# 1 Normalteiler

**Definition 1.1.** Sei $(G, \circ)$ eine Gruppe und $H \subset G$ eine Untergruppe.
H heißt Normalteiler

$$
\begin{aligned}
&:\Longleftrightarrow \forall g \in G\ \forall u \in H : g \circ u \circ g^{-1} \in H \\
&\Longleftrightarrow \forall g \in G : gHg^{-1} = H \\
&\Longleftrightarrow \forall g \in G : gH = Hg.
\end{aligned}
$$

**Beispiel 1.2.** Einige Beispiele für Normalteiler:

- Die triviale Untergruppe $\{e\}$ ist immer Normalteiler, denn es gilt für alle $g \in G : g \circ \{e\} = \{g\} = \{e\} \circ g$.
- G ist immer Normalteiler in sich selbst, denn es gilt $\forall g \in G\ \forall g' \in G : g \circ g' \circ g^{-1} \in G$.
- Ist G kommutativ, so ist jede Untergruppe $H \subset G$ Normalteiler, denn es gilt $\forall g \in G\ \forall u \in H : g \circ u \circ g^{-1} = g \circ g^{-1} \circ u = e \circ u = u \in H$.

TODO: Faktorgruppe einbauen, ggf. zweite und dritte Definition in Definition 1 entsprechend verschieben

# 2 Normalisator

Sei $(G, \circ)$ Gruppe, $U \subset G$ Untergruppe.
Im Allgemeinen ist $U$ kein Normalteiler in $G$. Also suchen wir uns eine größtmögliche Untergruppe von $G$, sodass $U$ in dieser Untergruppe Normalteiler ist.
Formal wollen wir eine Untergruppe $V \subset G$ finden, sodass

i) $U \subset V$ ($U$ ist in $V$ enthalten)

ii) $U$ ist Normalteiler in $V$

iii) Ist $V'$ eine weitere Untergruppe von $G$ die i) und ii) erfüllt, so gilt $V' \subset V$. ($V$ ist größtmöglich)

**Bemerkung 2.1.** $V$ existiert immer.
Ist $U$ Normalteiler in $G$, so wähle $V = G$.

Ist $U$ kein Normalteiler in G, so erfüllt $V' = U$ die ersten beiden Eigenschaften, also lässt sich auch eine größtmögliche Untergruppe $V$ finden, die die ersten beiden Eigenschaften erfüllt.

**Definition 2.2.**

$$N_G(U) := \{g \in G \mid gUg^{-1} = U\}$$

heißt Normalisator von $U$ in $G$.

**Satz 2.3.** *$N_G(U)$ ist Untergruppe von $G$ und erfüllt die Eigenschaften i) bis iii).*

**Beweis:**

- Untergruppe:

  Die Assoziativität wird vererbt.

  Es gilt $e \in N_G(U)$, denn $e \in G$ und $eUe^{-1} = eUe = U$.

  Sei $n \in N_G(U)$. Dann gilt

  $$\begin{aligned} & nUn^{-1} = U \\ \iff & n^{-1}nUn^{-1}n = n^{-1}Un \\ \iff & U = n^{-1}Un, \end{aligned}$$

  also auch $n^{-1} \in N_G(U)$.

  Seien $n_1, n_2 \in N_G(U)$. Dann gilt:

  $$\begin{aligned} (n_1n_2)U(n_1n_2)^{-1} &= n_1n_2Un_2^{-1}n_1^{-1} \\ &= n_1(n_2Un_2^{-1})n_1^{-1} \\ &= n_1Un_1^{-1} \\ &= U, \end{aligned}$$

  also auch $n_1 \circ n_2 \in N_G(U)$.

  Damit ist $N_G(U)$ Untergruppe von $G$.

- i):

  $U$ ist Normalteiler in sich selbst, also gilt $\forall u \in U : uUu^{-1} = U$. Zudem gilt $U \subset G$. Per Definition von $N_G(U)$ folgt sofort $U \subset N_G(U)$.

- ii):
  Es gilt per Definition $\forall n \in N_G(U) : nUn^{-1} = U$, d.h. U ist Normalteiler in $N_G(U)$.

- iii):
  Sei $V' \subset G$ eine weitere Untergruppe mit $U \subset V'$ und sodass $U$ Normalteiler in $V'$ ist.
  Sei $v \in V'$. Da $U$ Normalteiler in $V'$ ist, gilt $vUv^{-1} = U$, also per Definition $v \in N_G(U)$.
  $\implies V' \subset N_G(U)$.

■

## 3 Zauberhafte Folgerung

Welcher Mischvorgang muss auf einen aus n Karten bestehenden Kartenstapel angewendet werden, um eine Permutation der Form $\phi_{a,b}$ zu erhalten?

i) Mischvorgang $R_c$: Sei $c \in \mathbb{N}$. Teile die $n$ Karten von links nach rechts auf $c$ Stapel aus. Danach werden die Karten wieder aufgenommen, und zwar von rechts nach links. Nach ganz oben kommt also der am weitesten links liegende Stapel.

ii) Mischvorgang $L_c$: Von links nach rechts austeilen, und auch von links nach rechts aufnehmen.

*(Beispiel vorführen)*

**Definition 3.1.** i) Sei $c$ ein Teiler von $c-1$ und $a := (n-1)/n$. Dann sind $a$ und $n$ teilerfremd und $R_c$ entspricht $\phi_{a,a}$.

ii) Sei $c$ ein Teiler von $c+1$ und $a := (n+1)/n$. Dann sind $a$ und $n$ teilerfremd und $L_c$ entspricht $\phi_{-a,-1}$.

**Beweis:** • i) Teilerfremdheit folgt direkt aus $ac = n - 1$.

Es gilt dann $n - ac = 1$ (Mit $ggT(a,b) = s \cdot a + t \cdot b, \quad s,t \in \mathbb{Z}$ folgt Teilerfremdheit von a und n.

Aus der ursprünglichen Reihenfolge der Karten $(0,\ldots,n{-}1)$ passiert durch $R_c$ folgendes:

$$\begin{array}{ccccc}
ac & & & & \\
(a-1)c & (a-1)c+1 & \ldots & (a-1)c+c-2 & (a-1)c+(c-1) \\
\vdots & \vdots & \vdots & \vdots & \vdots \\
c & c+1 & \ldots & 2c-1 & 2c-1 \\
0 & 1 & \ldots & c-2 & c-1
\end{array}$$

Erster Stapel hat $a + 1$ Elemente, alle anderen $a$.

$\longrightarrow c$ Stapel von rechts nach links zusammenlegen:

Betrachte Karte $k$ aus dem Stapel $s \quad (s \in \{1,\ldots,c-2\})$. Dann liegt die Karte $k{+}1$ im Stapel $s{+}1$ genau $a$ Stellen weiter als $k$, da in jedem Stapel außer dem ersten genau $a$ Karten sind. In Stapel 1 gilt zusätzlich Karte 0 liegt $a$ Karten weiter als $ac$.

Die letzte Karte im Stapel ist $c-1$. Zyklisch weiterzählen. Wir sehen dass Karte $c$ die $a-$te Karte von oben ist.

Insgesamt: $R_c(0) = a$ und $R_c(k+1) = R_c(k) + a$. Mit Lemma 4.5 gilt also $R_c = \phi_{a,a}$.

• ii) Teilerfremdheit folgt direkt aus $ac = n + 1$.

$ac - n = 1 \longrightarrow$ wie vorhin

Aus der ursprünglichen Reihenfolge der Karten $(0,\ldots,n{-}1)$ passiert durch $L_c$ folgendes:

$$\begin{array}{ccccc}
(a-1)c & (a-1)c+1 & \ldots & (a-1)c+(c-2) & \\
(a-2)c & (a-2)c+1 & \ldots & (a-2)c+(c-2) & (a-2)c+(c-1) \\
\vdots & \vdots & \vdots & \vdots & \vdots \\
c & c+1 & \ldots & 2c-2 & 2c-1 \\
0 & 1 & \ldots & c-2 & c-1
\end{array}$$

Letzter Stapel hat $a - 1$ Elemente, alle anderen $a$.

Beweis wie vorhin, aber gehe $a$ Karten zurück um von der Karte $k$ zur Karte $k - 1$ zu kommen. Mit $L_c(0) = n - 1$ folgt $L_c = \phi_{-a,-1}$. (In $\mathbb{Z}_n$ ist $-1 \equiv n - 1$).

*Beispiele vorführen*

■

Erkenntnis aus 4.3, 4.4, 4.6 (umbenennen):

Für $n \in$ N sei $A_n := \{x | n-1$ durch $x$ teilbar$\}$ und $B_n := \{x | n+1$ durch $x$ teilbar$\}$.

Wähle $a_1, \ldots . a_r \in A_n$ und $a'_1, \ldots, a'_l \in B_n$ aus. Sei $a$ das Produkt aller $a_i$ und $a'_j$. Wähle $c_i$ bzw $c'_j$ sodass $c_i a_i = n-1$, bzw $c'_j a'_j = n+1$.

Führe auf einen Kartenstapel $R_{c_1}, \ldots, R_{c_r}$ und $L_{c'_1}, \ldots, L_{c'_l}$ in beliebiger Reihenfolge durch. Dazwischen darf noch zusätzlich abgehoben werden. Der Kartenstapel befindet sich in der Permutation $\phi_{a,b}$, mit $b$ unbekannt falls abheben beliebig. *Auf Erkenntnisse aus den jeweiligen Abschnitten verweisen.*

Für uns von Bedeutung: $a = 1$ oder $a = -1 \rightarrow$ Die Karten sind in der gleichen, bzw der gespiegelten zyklischen Reihenfolge.