2. Untergruppen, Nebenklassen, Normalteiler

<u>Def.</u> Sei G eine Gruppe. Eine nicht-leere Teilmenge $H \subseteq G$ heisst <u>Untergruppe</u> von G falls für alle $x, y \in H$ gilt:

$$xy^{-1} \in H \quad (\text{bzw. } x\bar{y} \in H)$$

Verknüpfung ist "Multiplikation"

<u>Notation:</u> Ist H eine Untergruppe von G, dann schreiben wir $H \leq G$. Ist $H \leq G$ und $H \neq G$, so schreiben wir $H < G$ und sagen "H ist echte Untergruppe von G".

<u>Proposition 2.1</u> Ist $H \leq G$, dann ist H eine Gruppe.

<u>Beweis:</u> GT_1 : Mit $x \in H$ ist auch $xx^{-1} \in H$, also $e \in H$.
GT_2 : Mit $e, x \in H$ ist auch $ex^{-1} \in H$, also $x^{-1} \in H$.
"$\cdot$" ist binäre Operation auf H: Mit $x, y \in H$ ist auch $y^{-1} \in H$, also auch $x(y^{-1})^{-1} = xy \in H$.
GT_0 gilt in G, also auch in H. ⊣

<u>Def.</u> Die Untergruppen $\{e\}$ und G (von G) heissen <u>triviale Untergruppen</u> von G. [Würfelgruppe C und einige Untergruppen]

<u>Proposition 2.2</u> Der Durchschnitt von beliebig vielen Untergruppen einer Gruppe G ist wieder eine Untergruppe von G.

<u>Beweis:</u> Sei I eine Indexmenge; $H_i \leq G$ (für $i \in I$);
$H = \bigcap_{i \in I} H_i$; $x, y \in H$:
$x, y \in H_i$ (für jedes $i \in I$), also $\underbrace{xy^{-1} \in H_i}_{\text{für alle } i \in I}$, also $xy^{-1} \in H \leq G$. ⊣

Def. Sei G eine Gruppe mit Neutralelement e und sei $x \in G$. Dann heisst die kl. positive nat. Zahl n so dass gilt $x^n = e$ die Ordnung von x, bezeichnet mit $\mathrm{ord}(x)$. Falls es keine solche Zahl gibt, definieren wir $\mathrm{ord}(x) := \infty$.

Bem. $\mathrm{ord}(e) = 1$ und $\mathrm{ord}(x) = 1 \iff x = e$.

Faktum: Ist G eine endliche Gruppe mit $\mathrm{ord}(G) = m$ und $x \in G$, so ist $\mathrm{ord}(x) \leq m$.

Beweis: Da die Menge $\{x^1, x^2, \ldots\} \subseteq G$ endlich ist existieren $0 < k < \ell$ mit $x^k = x^\ell = x^k \cdot x^{\ell - k}$. Somit ist $x^{\ell-k} = e$ und $\mathrm{ord}(x) \leq \ell - k$. Wählen wir das kleinste solche ℓ, so folgt direkt $\mathrm{ord}(x) \leq m$ (betrachte $\{x^1, \ldots, x^m\} \subseteq G$). $\dashv$

Def. Sei G eine Gruppe und $X \subseteq G$. Dann ist

$$\langle X \rangle := \bigcap_{\substack{H \leq G \\ X \subseteq H}} H.$$

Mit Prop. 2.2 ist $\langle X \rangle$ eine Untergruppe von G; die von X erzeugte Untergruppe. Ist $X = \{a\}$ für ein $a \in G$, so schreiben wir $\langle a \rangle$ anstelle von $\langle \{a\} \rangle$. $\left[\begin{array}{l} C_2 \times C_2 \leq C \\ C_4 \leq C \end{array}\right]$

Def. Ist G eine Gruppe*, $a \in G$, und gilt $G = \langle a \rangle$, so heisst G zyklisch. Ist G eine Gruppe, $X \subseteq G$ eine endliche Teilmenge von G, und gilt $G = \langle X \rangle$, so ist G eine endlich erzeugte Gruppe.

* endlich oder unendlich

Bem.
- Ist G eine Gruppe, $a \in G$, und gilt $G = \langle a \rangle$, so muss G nicht endlich sein.
  Bsp. $(\mathbb{Z}, +) = \langle 1 \rangle$.
- Im Gegensatz zu $(\mathbb{Z}, +)$ ist $(\mathbb{Q}, +)$ nicht endlich erzeugt.
- Nicht jede endlich erzeugte Gruppe ist zyklisch.
  Bsp. $C_2 \times C_2$, $\mathbb{Z} \times C_2$

Faktum: Ist G eine Gruppe, $a \in G$ mit $\mathrm{ord}(a) = n$, dann ist $\langle a \rangle \cong C_n$. Insbesondere hat jede nicht-triviale endliche Gruppe eine nicht-triviale zyklische Untergruppe. Ist G eine endl. Gruppe und $a \in G$, dann ist $\underset{\uparrow \text{Gruppenelement}}{\mathrm{ord}(a)} = |\langle a \rangle| = \underset{\uparrow \text{Gruppe}}{\mathrm{ord}(\langle a \rangle)}$.

Bem: $\mathrm{ord}(a) = n$; $(\{x^1, \ldots, x^n\}, \circ)$ ist zyklische Gruppe.
$e = x^n$; $\overline{x^k} = x^{n-k}$ $(k \neq n)$

Theorem 2.3 Untergruppen von zyklischen Gruppen (endl. oder unendl.) sind zyklisch.

[Beweis in den Übungen]

Bem. Thm. 2.3 gilt auch für <u>unendliche</u> zyklische Gruppen, z.B. für $(\mathbb{Z}, +)$.

Def. Für $H \leq G$ und $x \in G$ sei

$$xH := \{xh : h \in H\} \quad \text{und} \quad Hx := \{hx : h \in H\}.$$

Die Mengen xH und Hx heissen <u>links-</u> bzw. <u>rechts-Nebenklassen</u> von H in G.

[Nebenklassen werden im Folgenden eine wichtige Rolle spielen.]

Lemma 2.4 (links-Version) Sei G eine Gruppe, $H \leq G$, und $x, y \in G$.

(a) $|xH| = |H|$ (d.h. es ex. Bij. zwischen xH & H)

(b) $x \in xH$

(c) $xH = H \iff x \in H$

(d) $xH = yH \iff x^{-1}y \in H$

(e) $xH = \{g \in G : gH = xH\}$

Beweis: (a) Sei $\varphi_x : H \to xH$
$$h \mapsto xh$$

- φ_x ist offensichtlich surjektiv, denn jedes $g \in xH$ ist von der Form $g = xh$ (für $h \in H$).

- φ_x ist injektiv: Für $h_1, h_2 \in H$ sei $\varphi_x(h_1) = \varphi_x(h_2)$, also $xh_1 = xh_2 \underset{\cdot x^{-1}}{\Longrightarrow} h_1 = h_2$.

(b) $e \in H$ (weil $H \leq G$), also $\underbrace{xe}_{\in xH} = x \in H$

(c) · Ist $xH = H$, dann ist $xe = x \in H$.

· Ist $x \in H$, dann ist $xH \subseteq H$ (weil H eine Gruppe ist)

· Mit $x \in H$ ist auch $x^{-1} \in H$. Sei $h \in H$ beliebig, dann ist auch $\underbrace{x\underbrace{(x^{-1}h)}_{\in H}}_{\in xH} = h \in xH$, also $H \subseteq xH$.

(d) · Ist $xH = yH$, dann ist
$$\underbrace{\underbrace{x^{-1}x}_{=e} H}_{=H} = x^{-1}yH \overset{(c)}{\Longrightarrow} x^{-1}y \in H.$$

· Ist $x^{-1}y \in H$, dann ist mit (c) $x^{-1}yH = H$, d.h. $\underbrace{y}_{=x(x^{-1}y)}H = xH$.

(e) • Ist $g \in xH$, so ist $g = xh$ (für ein $h \in H$). Also gilt $gH = (xh)H = xH$ und somit ist $xH \subseteq \{g \in G : gH = xH\}$.

• Ist andererseits $xH = gH$ (für ein $g \in G$), dann folgt aus (b), $g \in xH$ (weil $g \in gH$), und somit gilt $\{g \in G : gH = xH\} \subseteq xH$.

$\dashv$

<u>Folgerung</u>: Aus (e) folgt $xH = yH \iff y \in xH$ (bzw. $x \in yH$).

<u>Bem.</u> Der Beweis der rechts-Version von Lemma 2.4 ist analog.

<u>Def.</u> Für eine Untergruppe $H \leq G$ sei

$$G/H := \{xH : x \in G\} \quad \text{und} \quad H\backslash G := \{Hx : x \in G\}.$$

Als Folgerung aus der links- und rechts-Version von Lemma 2.4(b) erhalten wir das folgende

<u>Faktum</u>: Ist $H \leq G$, dann gilt

$$\bigcup_{x \in G} xH = G = \bigcup_{x \in G} Hx \quad \text{bzw.} \quad \bigcup G/H = G = \bigcup H\backslash G.$$

Als Folgerung aus Lemma 2.4 (d) erhalten wir

<u>Lemma 2.5</u> (Links-Version) Sei $H \leq G$. Dann gilt für alle $x, y \in G$:

entweder $xH = yH$ oder $xH \cap yH = \emptyset$.

<u>Beweis</u>: Seien $x, y \in G$. Ist $xH \cap yH = \emptyset$, dann sind wir fertig.

besser:
$z \in xH \cap yH$
$\iff \underbrace{z \in xH}_{} \wedge \underbrace{z \in yH}_{}$
Lem. 2.4.(e) $zH = xH$, $zH = yH$

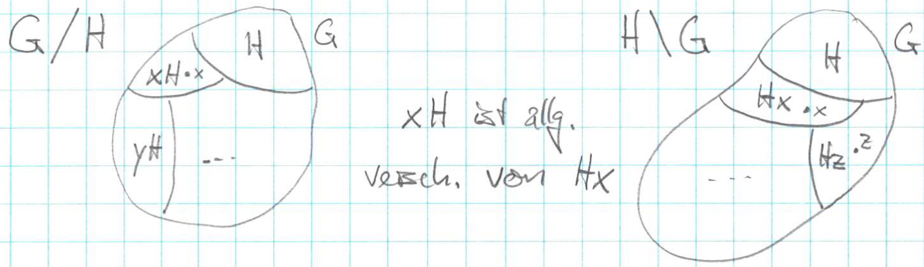
Andernfalls ex. ein $z \in xH \cap yH$, d.h. $z = xh_1 = yh_2$ für $h_1, h_2 \in H$. Es gilt $x^{-1}z = x^{-1}(xh_1) = h_1 \in H$ und $z^{-1}y = (yh_2)^{-1}y = (h_2^{-1}y^{-1})y = h_2^{-1} \in H$, und weil H eine Gruppe ist, ist auch $\underbrace{(x^{-1}z)}_{=h_1}\underbrace{(z^{-1}y)}_{=h_2} = x^{-1}y \in H$. Mit

Lemma 2.4 (d) ist also $xH = yH$, und somit bilden die Nebenklassen von H eine Partition von G. ⊣

Bem. Der Beweis der rechts-Version von Lemma 2.5 ist analog.

Aus Lemma 2.4 (e) folgt, dass jeder Teil der Partition von G dieselbe Kardinalität wie H hat; das führt zu folgender Definition.

Def. Ist $H \leq G$, dann ist $|G/H| = |H\backslash G|$ der <u>Index</u> von H in G, bezeichnet mit $[G:H]$.



Bsp: Sei C die Würfelgruppe (C für Cube) und T die Tetraedergruppe (T für Tetraeder); beide Gruppen orientierungserhaltend, also ohne Spiegelungen.

- $|C| = 24$, $|T| = 12$, $T \leq C$, $[C:T] = 2$.
  genau genommen: C enthält eine Untergruppe die isomorph ist zu T.
- $C_4 \leq D_4 \leq C$
- $[C:D_4] = 3$, $[D_4:C_4] = 2$
  $[C:C_4] = 6 = 2 \cdot 3$
- Sei σ eine Rotation um eine Raumdiagonale des Würfels. Dann ist $\sigma^3 = \imath$ (Identität) und es gilt:
  $$C = D_4 \,\dot\cup\, \sigma D_4 \,\dot\cup\, \sigma^2 D_4 \quad (\dot\cup \text{ disj. Vereinigung})$$

<u>**Korollar 2.6**</u> Sei G eine Gruppe und $H \leq G$. Ist $[G:H] = 2$, dann gilt für alle $x \in G$: $xH = Hx$ bzw. $xHx^{-1} = H$.

Beweis: Ist $x \in H$, dann ist $xH = H = Hx$ (weil H eine Gruppe ist).
Ist $x \in G$, $x \notin H$, dann ist $G = H \dot\cup xH$, aber auch $G = H \dot\cup Hx$, also ist $xH = Hx$ bzw. $xHx^{-1} = H$. ⊣

Bem. Für $K \leq H \leq G$ haben wir $K \leq G$ und es gilt:
$$[G:K] = [G:H] \cdot [H:K]$$

Theorem 2.7 (Lagrange) Sei G eine Gruppe und sei $H \leq G$.
Dann gilt:
$$|G| = [G:H] \cdot |H|$$
Ist G eine endliche Gruppe, so gilt $|H| \mid |G|$

Beweis: Betrachte die Partition G/H der Menge G. Diese Partition hat $[G:H]$ Teile und jeder Teil hat die Kardinalität $|H|$ (Lem. 2.4 (a)); also gilt $|G| = [G:H] \cdot |H|$.
Für endl. Gruppen muss $|H|$ ein Teiler von $|G|$ sein. ⊣

Bsp: Untergruppen von C der Kardinalität $1, \overset{C_2}{2}, \overset{C_3}{3}, \overset{C_4}{4}, 6, \overset{D_4}{8}, \overset{T}{12}, 24$.

Korollar 2.8 (a) Ist G eine endl. Gruppe der Ordnung p mit p prim, dann ist $G \cong C_p$. Insbesondere ist dann G abelsch.

(b) Ist G endl. und $x \in G$, dann gilt $\operatorname{ord}(x) \mid \operatorname{ord}(G)$. Insbesondere ist $x^{\operatorname{ord}(G)} = e_G$.

[Beweis in den Übungen]

Nächstes Ziel ist mit Nebenklassen zu rechnen:

Wir hätten gerne $(xH) \cdot (yH) = xyH$,

weil $xyH = xyHH = xyHy^{-1}yH = x\underbrace{(yHy^{-1})}_{= H?}yH$

brauchen wir $yHy^{-1} = H$ ...

Faktum 2.9 Sei G eine Gruppe, $H \leq G$, $x \in G$. Dann ist
$$xHx^{-1} := \{xhx^{-1} : h \in H\}$$
eine Untergruppe von G.

Beweis: Seien $\underbrace{xh_1x^{-1}}_{=a}$ und $\underbrace{xh_2x^{-1}}_{=b}$ in xHx^{-1}. Dann ist auch
$$\underbrace{(xh_1x^{-1})}_{=a}\underbrace{(xh_2^{-1}x^{-1})}_{=b^{-1}} = x\underbrace{h_1h_2^{-1}}_{\in H}x^{-1} \in xHx^{-1},$$
also ist $xHx^{-1} \leq G$. ⊣

Def.
- Ist $H \leq G$ und $x \in G$, so heissen H und xHx^{-1} <u>konjugierte Untergruppen</u>.
- Ist $N \leq G$ und gilt für alle $x \in G$, $xNx^{-1} = N$ (bzw. $xN = Nx$), so ist N ein <u>Normalteiler</u> von G; man sagt auch N ist eine <u>normale Untergruppe</u> von G.

Bem. $\{e\}$ und G sind Normalteiler von G; die trivialen Normalteiler.

Notation: Ist $N \leq G$ ($N < G$) ein Normalteiler von G, dann schreiben wir $N \trianglelefteq G$ ($N \triangleleft G$).

Bsp.
- Ist $H \leq G$ mit $[G:H] = 2$, dann ist $H \triangleleft G$. (Kor. 2.6)
- Ist $H \leq G$ und G abelsch, so ist $H \trianglelefteq G$.

Beispiele mit Würfelgruppe C:
- $T \trianglelefteq C$ (Index $= 2$)
- $H \cong C_2 \times C_2$; $H \ntrianglelefteq C$
  (3 Kopien)
- $H \cong C_2 \times C_2$; $H \triangleleft C$
  (1 Kopie) 3 Achsen durch Flächenmittelpunkte
  [Die Drehungen sind bzgl. Achsen die Identität]

Proposition 2.10 Für $N \leq G$ gilt:

$$N \trianglelefteq G \iff \forall x \in G \; \forall n \in N \; (x n x^{-1} \in N)$$

Beweis: ($\Rightarrow$) klar, folgt aus Definition

($\Leftarrow$) Aus der Annahme folgt $x N x^{-1} \subseteq N$.

Andererseits gilt, wenn wir x durch x^{-1} ersetzen:

$$N = (x x^{-1}) N (x x^{-1}) = x \underbrace{(x^{-1} N x)}_{\subseteq N} x^{-1} \subseteq x N x^{-1}$$

⊣

Analog zur Proposition 2.2 gilt

Faktum 2.11 Sind $K, N \trianglelefteq G$, dann ist $(K \cap N) \trianglelefteq G$.

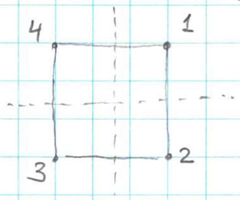
Beweis: Mit Prp. 2.2 ist $K \cap N \leq G$. Sind $K, N \trianglelefteq G$ so gilt mit Prp. 2.10 für alle $x \in G$ und alle $h \in K \cap N$:

$x h x^{-1} \in K$ (weil $K \trianglelefteq G$) und $x h x^{-1} \in N$ ($N \trianglelefteq G$).

Also $x h x^{-1} \in K \cap N$. ⊣

Bem. Gilt $H \triangleleft K \triangleleft G$, dann ist H nicht notwendigerweise ein Normalteiler von G.

Bsp. Sei $G = D_4$.



ρ um $\frac{\pi}{2}$

σ_1 Spiegelung $\quad 1 \longleftrightarrow 2,\; 3 \longleftrightarrow 4$

σ_2 Spiegelung $\quad 1 \longleftrightarrow 4,\; 2 \longleftrightarrow 3$

$\sigma_1 \circ \sigma_2$: $\quad 1 \longleftrightarrow 3,\; 2 \longleftrightarrow 4$

Rotation um π

Sei $H = \{1, \sigma_1\}$ und $K = \{1, \sigma_1, \sigma_2, \sigma_1 \circ \sigma_2\}$ $\quad [\sigma_2 \circ (\sigma_1 \circ \sigma_2) = \sigma_1]$

Dann ist $H \cong C_2$, $K \cong C_2 \times C_2$; $H \triangleleft K$ (K abelsch); $K \triangleleft G$ ($[G:K] = 2$)

Andererseits ist für ρ Rotation um $\frac{\pi}{2}$, $\rho \sigma_1 \rho^{-1} = \sigma_2 \notin H$, also mit Prp. 2.10, $H \ntrianglelefteq G$.

Def. Sei G eine Gruppe und $a \in G$. Der <u>Zentralisator</u> $Z_G(a)$ von a (in G) ist definiert als

$$Z_G(a) := \{x \in G : ax = xa\}.$$

[$Z_G(a)$ besteht aus allen Elementen von G welche mit a kommutieren.]

<u>Faktum 2.12</u> (a) Ist $x \in Z_G(a)$, so ist auch $x^{-1} \in Z_G(a)$.

(b) $Z_G(a) \leq G$

<u>Beweis:</u> (a) Ist $x \in Z_G(a)$, so gilt

$$ax = xa \quad \| \cdot x^{-1} \leftarrow$$
$$a = xax^{-1} \quad \| \cdot x^{-1} \rightarrow$$
$$x^{-1}a = ax^{-1}, \text{ also } x^{-1} \in Z_G(a).$$

(b) Sind $x, y \in Z_G(a)$, so ist mit (a) auch $y^{-1} \in Z_G(a)$.

Es gilt $a(xy^{-1}) = (ax)y^{-1} = (xa)y^{-1} = x(ay^{-1}) = x(y^{-1}a)$
$= (xy^{-1})a$,

also ist mit $x, y \in Z_G(a)$ auch $xy^{-1} \in Z_G(a)$.

$\dashv$

Def. Sei G eine Gruppe. Das <u>Zentrum</u> $Z(G)$ der Gruppe G ist definiert als

$$Z(G) := \{x \in G : \forall a \in G \, (ax = xa)\}$$

bzw. $Z(G) = \bigcap_{a \in G} Z_G(a)$

[$Z(G)$ besteht aus allen Elementen $x \in G$ welche mit allen Elementen $a \in G$ kommutieren.]

<u>Faktum 2.13</u> (a) $Z(G) = G \iff G$ ist abelsch

(b) $Z(G) \leq G$ (c) $Z(G) \trianglelefteq G$

(d) $Z(G)$ ist abelsch

(e) Ist $H \leq Z(G)$, dann ist $H \trianglelefteq G$.

<u>Beweis:</u> (a) ($\Leftarrow$) ist klar.

($\Rightarrow$): $\forall x \forall a\ (ax = xa)$, dann ist G abelsch

(b) Für $x \in Z(G)$ und $a \in G$ erhalten wir

Durchschnitt von Untergruppen

$ax = xa \Rightarrow x^{-1}ax = a \to x^{-1}a = ax^{-1}$, also $x^{-1} \in Z(G)$,

und wie im Beweis von Faktum 2.12 (b) zeigt man,

dass mit $x, y \in Z(G)$ auch $xy^{-1} \in Z(G)$.

(c) Für $x \in Z(G)$ und $a \in G$ gilt

$$axa^{-1} = aa^{-1}x = x \in Z(G).$$

(d) Für $x, y \in Z(G)$ gilt $xy = yx$.

(e) ~~Für $x \in Z(G)$ und $a \in G$ gilt $axa^{-1} = xaa^{-1} = x \in Z(G)$.~~

Wie (c) mit $h \in H$: $aha^{-1} = haa^{-1} = h \in H$. ⊣

<u>Def.</u> Seien H und K Untergruppen von G. Ist $G = HK$, so sagen wir "G ist das <u>innere Produkt</u> von H und K".

<u>Proposition 2.14</u> Sei G eine endl. Gruppe und $H, K \leq G$.

Dann gilt: $$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$$

<u>Beweis:</u>
- Es gilt $HK = \bigcup_{h \in H} hK$ und $(H \cap K) \leq H$ ($H \cap K$ Gruppe)
- Für $h_1, h_2 \in H$ gilt $h_1 K = h_2 K \Leftrightarrow h_1^{-1} h_2 \in K$

  [Nebenklassen von K in G]
- Für $h_1, h_2 \in H$ gilt $h_1(H \cap K) = h_2(H \cap K)$

  $\Leftrightarrow h_1^{-1}h_2 \in (H \cap K) \Leftrightarrow h_1^{-1} h_2 \in K$

  [Nebenklassen von $H \cap K$ in G]
- Somit gilt $h_1 K = h_2 K \Leftrightarrow h_1(H \cap K) = h_2(H \cap K)$,

und wir erhalten

$$|HK| = \left|\bigcup_{h \in H} hK\right| = [H : (H \cap K)] \cdot |K| = \frac{|H|}{|H \cap K|} \cdot |K| = \frac{|H| \cdot |K|}{|H \cap K|}.$$

⊣

Folgerung Gilt $K, H \leq G$, $|H \cap K| = 1$ und $|H| \cdot |K| = |G|$, dann gilt $HK = G = KH$.

Bem. Sind $H, K \leq G$, so ist HK im Allgemeinen keine Untergruppe von G. $\left[(\underbrace{hk}_{\in HK})^{-1} = \underbrace{k^{-1}h^{-1}}_{\in KH} \right]$

[Das ist anders wenn eine der Untergruppen ein Normalteiler ist.]

Theorem 2.15 Ist $K \leq G$ und $N \trianglelefteq G$, dann ist
$$KN = NK \leq G.$$

Beweis:
- Sei $k \in K$ und $n \in N$. Dann ist $\underbrace{knk^{-1}}_{=\tilde{n}} \in N$, also $kn = \tilde{n}k$ und somit $KN \subseteq NK$.
- $KN \supseteq NK$ wird analog gezeigt und somit ist $KN = NK$.
- Seien $k_1 n_1, k_2 n_2 \in KN$, dann ist
$$(k_1 n_1)(k_2 n_2)^{-1} = k_1 \underbrace{n_1 n_2^{-1}}_{= n_3 \in N} k_2^{-1} = \underbrace{k_1 k_2^{-1}}_{= k_3 \in K} \underbrace{k_2 n_3 k_2^{-1}}_{= n_4 \in N}$$
$$= k_3 n_4 \in KN.$$

$\dashv$

Bsp.
- Gruppe C; $N \cong C_2 \times C_2$ (Achsen durch Flächenmittelpunkte, Drehungen um π.)

  $K \cong C_4$; $N \triangleleft C$ (siehe vorheriges Beispiel)

  $|N| = |K| = 4$, $|K \cap N| = 2$, also $|KN| = \frac{4 \cdot 4}{2} = 8$,

  $KN \leq C$; es gilt $KN \cong D_4$.

nach der Folgerung

- Gruppe C; $C_3 \cong \{\iota, \rho, \rho^2\}$ mit ρ Rotation um $\frac{2\pi}{3}$ um Raumdiagonale

  $K \cong D_4$.

  $|C_3 \cap D_4| = 1$, $|C_3| \cdot |D_4| = |C| \Rightarrow C_3 D_4 = C = D_4 C_3$.

Proposition 2.16 Gilt $K, H \trianglelefteq G$, $|H \cap K| = 1$, dann gilt für alle $h \in H, k \in K$: $hk = kh$.

Beweis: Seien $h \in H$ und $k \in K$. Wir betrachten $hkh^{-1}k^{-1}$:

$$\left.\begin{array}{l} h\underbrace{kh^{-1}}_{\in H \trianglelefteq G}k^{-1} \in H \\ \underbrace{hkh^{-1}}_{\in K \trianglelefteq G}k^{-1} \in K \end{array}\right\} \Rightarrow hkh^{-1}k^{-1} \in H \cap K$$

d.h. $hkh^{-1}k^{-1} = e \Rightarrow hk = kh$. ⊣

Def. Sei G eine Gruppe. Für $a, b \in G$ definieren wir

$$[a,b] = aba^{-1}b^{-1}$$

und nennen dieses Produkt den Kommutator von a und b. Sind $A, B \leq G$, dann ist

$$[A,B] := \langle \{[a,b] : a \in A \text{ und } b \in B\} \rangle$$

die von A & B erzeugte Kommutatorgruppe (von G) und $K(G) := [G,G]$ heisst Kommutatorgruppe von G.

Bem. $\{[a,b] : a \in A, b \in B\}$ ist im Allg. keine Gruppe, denn $[a,b]^{-1} = (aba^{-1}b^{-1})^{-1} = bab^{-1}a^{-1} = [b,a]$.

Proposition 2.17 Sei G eine Gruppe und seien $A, B \leq G$.

(a) $[A,B] = [B,A]$

(b) Gilt $A, B \trianglelefteq G$, dann ist $[A,B] \leq A \cap B$ und $[A,B] \trianglelefteq G$.

(c) $K(G) \trianglelefteq G$

Beweis: (a) Mit $[a,b] \in [A,B]$ ist auch

$$[a,b]^{-1} = bab^{-1}a^{-1} = [b,a] \in [A,B],$$

also $[A,B] \leq [B,A]$, und umgekehrt.

(b) $\underbrace{aba^{-1}}_{\substack{=\tilde{b}\in B \\ \text{weil } B\trianglelefteq G}} b^{-1} = \tilde{b}b^{-1} \in B$

$a\underbrace{ba^{-1}b^{-1}}_{\substack{=\tilde{a}\in A \\ \text{weil } A\trianglelefteq G}} = a\tilde{a} \in A$

$\Rightarrow$ die Generatoren von $[A,B]$ sind in $A\cap B$ und somit ist $[A,B]\leq A\cap B$.

Sei $x\in G$ und seien $g_1=[a_1,b_1]^{\varepsilon_1}, \dots, g_n=[a_n,b_n]^{\varepsilon_n}$ mit $\varepsilon_i\in\{1,-1\}$ Generatoren von $[A,B]$.

$$x(g_1\cdots g_n)x^{-1} = (xg_1x^{-1})\dots(xg_nx^{-1})$$

Für $1\leq i\leq n$ betrachten wir xg_ix^{-1}:

$\varepsilon_i=1$: $xg_ix^{-1} = xa_ib_ia_i^{-1}b_i^{-1}x^{-1} = \underbrace{(xa_ix^{-1})}_{=\tilde{a}\in A}\underbrace{(xb_ix^{-1})}_{=\tilde{b}\in B}\underbrace{(xa_i^{-1}x^{-1})}_{=\tilde{a}^{-1}}\underbrace{(xb_i^{-1}x^{-1})}_{=\tilde{b}^{-1}}$

weil $A,B\trianglelefteq G$ gilt:

D.h. $\underbrace{xg_ix^{-1}}_{\tilde{g}_i} = \tilde{a}\tilde{b}\tilde{a}^{-1}\tilde{b}^{-1} = [\tilde{a},\tilde{b}]\in[A,B]$

$\varepsilon_i=-1$ ist analog.

Es gilt also $x(g_1\cdots g_n)x^{-1} = \tilde{g}_1\cdot\ldots\cdot\tilde{g}_n\in[A,B]$,
d.h. $[A,B]\trianglelefteq G$.

(c) Da $G\trianglelefteq G$ folgt mit (b): $\underbrace{[G,G]}_{K(G)}\trianglelefteq G$. $\dashv$

<u>Def.</u> Eine Gruppe heisst <u>einfach</u>, falls sie keine nicht-trivialen Normalteiler hat.

<u>Bem.</u> Eine abelsche Gruppe ist genau dann einfach, wenn sie keine nicht-trivialen Untergruppen besitzt.

<u>Bsp.</u> C nicht einfach; C_p einfach für p prim; D_n nicht einfach für $n\geq 3$

Bem. Auf nicht-einfachen Gruppen können wir mit den Nebenklassen eines nicht-trivialen Normalteilers eine "neue" Gruppe bilden.

Faktum 2.18 Ist $N \trianglelefteq G$, dann gilt für alle $x, y \in G$:
$$(xN)(yN) = (xy)N$$

Beweis: Weil $N \trianglelefteq G$ gilt
$$(xN)(yN) = (x\underbrace{(yNy^{-1})}_{=N})(yN) = (xy)\underbrace{N}_{}\overbrace{y^{-1} \, y}^{=e}\underbrace{N}_{} = (xy)\underbrace{NN}_{=N} = (xy)N.$$

$\dashv$

Damit können wir auf Nebenklassen eine binäre Operation definieren.

Proposition 2.19 Ist $N \trianglelefteq G$, dann ist die Menge der Nebenklassen
$$G/N = \{xN : x \in G\}$$
mit der Verknüpfung
$$(xN)(yN) := (xy)N$$
eine Gruppe.

Faktorgruppe oder Quotientengruppe

Beweis: • Zuerst zeigen wir, dass die Operation auf G/N wohldefiniert ist: [Was ist da zu zeigen und warum?]
Sei $xN = \tilde{x}N$, $yN = \tilde{y}N$, dann folgt aus Lem. 2.4 (d), $x^{-1}\tilde{x} \in N$ und $y^{-1}\tilde{y} \in N$. Aus $N \trianglelefteq G$ folgt nun:

$$\underbrace{(xy)^{-1}}_{=:a}\underbrace{(\tilde{x}\tilde{y})}_{=:b} = y^{-1}\underbrace{x^{-1}\tilde{x}}_{\in N}\tilde{y} \in y^{-1}N\tilde{y} = \underbrace{y^{-1}Ny}_{=N}\underbrace{y^{-1}\tilde{y}}_{\in N} = N$$

damit auch $ab^{-1} \in N$

Somit ist $a^{-1}b \in N$, d.h. $aN = bN$ bzw. $(xy)N = (\tilde{x}\tilde{y})N$, woraus folgt:
$$(xN)(yN) = (xy)N = (\tilde{x}\tilde{y})N = (\tilde{x}N)(\tilde{y}N)$$

- Nun überprüfen wir die Axiome:

$$GT_0: \quad (xN)\big(\underbrace{(yN)(zN)}_{=(yz)N}\big) = (x(yz))N = ((xy)z)N = \dots$$

GT_1: Für alle $x \in G$ gilt: $(eN)(xN) = xN$,
d.h. $eN = N$ ist das Neutralelement.

GT_2: Für alle $x \in G$ gilt: $(x^{-1}N)(xN) = N$,
d.h. $(xN)^{-1} = (x^{-1}N)$. ⊣

Def. G/N heisst Faktorgruppe.

Bsp. • Würfelgruppe C: $N \trianglelefteq C$, $N \cong T$, $C/N \cong C_2$
$N \trianglelefteq C$, $N \cong C_2 \times C_2$, $C/N \cong D_3$

• $C_3 \trianglelefteq D_3$, $D_3/C_3 \cong C_2$

Proposition 2.20 Sei G eine Gruppe und sei $K(G)$ die Kommutatorgruppe von G.

(a) $G/K(G)$ ist abelsch

(b) Ist G/N abelsch für $N \trianglelefteq G$, so ist $K(G) \trianglelefteq N$.

(c) $K(G)$ ist der kl. Normalteiler N von G, sodass G/N abelsch ist.

Beweis: (a) $(xK(G))(yK(G)) = (xy)K(G) = (xy)\overbrace{\underbrace{(y^{-1}x^{-1}yx)}_{\in K(G)}}^{=e}K(G)$

$$= (yx)K(G) = (yK(G))(xK(G))$$

(b) Sei $N \trianglelefteq G$ mit G/N abelsch. Dann gilt für alle $x, y \in G$:

$$(xy)N = (xN)(yN) \underset{G/N \text{ abelsch}}{=} (yN)(xN) = (yx)N$$

$\Rightarrow (xy)^{-1}(yx) = y^{-1}x^{-1}yx = [y^{-1}, x^{-1}] \in N$ und

somit ist $K(G) \subseteq N$, bzw. $K(G) \trianglelefteq N$ (weil $K(G) \trianglelefteq G$).

(c) Folgt direkt aus (a) & (b). ⊣

<u>Def.</u> Eine Gruppe G heisst <u>auflösbar</u>, falls es eine Folge $\{e\} = G_0 \lhd G_1 \lhd \dots \lhd G_{n-1} \lhd G_n = G$ von Untergruppen von G gibt, sodass für alle $1 \le i \le n$ gilt:

$$G_i / G_{i-1} \text{ ist abelsch}$$

<u>Bem.</u> Auflösbare Gruppen spielen in der Galoistheorie eine wichtige Rolle.

<u>Beispiele:</u>

1. abelsche Gruppen sind auflösbar, $G_1 = G \quad (n=1)$
2. Ist G einfach und nicht abelsch, so ist G <u>nicht</u> auflösbar.
3. D_n ist auflösbar für alle $n \geq 2$, denn D_2 ist abelsch und für $n \geq 3$ ist $C_n \lhd D_n$.
4. $\underline{\underline{S_2}} \cong C_2$ ist auflösbar (es ex. Lösungsformel für Gleichungen 2. Grades)
5. $C_3 \lhd \underline{\underline{S_3}} \cong D_3$ ist auflösbar (Existenz einer Lösungsformel für Gleichungen 3. Grades)
6. $C_2 \times C_2 \lhd \underline{\underline{T}}$ ist auflösbar
7. $C_2 \times C_2 \lhd T \lhd \underline{\underline{C}} \cong S_4$ ist auflösbar (Lösungsformel für Gl. 4. Grades)
8. D ist einfach, also <u>nicht</u> auflösbar (weil D nicht abelsch), und weil D der einzige Normalteiler von S_5 ist ex. für Gleichungen 5. Grades keine Lösungsformel.