

# 1 Normalteiler

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

$$:\Leftrightarrow \forall g \in G \forall u \in U : g \circ u \circ g^{-1} \in U.$$

Der Sauberkeit halber müsste das nächste Lemma ausgeführt werden, aber wenn die Zeit zu knapp ist sollte es weggelassen und in die Definition mit aufgenommen werden.

**Lemma 1.2.** *Definiere die Verknüpfung von Elementen und Mengen:*

$$x \circ A \circ y = \{x \circ a \circ y \mid a \in A\}.$$

*Dann ist  $U$  Normalteiler in  $G$  genau dann, wenn*

$$\begin{aligned} &\forall g \in G : gUg^{-1} = U \\ &\Leftrightarrow \forall g \in G : gU = Ug. \end{aligned}$$

**Beweis:** • „ $\Rightarrow$ “:

Es gilt  $\forall g \in G \forall u \in U : g \circ u \circ g^{-1} \in U$ , also  $gUg^{-1} \subset U$ .

Ohnehin gilt  $U \subset gUg^{-1}$ , denn  $\forall u \in U : u = e \circ u \circ e^{-1} \in gUg^{-1}$ .

• „ $\Leftarrow$ “:

Es gilt  $\forall g \in G : gUg^{-1} \subset U$ , also per Definition  $\forall g \in G \forall u \in U : g \circ u \circ g^{-1} \in U$ .

Weiterhin gilt

$$gUg^{-1} = U \Leftrightarrow gUg^{-1}g = Ug \Leftrightarrow gU = Ug.$$

■

**Beispiel 1.3.** 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  $U \subset G$  Normalteiler, denn es gilt  $\forall g \in G \forall u \in U : g \circ u \circ g^{-1} = g \circ g^{-1} \circ u = e \circ u = u \in U$ .

TODO: Faktorgruppe einbauen?

## 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  $v \in N_G(U)$ .

$\implies V' \subset N_G(U)$ .

■

**Satz 2.4.** Seien  $G, U$  und  $N_G(U)$  wie gehabt.

Seien ferner  $m \in \mathbb{N}$ ,  $x_1, \dots, x_m \in N_G(U)$  und  $u_0, \dots, u_m \in U$ . Dann gilt für ein geeignetes  $u \in U$ :

$$u_m \circ x_m \circ u_{m-1} \circ x_{m-1} \circ \dots \circ u_1 \circ x_1 \circ u_0 = x_m \circ \dots \circ x_1 \circ u.$$

Insbesondere:

$$x_m \circ \dots \circ x_1 \in U \implies u_m \circ x_m \circ u_{m-1} \circ x_{m-1} \circ \dots \circ u_1 \circ x_1 \circ u_0 \in U.$$

**Beweis:** Vollständige Induktion.

- Induktionsanfang ( $m = 1$ ): Zu zeigen:  $u_1 \circ x_1 \circ u_0 = x_1 \circ u$  für ein geeignetes  $u \in U$ .

$U$  ist Normalteiler in  $N_G(U)$ , also gilt  $u_1 \circ x_1 = x_1 \circ \hat{u}$  für ein geeignetes  $\hat{u} \in U$ . Damit gilt

$$\begin{aligned} u_1 \circ x_1 \circ u_0 &= x_1 \circ \hat{u} \circ u_0 \\ &= x_1 \circ u \end{aligned}$$

mit  $u := \hat{u} \circ u_0 \in U$ .

- Induktionsschritt ( $m \implies m + 1$ ): Es gilt:

$$\begin{aligned} &u_{m+1} \circ x_{m+1} \circ u_m \circ x_m \circ \dots \circ u_1 \circ x_1 \circ u_0 \\ &= u_{m+1} \circ x_{m+1} \circ (u_m \circ x_m \circ \dots \circ u_1 \circ x_1 \circ u_0) \\ &\stackrel{I.V.}{=} u_{m+1} \circ x_{m+1} \circ (x_m \circ \dots \circ x_1 \circ u') \\ &= (u_{m+1} \circ (x_{m+1} \circ \dots \circ x_1)) \circ u' \\ &\stackrel{NT}{=} ((x_{m+1} \circ \dots \circ x_1) \circ u'') \circ u' \\ &= x_{m+1} \circ \dots \circ x_1 \circ \underbrace{u'' \circ u'}_{=: u}. \end{aligned}$$

für geeignete  $u', u'' \in U$ .

■

### 3 Symmetrische Gruppe

Jegliche Operationen, die im Zaubertrick durchgeführt werden, ändern lediglich die Reihenfolge der Karten im Stapel. Zur Modellierung des Tricks genügt es also, die Karten durczunummerieren.

**Definition 3.1.** Wir führen Tricks mit  $n$  Karten durch und erzeugen beim Mischen Permutationen von  $\{0, \dots, n-1\}$ .

Die Gruppe aller dieser Permutationen heißt die **symmetrische Gruppe**  $S_n$ . Formal lässt sich mit  $\mathbb{Z}_n := \{0, \dots, n-1\}$  jedes Element von  $S_n$  als bijektive Abbildung  $\phi : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$  identifizieren.

**Erinnerung.**  $\mathbb{Z}_n$  wird mit der Addition und Multiplikation modulo  $n$  zu einem Ring, dem **Restklassenring**.

**Definition 3.2.** Sei  $r \in \mathbb{Z}_n$ .

$$\begin{aligned} s_r : \mathbb{Z}_n &\longrightarrow \mathbb{Z}_n \\ k &\longmapsto s_r(k) = k + r \pmod{n} \end{aligned}$$

heißt zyklischer Shift.  $s_r$  ist bijektiv, also  $s_r \in S_n$ .

**Bemerkung 3.3.**  $s_r$  lässt sich interpretieren als

- Die untersten  $r$  Karten nach oben zu legen
- Die obersten  $n - r$  Karten abzuheben und unter den Stapel zu legen

*Im Vortrag am Beispiel klar machen (Menge  $\{0, \dots, n-1\}$  von unten nach oben aufschreiben und Shift mit z.B.  $r = 3$  anwenden)*

**Satz 3.4.**

$$S := \{s_r \mid r \in \mathbb{Z}_n\}$$

*ist kommutative Untergruppe von  $S_n$ .*

*Das bedeutet insbesondere: Die Reihenfolge von mehrmaligem Abheben ist egal (Kommutativität), und mehrmaliges Abheben bringt die Karten nicht mehr durcheinander als einmaliges Abheben (Abgeschlossenheit).*

**Beweis:** Es gilt (kurz nachrechnen oder am Abheben klarmachen):

$$s_{r_1} \circ s_{r_2} = s_{r_2} \circ s_{r_1} = (k \mapsto k + r_1 + r_2 \pmod n) = s_{r_1+r_2},$$

womit die Kommutativität und Abgeschlossenheit gezeigt sind.

Zudem  $s_r^{-1} = s_{-r} = s_{n-r}$ , und  $id = s_0 \in S$ . ■

## 4 Normalisator von $S$

**Bemerkung 4.1.** Definiere

$$\begin{aligned} \phi_a : \mathbb{Z}_n &\longrightarrow \mathbb{Z}_n \\ k &\longmapsto \phi_a(k) = ak \pmod n. \end{aligned}$$

Wann ist  $\phi_a$  bijektiv?

Seien  $a$  und  $n$  teilerfremd. Dann gilt für  $k, k' \in \mathbb{Z}_n$ :

$$\begin{aligned} \phi_a(k) = \phi_a(k') &\iff ak = ak' \pmod n \\ &\iff a(k - k') = 0 \pmod n \\ &\iff k - k' = 0 \pmod n \\ &\iff k = k'. \end{aligned}$$

Also ist  $\phi_a$  injektiv und damit surjektiv (Abbildung zwischen zwei gleichen endlichen Mengen).

Seien nun  $a$  und  $n$  nicht teilerfremd.

$\implies \exists t \in \mathbb{N} : a = t \cdot k, n = t \cdot k'$  für geeignete  $k, k' \in \mathbb{N}$ . Dann gilt

$$\begin{aligned} \phi_a(k') &= ak' = t k k' = n k = 0 \pmod n \\ &= \phi_a(0), \end{aligned}$$

also ist  $\phi_a$  nicht injektiv.

Damit ist gezeigt:  $\phi_a$  ist bijektiv  $\iff a$  und  $n$  teilerfremd.

**Definition 4.2.** Seien  $a, b \in \mathbb{Z}$ . Definiere

$$\begin{aligned}\phi_{a,b} : \mathbb{Z}_n &\longrightarrow \mathbb{Z}_n \\ k &\longmapsto \phi_{a,b}(k) = ak + b \pmod n.\end{aligned}$$

**Lemma 4.3.**

$$a, n \text{ teilerfremd} \implies \phi_{a,b} \in S_n.$$

**Beweis:** Es gilt  $\phi_{a,b}(k) = ak + b \pmod n = s_b(ak) = (s_b \circ \phi_a)(k)$ . Es gilt  $s_b \in S_n$  und  $\phi_a \in S_n$  (haben Bijektivität eben gezeigt), also wegen der Abgeschlossenheit von  $S_n$ :  $\phi_{a,b} \in S_n$ . ■

**Lemma 4.4.** Sei  $\phi \in S_n$  bijektiv. Es gilt:

$$\exists a \in \mathbb{Z}_n^*, b \in \mathbb{Z}_n : \phi = \phi_{a,b} \iff \exists a \in \mathbb{Z}_n : \forall k \in \mathbb{Z}_n : \phi(k+1) = \phi(k) + a \pmod n.$$

**Beweis:** • „ $\implies$ “:

Es gilt ( $k \in \mathbb{Z}_n$  beliebig)

$$\phi(k+1) - \phi(k) = a(k+1) + b - (ak + b) = a.$$

• „ $\impliedby$ “:

Definiere  $\phi(0) = b$ . Zeige per Induktion:  $\phi = \phi_{a,b}$ .

– Induktionsanfang ( $k = 0$ ):

$$\text{Es gilt } \phi(0) = b = a \cdot 0 + b = \phi_{a,b}(0).$$

– Induktionsschritt ( $k \implies k+1$ ): Es gilt

$$\begin{aligned}\phi(k+1) &= \phi(k) + a \pmod n \\ &\stackrel{I.V.}{=} \phi_{a,b}(k) + a \pmod n \\ &= ak + b + a \pmod n \\ &= a(k+1) + b \pmod n \\ &= \phi_{a,b}(k+1).\end{aligned}$$

Da  $\phi$  zudem injektiv ist, müssen  $a$  und  $n$  teilerfremd sein.

■

**Satz 4.5.** *Es gilt*

$$N_{S_n}(S) = \{\phi_{a,b} \mid a, n \in \mathbb{N} \text{ teilerfremd}\}.$$

**Beweis:** • „ $\supset$ “:

Sei  $\phi_{a,b}$  beliebig mit  $a, n$  teilerfremd. Nach Lemma 4.3 gilt dann  $\phi_{a,b} \in S_n$ .

Ferner gilt für beliebige  $s_r \in S, k \in \mathbb{Z}_n$ :

$$\begin{aligned} (\phi_{a,b} \circ s_r)(k) &= \phi_{a,b}(k+r) \\ &= a(k+r) + b \pmod{n} \\ &= (ak+b) + ar \pmod{n} \\ &= (s_{ar} \circ \phi_{a,b})(k). \end{aligned}$$

Also  $\phi_{a,b} \circ s_r \circ \phi_{a,b}^{-1} = s_{ar} \in S$ .

$\implies \phi_{a,b} \in N_{S_n}(S)$ .

• „ $\subset$ “:

Sei  $\phi \in N_{S_n}(S)$ . Dann gilt insbesondere für alle  $k \in \mathbb{Z}_n$  mit geeignetem  $s_a \in S$ :

$$\begin{aligned} (\phi \circ s_1 \circ \phi^{-1})(k) &= s_a(k) \\ \iff (\phi \circ s_1)(k) &= (s_a \circ \phi)(k) \\ \iff \phi(k+1) &= \phi(k) + a \pmod{n}. \end{aligned}$$

Mit Lemma 4.4 folgt die Behauptung.

■

## 5 Zauberhafte Folgerung

**Bemerkung 5.1.** 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 5.2.** i) Sei  $c$  ein Teiler von  $c-1$  und  $a := (n-1)/c$ . 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 aus  $ac = n-1$ :

Angenommen  $t$  teilt sowohl  $a$  als auch  $n$ . Wir setzen  $tk = a$  und  $tk' = n$

$$\begin{aligned} n - ac = 1 &\Leftrightarrow tk' - tkc = 1 \\ &\Leftrightarrow t(k' - kc) = 1 \\ &\Leftrightarrow t \text{ ist Teiler von } 1 \end{aligned}$$

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

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

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

→  $c$  Stapel von rechts nach links zusammenlegen:

Betrachte Karte  $k$  aus dem Stapel  $s$  ( $s \in \{1, \dots, c-2\}$ ). 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  $(0, \dots, n-1)$  passiert durch  $L_c$  folgendes:

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

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*

■

**Lemma 5.3.** (Schlussfolgerung aus 2.4, 4.5, 5.2)

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

Wähle  $a_1, \dots, a_r \in A_n$  und  $a'_1, \dots, a'_l \in B_n$  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  $R_{c_1}, \dots, R_{c_r}$  und  $L_{c'_1}, \dots, L_{c'_l}$  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.

Wir machen uns klar dass das aus wirklich stimmt:

$$\begin{aligned} R_{c_1} R_{c_2}(k) &= \phi_{a_1, b_1} \circ \phi_{a_2, b_2}(k) \\ &= \phi_{a_1, b_1}(a_2 k + b_2) \\ &= a_1(a_2 k + b_2) + b_1 \\ &= \phi_{a_1 a_2, a_1 b_2 + b_1}(k) \end{aligned}$$

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