

## Zauberhafte Normalteiler

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

$U$  heißt **Normalteiler** von  $G \iff \forall g \in G : gUg^{-1} = U$

**Bemerkung.** Im Allgemeinen ist  $U \subset G$  kein Normalteiler. Wir suchen größte Untergruppe von  $G$ , in der  $U$  Normalteiler ist. Wir wollen also  $V$  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)

**Definition (2.2).** Der **Normalisator** von  $U$  in  $G$  ist definiert als  $N_G(U) := \{g \in G \mid gUg^{-1} = U\}$

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

**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:*

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

**Definition (3.1).** Die Gruppe aller Permutationen mit  $n$  Karten heißt die **symmetrische Gruppe**  $S_n$ . Jede Permutation lässt sich mit  $\mathbb{Z}_n := \{0, \dots, n-1\}$  als bijektive Abbildung  $\phi : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$  identifizieren.

**Definition (3.2).** Sei  $r \in \mathbb{Z}_n$ . Die Permutation  $s_r : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ ,  $k \mapsto s_r(k) = k + r \pmod n$  entspricht einem zyklischen Shift im Kartenstapel.  $s_r$  ist bijektiv, also  $s_r \in S_n$ .

**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).