname{N}_G(U)$ folgt.

Kerne von Homomorphismen sind Normalteiler, also ist $\operatorname{C}_G(U) \lhd \operatorname{N}_G(U)$. Mit dem Homomorphiesatz 0.1 folgt

$$\operatorname{N}_G(U)/\operatorname{C}_G(U) \cong \operatorname{Im}\psi \leq \operatorname{Aut} U.$$

□

2.5 Satz
Seien $K \leq H \leq G$ Untergruppen von $G, Y \subset X \subset G$ Teilmengen, $g, a \in G$ und $h \in H$. Dann gilt:

1. $\mathrm{C}_H(X)^g = \mathrm{C}_{H^g}(X^g)$, *also* $g^{-1}\mathrm{C}_H(X)\,g = \mathrm{C}_{g^{-1}Hg}(g^{-1}Xg)$.
2. $\mathrm{N}_H(X)^g = \mathrm{N}_{H^g}(X^g)$, *also* $g^{-1}\mathrm{N}_H(X)\,g = \mathrm{N}_{g^{-1}Hg}(g^{-1}Hg)$.
3. $\mathrm{C}_G(g^{-1}ag) = g^{-1}\mathrm{C}_G(a)\,g$.
4. $\mathrm{N}_G(g^{-1}Hg) = g^{-1}\mathrm{C}_G(H)\,g$.
5. $\mathrm{C}_H(h) = \mathrm{C}_G(h) \cap H$.
6. $\mathrm{N}_H(K) = \mathrm{N}_G(K) \cap H$.
7. $\mathrm{C}_H(X) \leq \mathrm{C}_G(X)$.
8. $\mathrm{N}_H(X) \leq \mathrm{N}_G(X)$.
9. $\mathrm{C}_H(X) \leq \mathrm{C}_H(Y)$.
   Die Aussage $\mathrm{N}_H(X) \leq \mathrm{N}_H(Y)$ *ist im Allgemeinen falsch.*

Beweis:
Hier beweisen wir nur den Punkt 1. und bringen ein Gegenbeispiel zur zweiten Aussage von Punkt 9. Denn 2. folgt analog 1., 3. & 4. sind Spezialfälle von 1. & 2. und 5. bis 9. sind sofort aus der Definition 2.1 klar.

1. Es gilt:

$$\begin{aligned} h^g \in \mathrm{C}_{H^g}(X^g) &\Leftrightarrow (h^g)^{-1} x^g h^g = x^g \quad \forall x \in X \\ &\Leftrightarrow g^{-1}h^{-1}gg^{-1}xgg^{-1}hg = g^{-1}xg \quad \forall x \in X \\ &\Leftrightarrow h^{-1}xh = x \quad \forall x \in X \\ &\Leftrightarrow h \in \mathrm{C}_H(X)\,. \end{aligned}$$

9. Gegenbeispiel zur zweiten Aussage: Sei $H = G = \mathrm{S}_4, X = \mathrm{A}_4, Y = \langle(123)\rangle$. Dann ist

$$(34)\,(123)\,(34) = (124) \notin \langle(123)\rangle = Y.$$

   Daher ist $(34) \notin \mathrm{N}_{\mathrm{S}_4}(Y)$ und deshalb $\mathrm{N}_{\mathrm{S}_4}(Y) < \mathrm{S}_4$. Aber $\mathrm{N}_{\mathrm{S}_4}(\mathrm{A}_4) = \mathrm{S}_4$. Widerspruch!

□

2.6 Definition *Konjugationsklasse*
Sei $g \in G, H \leq G$. Die Menge $K := \{h^{-1}gh \mid h \in H\}$ heißt *H-Konjugationsklasse von g*. G-Konjugationsklassen heißen einfach *Konjugationsklassen.*

Bemerkung
H-Konjugation ist eine Äquivalenzrelation, die Äquivalenzklassen sind die H-Konjugationsklassen. Sind $K_1, \ldots, K_r$ alle Konjugationsklassen von G, so gilt:

$$G = \bigcup_{i=1}^{r} K_i,$$

wobei $K_i \cap K_j = \emptyset$ falls $i \neq j$.

2.7 Lemma
Sei $g \in G, H \leq G$. Die H-Konjugationsklasse K von $g \in G$ enthält genau

$$|K| = \frac{|H|}{|\mathrm{C}_H(g)|} = \frac{|H|}{|\mathrm{C}_G(g) \cap H|}$$

Elemente.

Beweis:
Für $a, b \in H$ gilt:

$$\begin{aligned} a^{-1}ga = b^{-1}gb &\Leftrightarrow ba^{-1}g = gba^{-1} \\ &\Leftrightarrow ba^{-1} \in \mathrm{C}_H(g) \Leftrightarrow b \in \mathrm{C}_H(g)\, a. \end{aligned}$$

Damit ist

$$|K| = \frac{|H|}{|\mathrm{C}_H(g)|}.$$

□

2.8 Satz Klassengleichung
Sei $x_1, \ldots, x_r$ eine Transversale der nicht-zentralen Konjugationsklassen von G (das heißt der Klassen, die nicht in $\mathrm{Z}(G)$ liegen). Dann gilt:

$$|G| = \sum_{i=1}^{r} \frac{|G|}{|\mathrm{C}_G(x_i)|} + |\mathrm{Z}(G)|\,.$$

Beweis:
Es gilt:

$$\frac{|G|}{|\mathrm{C}_G(x)|} = 1 \Leftrightarrow G = \mathrm{C}_G(x) \Leftrightarrow x \in \mathrm{Z}(G)\,.$$

Also bildet jedes Element des Zentrums eine eigene Konjugationsklasse. Damit ist

$$G = \bigcup_{i=1}^{r} K(x_i) \cup \mathrm{Z}(G)$$

die disjunkte Vereinigung der $K(x_i)$ mit $\mathrm{Z}(G)$ und die Behauptung folgt aus Lemma 2.7. □

2.9 Definition *p-Gruppe, p′-Gruppe*
Sei p prim. Eine Gruppe G heißt *p-Gruppe*, wenn $|G| = p^n$ für ein $n \in \mathbb{N}$. G heißt p'-Gruppe, wenn $p \nmid |G|$.

2.10 Satz
Jede p-Gruppe hat ein nichttriviales Zentrum, das heißt $Z(G) > \langle 1 \rangle$.

Beweis:
Sei $x_1, \ldots, x_r$ eine Transversale der nicht-zentralen Konjugationsklassen. Nach der Klassengleichung 2.8 gilt:

$$|G| = \sum_{i=1}^{r} \frac{|G|}{|\mathrm{C}_G(x_i)|} + |\mathrm{Z}(G)|.$$

Da die Konjugationsklasse $K(x_i)$ nicht zentral ist, gilt $|K(x_i)| > 1$ (siehe Beweis von 2.8) also ist

$$1 < |K(x_i)| = \frac{|G|}{|\mathrm{C}_G(x_i)|} \mid |G| = p^n$$

und damit ist $p \mid \frac{|G|}{|\mathrm{C}_G(x_i)|}$. In der Klassengleichung sind sowohl die linke Seite als auch die Summanden $\frac{|G|}{|\mathrm{C}_G(x_i)|}$ durch p teilbar und daher ist $p \mid \mathrm{Z}(G)$. □

2.11 Folgerung
Sei p prim. Ist G Gruppe mit $|G| = p^2$*, so gilt:*

$$G \cong \mathbb{Z}_{p^2} \qquad \textit{oder} \qquad G \cong \mathbb{Z}_p \times \mathbb{Z}_p.$$

Beweis:
Nach Satz 2.10 gilt $|\mathrm{Z}(G)| = p$ oder p^2. Ist $|\mathrm{Z}(G)| = p^2$ so ist $g = \mathrm{Z}(G)$ und damit ist G abelsch. Ist $|\mathrm{Z}(G)| = p$, so ist $|G/\mathrm{Z}(G)| = p$, also ist $G/\mathrm{Z}(G) \cong \mathbb{Z}_p$ zyklisch.

Daraus folgt nach 2.2.9 dass G abelsch (und damit $|Z(G)| = p^2$). Mit dem Hauptsatz über endliche abelsche Gruppen 0.5 folgt: G ist direktes Produkt zyklischer Gruppen, dafür gibt es genau die zwei angegebenen Möglichkeiten. □

2.12 Definition *Kommutator*
Seien $g, h \in G, X, Y, Z \subset G$. Man definiert:

1. $[g,h] := g^{-1}h^{-1}gh$ heißt *Kommutator von g und h.*
2. $[X,Y] := \langle [x,y] \mid x \in X, y \in Y \rangle$.
3. $[X,Y,Z] := [[X,Y],Z]$.
4. $G' := \langle [g,h] \mid g,h \in G \rangle = [G,G]$ heißt *Kommutatorgruppe von G.*
5. Iterierte Kommutatorbildung liefert "höhere" Kommutatorgruppen:

$$G'' := [G',G'], \ldots, G^{(n)} := \left[G^{(n-1)}, G^{(n-1)}\right].$$

Beachte: G' ist das Erzeugnis aller Kommutatoren. Die Menge aller Kommutatoren bildet im Allgemeinen keine Untergruppe.

2.13 Lemma Rechenregeln
Wir werden nun einige Rechenregeln zum Kommutator beweisen:

1. $[g,h]^{-1} = [h,g]$.
2. *Ist $\varphi : G \to H$ Gruppenhomomorphismus, so gilt:*

$$\varphi([g,h]) = [\varphi(g), \varphi(h)].$$

   Ist H abelsch, so folgt: $G' \leq \operatorname{Ker} \varphi$.
3. $[g,h]^u = [g^u, h^u]$.
4. $[gh,u] = [g,u]^h [h,u]$.
5. $[u,gh] = [u,h] [u.g]^h$.
6. *Elemente von G' sind Produkte von Kommutatoren.*
7. *Kommutiert $[g,h]$ mit g, so gilt für alle $n \in \mathbb{Z}$: $[g^n,h] = [g,h]^n$.*
8. *Kommutiert $[g,h]$ mit h, so gilt für alle $n \in \mathbb{Z}$: $[g,h^n] = [g,h]^n$.*
9. *Kommutiert $[g,h]$ mit g und h, so gilt für alle $n \in \mathbb{Z}$:*

$$(gh)^n = g^n h^n [g,h]^{\binom{n}{2}}.$$

Beweis:
Auch hier beweisen wir nicht alle Punkte, denn 2. ist klar, wenn man die Homomorphieeigenschaft von φ betrachtet, 3. ist ein Speziallfall von 2. 5. folgt analog 4. und 8. analog zu 7. 6. folgt aus 1.

1. $[g,h]^{-1} = h^{-1}g^{-1}hg = [h,g]$.

4. Es gilt:

$$\begin{aligned}
[g,u]^h [h,u] &= h^{-1}g^{-1}u^{-1}guhh^{-1}u^{-1}u = h^{-1}g^{-1}u^{-1}guu^{-1}hu = \\
&= \left(h^{-1}g^{-1}\right) u^{-1} (gh)\, u = (gh)^{-1} u^{-1} (gh)\, u = \\
&= [gh,u]\,.
\end{aligned}$$

7. Für $n = 0$ und $n = 1$ klar. Induktion über n: Weil $[g,h]$ mit g^{n-1} vertauschbar ist, gilt:

$$\begin{aligned}
[g^n,h] &= \left[gg^{n-1},h\right] \overset{4.}{=} [g,h]^{g^{n-1}} \left[g^{n-1},h\right] = \\
&= [g,h]\,[g,h]^{n-1} = [g,h]^n\,.
\end{aligned}$$

Für $n > 0$ gilt nach *4.* weiter:

$$\begin{aligned}
1 = \left[g^n g^{-n},h\right] &= [g^n,h]^{g^{-n}} \left[g^{-n},h\right] = \left([g,h]^n\right)^{g^{-n}} \left[g^{-n},h\right] = \\
&= [g,h]^n \left[g^{-n},h\right] \\
&\Rightarrow \left[g^{-n},h\right] = [g,h]^{-n}\,.
\end{aligned}$$

9. Induktion über n: $n = 1$ klar. Wir benutzen, dass $[h,g] = [g,h]^{-1}$ mit g und h vertauscht:

$$\begin{aligned}
(gh)^n &= (gh)^{n-1}(gh) = g^{n-1}h^{n-1}\,[h,g]^{\binom{n-1}{2}}\, gh = \\
&= g^{n-1}h^{n-1}gh\,[h,g]^{\binom{n-1}{2}} = \\
&= g^{n-1}gh^{n-1}h^{-(n-1)}g^{-1}h^{n-1}gh\,[h,g]^{\binom{n-1}{2}} = \\
&= g^n h^{n-1}\left[h^{n-1},g\right] h\,[h,g]^{\binom{n-1}{2}} = \\
&\overset{7.}{=} g^n h^{n-1}\,[h,g]^{n-1}\,h\,[h,g]^{\binom{n-1}{2}} = \\
&= g^n h^n\,[h,g]^{n-1+\frac{1}{2}(n-1)(n-2)} = g^n h^n\,[h,g]^{(n-1)\left(1+\frac{1}{2}n-1\right)} = \\
&= g^n h^n\,[h,g]^{\binom{n}{2}}\,.
\end{aligned}$$

□

2.14 Lemma
Seien $U, V \leq G$. Dann gilt:

1. $[U,V] = [V,U]$.
2. $[U,V] \leq U \Leftrightarrow V \leq \mathrm{N}_G(U)$.
3. $[U,V] \lhd \langle U,V \rangle$.

Beweis:

1. klar mit 2.13.1.
2. Sei $v \in V$, dann gilt für alle $u \in U$:
$$[u,v] = u^{-1}\left(v^{-1}uv\right) \in U \Leftrightarrow v^{-1}uv \in U \Leftrightarrow v \in .\,\mathrm{N}_G(U).$$
3. Sei $u, u' \in U, v, v' \in V$. Dann gilt nach 2.13.4 und 2.13.6:
$$\begin{aligned} [u,v]^{v'} &= [u,v']^{-1}[u,vv'] \in [U,V] \\ [u,v]^{u'} &= [uu',v][u',v]^{-1} \in [U,V]. \end{aligned}$$
Also ist $[U,V] \lhd \langle U,V \rangle$.

□

2.15 Satz
Für die Kommutatorgruppe G' von G gilt:

1. *G ist abelsch $\Leftrightarrow G' = \langle 1 \rangle$.*
2. *G' $\mathrm{char}\, G$ (also ist G' insbesondere Normalteiler von G).*
3. *G/G' ist abelsch.*
4. *Für $H \leq G$ gilt: $H \lhd G$ und G/H abelsch $\Leftrightarrow G' \leq H$.*

Beweis:
Hier beweisen wir nur Punkt 4., denn 1. ist klar, 2. auch wegen $[g,h]^\alpha = [\alpha(g), \alpha(h)]$ für alle $\alpha \in \mathrm{Aut}\, G$ und 3. ist ein Spezialfall von 4.

4. Sei $a, b \in G$. Dann folgt aus $(aH)(bH) = (bH)(aH)$:
$$H = (aH)^{-1}(bH)^{-1}(aH)(bH) = \left(a^{-1}b^{-1}ab\right)H.$$
$\Rightarrow a^{-1}b^{-1}ab \in H \Rightarrow G' \leq H$.

Sei nun umgekehrt $G' \leq H \leq G$. Für $g \in G, h \in H$ gilt:

$$g^{-1}Hg = hh^{-1}g^{-1}hg = h\,[h,g] \in HG' = H.$$

$\Rightarrow H \lhd G$. Seien $a, b \in G$, dann gilt:

$$(aH)^{-1}\,(bH)^{-1}\,(aH)\,(bH) = \left(a^{-1}b^{-1}ab\right)H \overset{G' \leq H}{=} H.$$

$\Rightarrow (aH)\,(bH) = (bH)\,(aH) \Rightarrow G/H$ ist abelsch.

□

2.16 Lemma
Sei K eine Konjugationsklasse von G und $h \in K$. Dann gilt: $K \subset hG'$ und insbesondere $|K| \leq |G'|$.

Beweis:
Sei $g \in G$ beliebig. Dann ist $h^{-1}g^{-1}hg \in G'$, also $g^{-1}hg \in hG'$ und damit $K \subset hG'$. Damit ist $|K| \leq |hG'| = |G'|$. □

2.17 Satz
Seien G, H Gruppen, $N \lhd G$ und $U \leq G$. Dann gilt für alle $n \geq 0$:

1. $U^{(n)} \leq G^{(n)}$.
2. $(G/N)^{(n)} = G^{(n)}N/N \cong G^{(n)}/\left(G^{(n)} \cap N\right)$.
3. $(G \times H)^{(n)} = G^{(n)} \times H^{(n)}$.

Beweis:
1. und 3. sind mit Induktion sofort klar.

2. Induktion über n. $n = 0$ klar, $n \to n+1$:

$$(G/N)^{(n+1)} = \left((G/N)^{(n)}\right)' \overset{IV}{=} \left(G^{(n)}N/N\right)'.$$

Für $g \in G^{(n)}$ und $u \in N$ is $guN = gN$. Dann ist

$$\begin{aligned}\left(G^{(n)}N/N\right)' &= \left\langle h_1^{-1}Nh_2^{-1}Nh_1Nh_2N \mid h_1, h_2 \in G^{(n)}\right\rangle = \\ &= \left\langle h_1^{-1}h_2^{-1}h_1h_2N \mid h_1, h_2 \in G^{(n)}\right\rangle = \\ &= \left\langle [h_1,h_2]\,N \mid h_1, h_2 \in G^{(n)}\right\rangle = G^{(n+1)}N/N.\end{aligned}$$

Damit ist die erste Gleichung gezeigt, die zweite folgt aus dem ersten Isomorphiesatz 0.2.

□

Beispiel
Beispiele für charakteristische Untergruppen:

- $\langle 1 \rangle \operatorname{char} G, G \operatorname{char} G$.
- $\mathrm{Z}(G) \operatorname{char} G$.
- $G' \operatorname{char} G$.

2.18 Satz
Sei $A \operatorname{char} G$. *Dann gilt:* $\mathrm{C}_G(A) \operatorname{char} G$.

Beweis:
Sei $\alpha \in \operatorname{Aut} G$. Ist $x \in \mathrm{C}_G(A)$ und $a \in A$, so gilt:

$$\alpha(a) = \alpha\left(x^{-1}ax\right) = \alpha(x)^{-1}\alpha(a)\alpha(x).$$

Durchläuft a die Gruppe A, so durchläuft auch $\alpha(a)$ ganz A. Daher ist $\alpha(x) \in \mathrm{C}_G(A)$, also $\alpha(\mathrm{C}_G(A)) \leq \mathrm{C}_G(A)$ und deshalb $\mathrm{C}_G(A) \operatorname{char} G$. □

2.19 Satz
Sei $H \lhd G$ *mit* $\operatorname{ggT}(|H|, |G/H|) = 1$. *Dann gilt:* $H \operatorname{char} G$

Beweis:
Sei $\alpha \in \operatorname{Aut} G$, $|H| =: m$ und $|G/H| =: n$. Dann ist $|G| = mn$ und $\operatorname{ggT}(m,n) = 1$. Sei $\hat{H} := \alpha(H)$. Wir betrachten $H\hat{H}$: Nach dem 1. Isomorphiesatz 0.2 gilt, dass $H\hat{H} \leq G$. Sei $\left|H \cap \hat{H}\right| =: d$. Dann gilt: $d \mid m$ und nach 1.1 ist

$$\left|H\hat{H}\right| = \frac{|H|\left|\hat{H}\right|}{\left|H \cap \hat{H}\right|} = \frac{m^2}{d} \mid mn.$$

Wegen $\operatorname{ggT}(m,n) = 1$ folgt $d = m$ und somit $H \cap \hat{H} = H$, also $\hat{H} = H$ und daher $\alpha(H) = H$. □

2.20 Satz
Seien $A, B \leq G$. *Dann gilt:*

1. $A \operatorname{char} G \Rightarrow A \lhd G$.
2. $A, B \lhd G \Rightarrow A \cap B \lhd G, AB \lhd G$.
   $A, B \operatorname{char} G \Rightarrow A \cap B \operatorname{char} G, AB \operatorname{char} G$.

3. $A \operatorname{char} B \lhd G \Rightarrow A \lhd G$.
   $A \operatorname{char} B \operatorname{char} G \Rightarrow A \operatorname{char} G$.

4. *Vorsicht:*

$$\begin{aligned} A \lhd B \operatorname{char} G &\overset{i.A.}{\not\Rightarrow} A \lhd G. \\ A \lhd B \lhd G &\overset{i.A.}{\not\Rightarrow} A \lhd G. \\ A \leq B \leq G, A \operatorname{char} G &\overset{i.A.}{\not\Rightarrow} A \operatorname{char} B. \end{aligned}$$

5. *Sei $A \leq B \leq G$. Im Fall $A \lhd G$ gilt: $B/A \lhd G/A \Leftrightarrow B \lhd G$.*

   Im Fall $A \operatorname{char} G$ gilt: $B/A \operatorname{char} G/A \Rightarrow B \operatorname{char} G$.

   Die Umkehrung, aus $B \operatorname{char} G$ folgt $B/A \operatorname{char} G/A$, gilt im Allgemeinen nicht.

Beweis:
Punkt 4 bleibt dem Leser als Übungsaufgabe überlassen.

1. $A \operatorname{char} G \Rightarrow \alpha(A) = A$ für alle $\alpha \in \operatorname{Aut} G$. Daher gilt auch $\alpha(A) = A$ für alle $\alpha \in \operatorname{Inn} G \Leftrightarrow A \lhd G$.

2. Sei $\alpha \in \operatorname{Aut} G$. Dann folgt: $\alpha(A \cap B) = \alpha(A) \cap \alpha(B)$ wegen der Bijektivität und $\alpha(AB) = \alpha(A)\alpha(B)$, weil α ein Homomorphismus ist. Die Behauptung folgt, wenn wir einmal alle $\alpha \in \operatorname{Aut} G$ und einmal alle $\alpha \in \operatorname{Inn} G$ betrachten.

3. Sei $\alpha \in \operatorname{Aut} G$ mit $\alpha(B) = B$. Dann ist $\alpha_{|B} \in \operatorname{Aut} B$ und folglich auch $\alpha_{|B}(A) = A$. Also ist $\alpha(A) = A$.

5. Die erste Aussage ist der Korrespondenzsatz 1.4. Sei also nun $A \operatorname{char} G$ und $B/A \operatorname{char} G/A$. Sei Λ ein Vertretersystem der Nebenklassen von A in B. Dann ist $B = \bigcup_{\lambda \in \Lambda} \lambda A$. Sei $\alpha \in \operatorname{Aut} G$, dann:

$$\begin{aligned} \alpha(B) &= \alpha\left(\bigcup_{\lambda \in \Lambda} \lambda A\right) = \bigcup_{\lambda \in \Lambda} \alpha(\lambda A) = \\ &= \bigcup_{\lambda \in \Lambda} \alpha(\lambda)\alpha(A) \overset{1.4}{=} \bigcup_{\lambda \in \Lambda} \alpha(\lambda) A. \end{aligned}$$

   Weil $A \operatorname{char} G$, wird durch $\bar{\alpha} : G/A \to G/A, gA \mapsto \alpha(g)A$ ein Automorphismus von G/A gegeben. Ist $g_1 A = g_2 A$, so ist $g_1^{-1} g_2 \in A$ und daher $\alpha\left(g_1^{-1} g_2\right) = \alpha(g_1)^{-1} \alpha(g_2) \in A$ und folglich $\alpha(g_1) A = \alpha(g_2) A$, das heißt $\bar{\alpha}$ ist wohldefiniert. Die Bijektivität von $\bar{\alpha}$ folgt aus der Bijektivität von α. Nach Voraussetzung gilt $\bar{\alpha}(B/A) = B/A$. Daher ist

$\alpha(\lambda) A = \bar{\alpha}(\lambda A) \in B/A$ und demnach $\alpha(\lambda) \in B$. Also ist $\alpha(B) \leq B$ und daher $B \operatorname{char} G$.

□

2.21 Folgerung
Für alle $n \in \mathbb{N}$ gilt: $G^{(n)} \operatorname{char} G$.

Beweis:
$G^{(n)} \operatorname{char} G^{(n-1)}$, Induktion und 2.20.3.

2.22 Satz
Sei G eine Gruppe, die außer G und $\langle 1 \rangle$ keine charakteristischen Untergruppen enthält. Dann ist G einfach oder ein direktes Produkt von isomorphen einfachen Gruppen.

Beweis:
Sei $H > \langle 1 \rangle$ ein minimaler Normalteiler von G. Wir schreiben $H_1 = H$ und betrachten alle Untergruppen von G von der Form $H_1 \times \ldots \times H_n$ mit $H_i \cong H_i'$ und $H_i \lhd G$. Sei M eine solche Untergruppe mit maximaler Ordnung. Wir zeigen $H = G$, indem wir zeigen, dass $H \operatorname{char} G$:

Sei $\alpha \in \operatorname{Aut} G$. Es genügt zu zeigen, dass $\alpha(H_i) \subseteq M$ für alle i. Offensichtlich ist $\alpha(H_i) \cong H \cong H_1$. Weiter gilt $\alpha(H_i) \lhd G$. Ist $a \in G$, so existiert ein $b \in G$ mit $\alpha(b) = a$. Damit ist

$$a^{-1} \alpha(H_i)\, a = \alpha(b)^{-1}\, \alpha(H_i)\, \alpha(b) = \alpha\left(b^{-1} H_i b\right) = \alpha(H_i).$$

Ist $\alpha(H_i) \not\leq M$, so ist $|\alpha(H_i) \cap M| < |H_i|$ und wegen $\alpha(H_i) \lhd G, M \lhd G$ ist $\alpha(H_i) \cap M \lhd G$. Da H minimaler Normalteiler war, folgt $\alpha(H_i) \cap M = \langle 1 \rangle$. Damit ist $\langle \alpha(H_i), M \rangle \cong M \times \alpha(H_i)$ ein direktes Produkt von derselben Form wie M, aber mit größerer Ordnung. Widerspruch!

Damit folgt $\alpha(H_i) \leq M$ und somit $M \operatorname{char} G$, nach Voraussetzung also $M = G$. H ist einfach: Wäre $N \lhd H$ ein nichttrivialer Normalteiler, so wäre auch $N \lhd H_1 \times \ldots \times H_n = G$. Widerspruch zur Minimalität von H. □

3 Der Satz von Sylow

3.1 Satz
Sei p prim und G abelsche Gruppe mit $p \mid |G|$. Dann enthält G eine Untergruppe der Ordnung p.

Beweis:
Nach Lemma 1.1 gilt: $|AB| \mid |A|\,|B|$ fi¿$\frac{1}{2}$r Untergruppen A, B von G. Weil G abelsch ist, ist AB eine Untergruppe von G. Daher folgt durch Induktion über die Anzahl der Faktoren: Sind $A_1, \ldots, A_k$ Untergruppen von G, so gilt:

$$|A_1 \cdot \ldots \cdot A_k| \mid |A_1| \cdot \ldots \cdot |A_k|\,.$$

Für jedes $g \in G$ ist $\langle g \rangle$ eine zyklische Untergruppe von G und das Produkt all dieser Untergruppen ist G. Also folgt:

$$|G| \mid \prod_{g \in G} \operatorname{ord} g.$$

Daher gibt es ein $g \in G$ mit $p \mid \operatorname{ord} g$; setze $a := \frac{\operatorname{ord} g}{p}$. Dann it $\operatorname{ord}(g^a) = p$ und $\langle g^a \rangle \leq G$ mit $\langle g^a \rangle = p$. □

3.2 Definition *Sylowgruppe*
Sei p prim und $|G| = p^a m$ mit $p \nmid m$. Die Untergruppen $P \leq G$ mit $|P| = p^a$ heißen *p-Sylowgruppen von G*. Die Menge der p-Sylowgruppen wird mit $\operatorname{Syl}_p G$ bezeichnet.

3.3 Satz Satz von Cauchy
Sei p prim, $i \in \mathbb{N}_0$, so dass $p^i \mid |G|$. Dann enthält G eine Untergruppe der Ordnung p^i.

Beweis:
Beweis durch Induktion über die Gruppenordnung $|G|$. Sei die Behauptung schon für alle Gruppen kleinerer Ordnung bewiesen. Besitzt G eine Untergruppe $V < G$ mit $p^i \mid |V|$, so besitzt V eine Untergruppe der Ordnung p^i und damit auch G. Wir können dann annehmen, dass G keine solche Untergruppe V besitzt und betrachten die Klassengleichung 2.8:

$$|G| = \sum_{j=1}^{r} \frac{|G|}{|\mathrm{C}_G(x_j)|} + |\mathrm{Z}(G)|\,.$$

Die linke Seite $|G|$ ist durch p^i teilbar. Wegen $p^i \nmid |\mathrm{C}_G(x_j)|$ sind alle Summanden $\frac{|G|}{|\mathrm{C}_G(x_j)|}$ durch p teilbar. Damit folgt $p \mid |\mathrm{Z}(G)|$. Mit 3.1 folgt: Weil $\mathrm{Z}(G)$ abelsch, enthält $\mathrm{Z}(G)$ eine Untergruppe N der Ordnung p. Nach 2.2.7 gilt: $N \lhd G$. Die Ordnung der Faktorgruppe G/N ist kleiner als $|G|$, also gibt es nach Induktionsvoraussetzung eine Untergruppe $B/N \leq G/N$ mit $|B/N| = p^{i-1}$. Nach dem Korrespondenzsatz **??** gibt es eine Untergruppe

B mit $N \leq B \leq G$, so dass $\nu(B) = B/N$ ($\nu : G \to G/N$ kanonischer Epimorphismus). Es gilt:

$$|B| = |B/N|\,|N| = p^i.$$

□

3.4 Folgerung
Sei $M \leq G$ maximale Untergruppe. Gilt $M \lhd G$, so ist $[G : M]$ eine Primzahl.

Beweis:
Weil M maximal ist, gilt $M < G$ und es gibt kein $U \leq G : M < U < G$. Nach dem Korrespondenzsatz 1.4 besitzt daher die Faktorgruppe G/M keine nichttriviale Untergruppe. Da $|G/M| > 1$ existiert eine Primzahl p mit $p \nmid |G/M|$. Nach dem Satz von Cauchy **??** folgt: G/M besitzt eine Untergruppe der Ordnung p. Daher muss $p = |G/M|$ gelten. □

3.5 Lemma

1. *Ist $P \in \mathrm{Syl}_p G$ und $P \leq G$ eine p-Untergruppe mit $BP = PB$, dann gilt: $B \leq P$. Insbesondere ist P die einzige p-Sylowgruppe von $\mathrm{N}_G(P)$.*
2. *Ist $\alpha \in \mathrm{Aut}(G)$ und $P \in \mathrm{Syl}_p G$, so ist auch $\alpha(P) \in \mathrm{Syl}_p G$.*
3. *Für $P \in \mathrm{Syl}_p G$ gilt: $P \lhd G \Leftrightarrow \mathrm{Syl}_p G = \{P\} \Leftrightarrow P \,\mathrm{char}\, G$.*
4. *$\mathcal{O}_p(G) := \bigcap_{P \in \mathrm{Syl}_p G} P \,\mathrm{char}\, G$ und $\mathcal{O}_p(G)$ enthält alle p-Normalteiler von G, das heißt alle Normalteiler N mit Ordnung $p^k, k \in \mathbb{N}$.*

Beweis:

1. Nach Lemma **??** gilt: BP ist eine Untergruppe von G, und zwar eine p-Gruppe. Da offensichtlich $P \leq BP$ und $P \in \mathrm{Syl}_p G$ folgt: $P = BP$ und damit $B \leq P$. In $\mathrm{N}_G(P)$ gilt:

   $$xP = Px \qquad \forall x \in \mathrm{N}_G(P).$$

   Ist also $B \leq \mathrm{N}_G(P)$ eine p-Untergruppe, so folgt $BP = PB$.

2. Ist $\alpha \in \mathrm{Aut}(G)$, so gilt $|P| = |\alpha(P)|$, also ist auch $\alpha(P)$ eine p-Sylowgruppe.

3. Sei $Q \leq G$ eine weitere p-Sylowgruppe. Wegen $P \lhd G$ ist dann $PQ = QP$ und mit 1. folgt: $Q = P$.

   Für $\alpha \in \mathrm{Aut}(G)$ ist $\alpha(P)$ eine p-Sylowgruppe (nach 2.) und daher $\alpha(P) = P$.

   Der Rest folgt aus 2.20.1

4. Für $\alpha \in \mathrm{Aut}(G)$ gilt: Jede p-Sylow wird wieder auf eine p-Sylow abgebildet. Also ist $\alpha(\mathcal{O}_p(G)) = \mathcal{O}_p(G)$. Ist $B \lhd G$ p-Normalteiler und $P \in \mathrm{Syl}_p G$, so gilt: $BP = PB$ nach dem 1. Isomorphiesatz 0.2. Nach 1. folgt $B \leq P$. Folglich ist B in allen p-Sylowgruppen enthalten und damit $B \leq \mathcal{O}_p(G)$.

□

3.6 Definition $\mathcal{O}_{p'}(G), \mathcal{O}(G)$
Der größte Normalteiler $N \lhd G$ mit $p \nmid |N|$ wird mit $\mathcal{O}_{p'}(G)$ bezeichnet. Statt $\mathcal{O}_{2'}(G)$ schreibt man oft kurz $\mathcal{O}(G)$.

3.7 Lemma

1. *$\mathcal{O}_{p'}(G)$ enthält alle p'-Normalteiler von G, das heißt alle $N \lhd G$ mit $p \nmid |N|$.*
2. *$\mathcal{O}_{p'}(G)$ char G.*
3. *$\mathcal{O}_p(G/\mathcal{O}_p(G)) = \langle 1 \rangle, \mathcal{O}_{p'}(G/\mathcal{O}_{p'}(G)) = \langle 1 \rangle$.*

Beweis:

1. Seien $N, U \lhd G$ mit $p \nmid |N|, |U|$. Für $g \in G$ ist
$$g^{-1}NUg = g^{-1}Ngg^{-1}Ug = NU.$$
Also ist $NU \lhd G$ und nach 1.1 gilt: $|NU| \mid |N||U|$, das heißt es gilt $p \nmid |NU|$.
Folglich ist für jeden p'-Normalteiler N die Gruppe $N\mathcal{O}_{p'}(G) \lhd G$ mit $p \nmid |N\mathcal{O}_{p'}(G)|$ und $\mathcal{O}_{p'}(G) \leq N\mathcal{O}_{p'}(G)$. Nach Definition folgt $N\mathcal{O}_{p'}(G) = \mathcal{O}_{p'}(G)$ und damit $N \leq \mathcal{O}_{p'}(G)$.
2. Ist $\alpha \in \mathrm{Aut}(G)$, so gilt $\alpha(\mathcal{O}_{p'}(G)) \lhd G$ und
$$|\alpha(\mathcal{O}_{p'}(G))| = |\mathcal{O}_{p'}(G)|.$$
Nach 1. folgt
$$\alpha(\mathcal{O}_{p'}(G)) = \mathcal{O}_{p'}(G).$$
3. Enthält $G/\mathcal{O}_p(G)$ einen nichttrivialien p-Normalteiler $N/\mathcal{O}_p(G)$, so gibt es nach dem Korrespondenzsatz 1.4 ein $N \lhd G$ mit $\mathcal{O}_p(G) \leq N \leq G$ und $\nu(N) = N/\mathcal{O}_p(G)$ (ν kanonischer Epimorphismus). Es gilt:
$$|N| = |N/\mathcal{O}_p(G)|\,|\mathcal{O}_p(G)|$$
ist p-Potenz. Widerspruch!
Für $\mathcal{O}_{p'}(G)$ analog.

□

3.8 Lemma
Seien $P, H \leq G$. Dann gibt es $\frac{|H|}{|\mathrm{N}_H(P)|}$ verschiedene H-Konjugierte von P in G.

Beweis:
Analog zu 2.7. Für $a, b \in H$ gilt:

$$a^{-1}Pa = b^{-1}Pb \Leftrightarrow ba^{-1}Pab^{-1} = P \Leftrightarrow ab^{-1} \in \mathrm{N}_H(P) \Leftrightarrow a \in \mathrm{N}_H(P)\, b.$$

Das heißt a, b liegen in derselben Rechtsnebenklasse von $\mathrm{N}_H(P)$. □

3.9 Lemma
Sei H eine p-Untergruppe von G und $P \in \mathrm{Syl}_p G$. Dann gilt:

$$H \cap \mathrm{N}_G(P) = H \cap P$$

Beweis:
$H \cap \mathrm{N}_G(P) \supset H \cap P$ ist klar wegen $P \leq \mathrm{N}_G(P)$. Wir zeigen nun $H \cap \mathrm{N}_G(P) \subset H \cap P$. $H \cap \mathrm{N}_G(P)$ ist eine p-Untergruppe von $\mathrm{N}_G(P)$. Wegen $P \lhd \mathrm{N}_G(P)$ gilt:

$$(H \cap \mathrm{N}_G(P))\, P = P\, (H \cap \mathrm{N}_G(P)).$$

Nach 3.5.1 folgt:

$$H \cap \mathrm{N}_G(P) \leq P$$

und damit

$$H \cap \mathrm{N}_G(P) \leq H \cap P.$$

□

Damit können wir den wichtigsten Satz der Gruppentheorie beweisen:

3.10 Satz Satz von Sylow
Sei p prim und $|G| = p^a m$ mit $p \nmid m$. Es gilt:

1. *Jede p-Untergruppe von G ist in einer p-Sylowgruppe von G enthalten.*
2. *Alle p-Sylowgruppen von G sind konjugiert und für $P \in \mathrm{Syl}_p G$ gilt:*

$$\left|\mathrm{Syl}_p G\right| = \frac{|G|}{|\mathrm{N}_G(P)|}.$$

3. *Es gilt:*

$$\left|\mathrm{Syl}_p G\right| \mid |G| \quad \textit{und} \quad \left|\mathrm{Syl}_p G\right| \equiv 1 \mod p.$$

Genauer: $\left|\mathrm{Syl}_p G\right| \mid m$. Insbesondere gibt es eine p-Sylowgruppe in G.

Beweis:

1. Beweisen wir zusammen mit

2. Sei $P \in \mathrm{Syl}_p G$. Wir betrachten die Menge $M := \{x^{-1}Px \mid x \in G\}$ der Konjugierten von P. Nach 3.8 gilt: $|M| = \frac{|G|}{|\mathrm{N}_G(P)|}$. Weil $P \leq \mathrm{N}_G(P)$, teilt p nicht $\frac{|G|}{|\mathrm{N}_G(P)|}$. Sei $H \leq G$ eine p-Untergruppe. Wir betrachten die H-Konjugationen auf M. Sei $\left\{x_1^{-1}Px_1, \ldots, x_r^{-1}Px_r\right\}$ eine Transversale der H-Konjugationsklassen. Die H-Konjugationsklasse, die $x^{-1}Px$ enthält, hat nach 3.8 genau $\frac{|H|}{|\mathrm{N}_H(x^{-1}Px)|}$ Elemente. Insbesondere ist die Zahl dieser Elemente ein Teiler von $|H|$, also eine p-Potenz. M ist die disjunkte Vereinigung der H-Konjugationsklassen, also folgt:

$$\frac{|G|}{|\mathrm{N}_G(P)|} = |M| = \sum_{i=1}^{r} \frac{|H|}{\left|\mathrm{N}_H\left(x_i^{-1}Px_i\right)\right|}.$$

   p teilt nicht $\frac{|G|}{|\mathrm{N}_G(P)|}$ und

$$p \nmid \frac{|H|}{\left|\mathrm{N}_H\left(x_i^{-1}Px_i\right)\right|} \Leftrightarrow H = \mathrm{N}_H\left(x_i^{-1}Px_i\right).$$

   Weil die linke Seite nicht durch p teilbar ist, muss es ein $i \in \{1, \ldots, r\}$ geben, so dass $H = \mathrm{N}_H\left(x_i^{-1}Px_i\right)$. Damit ist $H \leq \mathrm{N}_G\left(x_i^{-1}Px_i\right)$ und folglich

$$H\left(x_i^{-1}Px_i\right) = \left(x_i^{-1}Px_i\right)H.$$

   Mit 3.5.1 folgt $H \leq x_i^{-1}Px_i$. Ist H eine beliebige p-Untergruppe von G, so ist H demnach in einer p-Sylowgruppe enthalten. Ist H eine p-Sylowgruppe, so ist $H = x_i^{-1}Px_i$, das heißt H ist konjugiert zu P. Damit ist auch $\mathrm{Syl}_p G = M$ und daher

$$\left|\mathrm{Syl}_p G\right| = \frac{|G|}{|\mathrm{N}_G(P)|}.$$

3. Setzen wir im ersten Teil $H = P$, so ergibt sich

$$\begin{aligned}\left|\mathrm{Syl}_p G\right| &= |M| = \sum_{i=1}^{r} \frac{|P|}{\left|\mathrm{N}_P\left(x_i^{-1}Px_i\right)\right|} = \\ &\overset{2.5}{=} \sum_{i=1}^{r} \frac{|P|}{\left|P \cap \mathrm{N}_G\left(x_i^{-1}Px_i\right)\right|} \overset{3.9}{=} \sum_{i=1}^{r} \frac{|P|}{\left|P \cap \left(x_i^{-1}Px_i\right)\right|}.\end{aligned}$$

Bei den Summanden $\left|P \cap \left(x_i^{-1} P x_i\right)\right|$ gibt es genau einen Summanden 1 (nämlich für $x_i^{-1} P x_i = P$), sonst ist

$$P \cap x_i^{-1} P x_i < P$$

und daher $p \mid \frac{|P|}{\left|P \cap \left(x_i^{-1} P x_i\right)\right|}$. Insgesamt folgt

$$\left|\mathrm{Syl}_p G\right| \equiv 1 \mod p.$$

Dass $\left|\mathrm{Syl}_p G\right| \mid |G|$ (genauer: $\left|\mathrm{Syl}_p G\right| \mid m$) haben wir bereits im 1. Teil gezeigt.

□

Bemerkung
Der Satz von Sylow ist der vielleicht wichtigste Satz der Gruppentheorie, weil er einen ersten Ansatzpunkt liefert, die Struktur der Gruppe näher zu untersuchen. In einigen Spezialfällen genügt er (mit einigen kleinen zusätzlichen Resultaten) sogar schon, um alle Gruppen mit einer bestimmten Ordnung zu klassifizieren. Naturgemäß ist der Satz von Sylow jedoch keine Hilfe bei der Untersuchung von p-Gruppen.

Die Bedeutung des Satzes legt die Frage nahe, ob er sich verallgemeinern lässt. Tatsächlich gibt es zwei Resultate, die dies in bestimmte Richtungen tun:

- Sei $|G| = p^a m$ mit $p \nmid m$ und sei $s \in \mathbb{N}_0$ mit $0 \leq s \leq a$. Sei r_s die Anzahl der Untergruppen von G mit Ordnung p^s. Dann gilt:

$$r_s \equiv 1 \mod p.$$

- Satz von Hall: Sei G *auflösbar* und $|G| = ab$ mit $\mathrm{ggT}\,(a, b) = 1$. Dann enthält G Untergruppen der Ordnung a und alle diese Untergruppen sind konjugiert.

3.11 Folgerung
Sei $P \in \mathrm{Syl}_p G, \mathrm{N}_G(P) \leq U \leq G$. *Dann gilt*

1. $\mathrm{N}_G(U) = U$.
2. $[G : U] = 1 \mod p$.

Beweis:

1. Sei $x \in \mathrm{N}_G(U)$, das heißt $x^{-1}Ux = U$. Dann gilt:

$$x^{-1}Px \leq x^{-1}\,\mathrm{N}_G(P)\,x \leq x^{-1}Ux \leq U.$$

   Also ist auch $x^{-1}Px$ eine p-Sylowgruppe und U, das heißt P und $x^{-1}Px$ sind in U konjugiert (als p-Sylowgruppe von U). Daher gibt es ein $u \in U$, so dass

$$u^{-1}\left(x^{-1}Px\right)u = P.$$

   Folglich ist $xu \in \mathrm{N}_G(P) \leq U$ und damit $x \in U$.

2. P ist eine p-Sylowgruppe von U. Wegen $\mathrm{N}_G(P) \leq U$ ist $\mathrm{N}_U(P) = \mathrm{N}_G(P)$. Mit dem Satz von Sylow 3.10 folgt

$$[U : \mathrm{N}_G(P)] \equiv 1 \mod p.$$

   Ebenfalls nach dem Satz von Sylow 3.10 ist aber auch

$$[G : U]\,[U : \mathrm{N}_G(P)] = [G : \mathrm{N}_G(P)] \equiv 1 \mod p.$$

   Deshalb ist $[G : U] \equiv 1 \mod p$

□

3.12 Folgerung
Sei $N \lhd G$ und $P \in \mathrm{Syl}_p G$. Dann ist $P \cap N \in \mathrm{Syl}_p N$ und $PN/N \in \mathrm{Syl}_p(G/N)$. Beachte: Ist nur $N \leq G$, so gilt die erste Aussage im Allgemeinen nicht.

Beweis:
Sei R eine p-Sylowgruppe von N. Nach dem Satz von Sylow 3.10 ist R in einer p-Sylowgruppe P_1 von G enthalten und es gibt ein $x \in G$ mit $x^{-1}P_1x = P$. Da R die maximale p-Gruppe von N ist, so ist $P_1 \cap N = R \cap N = R$. Nun gilt

$$P \cap N = x^{-1}P_1x \cap N \overset{N \lhd G}{=} x^{-1}P_1x \cap x^{-1}Nx = x^{-1}P_1 \cap Nx = x^{-1}Rx.$$

Daraus folgt:

$$|P_1 \cap N| = \left|x^{-1}Rx\right| = |R| \Rightarrow P \cap N \in \mathrm{Syl}_p N.$$

Sei $\overline{U} := PN/N \leq G/N =: \overline{G}$ ($N \lhd PN$ nach dem 1. Isomorphiesatz 0.2). Sei $|G| = p^a g, |N| = p^b n, p \nmid g, n$. Nach der ersten Aussage des Satzes

ist dann $P \cap N$ eine p-Sylowgruppe von N, also gilt $|P \cap N| = p^b$. Mit 1.1 folgt:

$$|PN| = \frac{|P|\,|N|}{|P \cap N|} = \frac{p^a p^b n}{p^b} = p^a n$$

und damit

$$\left|\overline{U}\right| = |PN/N| = \frac{p^a n}{p^b n} = p^{a-b}.$$

Wegen $|G/N| = \frac{p^a g}{p^b n} = p^{a-b}\frac{g}{n}$ ist $\overline{U}$ eine p-Sylowgruppe von $\overline{G}$. □

3.13 Bemerkung
Sei $|G| = p_1^{a_1} \cdot \ldots \cdot p_k^{a_k}$ die Primfaktorzerlegung der Ordnung von $G, P_i \in \mathrm{Syl}_{p_i} G$. Dann ist $G = \langle P_1, \ldots, P_k \rangle$.

Beweis:
Sei $G_1 := \langle P_1, \ldots, P_k \rangle \Rightarrow P_i \leq G_1; |G_1| = |G|$. Daraus folgt Behauptung. □

3.14 Satz Zerlegung von Gruppenelementen
Sei $g \in G$ mit $\operatorname{ord} G = p_1^{a_1} \cdot \ldots \cdot p_k^{a_k}$. Dann gibt es eindeutig bestimmte Elemente $g_1, \ldots, g_k$ mit $\operatorname{ord} g_i = p_i^{a_i}$, so dass $g = g_1 \cdot \ldots \cdot g_k$ und $g_i g_j = g_j g_i$. Die g_i sind Potenzen von g, das heißt $g_i \in \langle g \rangle$.

Beachte*: Die Zerlegung $g = g_1 \cdot \ldots \cdot g_k$ mit $\operatorname{ord} g_i = p_i^{a_i}$ ist nicht eindeutig.*

Beweis:
Sei $p := p_1^{a_1}$ und $q = \prod_{i=2}^{k} p_i^{a_i}$. Wegen $\mathrm{ggT}\,(p, q) = 1$ gibt es $x, y \in \mathbb{Z}$ mit $xp + yq = 1$. Wir setzen $g_1 := g^{yq}, g_2' := g^{xp}$. Dann ist

$$\begin{aligned} g_1^p &= (g^{yq})^p = (g^{pq})^{y'} = 1^y = 1 \Rightarrow \operatorname{ord} g_1 = p = p_1^{a_1} \\ (g_2')^q &= (g^{xp})^q = (g^{pq})^x = 1^x = 1 \Rightarrow \operatorname{ord} g_2' = q \end{aligned}$$

Zerlege nun g_2' in $k-1$ Schritten weiter. Dann erhalten wir schließlich eine Zerlegung $g = g_1 \cdot \ldots \cdot g_k$ mit $\operatorname{ord} g_i = p_i^{a_i}$. Alle g_i sind Potenzen von g (g_2' ist Potenz von g, g_2 ist Potenz von g_2' und damit auch von g usw.). Also gilt $g_i g_j = g_j g_i$.

Eindeutigkeit: Sei $g = g_1 g_2' = g_3 g_4$ mit $\operatorname{ord} g_1 = \operatorname{ord} g_3 = p, \operatorname{ord} g_2' = \operatorname{ord} g_4 = q$ und

$$g_1 g_2' = g_2' g_1 = g = g_3 g_4 = g_4 g_3.$$

Dann vertauschen die Elemente g_1, g_2', g_3, g_4 auch mit g, da z.B.

$$g_3^{-1} g g_3 = g_3^{-1} g_3 g_4 g_3 = g_4 g_3 = g.$$

Da g_3, g_4 mit g vertauschen, vertauschen sie auch mit den Potenzen g_1, g_2' von g. Dann gilt $g_3^{-1} g_1 = g_4 g_2'^{-1}$ und

$$\left(g_3^{-1} g_1\right)^p = \left(g_3^{-1}\right)^p g_1^p = 1 = g_4^q \left(g_2'^{-1}\right)^q = \left(g_4 g_2'^{-1}\right)^q$$

und wegen $\mathrm{ggT}\,(p,q)=1$ ist damit $g_3^{-1}g_1 = 1 = g_4 g_2'^{-1}$. Also ist $g_1 = g_3, g_4 = g_2'$. □

3.15 Definition *Exponent*
Der *Exponent* $\exp G$ einer Gruppe G ist die kleinste Zahl $m \in \mathbb{N}$ mit $g^m = 1$ für alle $g \in G$. Mit anderen Worten:

$$\exp G = \operatorname*{kgV}_{g \in G} (\operatorname{ord} g)$$

3.16 Folgerung
Sei $|G| = p_1^{a_1} \cdot \ldots \cdot p_n^{a_n}$ *und sei* $P_i \in \mathrm{Syl}_p G$. *Dann gilt:*

$$\exp G = \prod_{i=1}^{n} \exp P_i$$

Beweis:
Dass $\prod_{i=1}^{n} \exp P_i \mid \exp G$ ist klar, denn die $\exp P_i$ sind paarweise teilerfremd und für $U \leq G$ gilt $\exp U \mid \exp G$. Sei $g \in G$ mit $\operatorname{ord} g = p_1^{b_1} \cdot \ldots \cdot p_n^{b_n}$. Nach 3.14 gibt es $g_i \in G$ mit $\operatorname{ord} g_i = p_i^{b_i}$, so dass $G = g_1 \cdot \ldots \cdot g_n$. Nach dem Satz von Sylow 3.10 ist g_i in einer p-Sylowgruppe enthalten und daher $p_i^b = \operatorname{ord} g_i \mid \exp P_i$. Damit teilt $\operatorname{ord} g$ das Produkt $\prod_{i=1}^{n} \exp P_i$ und es gilt

$$\exp G \mid \exp P_i$$

□

Bemerkung *Alperin und Kuo*
Für jede Gruppe G gilt:

$$\exp G \mid [G : G' \cap \mathrm{Z}(G)]$$

4 Automorphismengruppen zyklischer Gruppen

4.1 Definition *Eulersche φ–Funktion*

1. $\varphi(u) := \#\{m \in \mathbb{N} \mid \mathrm{ggT}\,(n,m) = 1\}$ heißt *Eulersche φ-Funktion.*
2. Die multiplikative Gruppe des Rings $(\mathbb{Z}_n, +, \cdot)$ bezeichnen wir mit $\mathbb{Z}_n^*$. $|\mathbb{Z}_n^*| = \varphi(n)$, da $m \in \mathbb{Z}_n^* \Leftrightarrow \mathrm{ggT}\,(m,n) = 1$.

Bemerkung
Der Satz von Lagrange liefert sofort den Satz von Euler-Fermat: Für $\mathrm{ggT}(x,n)=1$ gilt:

$$x^{\varphi(n)} \equiv 1 \mod n.$$

4.2 Satz
Für $n \in \mathbb{Z}$ gilt:

$$\mathrm{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^*.$$

Beweis:
Sei $\mathbb{Z}_n = \langle g \rangle$. Jedes $\alpha \in \mathrm{Aut}\, G$ ist bereits eindeutig festgelegt durch $\alpha(g)$. Offensichtlich ist $\alpha(g) = g^k$ für ein $k \in \mathbb{N}$ mit $1 \leq k \leq n$. Weil α ein Automorphismus ist, gilt:

$$n = \mathrm{ord}\, g = \mathrm{ord}\, \alpha(g) = \mathrm{ord}\, g^k = \frac{n}{\mathrm{ggT}(n,k)}.$$

Daher ist $\mathrm{ggT}(n,k)=1$ und folglich $\overline{k} \in \mathbb{Z}_n^*$. Für $\overline{k} \in \mathbb{Z}_n^*$ ist

$$\alpha_k : \mathbb{Z}_n \to \mathbb{Z}_n, x \mapsto x^k$$

ein Automorphismus. Wir setzen:

$$\psi : \mathrm{Aut}(\mathbb{Z}_n) \to \mathbb{Z}_n^*, \alpha_k \mapsto \overline{k}.$$

Für $k, i \in \mathbb{Z}_n^*$ ist

$$(\alpha_k \circ \alpha_i)(g) = \alpha_k\left(g^i\right) = g^{ik} = g^{ki} = \alpha_{ki}(g).$$

Und damit ist

$$\psi(\alpha_k \circ \alpha_i)(g) = \psi(\alpha_{ki}) = \overline{ki} = \overline{k} \cdot \overline{i} = \psi(\alpha_k)\,\psi(\alpha_i)$$

Das heißt: ψ ist ein Homomorphismus. Die Bijektivität ist klar. □

4.3 Satz

1. $\mathrm{Aut}\, G \times \mathrm{Aut}\, H$ *ist isomorph zu einer Untergruppe von* $\mathrm{Aut}(G \times H)$
2. *Ist* $\mathrm{ggT}(|G|, |H|) = 1$, *so gilt*

$$\mathrm{Aut}(G \times H) \cong \mathrm{Aut}(G) \times \mathrm{Aut}(H).$$

Beweis:

1. Sei $\varphi \in \operatorname{Aut} G, \psi \in \operatorname{Aut} H$. Wir setzen

$$\varphi \times \psi : G \times H \to G \times H, (g,h) \mapsto (\varphi(g), \psi(h)).$$

Dann ist $\varphi \times \psi$ Automorphismus von $G \times H$ (leicht nachzurechnen). Sei

$$\Phi : \operatorname{Aut} G \times \operatorname{Aut} H \to \operatorname{Aut}(G \times H), (\varphi, \psi) \mapsto \varphi \times \psi.$$

Dann ist Φ ein injektiver Gruppenhomomorphismus:

Für $\alpha, \varphi \in \operatorname{Aut} G, \beta, \psi \in \operatorname{Aut} H$ gilt mit $g \in G, h \in H$:

$$\left(g^{\alpha\varphi}, h^{\beta\psi}\right) = \left(g^{\alpha}, h^{\beta}\right)^{\varphi\times\psi} = (g,h)^{(\alpha\times\beta)(\varphi\times\psi)}.$$

Also ist

$$\Phi((\alpha,\beta)\cdot(\varphi,\psi)) = \Phi(\alpha\varphi, \beta\psi) = (\alpha\times\beta)(\varphi\times\psi) = \Phi(\alpha,\beta)\Phi(\varphi,\psi).$$

Das heißt, Φ ist ein Homomorphismus. Φ ist injektiv, denn für $(\alpha,\beta) \neq (\varphi,\psi)$ ist $\alpha\times\beta \neq \varphi\times\psi$. Nach dem Homomorphiesatz 0.1 ist dann

$$\operatorname{Aut} G \times \operatorname{Aut} H \cong \Phi(\operatorname{Aut} G \times \operatorname{Aut} H) \leq \operatorname{Aut}(G \times H).$$

2. Für $\operatorname{ggT}(|G|, |H|) = 1$ ist $\operatorname{ord}(g,h) = \operatorname{ord}(g)\operatorname{ord}(h)$. Bei jedem Automorphismus $\varphi \in \operatorname{Aut}(G \times H)$ gilt $\operatorname{ord}\varphi(g,h) = \operatorname{ord}(g,h)$. Daher ist

$$\varphi(G \times \langle 1\rangle) = G \times \langle 1\rangle \qquad \text{und} \qquad \varphi(\langle 1\rangle \times H) = \langle 1\rangle \times H.$$

Seien

$$\pi_1 : G \times H \to G \qquad \text{und} \qquad \pi_2 : G \times H \to H$$

die Projektionen. Wir definieren

$$\begin{aligned} \varphi_G : G \to G \quad &, \quad \varphi_G(g) = (\pi_1 \circ \varphi)(g,1) \\ \varphi_H : H \to H \quad &, \quad \varphi_H(h) = (\pi_2 \circ \varphi)(h,1). \end{aligned}$$

Dann gilt: $\varphi_G \leq \operatorname{Aut} G, \varphi_H \in \operatorname{Aut} H$. Die Abbildung

$$\Psi : \operatorname{Aut}(G \times H) \to \operatorname{Aut} G \times \operatorname{Aut} H, \varphi \mapsto (\varphi_G, \varphi_H)$$

ist injektiv: Sind $\varphi, \tau \in \operatorname{Aut}(G \times H)$ mit $\varphi \neq \tau$, so gibt es $g \in G, h \in H$ mit $\varphi(g,h) \neq \tau(g,h)$, also ist $\varphi_G(g) \neq \tau_G(g)$ oder $\varphi_H(h) \neq \tau_H(h)$ und daher $(\varphi_G, \varphi_H) \neq (\tau_G, \tau_H)$. Damit ist

$$|\operatorname{Aut}(G \times H)| \leq |\operatorname{Aut} G \times \operatorname{Aut} H|.$$

Mit 1. folgt die Behauptung.

□

4.4 Folgerung
Sei $n = p_1^{a_1} \cdot \ldots \cdot p_n^{a_n}$ *die Primfaktorzerlegung. Dann ist auch*

$$\operatorname{Aut} \mathbb{Z}_n \cong \mathbb{Z}_n^* \cong \mathbb{Z}_{p_1^{a_1}}^* \times \ldots \times \mathbb{Z}_{p_n^{a_n}}^*.$$

Beweis:
Nach dem Hauptsatz über endliche abelsche Gruppen 0.5 ist $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{a_1}} \times \ldots \times \mathbb{Z}_{p_n^{a_n}}$. Mit 4.2 und 4.3 folgt die Behauptung. □

4.5 Folgerung
Für $n, m \in \mathbb{N}, \operatorname{ggT}(n, m) = 1$ *gilt:*

$$\varphi(n, m) = \varphi(n)\, \varphi(m).$$

4.6 Folgerung
Sei $n = p_1^{a_1} \cdot \ldots \cdot p_k^{a_k}$ *die Primfaktorzerlegung. Dann gilt:*

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_k}\right).$$

Beweis:
Ist p prim, so gibt es genau $p^a - p^{a-1}$ Zahlen m mit $1 \leq m \leq p^a$, die zu p^a teilerfremd sind. Daher ist

$$\varphi(p^a) = p^a - p^{a-1} = p^a \left(1 - \frac{1}{p}\right).$$

Der Rest folgt mit 4.5.

Nun wollen wir die Gruppen $\mathbb{Z}_{p^k}^*$ für p prim näher untersuchen. Für $\mathbb{Z}_p^*$ müssen wir eine Aussage aus der Körpertheorie verwenden:

4.7 Satz
Sei p *prim. Dann ist* $\mathbb{Z}_p^* \cong \mathbb{Z}_{p-1}$ *zyklisch.*

Beweis:
$\mathbb{Z}_p^*$ ist als multiplikative Gruppe des Körpers $(\mathbb{Z}_p, +, \cdot)$ abelsch und lässt sich daher nach dem Hauptsatz über endliche abelsche Gruppen 0.5 als direktes Produkt zyklischer Gruppen schreiben:

$$\mathbb{Z}_p^* \cong Z_1 \times \ldots \times Z_k.$$

Sind die Ordnungen $z_i := |Z_i|$ paarweise teilerfremd, so ist $\mathbb{Z}_p^*$ zyklisch. Sonst gibt es eine Primzahl q, die z_i und z_j für ein Paar i, j mit $i \neq j$ teilt. Daher

gibt es in $Z_1 \times \ldots \times Z_k \cong \mathbb{Z}_p^*$ mindestens q^2 Elemente x mit $x^q = 1$, das heißt das Polynom $X^q - 1 \in \mathbb{Z}_p[X]$ besitzt mindestens q^2 Nullstellen. Über einem Körper besitzt ein Polynom vom Grad m aber höchstens m Nullstellen $\Rightarrow$ Widerspruch! Also ist $\mathbb{Z}_p^*$ zyklisch und wegen $\left|\mathbb{Z}_p^*\right| = p - 1$ daher $\mathbb{Z}_p^* \cong \mathbb{Z}_{p-1}$. □

4.8 Definition *Primitivwurzel modulo n*
Ein Erzeuger von $\mathbb{Z}_n^*$ heiï¿½t *Primitivwurzel modulo n*. Für p prim lässt sich eine Primitivwurzel modulo p nur durch Raten finden. Es gibt dafür weder ein theoretisches Resultat, noch einen guten Algorithmus.

4.9 Lemma
Sei p prim und $E_n := \{\overline{x} \in \mathbb{Z}_{p^n} \mid x \equiv 1 \mod p\}$. *Dann ist*

$$E_n \leq \mathbb{Z}_{p^n}^* \qquad \textit{mit } |E_n| = p^{n-1}.$$

Beweis:
Seien $\overline{x}, \overline{y} \in E_n$. Aus $x, y \equiv 1 \mod p$ folgt $xy \equiv 1 \mod p$, also ist $\overline{x} \cdot \overline{y} \in E_n$ und damit $E_n \leq \mathbb{Z}_{p^n}^*$. $|E_n| = p^{n-1}$ ist klar. □

4.10 Lemma
Sei $p > 2$ *prim. Dann ist* E_n *zyklisch und für* $n > 1$ *gilt:*

$$E_n = \langle x \rangle \quad \Leftrightarrow \quad x \equiv 1 \mod p, \quad x \not\equiv 1 \mod p^2.$$

Beweis:
Sei $y \equiv 0 \mod p$, aber $y \not\equiv 0 \mod p^2$. Wir zeigen induktiv für $0 \leq k \leq n-2$: $p^{k+1} \mid (1+y)^{p^k} - 1$, aber $p^{k+2} \nmid (1+y)^{p^k} - 1$. Nach Wahl von y ist dies für $k = 0$ klar.

$k \mapsto k+1$: Nach Induktionsvoraussetzung gibt es ein $a \in \mathbb{N}$ mit $p \nmid a$, so dass

$$(1+y)^{p^k} - 1 = ap^{k+1} \Leftrightarrow (1+y)^{p^k} = ap^{k+1} + 1.$$

Also ist

$$\begin{aligned}
(1+y)^{p^{k+1}} &= \left(ap^{k+1} + 1\right)^p = \\
&= 1 + \binom{p}{1} ap^{k+1} + \sum_{i=2}^{p} \binom{p}{i} a^i \left(p^{k+1}\right)^i = \\
&= 1 + ap^{k+2} + \sum_{i=2}^{p} \binom{p}{i} a^i p^{ki+i}
\end{aligned}$$

Für $i < p$ gilt $p \mid \binom{p}{i}$. Also gilt: $p^{ki+i+1} \mid \binom{p}{i} a^i p^{ki+i}$ und es gilt

$$ik + i + 1 \geq k + 3 \quad \Leftrightarrow \quad (i-1)\,k + i \geq 2,$$

was für $i \geq 2$ und $k \geq 0$ erfüllt ist. Für $i = p$ ist der entsprechende Summand durch p^{kp+p} teilbar und es gilt: $pk + p \geq k + 3$ für $p \geq 3$. Also folgt:

$$(1+y)^{p^{k+1}} - 1 \equiv ap^{k+2} \mod p^{k+3}.$$

Das heißt p^{k+2} teilt $(1+y)^{p^{k+1}} - 1$, aber p^{k+3} teilt $(1+y)^{p^{k+1}} - 1$ nicht. Setzen wir nun $\overline{x} := \overline{1} + \overline{y}$, so ist $\overline{x} \in E_n$ und es ist $\overline{x}^{p^k} \neq \overline{1}$ in $\mathbb{Z}_{p^n}^*$ für $k \leq n-2, \overline{x}^{p^{n-1}} = \overline{1}$.

Da nach 4.9 $|E_n| = p^{n-1}$, folgt $E_n = \langle \overline{x} \rangle$, das heißt E_n ist zyklisch. Jedes $\overline{x}$ mit $x - 1 \not\equiv 0 \mod p^2$ erzeugt E_n und es gibt $p^{n-1} - p^{n-2}$ Erzeugende dieser Form. Wegen $\varphi(p^{n-1}) = p^{n-1} - p^{n-2}$ sind diese alle Erzeugenden. □

4.11 Satz
Sei $p > 2$ prim und $k \in \mathbb{N}$. Dann ist $\mathbb{Z}_{p^k}^* \cong \mathbb{Z}_{p^{k-1}} \times \mathbb{Z}_{p-1}$ zyklisch.

Beweis:
Sei a eine Primitivwurzel modulo p, das heißt $\mathbb{Z}_p^* \cong \langle a \rangle$. Wir setzen $r := a^p - p$ und zeigen: $\mathbb{Z}_{p^k}^* = \langle r \rangle$. Zunächst ist $r \equiv a^{p-1}a \equiv a \mod p$ und wegen $\mathbb{Z}_p^* = \langle a \rangle$ folgt

$$r^m \equiv 1 \mod p \quad \Leftrightarrow \quad p-1 \mid m.$$

Ist $r^m \equiv 1 \mod p^k$, so ist insbesondere $r^m \equiv 1 \mod p$, also folgt $p-1$ teilt $\operatorname{ord} r$.

Jetzt zeigen wir, dass es ein $b \in \mathbb{Z}$ gibt mit $p \nmid b$, so dass $r^{p-1} = 1 + bp$. Dann folgt die Behauptung mit Lemma 4.10. Wegen $r \equiv a \mod p$ ist $r^{p-1} \equiv 1 \mod p$, also ist $r^{p-1} = 1 + bp$ für ein $b \in \mathbb{Z}$. Wir zeigen noch $p \nmid b$: Es ist

$$\begin{aligned}
r^{p-1} - 1 &= (a^p - p)^{p-1} - 1 = \\
&= a^{p(p-1)} - \binom{p-1}{1} (a^p)^{p-2} p + \\
&+ \sum_{i=2}^{p-1} \binom{p-1}{i} (a^p)^{p-1-i} p^i (-1)^i - 1 = \\
&\overset{\mod p^2}{=} a^{p(p-1)} - p^2 (a^p)^{p-2} + a^{p(p-2)} p - 1 = \\
&\overset{\mod p^2}{=} a^{p(p-1)} - 1 + a^{p(p-2)} p.
\end{aligned}$$

Da $a^{p-1} = 1 \mod p$ gibt es ein $k \in \mathbb{Z}$, so dass $a^{p-1} = 1 + kp$. Damit ist

$$\begin{aligned}
\left(a^{p-1}\right)^p - 1 &= (1+kp)^p - 1 = \sum_{i=1}^{p} \binom{p}{i} (kp)^i = \\
&= p(kp) + \sum_{i=2}^{p} \binom{p}{i} (kp)^i \equiv 0 \mod p^2.
\end{aligned}$$

Also erhalten wir:

$$r^{p-1} - 1 \equiv a^{p(p-2)}p \mod p^2.$$

Da $a \not\equiv 0 \mod p$, ist auch $a^x \not\equiv 0 \mod p$ und daher $r^{p-1} - 1 \not\equiv 0 \mod p^2$, das heißt $r^{p-1} = 1 + bp$ mit $p \nmid b$. Mit Lemma 4.10 folgt nun $\langle r^{p-1} \rangle = E_k$, das heißt $\operatorname{ord} r^{p-1} ? p^{k-1}$ und damit $p^{k-1} \mid \operatorname{ord} r$. Zusammen mit $p - 1 \mid \operatorname{ord} r$ erhalten wir $\operatorname{ord} r = (p-1)\, p^{k-1}$, also $\mathbb{Z}_{p^k}^* = \langle r \rangle$. □

Bemerkung
In Definition 4.8 haben wir festgestellt, dass es schwierig ist, eine Primitivwurzel modulo p zu finden. Haben wir aber eine solche gefunden, etwa a, so können wir sofort eine Primitivwurzel modulo p^k angeben, nämlich $r = a^p - p$.

4.12 Satz
Sei $k \in \mathbb{N}$. Für $k \geq 3$ ist $\mathbb{Z}_{2^k}^*$ nicht zyklisch. Für $k \geq 2$ gilt:

$$\mathbb{Z}_{2^k}^* \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{k-2}} \cong \left\langle -\overline{1} \right\rangle \times \left\langle \overline{5} \right\rangle.$$

Beweis:
Wir zeigen zuerst: $\operatorname{ord} \overline{5} = 2^{k-2}$. Sei $r \geq 2$ und $z \equiv 0 \mod 2^{r+1}$. Dann ist $z^2 \equiv 0 \mod 2^{r+2}$ und $2z \equiv 0 \mod 2^{r+1}$, aber $2r \not\equiv 0 \mod 2^{r+2}$ und daher

$$(1+z)^2 - 1 = 2z + z^2 \equiv 0 \mod 2^{r+1}, \text{ aber } (1+z)^2 - 1 \not\equiv 0 \mod 2^{r+2}.$$

Da $5 = 2^2 + 1$ folgt induktiv

$$5^{2^m} - 1 \equiv 0 \mod 2^{m+2}, \text{ aber } 5^{2^m} - 1 \not\equiv 0 \mod 2^{m+2}.$$

Also ist $\operatorname{ord} \overline{5} = 2^{k-2}$ in $\mathbb{Z}_{2^k}^*$.

Wir definieren nun

$$\psi : \mathbb{Z}_2 \times \mathbb{Z}_{2^{k-2}} \to \mathbb{Z}_{2^k}^*, \left(\overline{a}, \overline{b}\right) \mapsto \left(-\overline{1}\right)^a \left(\overline{5}\right)^b.$$

Wegen

$$\begin{aligned} \psi\left(\left(\overline{a} + \overline{c}, \overline{b} + \overline{d}\right)\right) &= \left(-\overline{1}\right)^{a+c} \overline{5}^{b+d} = \\ &= \left(-\overline{1}\right)^a \overline{5}^b \left(-\overline{1}\right)^c \overline{5}^d = \\ &= \psi\left(\left(\overline{a}, \overline{b}\right)\right) \psi\left(\left(\overline{c}, \overline{d}\right)\right) \end{aligned}$$

ist ψ ein Gruppenhomomorphismus. Weil die Gruppen $\mathbb{Z}_2 \times \mathbb{Z}_{2^{k-2}}$ und $\mathbb{Z}_{2^k}^*$ dieselbe Ordnung haben, müssen wir $\operatorname{Ker} \psi = \left\langle \left(\overline{0}, \overline{0}\right) \right\rangle$ zeigen. Sei $\left(\overline{a}, \overline{b}\right) \in \operatorname{Ker} \psi$, das heißt $\left(-\overline{1}\right)^a \overline{5}^b = \overline{1}$, also $(-1)^a 5^b \equiv 1 \mod 2^k$. Da $5 \equiv 1 \mod 4$ ist insbesondere $5^b \not\equiv -1 \mod 2^k$. Deshalb folgt $(-1)^a \equiv 1 \mod 2^k$ und wegen $\operatorname{ord} \overline{5} = 2^{k-2}$ folgt $b \equiv 0 \mod 2^{k-2}$. Also ist $\operatorname{Ker} \psi = \left\langle \left(\overline{0}, \overline{0}\right) \right\rangle$, das heißt ψ ist ein Homomorphismus. □

4.13 Folgerung
Sei $m \in \mathbb{N}$ und $\mathbb{P}$ die Menge der Primzahlen. Es gilt: $\mathbb{Z}_m^*$ ist zyklisch, genau dann, wenn $m \in \{1, 2, 4, p^*, 2p^* \mid p \in \mathbb{P} \setminus \{2\}, k \in \mathbb{N}\}$.

Beweis:
Wir zeigen zunächst, dass $\mathbb{Z}_m^*$ zyklisch ist. $\mathbb{Z}_2^* = \langle \mathrm{id} \rangle$ und $\mathbb{Z}_4^* \cong \mathbb{Z}_2$ sind zyklisch; für $p \in \mathbb{P} \setminus \{2\}$ ist $\mathbb{Z}_{p^k}^*$ nach 4.11 zyklisch und $\mathbb{Z}_{2p^k}^* \cong \mathbb{Z}_2^* \times \mathbb{Z}_{p^k}^* = \mathbb{Z}_{p^k}^*$.

Sei nun $\mathbb{Z}_m^*$ zyklisch. $\mathbb{Z}_{2p^k}^*$ ist für $k \geq 3$ nach 4.12 nicht zyklisch. Ist $m = p_1^{a_1}, \ldots, p_n^{a_n}$ eine Primfaktorzerlegung mit $p_i > 2$, so ist

$$\mathbb{Z}_m^* \cong \mathbb{Z}_{p_1^{a_1}} \times \ldots \times \mathbb{Z}_{p_n^{a_n}}$$

und diese Gruppe ist genau dann zyklisch, wenn die Ordnungen paarweise teilerfremd sind. Wegen $2 \mid p_i - 1$ und $\left|\mathbb{Z}_{p_i^{a_i}}^*\right| = (p_i - 1)\, p_i^{a_i - 1}$ ist dies nur der Fall, wenn $k = 1$. $\mathbb{Z}_{2^a p^b}^*$ ist für $b \geq 1$ nur zyklisch, wenn $a = 1$. □

Nun können wir beginnen, in bestimmten Fällen die Gruppen einer Ordnung zu klassifizieren. In 2.11 haben wir bereits gezeigt, dass Gruppen der Ordnung p^2, p prim, isomorph sind zu $\mathbb{Z}_{p^2}$ oder zu $\mathbb{Z}_p \times \mathbb{Z}_p$.

4.14 Satz
Sei $p \geq 2$ prim. Jede Gruppe der Ordnung $2p$ ist isomorph zu $\mathbb{Z}_{2p}$ oder zu D_p.

Beweis:
Sei G eine Gruppe mit $|G| = 2p$. Nach dem Satz von Sylow 3.10 enthält G eine p-Sylowgruppe N. Da $|N| = p$, ist N zyklisch, etwa $N = \langle d \rangle$. Nach Sylow 3.10 ist $N \lhd G$. Weiter gibt es ebenfalls nach Sylow eine 2-Sylowgruppe $S = \langle s \rangle$ in G. Offensichtlich ist dann $G = N \cdot S$ und $N \cap S = \langle 1 \rangle$, also ist $G = N \rtimes_\varphi S$. Welche Homomorphismen $\varphi : S \to \operatorname{Aut} N$ gibt es? Da $\operatorname{Aut} N \cong \mathbb{Z}_p^* \cong \mathbb{Z}_{p-1}$ zyklisch ist, gibt es in $\operatorname{Aut} N$ genau eine Untergruppe der Ordnung 2, nämlich $\langle \alpha \rangle$, wobei

$$\alpha : N \to N, x \mapsto x^{-1}.$$

Daher gibt es genau 2 mögliche Homomorphismen, und zwar

$$\begin{aligned} \varphi_1 &: S \to \operatorname{Aut} N \quad , \quad \varphi_1(S) = \{\mathrm{id}\} \\ \varphi_2 &: S \to \operatorname{Aut} N \quad , \quad \varphi_2(S) = \alpha. \end{aligned}$$

Es ergeben sich

$$G_1 = N \rtimes_{\varphi_1} S \cong N \times S \cong \mathbb{Z}_p \times \mathbb{Z}_2 \cong \mathbb{Z}_{2p}$$

und

$$G_2 = N \rtimes_{\varphi_2} S \cong \mathrm{D}_p\,.$$

Wenn wir Gruppen der Ordnung pq mit $2 < p < q$ klassifizieren wollen, taucht ein neues Problem auf:

Im Fall $p \mid q-1$ enthält $\mathbb{Z}_q^*$ eine zyklische Untergruppe der Ordnung p, es gibt also ein nichttriviales semidirektes Produkt $\mathbb{Z}_q \rtimes \mathbb{Z}_p$. Allerings kann der Erzeuger von $\mathbb{Z}_p$ ja auf jeden Erzeuger von Z abgebildet werden. Es gibt also $p-1$ "verschiedene" semidirekte Produkte, die aber, wie sich herausstellen wird, alle isomorph sind. Wir brauchen also Kriterien, wann semidirekte Produkte isomorph sind. Diese liefert der folgende Satz: □

4.15 Satz
Seien U, N Gruppen, $\varphi : U \to \operatorname{Aut} N$ ein Homomorphismus. Dann gilt:

1. *Ist $\alpha \in \operatorname{Aut} U$ und $\varphi : U \to \operatorname{Aut} N, \psi = \varphi \circ \alpha$, so ist*

$$N \rtimes_{\varphi} U \cong N \rtimes_{\psi} U.$$

2. *Sei $B \in \operatorname{Aut} N$ und $\psi : U \operatorname{Aut} N, \psi(u) := B^{-1}\varphi(u)\,B$. Dann ist ψ ein Homomorphismus und es gilt:*

$$N \rtimes_{\varphi} U \cong N \rtimes_{\psi} U.$$

Beweis:

1. Setze

$$\tau : N \rtimes_{\varphi} U \to N \rtimes_{\psi} U, un \mapsto u^{\alpha^{-1}} n \qquad \forall u \in U, n \in \mathbb{N}.$$

Dann ist τ ein Isomorphismus: Jedes Element in $n \rtimes U$ besitzt eine eindeutige Darstellung der Form $g = un$ mit $u \in U, n \in \mathbb{N}$, also ist τ bijektiv. τ ist ein Homomorphismus:

Seien $u_1, u_2 \in U, n_1, n_2 \in \mathbb{N}$, dann gilt:

$$\begin{aligned}
\tau\left(\left(u_1 n_1\right)\left(u_2 n_2\right)\right) &= \tau\left(u_1 u_2 n_1^{u_2^{\varphi}} n_2\right) = \left(u_1 u_2\right)^{\alpha^{-1}} n_1^{u_2^{\varphi}} n_2 = \\
&= u_1^{\alpha^{-1}} u_2^{\alpha^{-1}} n_1^{\left(u_2^{\alpha^{-1}\alpha}\right)^{\varphi}} n_2 = \\
&= u_1^{\alpha^{-1}} u_2^{\alpha^{-1}} n_1^{\left(u_2^{\alpha^{-1}}\right)^{\psi}} n_2 = \\
&= \left(u_1^{\alpha^{-1}} n_1\right)\left(u_2^{\alpha^{-1}} n_2\right) = \\
&= \tau\left(u_1 n_1\right)\tau\left(u_2 n_2\right)
\end{aligned}$$

2. Für $u_1, u_2 \in U$ gilt:

$$\begin{aligned}\psi(u_1u_2) &= \beta^{-1}\varphi(u_1)\varphi(u_2)\beta = \\ &= \beta^{-1}\varphi(u_1)\beta^{-1}\beta\varphi(u_2)\beta \\ &= \psi(u_1)\psi(u_2),\end{aligned}$$

das heißt ψ ist Homomorphismus. Definieren nun:

$$\tau : N \rtimes_\varphi U \to N \rtimes_\psi U, un \mapsto un^\beta \qquad (\text{für } u \in U, n \in \mathbb{N}\ ).$$

Wie in 1. folgt: τ ist bijektiver Homomorphismus.

□

4.15 ist noch nicht ganz in der Form, die wir benötigen.

4.16 Lemma
Sei $\varphi : \mathbb{Z}_n \to \mathbb{Z}_k$ ein surjektiver Gruppenhomomorphismus. Dann gilt:

$$\varphi(\mathbb{Z}_n^*) = \mathbb{Z}_k^*.$$

(Beachte: $\mathbb{Z}_n^*$ ist keine Untergruppe von $\mathbb{Z}_n$, sondern nur eine Teilmenge, die Verknüpfung ist anders.)

Beweis:
Wegen $\operatorname{ord}\varphi(x) \mid \operatorname{ord} x$ (für jeden Homomorphismus), gilt $k \mid n$. Sei $n = p_1a_1 \cdot \ldots \cdot p_r^{a_r}$ die Primzahlzerlegung. Dann ist $k = p_1^{b_1} \cdot \ldots \cdot p_k^{b_k}$ mit $0 \le b_i \le a_i$ und es gilt:

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{a_1}} \times \ldots \times \mathbb{Z}_{p_r^{a_r}} \quad \text{und} \quad \mathbb{Z}_k \cong \mathbb{Z}_{p_1^{b_1}} \times \ldots \times \mathbb{Z}_{p_r^{b_r}}.$$

Aus Ordnungsgründen gilt dann: $\varphi\left(\mathbb{Z}_{p_i^{a_i}}\right) = \varphi\left(\mathbb{Z}_{p_i^{b_i}}\right)$. Es genügt wegen

$$\mathbb{Z}_n^* \cong \mathbb{Z}_{p_1^{a_1}}^* \times \ldots \times \mathbb{Z}_{p_r^{a_r}}^* \quad \text{und} \quad \mathbb{Z}_k^* \cong \mathbb{Z}_{p_1^{b_1}}^* \times \ldots \times \mathbb{Z}_{p_r^{b_r}}^*$$

daher zu zeigen: Ist p prim, $a \ge b$ und $\varphi_i : \mathbb{Z}_{p^a} \to \mathbb{Z}_{p^b}$ surjektiv, so ist $\varphi\left(\mathbb{Z}_{p^a}^*\right) = \mathbb{Z}_{p^b}^*$. Wegen $\mathbb{Z}_{p^a} = \langle\overline{1}\rangle$ ist $\mathbb{Z}_{p^b} = \langle\varphi(\overline{1})\rangle$. Für $z \in \mathbb{Z}$ ist

$$\varphi(\overline{z}) = \varphi(\underbrace{\overline{1} + \ldots + \overline{1}}_{z\text{–mal}}) = \underbrace{\varphi(\overline{1}) + \ldots + \varphi(\overline{1})}_{z\text{–mal}} = z\varphi(\overline{z}).$$

Ist $z \in \mathbb{Z}_{p^a}^*$, so gilt $p \nmid z$, also ist $z\varphi(\overline{1}) = \varphi(\overline{z}) \in \mathbb{Z}_{p^b}^*$ und damit $\varphi\left(\mathbb{Z}_{p^a}^*\right) \subset \mathbb{Z}_{p^b}^*$. In jeder Gruppe G gilt: Ist $g \in G$, so ist $G = \{xg \mid x \in G\}$. Wir haben $\varphi(\overline{1}) \in \mathbb{Z}_{p^b}^*$ und daher

$$\mathbb{Z}_{p^b}^* = \left\{\overline{z}\varphi(\overline{1}) \mid \overline{z} \in \mathbb{Z}_{p^b}^*\right\} = \left\{z\varphi(\overline{1}) \mid z \in \mathbb{Z}, p \nmid q\right\}$$

und damit $\varphi\left(\mathbb{Z}_{p^a}^*\right) = \mathbb{Z}_{p^b}^*$. □

4.17 Satz
Sei N eine Gruppe und $U = \langle u \rangle \cong \mathbb{Z}_n$. Sei $\varphi : U \to \operatorname{Aut} N$ gegeben durch $\varphi(u) = \gamma \in \operatorname{Aut} N$. Sei $\psi : U \to \operatorname{Aut} N$ gegeben durch $\psi(u) = \gamma^i \in \operatorname{Aut} N$. Gilt $\operatorname{ord}_\varphi \gamma = \operatorname{ord} \gamma^i$, so ist

$$N \rtimes_\varphi U = N \rtimes_\psi U.$$

Beweis:
Da $\operatorname{ord} \varphi(u) \mid \operatorname{ord} u = n$, ist $\varphi : \underbrace{\langle u \rangle}_{\cong \mathbb{Z}_n} \to \underbrace{\langle \gamma \rangle}_{\cong \mathbb{Z}_{\operatorname{ord}_\varphi \gamma}} = \operatorname{Im} \varphi$ surjektiv. Wegen $\operatorname{ord} \gamma = \operatorname{ord} \gamma^i$ ist $i \in \mathbb{Z}^*_{\operatorname{ord} \gamma}$. Also gibt es nach 4.16 ein $a \in \mathbb{Z}^*_n$, so dass $\varphi(u^\alpha) = \gamma^i$. Wegen $a \in \mathbb{Z}^*_n$ ist die Abbildung

$$\alpha : \langle u \rangle \to \langle u \rangle, x \mapsto x^\alpha$$

ein Automorphismus von $\langle u \rangle$ und es gilt $\psi = \varphi \circ \alpha$. Nach 4.15 gilt dann

$$N \rtimes_\varphi U \cong N \rtimes_\psi U.$$

□

4.18 Satz
Seien p, q prim mit $2 < p < q$ und sei G eine Gruppe der Ordnung pq. Dann gilt:

1. *Falls $p \nmid q - 1$, ist $G \cong \mathbb{Z}_{pq}$ zyklisch.*
2. *Gilt $p \mid q - 1$, so gibt es in $\operatorname{Aut} \mathbb{Z}_q \cong \operatorname{Aut} \mathbb{Z}^*_q$ ein Element r der Ordnung p und durch*
$$\varphi : \mathbb{Z}_p = \langle g \rangle \to \operatorname{Aut} \mathbb{Z}_q, g^i \mapsto r^i$$
wird ein nichttrivialer Homomorphismus definiert. Es gilt: G ist entweder zyklisch oder $G \cong \mathbb{Z}_q \rtimes_\varphi \mathbb{Z}_p$.

Beweis:
Sei Q eine q-Sylowgruppe von G. Nach dem Satz von Sylow 3.10 ist $\left|\operatorname{Syl}_q G\right| \equiv 1 \mod q$ und $\left|\operatorname{Syl}_q G\right| \mid p$, also ist $\left|\operatorname{Syl}_q G\right| = 1$ und damit $Q \lhd G$. Sei P eine p-Sylow. Dann ist $G = PQ$ und $P \cap Q = \langle 1 \rangle$ und daher $G = Q \rtimes_\varphi P$ für irgendein $\varphi : P \to \operatorname{Aut} Q \cong \mathbb{Z}^*_q \cong \mathbb{Z}_{q-1}$.

Gilt $p \nmid q - 1$, so gibt es in $\operatorname{Aut} Q$ kein Element der Ordnung p. Daher ist $\varphi(P) = \langle \mathrm{id} \rangle$ und folglich

$$G \cong P \times Q \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}.$$

Im Fall $p \mid q-1$ gibt es in $\operatorname{Aut} Q \cong \mathbb{Z}_{q-1}$ ein Element r der Ordnung p. Sei $P = \langle g \rangle$, dann wird durch

$$\varphi : P \to \operatorname{Aut} Q, g^i \mapsto r^i$$

ein nichttrivialier Homomorphismus gegeben. Die weiteren möglichen nichttrivialien Homomorphismen sind

$$\varphi_j : P \to \operatorname{Aut} Q, g^i \mapsto \left(r^j\right)^i, \quad 1 < j < p.$$

Nach 4.17 gilt: $P \ltimes_\varphi Q \cong P \ltimes_{\varphi_j} Q$. Also folgt insgesamt:

$$G \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq} \qquad \text{oder} \qquad G \cong P \ltimes_\varphi Q = \mathbb{Z}_p \ltimes_\varphi \mathbb{Z}_q.$$

□

4.19 Bemerkung *Beschreibung von Gruppen durch Erzeuger und Relationen*
Eine kurze Möglichkeit, Gruppen zu beschreiben, ist die Beschreibung durch Erzeuger und Relationen. Eine solche Beschreibung hat die Form

$$G = \langle g_1, \ldots, g_n \mid R \rangle,$$

wobei R eine Menge von Gleichungen ("Relationen") ist, die die Erzeuger $g_1, \ldots, g_n$ erfüllen, z.B.

$$G_1 = \left\langle g \mid g^6 = 1 \right\rangle$$

oder

$$G_2 = \left\langle s, d \mid d^n = s^2 = 1, sdsd = 1 \right\rangle.$$

Für endliche Gruppen gilt:

$$G = \langle g_1, \ldots g_n \mid R \rangle$$

ist die endliche Gruppe größtmöglicher Ordnung, die Erzeuger $g_1, \ldots, g_n$ besitzt, die die Relationen aus R erfüllen. In unseren Beispielen ist $G_1 \cong \mathbb{Z}_6$ ($\mathbb{Z}_3 = \langle\rangle$ erfüllt die Relationen auch, hat aber nciht die maximale Ordnung) und $G_2 \cong \mathrm{D}_n$.

Im allgemeinen ist es schwierig, die Ordnung einer durch Erzeuger und Relationen beschriebenen Gruppe herauszufinden. Bei semidirekten Produkten lässt sich zeigen: Ist $U = \langle u_1, \ldots, u_k \mid R_U \rangle$ und $N = \langle n_1, \ldots, n_m \mid R_N \rangle$ und $\varphi : U \to \operatorname{Aut} N$ ein Homomorphismus, so gilt:

$$\begin{aligned} N \rtimes_\varphi U \;=\; \Big\langle & u_1, \ldots, u_k, n_1, \ldots, n_m \mid R_U \cup R_N \cup \\ & \cup \left\{ u_j^{-1} n_i u_j = n_i^{\varphi(u_j)} \mid i = 1, \ldots, m, j = 1, \ldots, k \right\} \Big\rangle. \end{aligned}$$

Für die Gruppe aus 4.18 erhalten wir z.B.:

$$G = \left\langle a, b \mid a^q = b^p = 1, b^{-1}ab = a^r \right\rangle,$$

wobei $r \in \mathbb{Z}_q^*$ Ordnung p hat.

5 Gruppenoperationen

Gruppenoperationen sind ein wichtiges Hilfsmittel mit Anwendungen sowohl innerhalb als auch außerhalb der Gruppentheorie (z. B. in der Kombinatorik, Zahlentheorie,...). Um die Stärke zu demonstrieren, werden wir die Aussage des Satzes von Sylow verallgemeinern.

Für eine Menge Ω bezeichne S_Ω die symmetrische Gruppe auf Ω. Gruppenoperationen lassen sich auf zwei äquivalente Arten definieren.

5.1 Definition *Operation*
• Eine *Gruppenoperation von G auf Ω* ist ein Gruppenhomomorphismus

$$\varphi : G \to \mathrm{S}_\Omega .$$

Dazu äquivalent:
• Eine *Gruppenoperation von G auf Ω* ist eine Abbildung

$$\Omega \times G \to \Omega, (\alpha, g) \longmapsto \alpha^g$$

derart, dass für alle $\alpha \in \Omega$ und alle $g, h \in G$ gilt $(\alpha^g)^h = \alpha^{(gh)}, \alpha^1 = \alpha$.
Der Homomorphismus $\varphi : G \to \mathrm{S}_\Omega$ wird dann gegeben durch

$$\varphi(g) = \begin{pmatrix} \alpha \\ \alpha^g \end{pmatrix}.$$

Die Operation heißt *treu* oder *effektiv*, wenn φ injektiv ist.
Sie heißt *trivial*, wenn $\mathrm{Ker}(\varphi) = G$.

5.2 Beispiel

1. S_n operiert treu auf $\{1, \ldots, n\}$.

2. D_n operiert treu auf den Ecken eines regelmäßigen n-Ecks. Versieht man die Ecken mit den Zahlen $1, \ldots, n$, so operiert D_n auch treu auf $1, \ldots, n$. Daraus folgt $\mathrm{D}_3 \cong \mathrm{S}_3$, die 2-Sylowgruppen von S_4 sind isomorph zu D_4.

3. Sei $U \leq G$. G operiert auf den Rechtsnebenklassen von U durch Rechtsmultiplikation. Der zugehörige Homomorphismus ist gerade der in 1.8 konstruierte.

4. G operiert durch Konjugation auf

   - der Menge ihrer Elemente,
   - der Menge der nichtleeren Teilmengen von G,
   - der Menge der Untergruppen (der p-Untergruppen, der Untergruppen von Ordnung $n||G|, \ldots$) von G,
   - der Menge der p-Sylowgruppen von G.

5. $\mathrm{Gl}(n, \mathbb{F}_q)$ operiert auf der Menge der k-dimensionalen Untervektorräume von $(\mathbb{F}_q)^n$.

Der letzte Punkt in 4 verdient es, besonders hervorgehoben zu werden:

5.3 Satz
Sei G eine Gruppe mit genau n p-Sylowgruppen $P_1, \ldots, P_n, n > 1$. Durch $\psi : G \to \mathrm{S}_n, \psi(g) = \sigma$, wobei $g^{-1}P_1g = P_{\sigma(1)}, \ldots, g^{-1}P_ng = P_{\sigma(n)}$ wird ein nichttrivialer Homomorphismus definiert und es gilt $\mathrm{Ker}(\psi) = \bigcap_{i=1}^{n} \mathrm{N}_G(P_i)$.

Beweis:
Nach Sylow sind die p-Sylowgruppen konjugiert, d. h. ψ ist nicht trivial und es gilt $\mathrm{Ker}(\psi) = \{g \in G | g^{-1}P_ig = P_i, i = 1, \ldots, n\} = \bigcap_{i=1}^{n} \mathrm{N}_G(P_i)$.

Als kleine Anwendung zeigen wir:

5.4 Satz
Ist $|G| = 112 = 2^4 \cdot 7$, so ist G nicht einfach.

Beweis:
Ist die 2-Sylowgruppe nicht normal in G, so gilt $|\,\mathrm{Syl}_2\, G| = 7$ nach Sylow. Die Operation von G auf $\mathrm{Syl}_2\, G$ durch Konjugation liefert einen nichttrivialen Homomorphismus $\psi : G \to \mathrm{S}_7$. Dann ist auch $\mathrm{sign} \circ \psi : G \to \{-1, 1\}$ ein Homomorphismus. Ist $\mathrm{sign} \circ \psi$ nicht trivial, so ist $\mathrm{Ker}(\mathrm{sign} \circ \psi) \neq G$ und $\mathrm{Ker}(\mathrm{sign} \circ \psi) \lhd G$. Sonst ist $\mathrm{Im}(\psi) \leq \mathrm{A}_7$. Da $|G| \nmid |\,\mathrm{A}_7\,| = 2^3 \cdot 3^2 \cdot 5 \cdot 7$, kann A_7 keine zu G isomorphe Untergruppe enthalten, also ist ψ weder trivial noch injektiv und $\mathrm{Ker}(\psi)$ daher ein nichttrivialer Normalteiler von G.

5.5 Definition *Stabilisator*
G operiere auf Ω. Sei $\alpha \in \Omega$. Die Menge $G_\alpha := \{g \in G | \alpha^g = \alpha\}$ heißt *Stabilisator von α in G*. Andere Bezeichnungen sind *Fixuntergruppe, Isotropiegruppe* und *Standuntergruppe*.

5.6 Satz
G operiere auf Ω. Sei $\alpha \in \Omega$. G_α ist eine Untergruppe von G und für $x \in G$ gilt $G_{\alpha^x} = (G_\alpha)^x$.

Beweis:
Seien $x, y \in G_\alpha$, dann ist $\alpha^{xy} = (a^x)^y = \alpha^y = \alpha$. Also ist $xy \in G_\alpha$ und damit ist G_α Untergruppe von G.
Es gilt

$$\begin{aligned} y \in G_{\alpha^x} &\iff (\alpha^x)^y = \alpha^x \\ &\iff \alpha^{xyx^{-1}} = \alpha \\ &\iff xyx^{-1} \in G_\alpha \\ &\iff y \in x^{-1}G_\alpha x = (G_\alpha)^x \end{aligned}$$

Bemerkung
G operiert durch Konjugation

- auf der Menge ihrer Elemente. Der Stabilisator eines Elements $x \in G$ ist der Zentralisator $\mathrm{Z}_G(x)$.
- auf der Menge der Untergruppen $U \leq G$. Der Stabilisator von U ist der Normalisator $\mathrm{N}_G(U)$.

Einige Aussagen in (setze REF!) folgen daher aus 5.6

5.7 Definition *Bahn*
G operiere auf Ω. Sei $\alpha \in \Omega$. Die Menge$\alpha^G := \{\alpha^g | g \in G\}$ heißt *Bahn* (engl. *orbit*) *von* α. Die Anzahl der Elemente einer Bahn heißt auch *Länge der Bahn.*

Bemerkung
Die Bahnen gehen von einer Äquivalenzrelation hervor, nämlich aus

$$\alpha \sim \beta \iff \exists g \in G : \alpha^g = \beta.$$

Sind daher $B_1, \ldots, B_n$ die Bahnen von G auf Ω, so gilt

$$\Omega = \bigcup_{i=1}^{n} B_i \qquad \text{disjunkt.}$$

5.8 Satz Bahnengleichung
G operiere auf Ω. Für $\alpha \in \Omega$ gilt

$$|\alpha^g| = \frac{|G|}{|G_\alpha|}$$

. Ist Λ ein Vertretersystem der Bahnen von G auf Ω, so gilt

$$|\Omega| = \sum_{\alpha \in \Lambda} \frac{|G|}{|G_\alpha|} \qquad \text{(Bahnengleichung)}$$

Beweis:
Für $x, y \in G$ gilt

$$\begin{aligned} \alpha^x = \alpha^y &\iff \alpha^{yx^{-1}} = \alpha \\ &\iff yx \in G_\alpha \\ &\iff y \in G_\alpha x. \end{aligned}$$

Es gibt also in der Bahn α^G genauso viele Elemente, wie es Nebenklassen von G_α gibt, nämlich $\frac{|G|}{|G_\alpha|}$ Stück. Die Bahnengleichung folgt dann aus

$$\Omega = \bigcup_{\alpha \in \Lambda} \alpha^G$$

.

Bemerkung
Sei $H \leq G$. Betrachten wir die Operation von H auf G durch Konjugation, so sind die Bahnen gerade die H-Konjugationsklassen und (setze REF!) folgt aus 5.8. Auch die Klassengleichung (setze REF!) folgt sofort.
Lassen wir H auf der Menge der Untergruppen von G durch Konjugation operieren, so folgt (setze REF!).

Wir demonstrieren nun die Stärke des Konzepts der Gruppenoperationen, indem wir im folgenden Satz auf einen Schlag den Satz von Cauchy und die Aussage (setze REF!) des Satzes von Sylow erneut beweisen. Die Aussage aus dem Satz von Sylow wird dabei sogar noch verallgemeinert.
Beachte: Der Beweis verwendet außer Gruppenoperationen nur Aussagen über Nebenklassen von Untergruppen und Kenntnisse über Untergruppen zyklischer Gruppen.

5.9 Satz Cauchy, Sylow (setze REF!) und mehr
Sei p prim und $|G| = p^a \cdot m$ mit $p \nmid m$. Für $0 \leq s \leq a$ bezeichne r_s die Anzahl der Untergruppen der Ordnung p^s von G. Dann gilt $r_s \equiv 1 \mod p$. Insbesondere ist $r_s \leq 1$ (Cauchy) und $r_a \equiv 1 \mod p$ (Sylow).

Beweis nach Wielandt:
Sei $n := \frac{|G|}{p^s} = p^{a-s} \cdot m$ und sei $\Omega := \{M \subset G | |M| = p^s\}$. Offensichtlich gilt $|\Omega| = \binom{np^s}{p^s}$. G operiert auf Ω durch Rechtsmultiplikation, da für $g \in G$ gilt

$|Mg| = |M|$.
Seien T_i die Bahnen dieser Operation, M_i ein Repräsentant von T_i und sei $U_i := G_{M_i} = \{g \in G | M_i g = M_i\}$ der Stabilisator von M_i. Dann gilt $|T_i| = \frac{|G|}{|U_i|}$. Aus $M_i U_i = M_i$ folgt $M_i = \bigcup_{j=1}^{k_i} g_{ij} U_i$ für bestimmte $g_{ij} \in G$, das heißt M_i ist Vereinigung von Nebenklassen von U_i. Also ist $p^s = |M_i| = k_i \cdot |U_i| \iff |U_i| = \frac{p^s}{k_i}$ und folglich $|U_i| = p^{b_i}$ mit $b_i \leq s$. Ist $|U_i| = p^{b_i} < p^s$, so gilt $|T_i| = \frac{|G|}{|U_i|} = \frac{p^s n}{p^{b_i}} \equiv 0 \mod pn$. Ist $|U_i| = p^s$, so gilt $|T_i| = \frac{p^s n}{p^s} = n$. Insgesamt erhalten wir

$$\binom{np^s}{p^s} = |\Omega| \equiv \sum_{|T_i|=n} |T_i| \mod pn \qquad (*)$$

Wir zeigen nun: $\#\{T_i | |T_i| = n\} = r_s$.
Ist nämlich $|T_i| = n$, so gibt es ein $m_i \in M_i$ derart, dass $M_i = m_i U_i$. Dann ist $m_i U_i m_i^{-1} =: V_i \leq T_i$ eine Untergruppe der Ordnung p^s in T_i.
Ist andererseits $U \leq G$ mit $|U| = p^s$, so ist $T := \{Ug | g \in G\}$ eine Bahn mit $|T| = \frac{|G|}{|U|} = n$. Sind V_i, V_j Untergruppen von G mit $|V_i| = |V_j| = p^s$, so gilt $V_i = V_j g$ für ein $g \in G$. Also gibt es ein $v_j \in V_j$ mit $1 = v_j g$ und damit $g = v_j^{-1} \in V_j$, ergo $V_i = V_j$.
Kurz: verschiedene Untergruppen mit Ordnung p^s liegen in verschiedenen Bahnen. Setzen wir das Erhaltene in (*) ein, so erhalten wir $\binom{np^s}{p^s} \equiv nr_s \mod pn$. Diese Kongruenz gilt für alle Gruppen mit Ordnung $p^a m$, insbesondere auch für die zyklische. Bei der zyklischen Gruppe ist bekanntlich $r_s = 1$, also ist $\binom{np^s}{p^s} \equiv n \mod pn$. Damit gilt für beliebige Gruppen G mit $|G| = p^a m$: $n \equiv n \cdot r_s \mod pn$, also $pn | nr_s - n = n(r_s - 1)$ und damit $p | r_s - 1$ bzw. $r_s \equiv 1 \mod p$.

5.10 Folgerung
Sei p prim und P eine Gruppe der Ordnung p^a. Sei $1 \leq s \leq a$. Dann enthält P einen Normalteiler der Ordnung p^s.

Beweis:
P operiert durch Konjugation auf der Menge $\Omega := \{U \leq P | |U| = p^s\}$ der Untergruppen von P mit Ordnung p^s. Sei $r_s := |\Omega|$. Nach der Bahnengleichung gilt dann $r_s = |\Omega| = \sum_i \frac{|P|}{P_{U_i}}$, wobei U_i Repräsentanten der verschiedenen Bahnen sind. Für die Stabilisatoren P_{U_i} erhalten wir $P_{U_i} = \{g \in G | g^{-1} U_i g = U_i\} = \mathrm{N}_P(U_i)$. Also ist

$$r_s = \sum_i \frac{|P|}{|\,\mathrm{N}_P(U_i)|} \qquad (*)$$

Weil P eine p-Gruppe ist, gilt $p | \frac{|P|}{\mathrm{N}_P(U_i)} \iff \mathrm{N}_P(U_i) \neq P$. Nach 5.9 ist $r_s \equiv 1$

mod p, also $p \nmid r_s$. Also gibt es in (*) einen Summanden, der nicht durch p teilbar ist, d. h. es gibt $U_i \in \Omega$ mit $\mathrm{N}_P(U_i) = P \Longleftrightarrow U_i \lhd P$.

Für weitere Aussagen über Untergruppen von p-Gruppen benötigen wir zunächst eine Aussage über deren Normalisatoren:

5.11 Lemma Matsuyama
Sei p prim, P eine p-Gruppe und $H < G$. Dann ist entweder $H \lhd P$ oder es gibt ein $x \in P$ mit $H^x \neq H$ und $H^x \leq \mathrm{N}_P(H)$.

Beweis:
Sei $H \not\lhd P$. Wir setzen $X := \{H^x | x \in P\} \backslash \{H\}$. Dann ist $X \neq \varnothing$ und H operiert auf X durch Konjugation. Nach Lemma (setze REF!) gibt es $\frac{|P|}{|\mathrm{N}_P(H)|}$ H-Konjugierte von H in P, also ist $|X| = \frac{|P|}{|\mathrm{N}_P(H)|} - 1 \not\equiv 0 \mod p$. Die Längen der Bahnen von H auf X sind nach Lemma 5.8 Potenzen von p. Wegen $|X| \not\equiv 0 \mod p$ folgt, dass es eine Bahn der Länge 1 gibt, etwa $\{H^y\}$. Dann ist $h^{-1}H^y h = H^y$ für $h \in H$, das heißt es gilt $H \leq \mathrm{N}_P(H^y)$. Setzen wir $x := y^{-1}$, so ist nach (setze REF!) $H^x \leq \mathrm{N}_P(H^y)^x = \mathrm{N}_P(H^{yx}) = \mathrm{N}_P(H)$.

5.12 Folgerung
Sei p prim, P eine p-Gruppe. Ist $H < P$, so ist $H < \mathrm{N}_P(H)$.

Beweis:
Ist $H \lhd P$, so ist $\mathrm{N}_P(H) = P > H$. Ist $H \not\lhd P$, so gibt es nach 5.11 ein $H^x \neq H$ mit $H^x \leq \mathrm{N}_P(H)$, also ist $N_P(H) > H$.

5.13 Folgerung
Sei p prim, P eine p-Gruppe mit $|P| = p^n$. Alle Untergruppen der Ordnung p^{n-1} sind Normalteiler in P.

Beweis:
Nach 5.12 ist $\mathrm{N}_P(H) = P$ für $H < P$ mit $|H| = p^{n-1}$.

Mit 5.12 und 5.13 können wir einen weiteren Satz über Untergruppen von p-Gruppen beweisen:

5.14 Satz
Sei P eine p-Gruppe und $H < P$ mit $|H| = p^s$. Sei

$$a := |\{K < P | H < K \text{ und } |K| = p^{s+1}\}|$$

die Anzahl der Untergruppen von P mit Ordnung p^{s+1}, die H enthalten. Dann ist $a \equiv 1 \mod p$. Insbesondere ist $a \geq 1$.

Beweis:
Nach 5.12 ist $N < \mathrm{N}_P(H)$. Ist $K \leq P$ mit $H < K$ und $|K| = p^{s+1}$, so gilt $H \lhd K$ nach 5.13. Laut (setze REF!) ist daher $K \leq \mathrm{N}_P(H)$. Wir wenden nun den Korrespondenzsatz auf $\theta : \mathrm{N}_P(H) \to \mathrm{N}_P(H)/H$ an. Die Untergruppen K mit $H < K$ und $|K| = p^{s+1}$ entsprechen dabei den Untergruppen der Ordnung p von $\mathrm{N}_P(H)/H$. Für deren Anzahl a gilt $a \equiv 1 \mod p$ nach 5.9.

5.15 Bemerkung
Sei p prim, P eine p-Gruppe mit $|P| = p^n$. Für $1 \leq s < n$ sei r_s die Anzahl der Untergruppen von P mit Ordnung p^s. Nach 5.9 ist $r_s \equiv 1 \mod p$. Der einfachste Fall wäre also $r_s = 1$. In diesem Fall lässt sich zeigen:

- Ist $r_1 = 1$, so ist P zyklisch oder es ist $p = 2$ und P ist eine sogenannte *verallgemeinerte Quaternionengruppe.*
- Ist $r_s = 1$ für $s > 1$, so ist P zyklisch.

Für die Kombinatorik interessant ist das folgende Lemma

5.16 Satz Lemma von Cauchy-Frobenius
(oft falsch als Lemma von Burnside bezeichnet)
G operiere auf Ω. Für $g \in G$ bezeichne $F(g) := \{\alpha \in \Omega | \alpha^g = \alpha\}$. die Menge der Fixpunkte von g. Dann gilt für die Anzahl N der Bahnen von G auf Ω

$$N = \frac{1}{|G|} \sum_{g \in G} |F(g)|,$$

das heißt, die Zahl der Bahnen ist gleich der durchschnittlichen Zahl der Fixpunkte.

Beweis:
Es gilt $\alpha \in F(g) \Longleftrightarrow g \in G_\alpha$. Damit ist

$$\begin{aligned} \sum_{g \in G} |F(g)| &= \sum_{g \in G} \sum_{\alpha \in F(g)} 1 = \sum_{\alpha \in \Omega} \sum_{g \in G_\alpha} 1 = \\ &= \sum_{\alpha \in \Omega} |G_\alpha| \overset{5.8}{=} |G| \sum_{\alpha \in \Omega} \frac{1}{|\alpha^G|} = |G| \cdot N \end{aligned}$$

Im letzten Schritt wurde verwendet, dass jede Bahn den Beitrag 1 zur Summe liefert.

Eine gruppentheoretische Folgerung aus dem Lemma von Cauchy-Frobenius ist

5.17 Folgerung
Für die Anzahl c der Konjugationsklassen von g gilt

$$c = \frac{1}{|G|} \sum_{g \in G} |\,\mathrm{C}_G(g)|.$$

Beweis:
G operiert durch Konjugation auf sich selbst, die Bahnen sind die Konjugationsklassen und für $g \in G$ gilt

$$F(g) = \{x \in G | g^{-1}xg = x\} = \{x \in G | x^{-1}gx = g\} = \mathrm{C}_G(g).$$

5.18 Definition *transitiv*
G operiere auf Ω. Die Operation heißt *transitiv*, wenn es nur eine einzige Bahn gibt, d. h. wenn zu $\alpha, \beta \in \Omega$ ein $g \in G$ existiert mit $\alpha^g = \beta$.
Die Operation heißt *n-transitiv*, wenn zu jedem Paar $(\alpha_1, \ldots, \alpha_n), (\beta_1, \ldots, \beta_n)$ von n-Tupeln mit $\alpha_1, \ldots, \alpha_n$ paarweise verschieden (genauso für $(\beta_1, \ldots, \beta_n)$) ein $g \in G$ existiert derart, dass $\alpha_i^g = \beta_i$ für $i = 1, \ldots, n$.

5.19 Beispiel
Offensichtlich ist eine transitive Operation 1-transitiv und eine n-transitive Operation ist $(n-1)$-transitiv.

1. D_n operiert transitiv auf den Ecken des regelmäßigen n-Ecks.
2. S_n operiert n-transitiv auf $\{1, \ldots, n\}$.
3. A_n operiert $(n-2)$-transitiv auf $\{1, \ldots, n\}$.

Beweis:

1. D_n operiert transitiv, weil schon $\langle d \rangle$ transitiv operiert.
2. $\begin{pmatrix} \alpha_1 & \ldots & \alpha_n \\ \beta_1 & \ldots & \beta_n \end{pmatrix}$ tut es.
3. Seien $\alpha_1, \ldots, \alpha_{n-2} \in \{1, \ldots, n\}$ paarweise verschieden und $\beta_1, \ldots, \beta_{n-2} \in \{1, \ldots, n\}$ paarweise verschieden. Dann gibt es $\alpha_{n-1}, \alpha_n, \beta_{n-1}, \beta_n$ derart, dass $\{\alpha_1, \ldots, \alpha_n\} = \{1, \ldots, n\} = \{\beta_1, \ldots, \beta_n\}$. Wir betrachen

$$\sigma = \begin{pmatrix} \alpha_1 & \ldots & \alpha_{n-2} & \alpha_{n-1} & \alpha_n \\ \beta_1 & \ldots & \beta_{n-2} & \beta_{n-1} & \beta_n \end{pmatrix},$$

$$\pi = \begin{pmatrix} \alpha_1 & \ldots & \alpha_{n-2} & \alpha_{n-1} & \alpha_n \\ \beta_1 & \ldots & \beta_{n-2} & \beta_n & \beta_{n-1} \end{pmatrix}.$$

Dann ist $(\alpha_{n-1} \quad \alpha_n) \circ \sigma = \pi$ und daher $\mathrm{sign}(\pi) = -\mathrm{sign}(\sigma)$. Folglich liegt eine der beiden Permutationen in der A_n.

5.20 Satz Frattini-Argument I
G operiere auf Ω. Besitzt G eine Untergruppe U, die transitiv auf Ω operiert, so gilt $G = G_\alpha U$ für alle $\alpha \in \Omega$.

Beweis:
Sei $\alpha \in \Omega$ fest. Zu jedem $g \in G$ gibt es ein $x \in U$ derart, dass $\alpha^g = \alpha^x$. Also ist $\alpha^{gx^{-1}} = \alpha$ und damit $gx^{-1} \in G_\alpha$, d. h. es gilt $g \in G_\alpha x \subset G_\alpha U$.
Bemerke: es gilt auch $G = UG_\alpha$, ersetze g durch g^{-1} im Beweis.

5.21 Satz Frattini-Argument II
Sei $M \lhd G$. Dann gilt für jede p-Sylowgruppe P von M

$$G = M\,\mathrm{N}_G(P).$$

Beweis:
Wegen $M \lhd G$ operiert G auf $\mathrm{Syl}_P M$ durch Konjugation. Nach Sylow operiert M dabei transitiv. Für $P \in \mathrm{Syl}_P G$ ist der Stabilisator $G_P = \{g \in G | g^{-1}Pg = P\} = \mathrm{N}_G(P)$. Mit dem Frattini-Argument I folgt $G = M\,\mathrm{N}_G(P)$.

5.22 Satz
G operiere transitiv auf Ω. Dann sind äquivalent:

1. *G operiert 2-transitiv auf Ω.*
2. *Für jedes $x \in \Omega$ operiert G_x transitiv auf $\Omega \backslash \{x\}$.*

Beweis:
Operiere zunächst G 2-transitiv auf Ω. Seien $\beta, \gamma \in \Omega \backslash \{\alpha\}$. Nach Voraussetzung gibt es ein $g \in G$ mit $(\alpha_g, \beta_g) = (\alpha, \gamma)$. Offensichtlich ist $g \in G_\alpha$.
Operiere umgekehrt G_x transitiv auf $\Omega \backslash \{x\}$ für alle $x \in \Omega$, und seien $\alpha \neq \beta \in \Omega$ und $\gamma \neq \delta \in G$. Dann gibt es ein $g \in G_\alpha$ derart, dass $\beta^g = \delta$ und ein $h \in G_\delta$ mit $\alpha^h = \gamma$. Für das Element gh gilt dann $(\alpha^{gh}, \beta^{gh}) = (\alpha^h, \delta^h) = (\gamma, \delta)$.

6 Symmetrische und alternierende Gruppen

Neben der Zykelschreibweise sind als Vorkenntnisse bereits vorhanden:

- Jedes $\sigma \in \mathrm{S}_n$ lässt sich (bis auf die Reihenfolge eindeutig) als Produkt disjunkter Zykel schreiben.
- S_n wird von den Transpositionen (= 2-Zykel) erzeugt.
- A_n wird von 3-Zykeln erzeugt.

Wir beginnen damit, die Konjugationsklassen von S_n und A_n zu bestimmen. Dabei sind folgende Bezeichnungen hilfreich:

6.1 Definition *Zykelpartition, Zykeltyp*
Sei $\sigma \in \mathrm{S}_n, \sigma = \sigma_1 \cdot \ldots \cdot \sigma_k$ die Zerlegung in disjunkte Zykel. Sei $\operatorname{ord}\sigma_1 \geq \operatorname{ord}\sigma_2 \geq \ldots \geq \operatorname{ord}\sigma_k$. Das Tupel $(\operatorname{ord}\sigma_1, \ldots \operatorname{ord}\sigma_k)$ heiß *Zykelpartition von* σ. Sei nun a_i die Vielfachheit i in der Zykelpartition von σ. Das Tupel $(a_1, a_2, \ldots, a_n)$ heißt *Zykeltyp von* σ.

Beispiel
$\tau = (123)(45)(67)(89) \in \mathrm{S}_{11}$ hat die Zykelpartition $(3, 2, 2, 1, 1)$ und den Zykeltyp $(2, 3, 1, 0, 0, 0, 0, 0, 0, 0, 0)$. Beim Zykeltyp werden in der Regel die Nullen am Ende weggelassen. Steht n fest, so werden gelegentlich auch die Einsen am Ende der Zykelpartition weggelassen. Die Zykelpartition schreibt man abkürzend in der Form

$$\left(n^{a_n}, (n-1)^{a_{n-1}}, \ldots, 1^{a_1}\right),$$

das heißt die Zykelpartition von τ wäre $(3, 2^3, 1^2)$. Die folgende Rechenregel liefert uns die Konjugationsklassen der S_n:

6.2 Lemma Rechenregel
Sei $\sigma = (i_1, \ldots, i_{r_1})(i_{r+1}, \ldots, i_{r_2}) \ldots (\ldots, i_{r_k}) \in \mathrm{S}_n$ *die Zerlegung in disjunkte Zykel und sei* $\pi \in \mathrm{S}_n$. *Dann gilt:*

$$\pi^{-1}\sigma\pi = (\pi(i_1), \ldots, \pi(i_{r_1}))(\pi(i_{r+1}), \ldots, \pi(i_{r_2})) \ldots (\ldots,)(i_{r_k}).$$

Beweis:
Wir können σ in der Form $\binom{i}{\sigma(i)}$ als Abbildung schreiben. In dieser Schreibweise ist

$$\begin{aligned}
\pi^{-1}\sigma\pi &= \binom{\pi(i)}{i}\binom{i}{\sigma(i)}\binom{i}{\pi(i)} = \\
&= \binom{\pi(i)}{\sigma(i)}\binom{i}{\pi(i)} = \\
&\underset{\text{Bijektion}}{\overset{\sigma(i) \text{ ist}}{=}} \binom{\pi(i)}{\sigma(i)}\binom{\sigma(i)}{\pi(\sigma(i))} = \\
&= \binom{\pi(i)}{\pi(\sigma(i))}.
\end{aligned}$$

Ist also

$$\sigma = \ldots(\ldots i\ \sigma(i) \ldots) \ldots$$

in der Zykelschreibweise, so ist

$$\pi^{-1}\sigma\pi = \ldots(\ldots\pi(i)\ \ \pi(\sigma(i))\ldots)\ldots.$$

□

6.3 Satz Konjugationsklassen der S_n
σ, τ sind in S_n sind genau dann konjugiert, wenn sie dieselbe Zykelpartition haben. Insbesondere ist die Zahl der Konjugationsklassen von S_n gleich der Zahl der Partitionen von n.

Beweis:
Nach Lemma 6.2 haben konjugierte Elemente dieselbe Zykelpartition. Wir müssen noch zeigen, dass alle Elemente mit derselben Zykelpartition konjugiert sind.

Seien also

$$\sigma = \sigma_1 \cdot \ldots \cdot \sigma_k \quad \text{und} \quad \tau = \tau_1 \cdot \ldots \cdot \tau_k$$

Zerlegungen in disjunkte Zykel mit $\operatorname{ord}\sigma_i = \operatorname{ord}\tau_i$. Wir suchen ein $\pi \in S_n$ mit $\pi^{-1}\sigma\pi = \tau$. Dieses π erhalten wir nach 6.2 durch "Untereinanderschreiben":

$$\begin{aligned} \sigma &= \ldots(\ldots i\ \sigma(i)\ldots)\ldots \\ \tau &= \ldots(\ldots j\ \tau(j)\ldots)\ldots \end{aligned}$$

und interpretieren als Abbildung: $\pi \in S_n$ bildet untereinanderstehende Zahlen aufeinander ab, das heißt $\pi(i) = j, \pi(\sigma(i)) = \tau(j)$ usw. Nach 6.2 gilt dann: $\pi^{-1}\sigma\pi = \tau$. □

Bemerkung
Die Zahl der Partitionen wächst sehr schnell an, lässt sich aber mit kombinatorischen Methoden recht gut berechnen. Es ist

$$\begin{aligned} P(5) &= 7 \\ P(10) &= 42 \\ P(20) &= 627 \\ P(50) &= 204226 \\ P(100) &= 190569292 \end{aligned}$$

Für die Bestimmung der Konjugationsklassen der A_n brauchen wir in einem einfachen Fall Aussagen über die Zentralisatoren $C_{S_n}(\sigma)$. Wir bestimmen $C_{S_n}(\sigma)$ gleich allgemein:

6.4 Satz
Sei $\sigma \in \mathrm{S}_n$ ein Element vom Zykeltyp $(a_1, \ldots, a_n)$. Dann ist

$$\mathrm{C}_{\mathrm{S}_n}(\sigma) \cong \mathrm{S}_{a_1} \times (\mathbb{Z}_2 \wr_p \mathrm{S}_{a_2}) \times \ldots \times (\mathbb{Z}_n \wr_p \mathrm{S}_{a_n})$$

und es gilt:

$$|\mathbb{Z}_k \wr_p \mathrm{S}_{a_k}| = a_k! k^{a_k}.$$

Faktoren mit $a_k = 0$ sind dabei wegzulassen. Die Faktoren $\mathbb{Z}_k \wr_p \mathrm{S}_{a_k}$ lassen sich dabei folgendermaßen beschreiben:

Seien $(b_{11}, \ldots, b_{1k}), (b_{21}, \ldots, b_{2k}), \ldots, (b_{a_k 1}, \ldots, b_{a_k k})$ die Zykel der Länge k in der Zerlegung von σ. Sei

$$Y := \{b_{ij} \mid 1 \leq i \leq a_k, 1 \leq j \leq k\}$$

und

$$K := \langle (b_{11}, \ldots, b_{1k}), \ldots, (b_{a_k 1}, \ldots, b_{a_k k}) \rangle .$$

Dann ist $K \cong (\mathbb{Z}_k)^{a_k}$. Für jedes $\tau \in \mathrm{S}_{a_k}$ wird durch

$$\psi_\tau : K \to K, (b_{i1}, \ldots, b_{ik}) \mapsto \left(b_{\tau(i)1}, \ldots, b_{\tau(i)k}\right)$$

ein Automorphismus von K gegeben. Die Abbildung

$$\varphi : \mathrm{S}_{a_k} \to \operatorname{Aut} K, \tau \mapsto \psi_\tau$$

ist ein Gruppenhomomorphismus und es gilt:

$$\mathbb{Z}_k \wr \mathrm{S}_{a_k} = K \rtimes_\varphi \mathrm{S}_{a_k} \leq S_Y.$$

Beweis:
$\langle \sigma \rangle$ operiert als Untergruppe von S_n auf den Zahlen $\{1, \ldots, n\}$. Die Bahnen dieser Operation werden gerade durch die Zykel in der Zerlegung von σ in disjunkte Zykel gegeben, wobei wir die Zykel der Länge 1 hier *nicht* weglassen. Ist $\sigma = \sigma_1 \cdot \ldots \cdot \sigma_r$ eine Zerlegung in disjunkte Zykel und ist $\sigma_i = (b_1, \ldots, b_{l_i})$, so ist $B_i := \{b_1, \ldots, b_{l_i}\}$ eine Bahn von $\langle \sigma \rangle$.

Sei nun $\tau \in \mathrm{C}_{\mathrm{S}_n}(\sigma)$. Dann gilt $\tau^{-1}\sigma\tau = \sigma$, also ist $\tau^{-1}\sigma_i\tau = \sigma_j$ für ein $j \in \{1, \ldots, r\}$ (hier geht 6.2 ein!). Nach 6.2 liefert dies $\tau(B_i) = B_j$, das heißt τ permutiert die Bahnen von σ. Da τ bijektiv ist, werden dabei Bahnen gleicher Länge permutiert. Fassen wir die Bahnen gleicher Länge l in Y_l zusammen, also $Y_l := \bigcup_{|B_i|=l} B_i$, so ist demnach

$$\tau \in \mathrm{S}_{Y_1} \times \mathrm{S}_{Y_2} \times \ldots \times \mathrm{S}_{Y_n} \quad \text{und} \quad \mathrm{C}_{\mathrm{S}_n}(\sigma) \leq \mathrm{S}_{Y_1} \times \ldots \times \mathrm{S}_{Y_n},$$

wobei leere Mengen weggelassen werden. Sei nun $Y = Y_k$ und seien b_{ij}, K, φ wie im Satz. Wir setzen

$$\pi_k := (b_{11}, \ldots, b_{1k}) \cdot \ldots \cdot (b_{a_k 1}, \ldots, b_{a_k k}) .$$

Dann ist $\mathrm{C}_{\mathrm{S}_n}(\sigma) \cap \mathrm{S}_Y = \mathrm{C}_{\mathrm{S}_Y}(\pi_k)$ und $\mathrm{C}_{\mathrm{S}_n}(\sigma)$ ist (nach 6.2) das direkte Produkt der $\mathrm{C}_{\mathrm{S}_Y}(\pi_k)$ für $k = 1, \ldots, n$. Offensichtlich ist $K \rtimes_\varphi \mathrm{S}_{a_k} \leq \mathrm{C}_{\mathrm{S}_k}(\pi_k)$ und es gilt

$$|K \rtimes_\varphi \mathrm{S}_{a_k}| = |K|^{a_k} a_k! = k^{a_k} a_k!.$$

Die Konjugationsklasse C_{π_k} von π_k in S_Y besteht nach 6.3 aus den Elementen von S_Y mit der gleichen Zykelpartition wie π_k, also aus den Elementen, die Produkt von $a_k k$-Zykeln sind. Davon gibt es in $\mathrm{S}_Y \cong \mathrm{S}_{k \cdot a_k}$ gerade

$$|\mathrm{C}_{\pi_k}| = \frac{(ka_k)!}{k\,(ka_k - k)!} \cdot \frac{(ka_k - k)!}{k\,(ka_k - 2k)!} \cdot \ldots \cdot \frac{(2k)!}{kk!} \cdot \frac{k!}{k} \cdot \frac{1}{a_k} = \frac{(ka_k)!}{k^{a_k} a_k!}$$

Stück. Also ist

$$|\mathrm{C}_{\mathrm{S}_Y}(\pi_k)| = \frac{|\mathrm{S}_Y|}{|\mathrm{C}_{\pi_k}|} = \frac{(ka_k)! k^{a_k} a_k!}{(ka_k)!} = k^{a_k} a_k!.$$

Das liefert:

$$\mathrm{C}_{\mathrm{S}_Y}(\pi_k) = K \rtimes_\varphi \mathrm{S}_{a_k} \cong \mathbb{Z}_k \wr_p \mathrm{S}_{a_k} .$$

Damit können wir die Konjugationsklassen der A_n bestimmen (wobei wir 6.4 nur in einem einfachen Fall verwenden, den man auch wesentlich kürzer beweisen kann). □

6.5 Satz Konjugationsklassen der A_n
Sei $\sigma \in \mathrm{A}_n$ und $C \subset \mathrm{S}_n$ die S_n-Konjugationsklasse von σ, dann gilt: Entweder ist C auch die A_n-Konjugationsklasse von σ oder C zerfällt in zwei gleich große A_n-Klassen. C zerfällt genau dann in zwei A_n-Klassen, wenn in der Zykelpartition von σ (mit Einsen!) alle Teile paarweise verschieden und ungerade sind. Ist in diesem Fall $\tau \in \mathrm{S}_n \setminus \mathrm{A}_n$, so sind σ und $\tau^{-1}\sigma\tau$ in A_n nicht zueinander konjugiert.

Beweis:
Wegen $\mathrm{A}_n \lhd \mathrm{S}_n$ liegt jede S_n-Konjugationsklasse entweder ganz in A_n oder ganz in $\mathrm{S}_n \setminus \mathrm{A}_n$. Sei C_A die A_n-Klasse von σ und C_S die S_n-Klasse. Nach 2.7 gilt:

$$|C_\mathrm{S}| = \frac{|\mathrm{S}_n|}{|\mathrm{C}_{\mathrm{S}_n}(\sigma)|} \quad \text{und} \quad |C_\mathrm{A}| = \frac{|\mathrm{A}_n|}{|\mathrm{C}_{\mathrm{A}_n}(\sigma)|}.$$

Wegen $\mathrm{C}_{\mathrm{A}_n}(\sigma) = \mathrm{C}_{\mathrm{S}_n}(\sigma) \cap \mathrm{A}_n$ ist

$$|\mathrm{C}_{\mathrm{A}_n}(\sigma)| = |\mathrm{C}_{\mathrm{S}_n}(\sigma)| \quad \text{oder} \quad |\mathrm{C}_{\mathrm{A}_n}(\sigma)| = \frac{|\mathrm{C}_{\mathrm{S}_n}(\sigma)|}{2}.$$

Demnach gilt $|C_{\mathrm{A}}| = |C_{\mathrm{S}}|$ oder $|C_{\mathrm{A}}| = \frac{|C_{\mathrm{S}}|}{2}$. Offensichtlich zerfällt C_{S} genau dann in zwei A_n-Klassen, wenn $\mathrm{C}_{\mathrm{A}_n}(\sigma) = \mathrm{C}_{\mathrm{S}_n}(\sigma)$, das heißt, wenn $\mathrm{C}_{\mathrm{S}_n}(\mathrm{A}_n) \leq \mathrm{A}_n$ gilt. Enthält nun σ in seiner Zerlegung $\sigma = \pi_1 \cdot \ldots \cdot \pi_k$ in disjunkte Zykel einen Zykel π_i gerader Länge, dann ist $\pi_i \in \mathrm{C}_{\mathrm{S}_n}(\sigma) \setminus \mathrm{A}_n$. Enthält σ zwei Zykel derselben ungeraden Länge, also etwa

$$\sigma = \left(i_1\ \sigma(i_1) \ldots \sigma^{r-1}(i_1)\right)\left(i_2\ \sigma(i_2) \ldots \sigma^{r-1}(i_2)\right)$$

mit ungeradem r, so ist

$$\rho = (i_1 i_2)\left(\sigma(i_1)\,\sigma(i_2)\right) \ldots \left(\sigma^{r-1}(i_1)\,\sigma^{r-1}(i_2)\right) \in \mathrm{C}_{\mathrm{S}_n}(\sigma) \setminus \mathrm{A}_n\,.$$

Ist umgekehrt $\sigma = \pi_1 \cdot \ldots \cdot \pi_k$ ein Produkt disjunkter Zykel mit paarweise verschiedenen ungeraden Längen, so ist

$$\mathrm{C}_{\mathrm{S}_n}(\sigma) = \langle \pi_1 \rangle \times \langle \pi_2 \rangle \times \ldots \times \langle \pi_k \rangle \overset{6.4}{\leq} \mathrm{A}_n\,.$$

Ist $\tau \in \mathrm{S}_n \setminus \mathrm{A}_n$, so sind σ und $\tau^{-1}\sigma\tau$ in A_n nicht konjugiert. Andernfalls gäbe es ein $\pi \in \mathrm{A}_n$, so dass

$$\tau^{-1}\sigma\tau = \pi^{-1}\sigma\pi \Leftrightarrow \pi\tau^{-1}\sigma\tau\pi^{-1} = \sigma \ \Leftrightarrow \tau\pi^{-1} \in \mathrm{C}_{\mathrm{S}_n}(\sigma) = \mathrm{C}_{\mathrm{A}_n}(\sigma) \leq \mathrm{A}_n\,.$$

Dann ist aber $\tau \in \mathrm{A}_n\,\pi = \mathrm{A}_n$. Widerspruch! □

Als nächstes wollen wir beweisen, dass A_n für $n \geq 5$ einfach ist. Dafür gibt es verschiedene Beweise. Der folgende Beweis vermeidet weitgehend lange Rechnungen.

6.6 Lemma
A_5 *ist einfach.*

Beweis:
In S_5 gibt es $\frac{5!}{5} = 25$ 5-Zykel, $\frac{5\cdot4\cdot3}{3} = 20$ 3-Zykel und $\frac{1}{2}\left(\frac{5\cdot4}{2}\frac{3\cdot2}{2}\right) = 15$ Doppeltranspositionen. Diese bilden zusammen mit (1) die Gruppe A_5. Nach Satz 6.3 bilden diese Elemente jeweils S_5-Konjugationsklassen. Laut Satz 6.5 zerfällt die S_5-Klasse der 5-Zykel in zwei A_5-Klassen mit je 12 Elementen. Ist $\langle 1 \rangle < H \lhd \mathrm{A}_5$, so ist H Vereinigung von (1) mit einigen der Konjugationsklassen. Also ist $|H|$ Summe von 1 mit einigen der Zahlen 12, 12, 15, 20. Keine dieser Summen ist jedoch ein echter Teiler von 60, also $H = \mathrm{A}_5$. □

6.7 Lemma
Sei $H \lhd \mathrm{A}_n$ für $n \geq 5$. Liegt ein 3-Zykel in H, so ist $H = \mathrm{A}_n$.

Beweis:
Nach 6.4 enthält H die ganze Klasse, also alle 3-Zykel. Die 3-Zykel erzeugen aber A_n, also ist $H = \mathrm{A}_n$. □

6.8 Lemma
A_6 *ist einfach.*

Beweis:
Sei $\langle 1 \rangle < H \lhd \mathrm{A}_6$ und sei $\alpha \in H$ mit $\alpha \neq (1)$. Besitzt α einen Fixpunkt, das heißt gibt es $i \in \{1, \ldots, 6\}$ mit $\alpha(i) = i$, so betrachten wir

$$F := \{\beta \in \mathrm{A}_6 \mid \beta(i) = i\}.$$

Dann gilt $F \cong \mathrm{A}_5$ und $(1) \neq \alpha \in F \cap H$. Nach dem 1. Isomorphiesatz 0.2 gilt: $H \cap F \lhd F$. Weil F nach 6.6 einfach ist, folgt $H \cap F = F$ und daher $F \leq H$. Da F 3-Zykel enthält, folgt $H = \mathrm{A}_6$ mit 6.7.

Wir können annehmen, dass kein Element von H außer (1) einen Fixpunkt besitzt. Ist $\alpha \in H$ mit $\alpha \neq (1)$, so hat α daher entweder die Zykelpartition $(4, 2)$ oder $(3, 3)$. Nach 6.5 sind alle Elemente mit diesen Zykelpartitionen jeweils konjugiert in A_6, also ist entweder $\alpha_1 = (12)(3456) \in H$ oder $\alpha_2 = (123)(456) \in H$. Ist $\alpha_1 \in H$, so ist auch $\alpha_1^2 \in H$ und α_1^2 besitzt die Fixpunkte 1 und 2. Widerspruch! Ist $\alpha_2 \in H$, setzen wir $\beta = (356)$; H enthält als Normalteiler das Element $(\beta^{-1}\alpha\beta)\alpha^{-1} = (24536)$, das 1 als Fixpunkt hat. Widerspruch! Folglich kann so ein Normalteiler nicht existieren. □

6.9 Satz
Für $n \geq 5$ ist A_n einfach.

Beweis:
Sei $\langle 1 \rangle \neq H \lhd \mathrm{A}_n$. Ist $\beta \in H$ mit $\beta \neq (1)$, so gibt es ein $i \in \{1, \ldots, n\}$ mit $\beta(i) = j \neq i$. Ist α ein 3-Zykel mit $\alpha(i) = i$ und $\alpha(j) \neq j$, so gilt $\beta(\alpha(i)) = \beta(i) = j$ und $\alpha(\beta(i)) = \alpha(j) \neq j$. Also kommutieren α und β nicht, das heißt es ist $\beta^{-1}\alpha^{-1}\beta\alpha \neq 1$. Wegen $H \lhd \mathrm{A}_n$ ist $\beta^{-1}(\alpha^{-1}\beta\alpha) \in H$. Nach 6.3 ist $\beta^{-1}\alpha^{-1}\beta$ ein 3-Zykel, das heißt das Element $(\beta^{-1}\alpha^{-1}\beta)\alpha$ ist ein Produkt von 2 3-Zykeln und bewegt daher höchstens 6 Zahlen $i_1, \ldots, i_6$.

Sei $Y := \{i_1, \ldots, i_6\}$. Ist $|Y| < 6$, so ergänzen wir Y mit beliebigen Zahlen aus $\{1, \ldots, n\}$, sodass $|Y| = 6$. Wir betrachten

$$F := \{\gamma \in \mathrm{A}_n \mid \gamma(i) = i \quad \forall i \text{ mit } i \notin Y\}.$$

Dann ist $F \cong \mathrm{A}_6$ und wegen $\beta^{-1}\alpha^{-1}\beta\alpha \in F \cap H$ ist $F \cap H > \langle 1 \rangle$. Nach dem 1. Isomorphiesatz 0.2 gilt $F \cap H \lhd F$. Weil F nach 6.8 einfach ist, folgt

$F \cap H = F$, das heißt $F \leq H$. Damit liegt ein 3-Zykel in H und mit 6.7 folgt $H = \mathrm{A}_n$. □

6.10 Folgerung
S_n *und* A_n *sind nicht auflösbar für* $n \geq 5$.

6.11 Folgerung
Es gilt:

1. $\mathrm{S}_n' = \mathrm{A}_n$ *für* $n \geq 2$ *und* $\mathrm{Z}(\mathrm{S}_n) = \langle 1 \rangle$ *für* $n \geq 3$.
2. $\mathrm{A}_n' = \mathrm{A}_n$ *für* $n \geq 5$ *und* $\mathrm{Z}(\mathrm{A}_n) = \langle 1 \rangle$ *für* $n \geq 4$.

Beweis:

1. Da $\mathrm{S}_n / \mathrm{A}_n$ abelsch ist, gilt $\mathrm{S}_n' \leq \mathrm{A}_n$ nach 2.15 Für $n \geq 3$ ist $(ij)^{-1}(jk)^{-1}(ij)(jk) = (ijk)$, also liegen alle 3-Zykel im S_n'. Die 3-Zykel erzeugen A_n und $n = 2$ trivial. $\mathrm{Z}(\mathrm{S}_n) = \langle 1 \rangle$ folgt leicht mit 6.3.
2. Da $\mathrm{A}_n' \lhd \mathrm{A}_n$ und $\mathrm{Z}(\mathrm{A}_n) \lhd \mathrm{A}_n$ sind beide Aussagen für $n \geq 5$ klar. $\mathrm{Z}(\mathrm{A}_4) = \langle 1 \rangle$ bleibt dem Leser zur Übung überlassen.

□

A_5 ist eine einfache nicht abelsche Gruppe der Ordnung 60. Es gibt keine nicht abelsche einfache Gruppe mit kleinerer Ordnung. Wieviele nicht abelsche Gruppen mit Ordnung 60 gibt es? Der folgende Satz zeigt: Es gibt nur eine!

6.12 Satz
Sei G *eine nicht abelsche einfache Gruppe mit* $|G| = 60$. *Dann ist* $G \cong \mathrm{A}_5$.

Beweis:
Wir untersuchen 2 Fälle:

1. G besitzt eine Untergruppe mit $[G : U] \leq 5$. Dann operiert G durch Rechtsmultiplikation auf den Rechtsnebenklassen von U. Das liefert nach 1.8 einen nicht trivialen Homomorphismus

$$\varphi : G \to \mathrm{S}_n, \qquad \text{wobei } n = [G : U].$$

   Weil φ nicht trivial ist, gilt $\operatorname{Ker} \varphi \neq G$. Also muss $\operatorname{Ker} \varphi = \langle 1 \rangle$ gelten, das heißt φ ist injektiv und daher $n = 5$. Auch

$$\operatorname{sign} \circ \varphi : G \to \{1, -1\}$$

   ist ein Homomorphismus, offensichtlich nicht injektiv. Also ist $\operatorname{Ker}(\operatorname{sign} \circ \varphi) = G$ und daher $\varphi(G) = \mathrm{A}_5$, das heißt $G \cong \mathrm{A}_5$ via φ.

2. Für alle $U < G$ gilt $[G : U] \geq 6$. Sei S eine 2-Sylowgruppe von G. Jede Gruppe U mit $S < U \leq G$ hat Ordnung $4 \cdot 3 = 12, 4 \cdot 5 = 20$ oder $4 \cdot 3 \cdot 5 = 60$. Nach Voraussetzung besitzt G aber keine Untergruppen mit Ordnung 12 oder 20, also ist in diesem Fall bereits $U = G$.

   Da $S \leq \mathrm{N}_G(S)$ und $\mathrm{N}_G(S) \neq G$ (sonst wäre S Normalteiler), folgt $\mathrm{N}_G(S) = S$. Nach dem Satz von Sylow 3.10 gibt es in G daher $[G : \mathrm{N}_G(S)] = 15$ 2-Sylowgruppen. Schneiden sich je 2 beliebige 2-Sylowgruppen in $\langle 1 \rangle$, so enthalten die 15 2-Sylowgruppen zusammen $1 + 15 \cdot 3 = 46$ Elemente. Gleichzeitig enthält G mindestens 6 5-Sylowgruppen. Da diese trivialerweise Durchschnitt $\langle 1 \rangle$ haben, enthalten sie $6 \cdot 4 = 24$ Elemente der Ordnung 5. Das liefert $|G| \geq 70$. Widerspruch!

   Also gibt es 2-Sylowgruppen R, T von G mit $|R \cap T| = 2$. Sei $R \cap T = \{1, y\}$. Als Gruppen der Ordnung 4 sind R und T abelsch, also kommutiert y mit den Elementen von R und T. Wir betrachten nun $\langle R, T \rangle$. Wegen $R < \langle R, T \rangle$ folgt $\langle R, T \rangle = G$, denn G enthält ja keine Untergruppen mit Ordnung 12 beziehungsweise 20. Das Element y kommutiert mit den Erzeugern von $\langle R, T \rangle = G$, also ist $y \in \mathrm{Z}(G)$ und damit $\mathrm{Z}(G) > \langle 1 \rangle$. Da $\mathrm{Z}(G) \neq G$ ist $\mathrm{Z}(G)$ also nichttrivialer Normalteiler von G.

□

Bemerkung
Die nachstgrößere nicht-abelsche Gruppe ist die $\mathrm{PSL}(2, \mathbb{F}_7)$ mit Ordnung 128.

Als nächstes wollen wir die p-Sylowgruppen der S_n bestimmen. Dabei werden erneut die Kranzprodukte eine Rolle spielen. Wir berechnen zunächst die Ordnung der p-Sylowgruppen.

6.13 Lemma
Sei p prim, $n \in \mathbb{N}$. Für $m \in \mathbb{N}$ sei

$$\mu(m) := p^{m-1} + p^{m-2} + \ldots + p + 1.$$

Wir schreiben n in der Basis p, also

$$n = a_0 + a_1 p + a_2 p^2 + \ldots + a_t p^t \qquad \text{mit } 0 \leq a_i \leq p - 1.$$

Die Ordnung einer p-Sylowgruppe der S_n ist p^N, wobei

$$N = a_1 + a_2 \mu(2) + \ldots + a_t \mu(t).$$

Insbesondere ist $p^{\mu(k)}$ die Ordnung einer p-Sylowgruppe S_{p^k}.

Beweis:
Schreiben wir $n! = p^\mu \cdot n'$ mit $p \nmid n'$, so gilt

$$\mu = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots,$$

denn $\left[\frac{n}{p}\right]$ Faktoren von $n!$ sind durch p teilbar, $\left[\frac{n}{p^2}\right]$ Faktoren von $n!$ sind durch p^2 teilbar usw.

Ist nun $n = a_0 + a_1 p + \ldots + a_t p^t$ wie im Satz, so gilt:

$$\begin{aligned}
\mu &= \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots + \left[\frac{n}{p^2}\right] = \\
&= a_1 + a_2 p + a_3 p^2 + \ldots + a_t p^{t-1} + \\
&+ a_2 + a_3 p + a_4 p^2 + \ldots + a_t p^{t-2} \\
&\vdots \\
&= a_1 + a_2 (p+1) + a_3 \left(p^2 + p + 1\right) + \ldots = \\
&= a_1 + a_2 \mu(2) + a_3 \mu(3) + \ldots + a_t \mu(t).
\end{aligned}$$

□

6.14 Satz Kaloujnine
Sei p prim. Die p-Sylowgruppe von S_{p^n} ist ein n-fach iteriertes reguläres Kranzprodukt $W_n = \mathbb{Z}_p \wr_r \mathbb{Z}_p \wr_r \ldots \wr_r \mathbb{Z}_p$, das heißt $W_1 = \mathbb{Z}_p$ und $W_{i+1} = W_i \wr_r \mathbb{Z}_p$.

Beweis:
Induktion über n, $n = 1$ ist klar, also etwa:

$$\begin{aligned}
Y_1 &:= \left\{1, \ldots, p^{n-1}\right\}, \\
Y_2 &:= \left\{p^{n-1} + 1, \ldots, 2p^{n-1}\right\}, \\
&\ldots \\
Y_p &:= \left\{(p-1)\, p^{n-1}, \ldots, p^n\right\}.
\end{aligned}$$

Sei $W_{n-1}^{(i)}$ eine p-Sylowgruppe von $S_{Y_i} \leq S_{p^n}$. Offensichtlich ist dann das direkte Produkt

$$W := W_{n-1}^{(1)} \times W_{n-1}^{(2)} \times \ldots \times W_{n-1}^{(p)}$$

eine p-Untergruppe von S_{p^n} mit Ordnung

$$|W| = \left|W_{n-1}^{(1)}\right|^p = p^{p\mu(n-1)}$$

(mit den Bezeichnungen von 6.13). Wir setzen nun:

$$\begin{aligned}\sigma \;:=\; & \left(1, p^{n-1}+1, \ldots, (p-1)\,p^{n-1}+1\right) \cdot \\ & \cdot \left(2, p^{n-1}+2, \ldots, (p-1)\,p^{n-1}+2\right) \cdot \ldots \cdot \left(p^{n-1}, 2p^{n-1}, \ldots, p^n\right)\end{aligned}$$

und $Z := \langle\sigma\rangle \cong \mathbb{Z}_p$. Mit der Bezeichnung $\tau = (1, 2, \ldots, p)$ ist $\sigma\,(Y_i) = Y_{\tau(i)}$. Nun können wir das semidirekte Produkt $P := W \rtimes_\varphi Z$ mit

$$\varphi : Z \to \operatorname{Aut} W, \sigma \mapsto \left(g \mapsto \sigma^{-1} g \sigma\right)$$

bilden und erhalten eine p-Untergruppe der Ordnung

$$|P| = p\,|W| = p \cdot p^{pn(n-1)} = p^{\mu(n)}.$$

Laut 6.13 ist P damit eine p-Sylowgruppe von S_{p^n}. Identifizieren wir jeweils alle Zahlen Zahlen in Y_i mit den entsprechenden Zahlen in Y_1, so lassen sich die Elemente $g \in W$ in der Form $g = (g_1, \ldots, g_p)$ mit $g_i \in W_{n-1}$ schreiben und es gilt:

$$\sigma^{-1} g \sigma = \left(g_{\tau(1)}, \ldots, g_{\tau(p)}\right),$$

deshalb können wir P auch als Kranzprodukt

$$P \cong W_{n-1} \wr_p \langle\tau\rangle \cong W_{n-1} \wr_r \mathbb{Z}_p$$

auffassen. □

6.15 Satz
Sei p prim, $n \in \mathbb{N}$. Sei $n = a_0 + a_1 p + \ldots + a_t p^t$ mit $0 \le a_i \le p-1$. Für $k \in \mathbb{N}$ bezeichne W_n eine p-Sylowgruppe von S_{p^n} und sei P eine p-Sylowgruppe von S_n. Dann gilt:

$$P \cong W_1^{a_1} \times W_2^{a_2} \times \ldots \times W_t^{a_t}.$$

Beweis:
Wir teilen die Menge $X = \{1, \ldots, n\}$ auf in a_0 einelementige Teilmengen, a_1 p-elementige, …, a_k p^t-elementige. Ist Y so eine Teilmenge, so betrachten wir eine p-Sylowgruppe auf S_Y. Diese hat nach 6.13 $p^{\mu(i)}$ Elemente, falls $|Y| = p^i$.

Nun sei P das direkte Produkt der p-Sylowgruppen auf den Teilmengen. Dann ist $P \le \mathrm{S}_X \cong \mathrm{S}_n$ eine p-Untergruppe der Ordnung p^N, wobei

$$N = a_1 + a_2\mu\,(2) + \ldots + a_t\mu\,(t).$$

Nach 6.13 ist P damit eine p-Sylowgruppe von $\mathrm{S}_X \cong \mathrm{S}_n$. □

Wir beenden das Kapitel mit einem Satz , der dazu dient, eine Gruppe der Ordnung 24 als S_4 zu erkennen:

6.16 Satz
Sei G eine Gruppe mit $|G| = 24$. Besitzt G genau vier 3-Sylowgruppen und gilt $\mathrm{Z}(G) = \langle 1 \rangle$, so ist $G \cong \mathrm{S}_4$.

Beweis:
G operiert durch Konjugation auf der Menge $\mathrm{Syl}_3 G$ der 3-Sylowgruppen. Das liefert einen nicht trivialen Homomorphismus

$$\varphi : G \to \mathrm{S}_4$$

mit $\operatorname{Ker}\varphi = \bigcap_{i=1}^{4} \mathrm{N}_G(P_i)$ (siehe **??**), wobei $P_1, \ldots, P_4$ die 3-Sylowgruppen G bezeichnen. Nach dem Satz von Sylow 3.10 ist

$$4 = |\mathrm{Syl}_3 G| = \frac{|G|}{|\mathrm{N}_G(P_i)|}$$

und daher $|\mathrm{N}_G(P_i)| = 6$. Weil $P_i \lhd \mathrm{N}_G(P_i)$, liegt nur eine 3-Sylowgruppe in $\mathrm{N}_G(P_i)$. Wegen $P_i \cap P_j = \langle 1 \rangle$ für $i \neq j$ folgt

$$|\mathrm{N}_G(P_i) \cap \mathrm{N}_G(P_j)| \leq 2.$$

Angenommen, $a \in \bigcap_{i=1}^{4} \mathrm{N}_G(P_i)$ ist ein Element der Ordnung 2. Für $g \in G$ ist dann

$$\begin{aligned} g^{-1}ag \in g^{-1}\left(\bigcap_{i=1}^{4} \mathrm{N}_G(P_i)\right) g &= \bigcap_{i=1}^{4} \left[g^{-1}\,\mathrm{N}_G(P_i)\,g\right] \\ &= \bigcap_{i=1}^{4} \mathrm{N}_G(P_i^g) = \\ &= \bigcap_{i=1}^{4} \mathrm{N}_G(P_i)\,. \end{aligned}$$

Da $\left|\bigcap_{i=1}^{4} \mathrm{N}_G(P_i)\right| = 2$ nach Annahme, folgt $g^{-1}ag = a$ für alle $g \in G$ und damit $a \in \mathrm{Z}(G)$. Dies steht im Widerspruch zu $\mathrm{Z}(G) = \langle 1 \rangle$. Damit ist $\operatorname{Ker}\varphi = \langle 1 \rangle$, also $G \cong \mathrm{S}_4$. □

Nach diesem Ausflug zu den nicht auflösbaren Gruppen widmen wir uns im nächsten Kapitel besonders "schoönen" auflösbaren Gruppen, den sogenannten *nilpotenten Gruppen*.

7 Nilpotente Gruppen

7.1 Definition *Absteigende und aufsteigende Zentralreihe*
Die *absteigende Zentralreihe*

$$G = K_1(G) \geq \mathrm{K}_2(G) \geq \ldots$$

wird rekursiv definiert durch

$$\mathrm{K}_1(G) = G \quad \text{und} \quad \mathrm{K}_{i+1}(G) := [\mathrm{K}_i(G), G].$$

Die Gruppen $\mathrm{Z}_i(G)$ der *aufsteigenden Zentralreihe*

$$\langle 1 \rangle \leq \mathrm{Z}_0(G) \leq \mathrm{Z}_1(G) \leq \ldots$$

werden rekursiv definiert durch

$$\mathrm{Z}_0(G) = \langle 1 \rangle \quad \text{und} \quad \mathrm{Z}_{i+1}(G) / \mathrm{Z}_i(G) = \mathrm{Z}(G/\mathrm{Z}_i(G)).$$

Nach dem Korrespondenzsatz 1.4 ist $\mathrm{Z}_{i+1}(G)$ dadurch eindeutig bestimmt und Normalteiler von G.

Abkürzend schreiben wir auch K_i und Z_i, wenn die Gruppe G klar ist. Offensichtlich ist $\mathrm{K}_2(G) = G'$ und $\mathrm{Z}_1(G) = \mathrm{Z}(G)$. Weitere einfache Eigenschaften von K_i und Z_i fassen wir im folgenden Satz zusammen:

7.2 Satz
Für $i \in \mathbb{N}$ gilt:

1. $\mathrm{K}_i(G)$ char G.
2. $\mathrm{Z}_i(G)$ char G.
3. *Sei $N \lhd G$ mit $N \leq \mathrm{K}_i(G)$, dann gilt:*

$$\mathrm{K}_i(G)/N \leq \mathrm{Z}(G/N) \quad \Leftrightarrow \quad \mathrm{K}_{i+1}(G) \leq N.$$

4. $[\mathrm{Z}_{i+1}(G), G] \leq \mathrm{Z}_i(G)$.

Beweis:

1. folgt induktiv, $i = 1$ ist klar, $i \mapsto i+1$: Sei $\alpha \in \mathrm{Aut}\, G$, dann gilt:

$$\begin{aligned} \mathrm{K}_{i+1}(G)^\alpha &= [\mathrm{K}_i(G), G]^\alpha \overset{2.13}{=} \\ &= [\mathrm{K}_i(G)^\alpha, G^\alpha] \overset{IV}{=} [\mathrm{K}_i(G), G] = \mathrm{K}_{i+1}(G). \end{aligned}$$

2. folgt ebenfalls induktiv mit 2.20.4. $i = 0$ klar und aus $\mathrm{Z}_i(G) \operatorname{char} G$ und

$$\mathrm{Z}_{i+1}(G) / \mathrm{Z}_i(G) = \mathrm{Z}(G/\mathrm{Z}_i(G)) \operatorname{char} G/\mathrm{Z}_i(G)$$

folgt $\mathrm{Z}_{i+1}(G) \operatorname{char} G$ mit 2.20.4.

3. Es gilt:

$$\begin{aligned}
\mathrm{K}_i/N \leq \mathrm{Z}(G/N) &\Leftrightarrow \forall x \in \mathrm{K}_i, \forall y \in G : xyN = yxN \\
&\Leftrightarrow \forall x \in \mathrm{K}_i, \forall y \in G : x^{-1}y^{-1}xyN = N \\
&\Leftrightarrow \forall x \in \mathrm{K}_i, \forall y \in G : [x,y]\,N = N \\
&\Leftrightarrow \forall x \in \mathrm{K}_i, \forall y \in G : [x,y] \in N \\
&\Leftrightarrow [\mathrm{K}_i, G] \leq N \\
&\Leftrightarrow \mathrm{K}_{i+1} \leq N.
\end{aligned}$$

4. Es gilt:

$$\begin{aligned}
\mathrm{Z}_{i+1}/\mathrm{Z}_i = \mathrm{Z}(G/\mathrm{Z}_i) &\Leftrightarrow \forall z \in \mathrm{Z}_{i+1}, \forall g \in G : zg\,\mathrm{Z}_i = gz\,\mathrm{Z}_i \\
&\Leftrightarrow \forall z \in \mathrm{Z}_{i+1}, \forall g \in G : \\
&\qquad z^{-1}g^{-1}zg\,\mathrm{Z}_i = [z,g]\,\mathrm{Z}_i = \mathrm{Z}_i \\
&\Leftrightarrow [z,g] \in \mathrm{Z}_i \\
&\Leftrightarrow [\mathrm{Z}_{i+1}, G] \leq \mathrm{Z}_i\,.
\end{aligned}$$

□

Wir kommen nun zum Hauptsatz dieses Kapitels:

7.3 Definition und Satz *Nilpotente Gruppen*
Eine Gruppe G heißt *nilpotent*, wenn sie folgende äquivalente Bedingungen erfüllt:

1. Die absteigende Zentralreihe von G erreicht die $\langle 1 \rangle$.
2. Ist $U < G$, so ist $U < \mathrm{N}_G(U)$.
3. Jede maximale Untergruppe von G ist Normalteiler in G.
4. G ist das direkte Produkt ihrer Sylowgruppen.
5. Die aufsteigende Zentralreihe von G erreiht G.
6. Je zwei Elemente von G mit teilerfremden Ordnung kommutieren.

7. Für alle Normalteiler $N \lhd G$ mit $N \neq G$ gilt: $\mathrm{Z}(G/N) \neq \langle 1 \rangle$.

Beweis:

1. $\Rightarrow$ 2. Sei $G = \mathrm{K}_1(G) \geq \ldots \geq \mathrm{K}_m(G) = \langle 1 \rangle$ die absteigende Zentralreihe von G und sei $U < G$. Dann ist $\mathrm{K}_1(G) \not\subset U$, aber $\mathrm{K}_m(G) \leq U$. Also gibt es ein $i \in \{1, \ldots, m\}$, so dass $\mathrm{K}_i(G) \not\subset U, \mathrm{K}_{i+1}(G) \leq U$. Damit ist

$$[\mathrm{K}_i, G] \leq [\mathrm{K}_i, G] = \mathrm{K}_{i+1} \leq U.$$

   Mit 2.14.2 folgt daraus $\mathrm{K}_i \leq \mathrm{N}_G(U)$ und somit $U < \mathrm{N}_G(U)$.

2. $\Rightarrow$ 3. Ist $U < G$ maximal, so liefert $U < \mathrm{N}_G(U)$, dass $\mathrm{N}_G(U) = G$ und damit $U \lhd G$.

3. $\Rightarrow$ 4. Sei $P \leq G$ eine p-Sylowgruppe von G. Dann ist $P < \mathrm{N}_G(P)$. Ist $\mathrm{N}_G(P) < G$, so gibt es eine maximale Untergruppe $U < G$ mit $\mathrm{N}_G(P) \leq U$. Nach 3.11 gilt dann $\mathrm{N}_G(U) = U$, Widerspruch zu 3. Also gilt $\mathrm{N}_G(P) = G$, das heißt $P \lhd G$ für jede Sylowgruppe P von G. Mit Satz **??** folgt die Behauptung 4.

4. $\Rightarrow$ 5. Wir zeigen $\mathrm{Z}_i < \mathrm{Z}_{i+1}$, falls $\mathrm{Z}_i < G$. Seien $P_1, \ldots, P_r$ die verschiedenen Sylowgruppen von G. Nach 4. ist dann

$$G = P_1 \times \ldots \times P_r.$$

   Laut Satz **??** gibt es dann Untergruppen $U_j \leq P_j$, so dass

$$\mathrm{Z}_i = U_1 \times \ldots \times U_r.$$

   Also ist

$$G/\mathrm{Z}_i \cong P_1/U_1 \times \ldots \times P_r/U_r$$

   das direkte Produkt von Sylowgruppen. Ist $P_j/U_j \neq \langle 1 \rangle$, gilt $\mathrm{Z}(P_j/U_j) \neq \langle 1 \rangle$ für die p-Gruppe P_j/U_j nach Satz 2.10. Also ist

$$\mathrm{Z}(G/\mathrm{Z}_i) = \mathrm{Z}(P_1/U_1) \times \ldots \times \mathrm{Z}(P_r/U_r) \neq \langle 1 \rangle$$

   und daher $\mathrm{Z}_{i+1} > \mathrm{Z}_i$.

5. $\Rightarrow$ 1. Sei

$$\langle 1 \rangle = \mathrm{Z}_0 \leq \mathrm{Z}_1 \leq \ldots \leq \mathrm{Z}_m = G$$

   die aufsteigende Zentralreihe von G. Nach 4. gilt $[\mathrm{Z}_{i+1}, G] \leq \mathrm{Z}_i$. Durch Induktion über i folgt damit

$$\mathrm{K}_i \leq \mathrm{Z}_{m+1-i} \quad \text{für} \quad i = 1, \ldots, m+1.$$

$i = 1$ ist klar und es gilt

$$\mathrm{K}_{i+1} = [K_i, G] \overset{\mathrm{IV}}{=} [\mathrm{Z}_{m+1-i}, G] \overset{7.2}{\leq} \mathrm{Z}_{m-i}\,.$$

Wegen $\mathrm{Z}_{m-m} = \langle 1\rangle$ ist also $\mathrm{K}_m = \langle 1\rangle$.

6. $\Rightarrow$ 4. Sei $|G| = p_1^{a_1} \cdot \ldots \cdot p_r^{a_r}$ die Primfaktorzerlegung und sei P_i eine p_i-Sylowgruppe von G. Nach Voraussetzung gilt dann:

$$P_j \leq \mathrm{C}_G(P_i) \qquad \text{für } i \neq j.$$

Induktiv folgt mit Lemma **??**: $P_1 \cdot \ldots \cdot P_i$ ist Untergruppe von G, da

$$(P_1 \cdot \ldots \cdot P_{i-1}) \cdot P_i = P_i \cdot (P_1 \cdot \ldots \cdot P_{i-1})\,.$$

Es gilt $(P_1 \cdot \ldots \cdot P_{i-1}) \cap P_i = \langle 1\rangle$ und $P_i \lhd P_1 \cdot \ldots \cdot P_{i-1}$. Mit dem Satz über das innere direkte Produkt **??** folgt

$$P_1 \cdot \ldots \cdot P_i \cong P_1 \times \ldots \times P_i.$$

Insgesamt erhalten wir

$$G = \langle P_1, \ldots, P_r\rangle = P_1 \cdot \ldots \cdot P_r \cong P_1 \times \ldots \times P_r.$$

7. $\Rightarrow$ 5. Nach 7.2 ist $\mathrm{Z}_i(G) \lhd G$. In der Faktorgruppe G/Z_i gilt

$$\mathrm{Z}(G/\mathrm{Z}_i) \neq 1, \text{ falls } \mathrm{Z}_i < G.$$

Also ist in diesem Fall $\mathrm{Z}_{i+1} > \mathrm{Z}_i$. Wegen $|G| < \infty$ folgt: Die aufsteigende Zentralreihe erreicht G.

4. $\Rightarrow$ 6. Sei $|G| = p_1^{a_1} \cdot \ldots \cdot p_r^{a_r}$ die Primfaktorzerlegung und sei P_i eine p_i-Sylowgruppe von G. Nach 4. gilt $G = P_1 \times \ldots \times P_r$. Ist $g \in P_i$ und $h \in P_j$ für $i \neq j$, so gilt $gh = hg$. Für beliebiges $g \in P$ gibt es eindeutig bestimmte $g_i \in P_i$ so, dass $g = g_1 \cdot \ldots \cdot g_r$. Ist $h = h_1 \cdot \ldots \cdot h_r$ mit $h_i \in P_i$ ein Element teilerfremder Ordnung, so gilt $h_i = 1$, falls $g_i \neq 1$ und umgekehrt, da $\operatorname{ord} g = \prod_{i=1}^{r} \operatorname{ord} g_i$. Wegen $g_i h_j = h_j g_i$ für $i \neq j$ gilt dann $gh = hg$.

4. und 5. $\Rightarrow$ 7. Aus $G = P_1 \times \ldots \times P_r$ folgt $N = U_1 \times \ldots \times U_r$ mit $U_i \leq P_i$ nach **??**. Damit ist $G/N \equiv P_1/U_1 \times \ldots \times P_r/U_r$, das heißt auch G/N ist direktes Produkt von Sylowgruppen und daher nilpotent. Nach 5. erreicht die aufsteigende Zentralreihe von G/N daher G/N, also ist insbesondere

$$\mathrm{Z}_1(G/N) = \mathrm{Z}(G/N) \neq \langle 1\rangle\,.$$

□

Bemerkung
Weitere zur Nilpotenz äquivalente Aussagen werden wir in **??** beweisen.

7.4 Folgerung

1. *Unter- und Faktorgruppen nilpotenter Gruppen sind nilpotent.*
2. *p-Gruppen sind nilpotent.*
3. *Sind G_1 und G_2 nilpotent, so auch $G_1 \times G_2$.*
4. *Sei $M \leq \mathrm{Z}(G)$ und G/M nilpotent. Dann ist G nilpotent.*

Beweis:

1. Sei $U \leq G = P_1 \times \ldots \times P_r$, wobei P_i Sylowgruppen von G sind. Nach **??** ist dann $U = U_1 \times \ldots \times U_r$ mit $U_i \leq P_i$, das heißt auch U ist das direkte Produkt von Sylowgruppen. Die Aussage für Faktorgruppen wurde in "4. und 5. $\Rightarrow$ 7." im Beweis des letzten Satzes bewiesen.
2. Das Kriterium 7.3.4 ist für p-Gruppen trivialerweise erfüllt.
3. Seien $G_1 = P_1 \times \ldots \times P_r$ und $G_2 = Q_1 \times \ldots \times Q_s$ die Zerlegungen in direkte Produkte von Sylowgruppen. Dann ist auch $G_1 \times G_2 = P_1 \times \ldots \times P_r \times Q_1 \times \ldots \times Q_s$ nach Zusammenfassen von Faktoren zur selben Primzahl ein direktes Produkt von Sylowgruppen.
4. Wir verwenden 7.3.7: Sei $N \lhd G, N \neq G$. Ist $M \leq N$, so ist

   $$(G/M)\,((N/M) \overset{0.3}{\cong} G/N$$

   als Faktorgruppe der nilpotenten Gruppe G/M nilpotent, das heißt die aufsteigende Zentralreihe von G/N erreicht G/N. Insbesondere ist $\mathrm{Z}(G/N) \neq \langle 1 \rangle$.

   Ist $M \not\leq N$, so ist $MN/N \leq \mathrm{Z}(G/N)$, da $M \leq \mathrm{Z}(G)$. Wegen $M \not\leq N$ ist $MN > N$ und daher $\mathrm{Z}(G/N) \neq \langle 1 \rangle$. Mit 7.3.7 folgt die Nilpotenz von G.

□

7.5 Satz
Sei G nilpotent und $\langle 1 \rangle \neq N \lhd G$. Dann ist $N \cap \mathrm{Z}(G) > \langle 1 \rangle$.

Beweis:
Sei p prim mit $p \mid |N|$ und sei P eine p-Sylowgruppe von G. Dann ist $P \cap N$ nach 3.12 eine p-Sylowgruppe von N und nach dem 1. Isomorphiesatz 0.2 ist $P \cap N \lhd P$. Deshalb operiert P auf der p-Gruppe $P \cap N$ durch Konjugation. Sind $B_1, \ldots, B_k$ die Bahnen dieser Operation, so gilt

$$|P \cap N| = \sum_{i=1}^{k} |B_i| .$$

Das 1-Element bildet eine Bahn, das heißt einer der Summanden auf der rechten Seite ist 1. Weil $|P \cap N|$ und $|B_i|$ Potenzen von p sind, folgt:

Es gibt noch weitere einelementige Bahnen, etwa $\{x\}$. Dann ist aber $g^{-1}xg = x$ für alle $g \in P$, also ist $x \in \mathrm{Z}(P)$ und damit $N \cap \mathrm{Z}(P) > \langle 1 \rangle$. Weil G das direkte Produkt der Sylowgruppe ist, ist $\mathrm{Z}(P) \leq \mathrm{Z}(G)$ und daher $N \cap \mathrm{Z}(G) > \langle 1 \rangle$. □

Bemerkung
Beachte: Satz 7.5 gilt insbesondere für p-Gruppen.

7.6 Definition und Satz *Nilpotenzklasse*
Ist

$$\langle 1 \rangle = \mathrm{Z}_0 < \mathrm{Z}_1 < \ldots < \mathrm{Z}_m = G$$

die aufsteigende Zentrahlreihe einer nilpotenten Gruppe G, so gilt für die absteigende Zentralreihe

$$G = \mathrm{K}_1 > \mathrm{K}_2 > \ldots > \mathrm{K}_{m+1} = \langle 1 \rangle ,$$

das heißt die beiden Reihen sind gleich lang. Die Länge m der Reihen heißt *Nilpotenzklasse* von G.

Beweis:
Sei

$$G = \mathrm{K}_1 > \mathrm{K}_2 > \ldots > \mathrm{K}_{n+1} = \langle 1 \rangle$$

die absteigende Zentralreihe vo G. Im Beweis von 7.3, "5. ⇒ 1." wurde gezeigt, dass $\mathrm{K}_i \leq \mathrm{Z}_{m+1-i}$. Das liefert $n \leq m$. Wir zeigen nun induktiv:

$$\mathrm{K}_{n+1-1} \leq \mathrm{Z}_i, \qquad \text{für } i = 0, \ldots, n.$$

$i = 0$: klar ($\langle 1 \rangle \leq \langle 1 \rangle$). $i \mapsto i + 1$: Nach 7.2.3 gilt:

$$\mathrm{K}_{n-1} / \mathrm{K}_{n+1-i} \leq \mathrm{Z}(G / \mathrm{K}_{n+1-i}) .$$

Nach Induktionsvoraussetzung ist $\mathrm{K}_{n+1-i} \leq \mathrm{Z}_i$. Wir betrachten nun den kanonischen Epimorphismus

$$\varphi : G/\mathrm{K}_{n+1-i} \to G/\mathrm{Z}_i, \quad g\,\mathrm{K}_{n+1-i} \mapsto g\,\mathrm{Z}_i\,.$$

Es ist

$$\varphi\left(\mathrm{K}_{n-i}\,/\,\mathrm{K}_{n+1-i}\right) \leq \varphi\left(\mathrm{Z}\left(G/\mathrm{K}_{n+1-i}\right)\right) \overset{\varphi \text{ surj.}}{\leq} \mathrm{Z}\left(G/\mathrm{Z}_i\right) = \mathrm{Z}_{i+1}\,/\,\mathrm{Z}_i,$$

das heißt für $g \in \mathrm{K}_{n-i}$ ist $\varphi\left(g\,\mathrm{K}_{n+1-i}\right) \in \mathrm{Z}_{i+1}\,/\,\mathrm{Z}_i$. Dann ist $g\,\mathrm{K}_{n+1-i} \subset \mathrm{Z}_{i+1}$, also $g \in \mathrm{Z}_{i+1}$ für $g \in \mathrm{K}_{n-i}$. Das liefert $\mathrm{K}_{n-i} \leq \mathrm{Z}_{i+1}$.

Insgesamt folgt $G = \mathrm{K}_{n+1-n} \leq \mathrm{Z}_n$, also $\mathrm{Z}_n = G$ und damit $n \geq m$. □

7.7 Folgerung
Wenn G nilpotent mit Nilpotenzklase m, dann gilt:

$$\mathrm{K}_i \leq \mathrm{Z}_{m+1-i} \qquad \textit{und} \qquad \mathrm{K}_{m+1-i} \leq \mathrm{Z}_i\,.$$

Beweis:
Beweis von 7.6 und 7.3, "5. ⇒ 1." □

In nilpotenten Gruppen gilt der folgende Zusammenhang zwischen G' und $\mathrm{Z}(G)$:

7.8 Satz J. Wiesgold, 1965
Sei p prim, G Gruppe mit $|G/\mathrm{Z}(G)| = p^n$. Dann ist G' eine p-Gruppe und es gilt

$$|G'| \leq p^{\frac{1}{2}n(n-1)}.$$

Beweis:
Für $n \leq 1$ ist G nach 2.2 abelsch und daher alles gezeigt. Sei nun $n \geq 2$ und sei die Behauptung induktiv bereits bewiesen für Gruppen G mit $|G/\mathrm{Z}(G)| = p^n$ und $m \leq n$. Die Idee des Beweises ist: Wir definieren ein $N \lhd G$ mit $N \leq G' \cap \mathrm{Z}(G)$ und benutzen, dass die Behauptung für G/N bereits gezeigt ist. Weil $G/\mathrm{Z}(G)$ eine p-Gruppe ist, gilt

$$\mathrm{Z}\left(G/\mathrm{Z}(G)\right) \neq \langle 1 \rangle$$

nach 2.10. Also ist $\mathrm{Z}_2(G) > \mathrm{Z}(G)$. Sei nun $x \in \mathrm{Z}_2(G)\,/\,\mathrm{Z}(G)$. Wir definieren

$$N := \langle [x,g] \mid g \in G \rangle\,.$$

Nach 7.2 ist

$$[\mathrm{Z}_2(G), G] \leq \mathrm{Z}_1(G) = \mathrm{Z}(G)\,,$$

das heißt es gilt $N \leq \mathrm{Z}(G)$ und daher $N \lhd G$.

Wir setzen nun $H := G/N$. $\mathrm{Z}(H)$ enthält natürlich $\mathrm{Z}(G)/N$, aber auch $x \in N$, denn für $y \in G$ ist

$$[xN, yN] = [x, y]\, N = N \qquad \text{für alle } y \in G.$$

Wegen $x \in \mathrm{Z}(G)$ liegt xN allerdings nicht in $\mathrm{Z}(G)/N$. Damit ist $\mathrm{Z}(H) > \mathrm{Z}(G)/N$. Mit dem 2. Isomorphiesatz 0.3 erhalten wir

$$H/\left(\mathrm{Z}(G)/N\right) = (G/N)/\left(\mathrm{Z}(G)/N\right) \cong G/\mathrm{Z}(G),$$

das heißt $H/\left(\mathrm{Z}(G)/N\right)$ ist p-Gruppe der Ordnung p^n. Damit ist $|H/\left(\mathrm{Z}(G)/N\right)| = p^m$ mit $m < n$. Nach Induktionsvoraussetzung ist aber H' eine p-Gruppe mit $|H'| \leq p^{\frac{1}{2}(n-1)(n-2)}$. Da $N \leq G'$ nach Definition von N, ist nach 2.17

$$H' = (G/N)' = G'N/N = G'/N. \tag{1}$$

Wir müssen daher nun zeigen, dass N eine p-Gruppe ist und $|N|$ abschätzen. Wegen $N' \in \mathrm{Z}(G)$ gilt

$$[x, g] \cdot [x, h] = [x, g]\, g^{-1}\, [x, h]\, g \overset{2.13.6}{=} [x, gh]$$

und

$$[x, g]^{-1} \overset{2.13.9}{=} \left[x, g^{-1}\right]$$

für alle $g, h \in G$. Jdes Element von N ist daher ein Kommutator der Form $[x, g]$ mit einem $g \in G$. Nun ist

$$[x, g] = [x, h] \qquad \Leftrightarrow \qquad g^{-1}xg = h^{-1}xh,$$

das heißt $|N|$ ist gerade die Zahl der Konjugierten von $x \in G$. Daher gilt

$$|N| = \frac{|G|}{|\mathrm{C}_G(x)|}$$

nach 2.7. Der Zentralisator $\mathrm{C}_G(x)$ enthält sowohl das Zentrum, als auch x, folglich gilt $\mathrm{C}_G(x) > \mathrm{Z}(G)$ und damit $[G : \mathrm{C}_G(x)] \mid p^{n-1}$. Demnach ist N eine p-Gruppe mit $|N| \leq p^{n-1}$. Mit (1) folgt daher nun: G' ist eine p-Gruppe mit Ordnung

$$|G'| = |H'| \cdot |N| \leq p^{\frac{1}{2}(n-1)(n-2)} \cdot p^{n-1} = p^{\frac{1}{2}n(n-1)}.$$

□

Bemerkung

1. Gruppen $|G/\operatorname{Z}(G)| = p^n$ sind nach 7.4.4 nilpotent.

2. Es gibt Gruppen mit $|G/\operatorname{Z}(G)| = p^n$ und $|G'| = p^{\frac{1}{2}n(n-1)}$ für jedes n, das heißt die Abschätzung kann nicht verbessert werden.

3. Die Ordnungen von $G', \operatorname{Z}(G)$ und der im nächsten Kapitel behandelten Frattini-Gruppe $\Phi(G)$ hängen allgemein eng zusammen. Eine weitere Aussage, die G' mit $\operatorname{Z}(G)$ verknüpft, ist der folgende

Satz Herzog, Kaplan, Lev 2004
Sei $G \neq \langle 1 \rangle$ *mit* $\exp(G/G') \geq |G'|$. *Dann ist* $\operatorname{Z}(G) \neq \langle 1 \rangle$.

Unser nächstes Ziel ist eigentlich die Untersuchung von p-Gruppen. Vorher müssen wir aber noch ein Kapitel über die Frattini-Gruppe einschieben, die sich bei der Untersuchung von p-Gruppen als nützlich erweist.

8 Der Satz von Schur-Zassenhaus

Der Satz von Schur-Zassenhaus ist wohl nach dem Satz von Sylow der wichtigste Satz der Gruppentheorie. Wie der Satz von Hall macht er eine Aussage über Existenz und Konjugiertheit von Untergruppen mit bestimmten Ordnungen, ohne allerdings, wie im Satz von Hall, die Auflösbarkeit vorauszusetzen. Im folgenden Lemma wird der Satz zunächst für einen Spezialfall bewiesen:

8.1 Lemma
Sei $N \lhd G$ *abelsch und* $\operatorname{ggT}(|N|, |G/N|) = 1$. *Dann besitzt* N *ein Komplement in* G *und alle Komplemente von* G *sind konjugiert.*

Beweis:
Ist K ein Komplement von N in G, so gilt $G = NK = KN$, das heißt es ist $G = \bigcup_{x \in K} N_x$ die disjunkte Vereinigung. K ist also eine Transversale der Rechtsnebenklassen von N in G. Sei Θ die Menge aller Transversalen von Rechtsnebenklassen von N in G. Wir konstruieren ein Komplement von N als Stabilisator einer geeigneten Gruppenoperation auf $\Theta/\sim$ mit einer Äquivalenzrelation $\sim$.

Für $S, T \in \Theta$ sei

$$S \mid T = \prod_{(s,t) \in S \times T} \left(st^{-1}\right).$$

Wegen $Ns = Nt \Leftrightarrow st^{-1} \in N$ ist $S \mid T \in N$. Weil N abelsch ist, ist die Reihenfolge in dem Produkt unerheblich. Für $R, S, T \in \Theta$ gilt:

$$(S \mid T)^{-1} = \prod_{\substack{(s,t)\in S\times T \\ Ns=Nt}} \left(st^{-1}\right) = T \mid S. \tag{2}$$

$$(R \mid S)(S \mid T) = \prod_{\substack{(r,s)\in R\times S \\ Nr=Ns}} \left(rs^{-1}\right) \prod_{\substack{(s,t)\in S\times T \\ Ns=Nt}} \left(st^{-1}\right) = R \mid T \tag{3}$$

Durch die Festsetzung $S \sim T \Leftrightarrow S \mid T = 1$ wird wegen (2) und (3) eine Äquivalenzrelation auf Θ definiert. Im folgenden bezeichnen wir die Äquivalenzklasse von T mit $\widetilde{T}$.

Nun wollen wir eine Gruppenoperation auf $\Theta/\sim$ definieren. Da $N \lhd G$, ist jedes $T \in \Theta$ auch eine Transversale von Linksnebenklassen, das heißt es ist $G = \bigcup_{t\in T} tN$ eine disjunkte Vereinigung. G operiert durch Linksmultiplikation auf $Theta$ vermöge

$$\Theta \times G \to \Theta, (T, g) \mapsto g^{-1}T.$$

Aus

$$(xS) \mid (xT) = \prod_{\substack{(s,t)\in S\times T \\ Nxs=Nxt}} x\left(st^{-1}\right)x^{-1} = x\,(S \mid t)\,x^{-1}$$

folgt

$$S \mid T = 1 \Rightarrow (xS) \mid (xT) = 1. \tag{4}$$

Deshalb wird durch $\widetilde{T}^x = \widetilde{x^{-1}T}, x \in G$ eine Operation von G auf $\Theta/\sim$ definiert. Wir zeigen nun, dass N dabei transitiv operiert:

Für $n \in N$ gilt

$$(nS) \mid T = \prod_{\substack{(ns,t)\in nS\times T \\ Nns=Nt}} \left(nst^{-1}\right) \underset{|G/N| \text{ Faktoren}}{\overset{N \text{ abelsch}}{=}} n^{|G/N|}\,(S \mid T)\,. \tag{5}$$

Weil $|N|$ und $|G/N|$ teilerfremd sind und N abelsch ist, ist die Abbildung

$$\alpha : N \to N, \quad n \mapsto n^{|G/N|}$$

ein Automorphismus von N. Wählen wir nun $n \in N$ so, dass $n^{|G/N|} = (S \mid T)^{-1}$, so gilt nach (5) folglich:

$$(nS) \mid T = 1 \tag{6}$$

$$S \mid T = 1 = (nS) \mid T \Rightarrow n = 1. \tag{7}$$

Also ist $\widetilde{S}^{n^{-1}} = \widetilde{nS} = \widetilde{T}$, das heißt N operiert transitiv auf $\Theta/\sim$. Wegen (7) ist der Stabilisator von $\widetilde{T}$ in N trivial. Nach dem Frattiniargument I **??.??** ist folglich der Stabilisator

$$K := G_{\widetilde{T}} = \{x \in G : \quad (xT) \mid T = 1\}.$$

ein Komplement von N in G.

Ist umgekehrt X ein Komplement von N in G, so gilt $xX = X$ für alle $x \in X$ und daher

$$(xX) \mid X = X \mid X = \prod_{\substack{(y,z)\in X\times X \\ Ny=Nz}} \left(yz^{-1}\right) = 1,$$

denn für $y, z \in X$ gilt

$$Ny = Nz \Leftrightarrow y = z,$$

weil X ein Komplement. Also ist $X = G_{\widetilde{T}}$ für $T = X$. Weil N und damit G transitiv auf $\Theta/\sim$ operieren, ergibt sich die Konjugiertheit der Komplemente daher aus der Konjugiertheit der Stabilisatoren, also aus 5.6. □

Mit diesem Spezialfall können wir nun den allgemeinen Fall beweisen.

8.2 Satz Schur-Zassenhaus
Sei $N \lhd G$ mit $\mathrm{ggT}(|N|, |G/N|) = 1$. *Dann gilt:*

1. *N besitzt ein Komplement in G.*
2. *Ist N oder G/N auflösbar, so sind alle Komplemente von N in G konjugiert.*
3. *Sei $U < G$ mit $|U| \mid |G/N|$. Sind N oder G/N auflösbar, so ist U in einer Untergruppe der Ordnung $|G/N|$ von G enthalten.*

Beweis:
Sei $U \leq G$. Wegen $UN/N \cong U/U \cap N$ (1. Isomorphiesatz 0.2) ist $U \cap N \lhd TODO$ mit $\mathrm{ggT}(|U \cap N|, |WU \cap N|) = 1$. Sei $M \lhd G$. Wegen

$$(G/M) / (MN/M) \overset{0.3}{\cong} G/MN$$

ist $MN/M \lhd G/M$ mit $\mathrm{ggT}(|MN/M|, |G/MN|) = 1$. Die Voraussetzungen vererben sich also auf Unter- und Faktorgruppen. Sind N oder G/N auflösbar, dann vererbt sich auch diese Voraussetzung auf die entsprechenden Unter- und Faktorgruppen.

1. Wir machen Induktion über $|G|$ und setzen voraus, dass die Behauptung für Gruppen kleinerer Ordnung gilt. Sei p prim mit $p \mid |N|$. Sei P eine p-Sylowgruppe von N und sei $U := \mathrm{N}_G(P)$. Ist $U < G$, so besitzt $U \cap N$ ein Komplement K in U. Nach dem Frattini-Argument II **??**.**??** erhalten wir
$$G = NU = N(U \cap N)K = NK.$$
Da $N \cap K = (N \cap U) \cap K = \langle 1 \rangle$, ist K sogar ein Komplement von N in G. Sei nun $U = G$. Dann ist $P \lhd G$. Aus $\mathrm{Z}(P) \operatorname{char} P \lhd G$ folgt
$$\langle 1 \rangle \overset{2.10}{\neq} \mathrm{Z}(P) \lhd G.$$
Wir setzen nun $\overline{G} := G/\mathrm{Z}(P)$.

   Sei nun $\mathrm{Z}(P) \leq V \leq G$, so dass $\overline{V} := V/\mathrm{Z}(P)$ ein Komplement von $\overline{N} := N/\mathrm{Z}(P)$ in $\overline{G}$ ist. Dann ist
$$V \cap N = \mathrm{Z}(P) \qquad \text{und} \qquad G = NV.$$
Daher ist ein Komplement von $\mathrm{Z}(P)$ in V zugleich Komplement von N in G. Ist $V < G$, so besitzt $\mathrm{Z}(P)$ nach Induktionsvoraussetzung ein Komplement n V und wir sind fertig. Ist $V = G$, so ist $N = \mathrm{Z}(P)$ ein abelscher Normalteiler. Diese Gruppe besitzt nach 8.1 ein Komplement.

2. Wir machen wieder Induktion über $|G|$. Seien K_1 und K_2 Komplemente von N in G. Sei M ein minimaler Normalteiler von G, der in N liegt und sei $\overline{G} := G/M$. Dann sind $\overline{K_1} := K_1M/M$ und $\overline{K_2} := K_2M/M$ Komplemente von $\overline{N} = N/M$ in $\overline{G}$. Nach Induktionsvoraussetzung sind $\overline{K_1}$ und $\overline{K_2}$ konjugiert in $\overline{G}$, das heißt es gibt ein $g \in G$, so dass
$$K_1M = (K_2M)^g = K_2^gM^g = K_2^gM.$$
K_1 und K_2^g sind somit zwei Komplemente von M in K_1M. Im Falle $M \neq N$ ist $K_1M \neq G$. Die Komplemente K_1 und K_2^g sind daher nach Induktionsvoraussetzung konjugiert in K_1M, also auch in G. Sei nun $M = N$. Ist N auflösbar, so ist M also auflösbarer minimaler Normalteiler von G abelsch nach **??** (der Beweis gibt das her). Damit folgt die Behauptung in diesem Fall aus 8.1.

   Sei nun N nicht auflösbar, also $\overline{G} := G/N$ auflösbar. In $\overline{G}$ existiert dann ein Normalteiler $\overline{A} \lhd \overline{G}$, so dass $\overline{G}/\overline{A}$ eine nicht trivialie p-Gruppe ist (in einer Kompositionsreihe von $\overline{G}$ sind alle Gruppen zyklisch von Primzahlordnung). Sei A das Urbild von $\overline{A}$ in G. Dann gilt $N \leq A \lhd G$

nach dem Korrespondenzsatz 1.4. Wenden wir in dieser Situation die Dedekind-Identität **??** an, so ergibt sich

$$A = G \cap A = (NK_1) \cap A = N(K_1 \cap A)$$

(und analog für K_2), also sind $K_1 \cap A$ und $K_2 \cap A$ Komplemente von N in A. Nach Induktionsvoraussetzung sind diese Komplemente in A konjugiert. Nach einer geeigneten Konjugation können wir daher ohne Einschränkung

$$K_1 \cap A = K_2 \cap A =: D$$

annehmen. Wegen $A \lhd G$ gilt $K_1 \cap A \lhd K_1$ und $K_2 \cap A \lhd K_2$ und daher $D \lhd \langle K_1, K_2 \rangle$. Wegen

$$K_1/D \overset{0.2}{\cong} K_1A/A = G/A \,(\cong K_2/D)$$

sind K_1/D und K_2/D Gruppen derselben Primzahlordnung p. Folglich existieren p-Sylowgruppen P_1 von K_1 udn P_2 von K_2, so dass $K_1 = DP_1$ und $K_2 = DP_2$.

Da $\mathrm{ggT}(|N|, |K_1|) = 1$ sind P_1 und P_2 auch p-Sylowgruppen von G und somit auch von $\mathrm{N}_G(D) > \langle K_1, K_2 \rangle$. Nach dem Satz von Sylow 3.10 existiert daher ein $g \in \mathrm{N}_G(D)$ mit $P_1 g = P_2^g$. Es folgt

$$K_1^g = (DP_1)^g = D^g P_1^g = DP_2 = K_2.$$

3. Sei K ein Komplement von N in G und sei $U < G$ mit $|U| \mid |K|$. Sei $|U| =: d$. Es gilt $G = KN$ und die Dedekind-Identität **??** mit $A := N \leq UN =: C$ und $B := K$ angewendet lierfert

$$UN = UN \cap KN = (UN \cap K)\, N.$$

Damit erhalten wir

$$|UN| \overset{??}{=} \frac{|U|\,|N|}{|U \cap N|} = \frac{|UN \cap K|\,|N|}{|UN \cap K \cap N|}$$

und damit

$$d = |U| = |UN \cap K|,$$

da

$$|U \cap N| \underset{|U|\mid|K|}{=} 1 = |UN \cap K \cap N|.$$

Wenden wir (3) auf UN, N statt G, N an, so gibt es ein $g \in UN$ mit $U = (UN \cap K)^g \leq K^g$ und $|K^g| = |K|$.

□

8.3 Bemerkung

1. Die Bedinung "N oder G/N auflösbar" in Teil 2 und 3 ist überflüssig, denn wegen $\mathrm{ggT}(|N|, |G/N|) = 1$ ist die Ordnung von mindestens einer der beiden Gruppen ungerade. Diese Gruppe ist nach dem Satz von Feit-Thompson auflösbar. Es ist aber kein Beweis dieses verschärften Satzes bekannt, der nicht den tiefliegenden Satz von Feit-Thompson oder ähnlich tiefliegende Resultate verwendet.

2. Als direkte Anwendung des Satzes von Schur-Zassenhaus folgt, dass der Normalisator $\mathrm{N}_G(P)$ einer p-Sylowgruppegruppe P von G immer ein semidirektes Produkt $\mathrm{N}_G(P) = P \rtimes K$ für ein $K \leq G$ ist. Dies wird häufig verwendet, so auch im Beweis des folgenden Satzes:

8.4 Satz
Sei p prim. Gilt $p \mid |\Phi(G)|$, so gilt auch $p \mid |G/\Phi(G)|$.

Beweis:
Angenommen, es gilt $p \nmid |\Phi(G)|$. Sei P eine p-Sylowgruppe von $\Phi(G)$. Weil $\Phi(G)$ nilpotent ist (**??**) gilt:

$$P \operatorname{char} \Phi(G) \operatorname{char} G$$

und daher $P \lhd G$. Da P SYlowgruppe ist, haben wir $\mathrm{ggT}(|P|, |G/P|) = 1$. Nach dem Satz von Schur-Zassenhaus 8.2 besitzt P folglich ein Komplement K in G. Also ist

$$G = PK \leq \Phi(G) K \overset{??}{=} K < G.$$

Widerspruch! Eine weitere Möglichkeit, Komplemente von Untergruppen zu finden, werden wir im nächsten Kapitel kennen lernen. □

9 Die Verlagerung

Für eine beliebige Untergruppe $Q \leq G$ definiert die Verlagerung V einen Homomorphismus $V : G \to Q/Q'$. In bestimmten Fällen ist $\operatorname{Ker} V$ ein (normales) Komplement zu Q in G.

9.1 Lemma
Sei $Q \leq G$ mit $[G : Q] = n$. Seien $\{l_1, \ldots, l_n\}$ und $\{h_1, \ldots, h_n\}$ Linkstransversalen von Q in G. Sei $g \in G$. Zu jedem i gibt es genau ein $\sigma(i) \in \{1, \ldots, n\}$ und genau ein $x_i \in Q_i$, so dass

$$gh_i = l_{\sigma(i)} x_i.$$

σ ist eine Permutation der Zahlen $\{1, \ldots, n\}$.

Beweis:
Da $G = \bigcup_{i=1}^{n} l_i Q$ eine disjunkte Vereinigung, gibt es genau eine Linksnebenklasse $l_{\sigma(i)Q}$ mit $gh_i \in l_{\sigma(i)}Q$. Auch das $x_i \in Q$ mit $gh_i = l_{\sigma(i)}x_i$ ist eindeutig bestimmt.

Nun gelte $\sigma(i) = \sigma(k) = j$. Dann ist $gh_i = l_i x_i$ und $gh_k = l_j x_k$. Daraus folgt:

$$\begin{aligned} gh_i x_i^{-1} = gh_k x_k^{-1} &\Leftrightarrow h_i^{-1}h_k = x_i^{-1}x_k \in Q \\ &\Leftrightarrow h_i Q = h_k Q \\ &\Leftrightarrow i = k. \end{aligned}$$

Also ist σ injektiv und damit bijektiv. □

9.2 Definition *Verlagerung*
Sei $Q \leq G$ eine Untergruppe mit $[G : Q] = n, Q'$ die Kommutatorgruppe von Q. Sei $\{P_1, \ldots, P_n\}$ eine Linkstransversale von Q in G. Die *Verlagerung* ist die Abbildung

$$V : G \to Q/Q', \qquad V(g) = \prod_{i=1}^{n} x_i Q',$$

wobei $gl_i = l_j x_i$. Oft schreibt man kurz $V_{G\to Q}$ für die Verlagerung.

Bemerkung
Die über Rechtstransversalen definierte Verlagerung ist mit V identisch.

9.3 Satz
Sei $Q \leq G$ mit $[G : Q] = n$. Dann ist die Verlagerung $V : G \to Q/Q'$ ein Homomorphismus und die Definition von V ist unabhängig von der Wahl der Linkstransversale von Q in G.

Beweis:
Seien $\{l_1, \ldots, l_n\}$ und $\{h_1, \ldots, h_n\}$ Linkstransversalen von Q in G. Sei $g \in G$. Nach 9.1 gibt es $\sigma, \tau, \alpha \in \mathrm{S}_n$ und $x_i, y_i, z_i \in Q$, so dass

$$\begin{aligned} gl_i &= l_{\sigma(i)}x_i, \\ gh_i &= h_{\tau(i)}y_i, \\ h_i &= l_{\alpha(i)}z_i. \end{aligned}$$

Damit ist

$$gh_i = gl_{\alpha(i)}z_i = l_{\sigma(\alpha(i))}x_{\alpha(i)}z_i.$$

Definieren wir j durch $\alpha(j) = \sigma(\alpha(i))$, so haben wir $h_j = l_{\sigma(\alpha(j))}z_j$ und damit $gh_i = h_j z_j^{-1} x_{\alpha(i)} z_i$. Die Eindeutigkeitsaussage in 9.1 und die Definition von j liefern uns $j = \tau(i)$ und

$$y_i = z_j^{-1} x z_i = z_{(\alpha^{-1}\sigma\alpha)(i)} x_{\alpha(i)} z_i.$$

In der abelschen Gruppe Q/Q' können wir Faktoren vertauschen, also ist

$$\prod_{i=1}^{n} y_i Q' = \prod_{i=1}^{n} x^{-1}_{(\alpha^{-1}\sigma\alpha)(i)} x_{\alpha(i)} z_i Q' = \prod_{i=1}^{n} x_{\alpha(i)} Q' = \prod_{i=1}^{n} x_i Q',$$

denn wegen $\alpha^{-1}\sigma\alpha \in \mathrm{S}_n$ taucht das Inverse von allen z_i auf und annulliert z_i. Also ist V unabhängig von der Wahl der Transversalen.

Sei nun $g, g' \in G$ und sei $\{l_1, \ldots, l_n\}$ eine Linkstransversale von Q in G. Dann gibt es $\sigma, \tau \in \mathrm{S}_n$ und $x_i, y_i \in Q$, so dass $g l_i = l_{\sigma(i)}$ und $g' l_i = l_{\tau(i)} y_i$. Es folgt

$$g g' l_i = g l_{\tau(i)} y_i = l_{\sigma(\tau(i))} x_{\tau(i)} y_i.$$

Deshalb ist

$$V(gg') = \prod_{i=1}^{n} x_{\tau(i)} y_i Q' = \left(\prod_{i=1}^{n} y_i Q' \right) \left(\prod_{i=1}^{n} x_{\tau(i)} Q' \right) = V(g)\, V(g').$$

Also ist V ein Homomorphismus. □

Das folgende Lemma sagt aus, dass $V(g)$ das Produkt von konjugierten von Potenzen von G ist:

9.4 Lemma
Sei $Q \leq G$ mit $[G : Q] = n$ und sei $\{l_1, \ldots, l_n\}$ eine Linkstransversale von Q in G. Für jedes $g \in G$ existieren Elemente $h_1, \ldots, h_m \in G$ und Zahlen $n_1, \ldots, n_m \in \mathbb{N}$ (alle von g abhängig), so dass gilt:

1. $h_i \in \{l_1, \ldots, l_n\}$.
2. $h_i^{-1} g_i^{-1} h_i \in Q$.
3. $\sum_{i=1}^{m} n_i = n = [G : Q]$.
4. $V(g) = \prod_{i=1}^{m} \left(h_i^{-1} g^{n_i} h_i \right) Q'$.

Beweis:
Nach 9.1 gibt es $\sigma \in \mathrm{S}_n$ und $x_i \in Q$, so dass $g l_i = l_{\sigma(i)} x_i$. Wir zerlegen σ in ein Produkt $\sigma = \alpha_1 \cdot \ldots \cdot \alpha_n$ disjunkter Zykel, wobei wir Fixpunkte nicht weglassen. Ist $\alpha = (j_1, \ldots, j_r)$, so gilt:

$$g l_{j_1} = l_{\sigma(j_1)} x_{j_1} = l_{j_2} x_{j_1} g l_{j_2} = l_{j_3} x_{j_2}, \ldots, g l_{j_r} = l_{j_1} x_{j_r}.$$

Q enthält das Element

$$x_{j_r} \cdot \ldots \cdot x_{j_1} = \left(l_{j_1}^{-1} g l_{j_r} \right) \cdot \ldots \cdot \left(l_{j_3}^{-1} g l_{j_2} \right) \left(l_{j_2}^{-1} g l_{j_1} \right) = l_{j_1}^{-1} g^r l_{j_1}.$$

Wir setzen nun $h_i := l_{j_1}$ und $n_i := r$ und erhalten die Behauptung. □

9.5 Satz
Sei $Q < G$ mit $[G : Q] = n$ und $V : G \to Q/Q'$ die Verlagerung. Dann gilt:

1. *Für $g \in \mathrm{Z}(G)$ ist $V(g) = g^n Q'$.*
2. *Ist $Q \leq \mathrm{Z}(G)$, so ist $V(g) = g^n$ für alle $g \in G$.*

Beweis:

1. Nach 9.4 gibt es $h_i \in G, n_i \in \mathbb{N}$, so dass

$$V_i(g) = \prod_{i=1}^{m} h_i^{-1} g^{n_i} h_i Q'.$$

   Für $g \in \mathrm{Z}(G)$ ist aber $h_i^{-1} g^{n_i} h_i = g^{n_i}$ und daher

$$V(g) = \prod_{i=1}^{m} g^{n_i} Q' = g^n \underbrace{Q'}_{=\langle 1 \rangle}.$$

2. Ist $Q \leq \mathrm{Z}(G)$, so ist $Q \lhd G$. Falls $h^{-1} g^r h \in Q$ für $h, g \in G$, gilt auch

$$g^r = h \left(h^{-1} g^r h\right) h^{-1} \in Q.$$

   Nach 9.4 gibt es für $g \in G$ Elemente $h_i \in G$ und Zahlen $n_i \in \mathbb{N}$ mit $\sum_{i=1}^{m} n_i = n$, so dass

$$V(g) = \prod_{i=1}^{m} \underbrace{h_i^{-1} g h_i}_{\in Q} Q' = \prod_{i=1}^{m} g^{n_i} Q' = g^n Q',$$

   denn wegen $h_i^{-1} g^{n_i} h_i \in Q \leq \mathrm{Z}(G)$ ist auch $g^{n_i} \in \mathrm{Z}(G)$ und daher

$$h_i^{-1} g^{n_i} h_i = g^{n_i}.$$

□

9.6 Folgerung
Besitzt eine Gruppe G eine Untergruppe $Q \leq \mathrm{Z}(G)$ mit $[G : Q] = n$, so ist die Abbildung

$$\varphi : G \to Q, \qquad g \mapsto g^n$$

ein Homomorphismus.

Beweis:
Wegen $Q \leq \mathrm{Z}(G)$ ist Q abelsch und daher $Q' = \langle 1 \rangle$, das heißt wir können die Verlagerung als Homomorphismus $V : G \to Q$ auffassen. Gemäß 9.5 ist $V(g) = g^n$ und V ist nach 9.3 ein Homomorphismus. □

9.7 Satz
Sei $H < G$ und sei $\mathrm{ggT}([G:H],[H,H']) = 1$. *Dann gilt:*

$$H \cap G' \cap \mathrm{Z}(G) \leq H'.$$

Beweis:
Wir betrachten die Verlagerung $V : G \to H/H'$. Sei $g \in H \cap G' \cap \mathrm{Z}(G)$. Da $g \in \mathrm{Z}(G)$, gilt $V(g) = g^{[G:H]}H'$. Weil V ein Homomorphismus in die abelsche Gruppe H/H' ist, gilt

$$V(g) = 1 \cdot H' \qquad \forall g \in G'$$

nach 2.13.3. Für $g \in G' \cap \mathrm{Z}(G)$ ist daher $V(g) = g^{[G:H]}H' = 1 \cdot H'$.
Wegen $g \in H$ und

$$\mathrm{ggT}([G:H],[H:H']) = 1$$

gilt auch

$$\mathrm{ggT}(\mathrm{ord}\, gH', [G:H]) = 1.$$

Daraus folgt $g \in H'$. □

9.8 Folgerung
Sei P eine p-Sylowgruppe von G. Dann gilt $P \cap G \cap \mathrm{Z}(G) \leq P'$. Ist P abelsch, so ist insbesondere $P \cap G' \cap \mathrm{Z}(G) = \langle 1 \rangle$. Sind alle Sylowgruppen von G abelsch, so ist $G' \cap \mathrm{Z}(G) = \langle 1 \rangle$.

Beweis:
Für die p-Sylowgruppe P ist die in 9.7 nötige Bedingung

$$\mathrm{ggT}([G:P],[P:P']) = 1$$

automatisch erfüllt. Sind alle Sylowgruppen von G abelsch, so sei $g \in G' \cap \mathrm{Z}(G)$ mit $\mathrm{ord}\, g = p$ prim. Dann gibt es eine p-Sylowgruppe P von G mit $g \in P$. Aus $P \cap G' \cap \mathrm{Z}(G) = \langle 1 \rangle$ folgt aber $g = 1$. ⇒ Widerspruch! □

9.9 Lemma
Sei p prim und P eine p-Sylowgruppe von G. Sind $g, h \in \mathrm{C}_G(P)$ konjugiert in G, so sind sie konjugiert in $\mathrm{N}_G(P)$.

Beweis:
Sei $h = x^{-1}gx$ für $x \in G$. Dann ist

$$h \in x^{-1}\,\mathrm{C}_G(P)\,x \overset{2.5}{=} \mathrm{C}_G\left(x^{-1}Px\right).$$

Damit sind P und $x^{-1}Px$ p-Sylowgruppen von $\mathrm{C}_G(H)$. Nach dem Satz von Sylow 3.10 sind die beiden Gruppen daher in $\mathrm{C}_G(H)$ konjugiert, das heißt es gibt ein $c \in \mathrm{C}_G(H)$, so dass

$$P = c^{-1}x^{-1}Pxc.$$

Das Element xc ist folglich in $\mathrm{N}_G(P)$ enthalten und es gilt

$$c^{-1}x^{-1}gxg = c^{-1}hc = h.$$

□

9.10 Satz Satz vom normalen Komplement, Burnside (1900)
Sei $P \leq G$ eine abelsche Sylowgruppe mit $P \leq \mathrm{Z}(\mathrm{N}_G(P))$, das heißt P sei im Zentrum ihres Normalisators enthalten. Dann hat P ein normales Komplement K in G.

Beweis:
P ist abelsch, das heißt es gilt $P' = \langle 1\rangle$ und wir können die Verlagerung als Homomorphismus $V : G \to P$ auffassen. Wir berechnen $V(g)$ für $g \in P$. Nach 9.4 gibt es Elemente $h_i \in G$ und Zahlen $n_i \in \mathbb{N}$, so dass

$$V(g) = \sum_{i=1}^{m} h_i^{-1}gh_i.$$

Dabei gilt $g^{n_i} \in P$ (weil $g \in P$) und $h_i^{-1}g^{n_i}h_i \in P$ nach 9.4. Weil P abelsch ist, ist $P \leq \mathrm{C}_G(P)$ und daher $g^{n_i}, h_i^{-1}g^{n_i}h_i \in \mathrm{C}_G(P)$. Gemäß Lemma 9.9 sind die Elemente g^{n_i} und $h_i^{-1}g^{n_i}h_i \in \mathrm{N}_G(P)$ konjugiert, das heißt $\exists c_i \in \mathrm{N}_G(P)$, sodass

$$h_i^{-1}g^{n_i}h_i = c_i^{-1}g^{n_i}c_i.$$

Aus $g^{n_i} \in P \leq \mathrm{Z}(\mathrm{N}_G(P))$ folgt nun aber sogar $c_i^{-1}g^{n_i}c_i = g^{n_i}$. Damit ist $V(g) = g^n$ für alle $g \in P$, wobei $n := [G : P]$. Sei $|P| =: q$. Weil n und q teilerfremd sind, gibt es ganze Zahlen α, β mit $\alpha n + \beta q = 1$. Daher ist

$$g^{\alpha n+\beta q} = g^{\alpha n}g^{\beta q} = (g^{\alpha})^{n},$$

das heißt $V : G \to P$ ist surjektiv. Sei nun $K := \operatorname{Ker} V$. Nach dem Homomorphiesatz gilt $G/K \cong P$ und wegen $|K| = n$ und $\mathrm{ggT}(|K|, |P|) = 1$ ist dann $G = KP$ und $K \cap P = \langle 1\rangle$. □

9.11 Definition *p-nilpotent*
Wenn eine p-Sylowgruppe von G ein normales Komplement besitzt, heißt G *p-nilpotent*. Damit lautet der Satz von Burnside:

Ist $P \leq G$ eine abelsche p-Sylowgruppe mit $P \leq \mathrm{Z}(\mathrm{N}_G(P))$, so ist G p-nilpotent.

9.12 Satz
Sei p der kleinste Primteiler von $|G|$. Sind die p-Sylowgruppen von G zyklisch, so ist G p-nilpotent.

Beweis:
Sei P eine p-Sylowgruppe von G. Nach Satz 2.4 ist $\mathrm{N}_G(P) / \mathrm{C}_G(P)$ isomorph zu einer Untergruppe von $\operatorname{Aut} P$. Insbesondere gilt

$$|\mathrm{N}_G(P) / \mathrm{C}_G(P)| \mid |\operatorname{Aut} P|.$$

Ist $|P| = p^m$, so ist $|\operatorname{Aut} P| = p^{m-1}(p-1)$ nach Folgerung 4.6. Da P zyklisch ist, gilt $P \leq \mathrm{C}_G(P)$ und daher

$$p \nmid |\mathrm{N}_G(P) / \mathrm{C}_G(P)|.$$

Also ist

$$|\mathrm{N}_G(P) / \mathrm{C}_G(P)| \mid (p-1).$$

Gleichzeitig gilt aber

$$|\mathrm{N}_G(P) / \mathrm{C}_G(P)| \mid |G|$$

und p ist der kleinste Primteiler von $|G|$. Also folgt

$$|\mathrm{N}_G(P) / \mathrm{C}_G(P)| = 1,$$

das heißt $\mathrm{N}_G(P) = \mathrm{C}_G(P)$ und daher

$$P \leq \mathrm{Z}(\mathrm{N}_G(P)).$$

Also folgt die Behauptung mit 9.10. □

9.13 Folgerung
Sei G eine Gruppe mit einer zyklischen 2-Sylowgruppe P. Dann ist

$$G = \mathcal{O}(G) \rtimes P$$

ein semidirektes Produkt.

9.14 Folgerung
Eine nicht abelsche einfache Gruppe kann keine zyklischen 2-Sylowgruppen enthalten.

9.15 Bemerkung
Der Satz von Brauer-Suzuki macht eine ähnliche Aussage, wenn die 2-Sylowgruppen verallgemeinerte Quaternionengruppen sind. Genauer gilt:

Sei G eine Gruppe, deren 2-Sylowgruppen verallgemeinerte Quaternionengruppen sind. Ist $\mathcal{O}_{2'}(G) = \langle 1 \rangle$, so ist $|\mathrm{Z}(G)| = 2$. Insbesondere ist G nicht einfach.

Die einfachen Gruppen, die Diedergruppen als 2-Sylowgruppen haben, wurden in einer Serie längerer Arbeiten von Gorenstein und Walter klassifiziert.

9.16 Folgerung
Sei G eine nicht abelsche einfache Gruppe und p der kleinste Primteiler von $|G|$. Dann gilt entweder $p^3 \mid |G|$ oder $12 \mid |G|$.

Beweis:
Sei P eine p-Sylowgruppe von G und sei $N := \mathrm{N}_G(P)$ und $C := \mathrm{C}_G(P)$. Nach 9.12 ist P nicht zyklisch. Also ist $|P| \geq p^2$ und falls $p^3 \nmid |G|$ gilt $P \cong \mathbb{Z}_p \times \mathbb{Z}_p$. Laut 2.4 ist N/C isomorph zu einer Untergruppe von $\mathrm{Aut}\, P$ und es gilt

$$|\mathrm{Aut}\, P| = |\mathrm{Gl}(2, \mathbb{F}_p)| = \left(p^2 - 1\right)\left(p^2 - p\right) = p\,(p-1)^2\,(p+1)\,.$$

Aus $|N/C| \mid |\mathrm{Aut}\, P|$ und $|N/C| \mid |G|$ folgt $|N/C|$ teilt $(p+1)$, da p der kleinste Primteiler von $|G|$ ist und $P \leq C$ gilt. Da $|N/C| > 1$ nach 9.10 (sonst hätte P ein normales Komplement), muss $|N/C| = p+1$ gelten und diese Zahl muss prim sein. Also folgt in diesem Fall $p = 2$ und $|AutP| = 6$, das heißt $|N/C| = 3$. Damit gilt in diesem Fall $12 \mid |G|$. □

9.17 Satz (Hölder, 1985)
Ist jede Sylowgruppe einer endlichen Gruppe G zyklisch, so ist G auflösbar.

Beweis:
Induktion über $|G|$. Sei p der kleinste Primteiler von $|G|$ und sei P eine p-Sylowgruppe von G. Nach Satz 9.12 besitzt P ein normales Komplement K. K besitzt als Untergruppe von G lauter zyklische Sylowgruppen, ist also wegen $|K| < |G|$ nach Induktionsvoraussetzung auflösbar. $G/K \cong P$ ist als zyklische Gruppe ebenfalls auflösbar. Mit Satz **??** folgt daraus die Auflösbarkeit von G. □

9.18 Folgerung (Hölder)
Gruppen quadratfreier Ordnung sind auflösbar.

Beweis:
Die Sylowgruppen von Gruppen quadratfreier Ordnung sind zyklisch. Die Behauptung folgt mit 9.17 □

Ausblicke

In der Vorlesung habe ich versucht, einen Überblick über die wichtigsten Sätze der *elementaren Gruppentheorie* zu geben, soweit das in diesem Rahmen möglich war. Man hätte die Schwerpunkte auch anders setzen können. Ein wichtiges Kapitel, das leider nicht behandelt werden konnte, ist *Matrizengruppen*, in dem neben einfachen Eigenschaften von $\mathrm{Gl}(n, \mathbb{F}_q), \mathrm{Sl}(n, \mathbb{F}_q)$ auch behandelt wird, dass die Gruppen

$$\mathrm{PSL}(n, \mathbb{F}_q) := \mathrm{Sl}(n, \mathbb{F}_q) / \mathrm{Z}(\mathrm{Sl}(n, \mathbb{F}_q))$$

für $(n, q) \neq (2, 2), (2, 3)$ und $n > 1$ einfach sind.

Für einen tieferen Einblick in die Gruppentheorie muss man sich mit der sogenannten *Darstellungstheorie* beschäftigen. Diese untersucht systematisch Homomorphismen

$$D : G \to \mathrm{Gl}(n, K)$$

(*Darstellungen*) für verschiedene Körper K (manchmal auch für Ringe). Die Untersuchung der Darstellungen ist äquivalent zur Untersuchung der Untermoduln des sogenannten *Gruppenrings*

$$KG := \left\{ \sum_{g \in G} a_g g \mid a_g \in K \right\}$$

(mit der natürlichen Multiplikation). Schnell stellt sich heraus, dass sich die Darstellungstheorie sehr stark unterscheidet, je nachdem ob $\mathrm{char}\, K \mid |G|$ oder nicht. In der gewöhnlichen Darstellungstheorie ($\mathrm{char}\, K \nmid |G|$ bzw. $\mathrm{char}\, K = 0$) genügt normalerweise die Untersuchung der Charaktere

$$\chi_D : G \to K, \qquad \chi_D(g) := \mathrm{Spur}\, D(g).$$

Mit der Charaktertheorie lässt sich zum Beispiel der $p^a q^b$-Satz von Burnside beweisen.

In der modularen Darstellungstheorie ($\mathrm{char}\, K \mid |G|$) muss man - wie der Name schon sagt - in der Regel tatsächlich die Untermoduln von KG betrachten. Dafür sind dann auch weitergehende Kenntnisse der Ringtheorie nötig. Der Satz von Brauer-Suzuki (siehe 9.15) wird beispielsweise mit Hilfe der modularen Darstellungstheorie bewiesen.

Index