Definition 1

Eine Gruppe $(G, \cdot)$ ist eine Menge G mit einer Verknüpfung $\cdot : G \times G \longrightarrow G$, so dass

(1) $\forall f, g, h \in G: \quad (f \cdot g) \cdot h = f \cdot (g \cdot h)$ (Assoziativgesetz)

(2) $\exists e \in G: \quad \forall g \in G: \quad g \cdot e = g$ (und $e \cdot g = g$)

(3) $\forall g \in G \ \exists g^{-1} \in G: \quad g \cdot g^{-1} = e$ (und $g^{-1} \cdot g = e$.)

In der Definition heißt e neutrales Element und g^{-1} inverses Element.

Bemerkung $\boxed{f \cdot g} := \boxed{\cdot (f, g)}$

Definition 2

Sei $(G, \cdot)$ eine Gruppe. Sie heißt kommutativ oder abelsch, falls:

$$\forall g, h \in G: \quad g \cdot h = h \cdot g$$

Satz 3

Sei $n \in \mathbb{N}$ und $S_n := \{\pi : \{1, \ldots, n\} \longrightarrow \{1, \ldots, n\} \mid \pi \text{ bijektiv}\}$

Sei $\circ$ die Verknüpfung von Abbildungen. Dann ist $(S_n, \circ)$ eine Gruppe, die sogenannte Permutationsgruppe oder symmetrische Gruppe.

Beweis: Übung.

Andere Beispiele: $(\mathbb{Z}, +)$, $(GL(n), \cdot)$, etc.

Insbesondere muss "$\cdot$" nicht unbedingt "Multiplikation" bedeuten.

Satz 4

Sei $(G, \cdot)$ eine Gruppe. Dann gilt:

(1) $\forall g \in G$: Falls $g \cdot g^{-1} = e$, so auch $g^{-1} \cdot g = e$

(2) Für alle $g \in G$ gibt es ein eindeutiges Inverses Element.

(3) $\forall g \in G$: $e \cdot g = g$.

(4) Das neutrale Element ist eindeutig.

Beweis

Erinnerung:

> Definition 1
>
> Eine Gruppe $(G, \cdot)$ ist eine Menge G mit einer Verknüpfung $\cdot\ G \times G \to G$, so dass
>
> (1) $\forall f, g, h \in G$: $(f \cdot g) \cdot h = f \cdot (g \cdot h)$ (Assoziativgesetz)
>
> (2) $\exists e \in G$: $\forall g \in G$: $g \cdot e = g$
>
> (3) $\forall g \in G$ $\exists g^{-1} \in G$: $g \cdot g^{-1} = e$

(1) $$g^{-1} \cdot g = g^{-1} \cdot g \cdot e = g^{-1} \cdot \underbrace{g \cdot g^{-1}}_{=e} \cdot (g^{-1})^{-1}$$
$$= \underbrace{g^{-1} \cdot e}_{g^{-1}} (g^{-1})^{-1}$$
$$= g^{-1} (g^{-1})^{-1} = e$$

(3) $$g = g \cdot e \overset{(1)}{=} g \cdot (g^{-1} \cdot g) = (g g^{-1}) \cdot g = e \cdot g$$

(2) Seien $f, g \in G$ mit $g \cdot h = g \cdot f = e$. Dann gilt:

$h = h \cdot g \cdot h$ und $h \cdot g \cdot h = h \cdot g \cdot f$. Wegen (1): $h \cdot g = e$

$$= e \cdot f$$
$$\overset{(3)}{=} f$$

$$\Rightarrow \quad h = h \cdot g \cdot h = f$$

(4) Seien e und e' neutrale Elemente. Es gilt:

$$\underline{e \cdot e'} = e' = e$$

<u>Notation</u> Im Folgenden bezeichnet immer e <u>das</u> neutrale Element in einer Gruppe und g^{-1} bezeichnet das Inverse von g.

<u>Satz 5</u>

Sei $(G, \circ)$ eine Gruppe. Dann gilt:

(1) $\forall g, h \in G: \quad (g \cdot h)^{-1} = h^{-1} \cdot g^{-1}$ (<— wichtige Formel!!)

(2) $\forall g \in G: \quad (g^{-1})^{-1} = g.$

(3) $\forall f, g, h \in G:$ Falls $f \cdot g = f \cdot h \Rightarrow g = h$
und $g \cdot f = h \cdot f \Rightarrow g = h.$

<u>Beweis</u> Übung.

<u>Definition 6</u>

Sei $(G, \cdot)$ eine Gruppe, und $g \in G$. Die Ordnung von g ist

$$\mathrm{ord}(g) := \min \{ r > 0 \mid g^r = e \}$$

Falls $\mathrm{ord}(g)$ nicht definiert ist, setzen wir $\mathrm{ord}(g) := \infty$.

<u>Bemerkung</u>: Für $(G, \cdot) = (\mathbb{Z}, +)$ gilt: Für $g \in \mathbb{Z}$ ist

$$\mathrm{ord}(g) = \min \{ r > 0 \mid r \cdot g = 0 \}$$

Multiplikation!

Lemma 7

Sei $(G, \cdot)$ mit $|G| < \infty$. Dann gilt für alle $g \in G$: $\mathrm{ord}(g) < \infty$.

Beweis

Betrachte $\{g, g^2, g^3, \dots\} \subseteq G$. Behauptung: es gibt $i \neq j$ so dass $g^i = g^j$. Beweis: Angenommen, das stimmt nicht. Dann sind $g, g^2, g^3, \dots$ alle verschieden. Aber wenn diese alle verschieden sind, dann ist $|\{g, g^2, g^3, \dots\}| = \infty$. Da $\{g, g^2, g^3, \dots\} \subseteq G$, ist auch G unendlich. Aber G ist nicht unendlich!

$\rightarrow$ es existieren i, j, $i \neq j$, mit $g^i = g^j$ (oBdA $i < j$).

Satz 5(3)
$\Rightarrow$ für $i < j$ gilt $g^{j-i} = e$.

$\Rightarrow$ $\mathrm{ord}(g) \leq j - i < \infty$

$\square$