$(\mathbb{Z}, +)$ $e = 0$, $a' = -a$

$(\mathbb{Q}, +)$

$(\mathbb{R}, +)$

~~$(\mathbb{N}, +)$ $-a \notin \mathbb{N}$~~

$(\mathbb{R}^\times, \cdot)$ $e = 1$, $a' = \bar{a}^1 = \frac{1}{a}$

~~$(\mathbb{R}, \cdot)$ $\neq 0$~~

Beweis:

① $\boxed{\tau_a \circ \tau_{\bar{a}^1} = id_G}$, denn $\forall g \in G$ ist

$(\tau_a \circ \tau_{\bar{a}^1})(g) = \tau_a(g * \bar{a}^1)$

$= g * (\bar{a}^1 * a)$

$= g * e$

$= g = id_G(g)$

Genauso ist

$\boxed{\tau_{\bar{a}^1} \circ \tau_a = id_G}$

Also τ_a bijektiv (Lemma 2.1.5)

Analog:

$$\left.\begin{aligned} a^{\tau} \circ a^{\bar{\tau}} &= id_G \\ a^{\bar{\tau}} \circ a^{\tau} &= id_G \end{aligned}\right\} \Rightarrow a^{\tau} \text{ bijektiv.}$$

② Da $G \neq \emptyset$, $\exists x \in G$.

Da $x \in \tau_x(G)$, $\exists e \in G$:

$x = \tau_x(e)$, also

$x = e * x$.

(n.E.) Sei $a \in G$ beliebig.

Da $a \in {}_x\tau(G)$, $\exists y \in G$

$a = {}_x\tau(y)$, also

$a = x * y$.

Somit ist

$$e * a = (e * x) * y$$
$$= x * y$$
$$= a$$ ✓

(Inv.) Sei $a \in G$ beliebig.

Da $e \in \tau_a(G)$, $\exists a' \in G$

$e = a' * a$ ✓ □

$\tau_a \quad a\tau \quad$ „tau"

Gruppe mit 2 Elementen

$G = \{e, a\}$

$*$	e	a
e	e	a
a	a	e

$\tau_a(G)$

$*$	b
a	$a*b$

$a\tau(G)$

in jeder Spalte und in jeder Zeile muss jedes Element genau einmal auftreten

$(G, *)$ ist eine (abelsche) Gruppe

!!

C_2

Gruppen mit 3 Elementen

$G = \{e, a, b\}$

$*$	e	a
e	e	a
a	a	e

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

$*$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

$\odot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Beweis:

(wohldef.) $*: H \times H \longrightarrow H$ ✓

(assoziativ) ✓

$e \in H$: $\exists\, h \in H$, $h^{-1} \in H$ $\Rightarrow$ $\underbrace{h^{-1} * h}_{e} \in H$

(neutrales Element von G)

(u.E.) ✓

(Inv.) ✓

Beispiele:

$\mathbb{Z} \subset (\mathbb{R}, +)$ Untergruppe

~~$\mathbb{N} \subset (\mathbb{R}, +)$~~ $1 \in \mathbb{N}$ aber $-1 \notin \mathbb{N}$

$5 \cdot \mathbb{Z} \subset (\mathbb{Z}, +)$ Untergruppe

$=$

$\{\ldots, -5, 0, 5, 10, 15, \ldots\}$

$=$

$\{n \in \mathbb{Z} \mid 5 \mid n\}$ ↖ "teilt"

$=$

$\{n \in \mathbb{Z} \mid \exists k \in \mathbb{Z}: n = 5 \cdot k\}$

Notiz: Für jede Untergruppe H von $(G,*)$ ist die Inklusion

$$\begin{array}{ccc} (H,*) & \longrightarrow & (G,*) \\ h & \mapsto & h \end{array}$$

ein Homomorphismus

Beweis:

(i) $e_H \circ f(e_G) = f(e_G)$

$= f(e_G * e_G)$

$= f(e_G) \circ f(e_G)$

(f Homo)

Wende auf beiden Seiten $f(e_G)^{-1}$ an.

$e_H = f(e_G)$

(ii) $\underbrace{f(a')}_{f(a)^{-1}} \circ f(a) = f(a' * a)$

(f Homo) $= f(e_G)$

$\overset{(i)}{=} e_H$

Nutze Eindeutigkeit von Inversen.

Beispiele

$(\mathbb{Z},+) \xrightarrow{f} (\mathbb{Z},+)$

$n \longmapsto n+1$

$f(0) = 1$

$\uparrow e \qquad \uparrow \neq e$

$(\mathbb{Z},+) \xrightarrow{f} (\mathbb{Z},+)$

$n \longmapsto 5 \cdot n$

Homo

$f(n+m) = 5(n+m)$

$= 5n + 5m$

$= f(n) + f(m)$ ✓

$C_2 \xrightarrow{f} \{\pm 1, \cdot\}$

$e \longmapsto 1$

$a \longmapsto -1$

Homo

Iso

$*$	e	a
e	e	a
a	a	e

$f(a*a) \quad f(a) \cdot f(a)$

$\| \qquad \| \qquad (-1)\cdot(-1)$

$f(e) \qquad \|$

$\| \qquad 1$

1

$(\mathbb{R}, +) \longrightarrow (\mathbb{R}^+, \cdot)$ Homo

$x \longmapsto e^x$

$e^{x+y} = e^x \cdot e^y$ ✓

Beweis: Für $a, b \in H$ ist

$$f^{-1}(a \circ b) = f^{-1}\Big(f(f^{-1}(a)) \circ f(f^{-1}(b))\Big)$$

$$= f^{-1}\Big(f(f^{-1}(a) * f^{-1}(b))\Big)$$

f Homo

$$= (f^{-1} \circ f)(f^{-1}(a) * f^{-1}(b))$$

$$= id_G$$

$$= f^{-1}(a) * f^{-1}(b)$$

Also f^{-1} Homomorphismus. □

z.B. $17 = 3 \cdot 5 + 2$

$$n = q \cdot m + r$$

Beweis: Es ist $n \sim_m r$,

denn $m \mid \underbrace{n - r}_{q \cdot m}$ □

$n = 3$

$$\mathbb{Z} = \{\ \dots, 8, 7, 6, 5, 4, 3, 2, 1, 0, -1, -2, -3, \dots\ \}$$

$$\mathbb{Z}/3\mathbb{Z} = \mathbb{Z}/n_3 = \{\ \dots, 3, 0, -3, \dots \ ;\ \dots, 4, 1, -2, \dots \ ;\ \dots, 5, 2, -1, \dots\ \}$$

$$[-3] = [30] = [0] \qquad [1] \qquad [2]$$

Beweis:

Seien x', y' alternative Repräs. von $[x]$ und $[y]$, also

$$\left.\begin{aligned} [x'] &= [x] \\ \text{und } [y'] &= [y] \end{aligned}\right\} \text{(I)}$$

Zu zeigen ist: $[x'+y'] = [x+y]$.

(I) bedeutet:

$x' \sim_m x$, also $x' - x = q \cdot m$ für ein $q \in \mathbb{Z}$

$y' \sim_m y$, also $y' - y = p \cdot m$ für ein $p \in \mathbb{Z}$

Daher

$$(x'+y') - (x+y) = qm + pm = (q+p) \cdot m,$$

d.h.

$$x'+y' \sim_m x+y,$$

also $[x'+y'] = [x+y]$ □

Beweis:

z.B.

(Assoziativität von $\oplus$)

$$\begin{aligned}
&([x] \oplus [y]) \oplus [z] \\
&= [x+y] \oplus [z] \\
&= [(x+y)+z] \qquad + \text{ auf } \mathbb{Z} \text{ assoziativ} \\
&= [x+(y+z)] \\
&= [x] \oplus [y+z] \\
&= [x] \oplus ([y] \oplus [z])
\end{aligned}$$

n.E. $[0]$

$-[x] = [-x]$ $[\ldots]$ □

Schreiben in Zukunft

$\left(\mathbb{Z}/m\mathbb{Z}, +\right)$ statt $\left(\mathbb{Z}/m\mathbb{Z}, \oplus\right)$

$\mathbb{Z}/2\mathbb{Z}$

+	[0]	[1]
[0]	[0]	[1]
[1]	[1]	[0] = [2]

$(\simeq C_2)$

$\mathbb{Z}/3\mathbb{Z}$

+	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

$(\simeq C_3)$