Lineare Algebra I

Woche 05

14.11.2023 und 16.11.2023

bzgl. Verknüpfung abgeschlossene Menge

Definition

Abkürzung für $\star|_{Y\times Y}^{Y}$

Es sei $(X, \star)$ eine Menge mit Verknüpfung.

Eine Teilmenge $Y \subseteq X$ heißt **abgeschlossen** bzgl. $\star$, wenn $\star\colon X \times X \to X$ eingeschränkt werden kann zu $\star_Y\colon Y \times Y \to Y$.

In diesem Fall heißt $\star_Y$ die auf Y **induzierte Verknüpfung**.

Beispiel

In $(\mathbb{Z}, +)$ sind $\mathbb{N}$ und $\mathbb{N}_0$ abg. bzgl. $+$.

Auch $m\mathbb{Z} = \{mz \mid z \in \mathbb{Z}\}$ ist abg. bzgl. $+$.
$m \in \mathbb{N}$

Definition

Es sei $(G, \star)$ eine Gruppe.

1. Eine bzgl. $\star$ abgeschlossene Teilmenge $U \subseteq G$ heißt eine **Untergruppe** von $(G, \star)$, wenn $(U, \star_U)$ selbst wieder eine Gruppe ist. (UG)

   neutrales Element
   alle invertierbar

2. Eine Untergruppe $(U, \star_U)$ von $(G, \star)$ heißt **echt**, wenn $U \subsetneq G$ gilt.

- Wir schreiben auch $(U, \star_U) \leq (G, \star)$
- $\leq$ ist Ordnungsrelation auf der Menge aller UG von $(G, \star)$.
  (reflexiv, antisymm., transitiv)

neutrale und inverse Elemente in einer Untergruppe

Lemma

Es sei $(U, \star_U)$ eine Untergruppe der Gruppe $(G, \star)$.

1. Das neutrale Element e_U von $(U, \star_U)$ ist gleich dem neutralen Element e von $(G, \star)$.
2. Das Inverse von $a \in U$ ist gleich dem Inversen von a in G.

Beweis. Hausaufgabe

Konsequenz: Schreibe $*$ statt $*_U$

Untergruppenkriterium

Teilmenge

Satz

Es sei $(G, \star)$ eine Gruppe mit dem neutralen Element e sowie $U \subseteq G$. Dann sind äquivalent:

1. $(U, \star)$ ist eine Untergruppe von $(G, \star)$.
2. $U \neq \emptyset$, und für alle $a, b \in U$ gilt $a \star b' \in U$.

Beweis. ① $\Rightarrow$ ② U als Gruppe enthält ein neutrales Element, nämlich e. Also ist $U \neq \emptyset$.
Für $a, b \in U$ gilt $b' \in U$ nach dem Lemma eben.
U ist bzgl. $*$ abg., also $a * b' \in U$.

Satz

Es sei $(G, \star)$ eine Gruppe mit dem neutralen Element e sowie $U \subseteq G$. Dann sind äquivalent:

1. $(U, \star)$ ist eine Untergruppe von $(G, \star)$.
2. $U \neq \emptyset$, und für alle $a, b \in U$ gilt $a \star b' \in U$.

Beweis. ② $\Rightarrow$ ①

- U enthält das neutrale Element e von G:
  $U \neq \emptyset$, $\exists a \in U$, und nach Vor. ist $e = a \star a' \in U$
- U enthält die Inversen seiner Elemente:
  $a \in U \Rightarrow a' = e \star a' \in U$ nach Vor.
- U ist abg. bzgl. $\star$!
  $a, b \in U \Rightarrow b' \in U \Rightarrow a \star b = \underbrace{a}_{\in U} \star \underbrace{(b')}_{\in U}{}' \in U$.

Beispiel

1. Es sei $(G, \star)$ eine Gruppe mit dem neutralen Element e. Dann sind $(\{e\}, \star)$ und $(G, \star)$ die **trivialen Untergruppen** von $(G, \star)$.

   Minimum Maximum aller Untergr. von G bzgl. $\subseteq$

2. $(\underbrace{\mathbb{R}_{>0}}_{\neq \emptyset}, \cdot)$ ist eine Untergruppe von $(\mathbb{R}_{\neq 0}, \cdot)$.

   und $a \cdot b^{-1} \in \mathbb{R}_{>0}$

3. Für Zahl $m \in \mathbb{N}$ ist $m\mathbb{Z} := \overset{\neq \emptyset}{\{m\,z \mid z \in \mathbb{Z}\}}$ mit der Operation $+$ eine Untergruppe der Gruppe $(\mathbb{Z}, +)$.

und $m z_1 - m z_2 = m(z_1 - z_2) \in m\mathbb{Z}$

Beispiel

$S_3 = \{\sigma_0, \dots, \sigma_5\}$

$\{\sigma_0, \sigma_1, \sigma_2\}$ UG der Drehungen

$\{\sigma_0, \sigma_3\}$ $= \sigma_3^{-1}$

$\{\sigma_0, \sigma_4\}$ $= \sigma_4^{-1}$

$\{\sigma_0, \sigma_5\}$ $= \sigma_5^{-1}$

$\{\sigma_0\}$

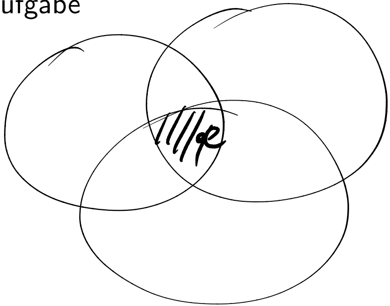
Durchschnitt von Untergruppen

Lemma

Es sei $(G, \star)$ eine Gruppe und $(U_i, \star)_{i \in I}$ eine Familie von Untergruppen mit Indexmenge $I \neq \emptyset$.

Dann ist auch $\bigcap_{i \in I} U_i$ mit $\star$ eine Untergruppe von $(G, \star)$.

Beweis. Hausaufgabe



Definition

Es sei $(G, \star)$ eine Gruppe und $E \subseteq G$.

Dann heißt

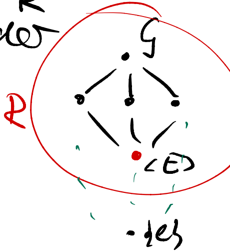
Durchschnitt über Untergruppen

$$\langle E \rangle := \bigcap \underbrace{\{U \mid (U, \star) \text{ ist Untergruppe von } (G, \star) \text{ und } E \subseteq U\}}_{R}$$

die von E **erzeugte Untergruppe** in $(G, \star)$.

$\langle E \rangle$ ist das Minimum der Teilmenge R in der Menge aller UG von $(G,*)$ bzgl. der Halbordnung $\subseteq$.

Wie soll man das berechnen?



Darstellung der erzeugten Untergruppe

Satz

Es sei $(G, \star)$ eine Gruppe und $E \subseteq G$.

Dann gilt für die von E erzeugte Untergruppe:

$$\langle E \rangle = \left\{ a_1 \star \cdots \star a_n \,\middle|\, \exists n \in \mathbb{N}_0 \; \forall i = 1, \ldots, n \; (a_i \in E \cup E') \right\},$$

wobei E' die Menge der Inversen von E bezeichnet.

z.B. $\langle \{a_1, a_2\} \rangle$ enthält

$n=0$: e

$n=1$: $a_1, a_2, a_1^{-1}, a_2^{-1}$

$n=2$: $a_1 \star a_1, a_1 \star a_1^{-1}, a_1 \star a_2^{-1}, \ldots, a_2^{-1} \star a_2^{-1}$

$\vdots$

nicht alle verschieden

$E = \emptyset$ ist möglich, E kann unendlich sein!

$$\langle E \rangle := \bigcap \underbrace{\{U \mid (U, \star) \text{ ist Untergruppe von } (G, \star) \text{ und } E \subseteq U\}}_{=R} = \bigcap R$$

$$M := \{a_1 \star \cdots \star a_n \mid \exists n \in \mathbb{N}_0 \ \forall i = 1, \ldots, n \ (a_i \in E \cup E')\}$$

Beweis. $M \subseteq \langle E \rangle$: Es sei $U \in R$ beliebig.

Da $E \subseteq U$ und U UG ist, gilt $E' \subseteq U$.

U ist abg. bzgl $\star$ $\Rightarrow$ U enthält

$(n=0)$ e $(n=1)$ a_1 für $a_1 \in E \cup E'$ und $(n=2)$

$a_1 \star a_2$ für $a_1, a_2 \in E \cup E'$. Induktion über $n \in \mathbb{N}_0$:

$M \subseteq U$. U war beliebig in R.

$\Rightarrow M \subseteq \bigcap R = \langle E \rangle$.

$$\langle E \rangle := \bigcap \{ U \mid (U, \star) \text{ ist Untergruppe von } (G, \star) \text{ und } E \subseteq U \}$$
$$M := \{ a_1 \star \cdots \star a_n \mid \exists n \in \mathbb{N}_0 \ \forall i = 1, \ldots, n \ (a_i \in E \cup E') \}$$

Beweis. $\langle E \rangle \subseteq M$!

- M ist UG von G: Nutze das UG-Krit.!

  $M \neq \emptyset$, denn $e \in M$.

  Sind $a_1 * \cdots * a_n$ und $b_1 * \cdots * b_m$ beide in M, dann auch $a_1 * \cdots * a_n * \underbrace{(b_1 * \cdots * b_m)'}_{\in M} \in M$!

  Also ist M selbst eine UG von G.

- Weiter ist $E \subseteq M$, d.h. $M \in R$.

  $\Rightarrow \langle E \rangle = \bigcap R \subseteq M$.

erzeugte Untergruppe

Beispiel

Für die Elemente von S_3

$$\sigma_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad \text{Drehungen}$$

$$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \text{Spiegelungen}$$

gilt $\langle \{\sigma_3\} \rangle = \{ \underbrace{\sigma_3^0}_{=\mathrm{id}}, \sigma_3, \underbrace{\sigma_3^{-1}}_{=\sigma_3}, \sigma_3 \circ \sigma_3, \dots, \sigma_3 \circ \sigma_3^{-1} \dots \}$

$= \{\sigma_0, \sigma_3\}$

$\langle \{\sigma_1\} \rangle = \{ \underbrace{\sigma_1^0}_{=\mathrm{id}}, \sigma_1, \underbrace{\sigma_1^{-1}}_{=\sigma_2}, \sigma_1 \circ \sigma_1, \dots \} = \underbrace{\{\sigma_0, \sigma_1, \sigma_2\}}_{= A_3}$

$\langle \{\sigma_1, \sigma_3\} \rangle = S_3$

Erzeugendensystem

von nur einem Element erzeugte Untergruppe

Definition

Es sei $(G, \star)$ eine Gruppe.

1. Die von $a \in G$ erzeugte Untergruppe $\langle a \rangle := \langle \{a\} \rangle$ heißt die von a erzeugte **zyklische Untergruppe** von $(G, \star)$.

2. Falls $G = \langle a \rangle$ für ein $a \in G$ gilt, so heißt $(G, \star)$ eine **zyklische Gruppe**.

von nur einem Element erzeugte Untergruppe

Beispiel

1. In $(\mathbb{Z},+)$ erzeugt $m \in \mathbb{Z}$ die zykl. UG $\langle m \rangle = m\mathbb{Z}$.

2. $m=1$ und $m=-1$ erzeugen ganz $(\mathbb{Z},+)$: $\langle 1 \rangle = \langle -1 \rangle = \mathbb{Z}$.

abkürzende Schreibweisen

Definition

Es sei $(H, \star)$ eine Halbgruppe, $a \in H$ sowie $A, B \subseteq H$.

$$\begin{aligned} a \star B &:= \{a \star b \,|\, b \in B\} \\ B \star a &:= \{b \star a \,|\, b \in B\} \\ A \star B &:= \{a \star b \,|\, a \in A,\ b \in B\} \\ A' &:= \{a' \,|\, a \in A \text{ ist invertierbar}\} \end{aligned}$$

Beispiel

UG-Krit.: $U \neq \emptyset$ und $U \star U' \subseteq U$.

Untergruppe induziert eine Äquivalenzrelation

Lemma

Es sei $(U, \star)$ eine Untergruppe der Gruppe $(G, \star)$. Dann gilt:

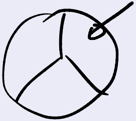
1. $a \sim^U b \; :\Leftrightarrow \boxed{b \in a \star U}$ ist eine Äquivalenzrelation.

   $\Leftrightarrow a^{-1} \star b \in U$

2. Die Äquivalenzklassen sind $[a] = a \star U$. Linksnebenklassen

   $U = [e]$

3. Jede Äquivalenzklasse ist gleichmächtig zu U.



Beweis.

Definition

Es sei $(U, \star)$ eine Untergruppe der Gruppe $(G, \star)$.

$\Leftrightarrow a' \star b \in U$ $\qquad\qquad$ $\Leftrightarrow a \star b' \in U$

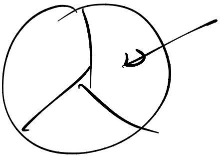
$a \sim^U b \;:\Leftrightarrow\; b \in a \star U$ $\qquad$ $a \;{}^U\!\!\sim b \;:\Leftrightarrow\; a \in U \star b$

$[a]_{\sim^U} = \boxed{a \star U}$ **Linksnebenklasse** $\qquad$ $[a]_{{}^U\!\sim} = \boxed{U \star a}$ **Rechtsnebenklasse**

$G \,/ \sim^U$ oder $G \,/\, U$ $\qquad$ $G \,/\, {}^U\!\!\sim$ oder $U \backslash G$

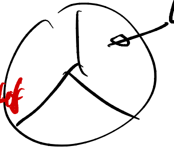
Wenn G kommut. ist, dann sind beide Rel. identisch

Repr. steht links



$U = [e]$

Repr. steht rechts

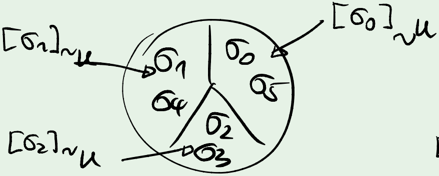


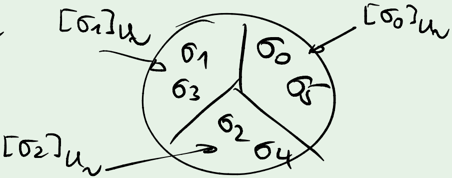
$U = [e]$

nicht kommutativ

Beispiel

$G = S_3$ $\qquad$ $U = \{\sigma \in S_3 \mid \sigma(3) = 3\} = \{\sigma_0, \sigma_5\}$





$$\sigma_1 \circ U = \{\sigma_1 \circ \sigma_0, \sigma_1 \circ \sigma_5\} = \{\sigma_1, \sigma_4\}$$

$$\sigma_2 \circ U = \{\sigma_2 \circ \sigma_0, \sigma_2 \circ \sigma_5\} = \{\sigma_2, \sigma_3\}$$

$$U \circ \sigma_1 = \{\sigma_0 \circ \sigma_1, \sigma_5 \circ \sigma_1\} = \{\sigma_1, \sigma_3\}$$

$$U \circ \sigma_2 = \{\sigma_0 \circ \sigma_2, \sigma_5 \circ \sigma_2\} = \{\sigma_2, \sigma_4\}$$

Satz

Es sei $(G, \star)$ eine endliche Gruppe und $(U, \star)$ eine Untergruppe.

Dann gilt $\#U \mid \#G$.

Beweis. Hausaufgabe

Dieser Satz schränkt die möglichen Kardinalitäten von Untergruppen ein!

Definition

Es seien $(H_1, \star)$ und $(H_2, \square)$ zwei Halbgruppen.

1. Eine Abbildung $f\colon H_1 \to H_2$ heißt **strukturverträglich** oder ein **Homomorphismus** von $(H_1, \star)$ in $(H_2, \square)$, wenn gilt:

$$f(a \star b) = f(a) \,\square\, f(b) \quad \text{für alle } a, b \in H_1.$$

erst verknüpfen dann rüber   erst rüber dann verknüpfen

2. Ist zudem $f\colon H_1 \to H_2$ bijektiv, so heißt f auch **strukturerhaltend** oder ein **Isomorphismus**.

Endomorphismus

Beispiel

1. $f\colon (\mathbb{N},+) \to (\mathbb{N},+)$ mit $f\colon n \mapsto 2\,n$ $= n+n$

   $f(n+m) = 2(n+m) = n+m+n+m = n+n+m+m$
   $= 2n+2m = f(n)+f(m)$ ✓

2. Es sei X eine Menge und $x_0 \in X$.
   $\Phi\colon \underbrace{(\mathbb{N}^X,+)} \to (\mathbb{N},+)$ mit $\Phi\colon f \mapsto f(x_0)$ Auswertungsabb.

   Funktionen $X \to \mathbb{N}$ mit punktweise $+$

   $\Phi(f+g) = (f+g)(x_0) = f(x_0)+g(x_0) = \Phi(f)+\Phi(g)$ ✓

Homomorphismus von Monoiden

Definition

Es seien $(M_1, \star)$ und $(M_2, \square)$ zwei Monoide.

1. Eine Abbildung $f\colon M_1 \to M_2$ heißt **strukturverträglich** oder ein **Homomorphismus** von $(M_1, \star)$ in $(M_2, \square)$, wenn gilt:

$$\begin{aligned} f(a \star b) &= f(a) \,\square\, f(b) \quad \text{für alle } a, b \in M_1, \\ f(e_1) &= e_2. \end{aligned}$$

Idee: „Respektiere alles, was die Strukturen ausmacht"

2. Ist zudem $f\colon M_1 \to M_2$ bijektiv, so heißt f auch **strukturerhaltend** oder ein **Isomorphismus**.

Beispiel

1. $f\colon \underbrace{(\mathbb{N}_0, +)}_{\text{Monoid}} \to \underbrace{(\mathbb{N}_0, +)}_{\text{Monoid}}$ mit $f\colon n \mapsto 2\,n$

   $f(0) = 0 + 0 = 0$ ✓

2. Es sei X eine Menge und $x_0 \in X$.
   $\Phi\colon (\mathbb{N}_0^X, +) \to (\mathbb{N}_0, +)$ mit $\Phi\colon f \mapsto f(x_0)$

neutrales Element ist $0_{\mathbb{N}_0^X}$ (Nullfunktion)

$\Phi(0_{\mathbb{N}_0^X}) = 0_{\mathbb{N}_0^X}(x_0) = 0$ ✓

Homomorphismus von Gruppen

Definition

Es seien $(G_1, \star)$ und $(G_2, \square)$ zwei Gruppen.

1. Eine Abbildung $f\colon G_1 \to G_2$ heißt **strukturverträglich** oder ein **Homomorphismus** von $(G_1, \star)$ in $(G_2, \square)$, wenn gilt:

$$f(a \star b) = f(a) \square f(b) \quad \text{für alle } a, b \in G_1.$$

2. Ist zudem $f\colon G_1 \to G_2$ bijektiv, so heißt f auch **strukturerhaltend** oder ein **Isomorphismus**.

Wieso fordern wir nicht $f(e_1) = e_2$
und $f(a') = f(a)'$?

Man muss diese Eigenschaften nicht fordern!

Lemma

Ein Gruppenhomomorphismus erfüllt

1. $f(e_1) = e_2$
2. $(f(a))' = f(a')$

Beweis. ① $f(e_1) \boxtimes e_2 = f(e_1) = f(e_1 * e_1)$

$= f(e_1) \boxtimes f(e_1) \Rightarrow e_2 = f(e_1)$. (Kürzungsregel)

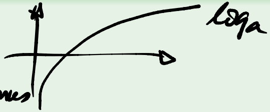
② $f(a') \boxtimes f(a) = f(a' * a) = f(e_1) \overset{①}{=} e_2$.

Einseitiger Test reicht in Gruppen aus!

Homomorphismus von Gruppen

Beispiel

1. Es sei $a > 0$, $a \neq 1$.
   $\log_a\colon \underbrace{(\mathbb{R}_{>0}, \cdot)}_{\text{Gruppe}} \to \underbrace{(\mathbb{R}, +)}_{\text{Gruppe}}$ bijektiv, also Isomorphismus

   $$\log_a(x \cdot y) = \log_a x + \log_a y$$

2. $\operatorname{sgn}\colon (S_n, \circ) \to (\{\pm 1\}, \cdot)$

   $$\operatorname{sgn}(\sigma_1 \circ \sigma_2) = (\operatorname{sgn} \sigma_1) \cdot (\operatorname{sgn} \sigma_2)$$ Satz 7.29

Lemma $\cong$

Die Isomorphie von Halbgruppen bzw. von Monoiden bzw. von Gruppen ist eine Äquivalenzrelation.

Beweis. (für Halbgruppen)

- Reflexivität: $(H_1, *) \cong (H_1, *)$ mit id_{H_1}
- Symmetrie: $(H_1, *) \cong (H_2, \square)$ mit $f: H_1 \to H_2$.

  $f^{-1}: H_2 \to H_1$ ist bijektiv und ebenfalls Homomorphismus:

$$f^{-1}(\underbrace{x}_{f(a)} \square \underbrace{y}_{f(b)}) = f^{-1}(f(a) \square f(b)) = f^{-1}(f(a*b)) = a*b = f^{-1}(x) * f^{-1}(y)$$

- Transitivität: Komposition von Isomorphismen ist Isomorphismus

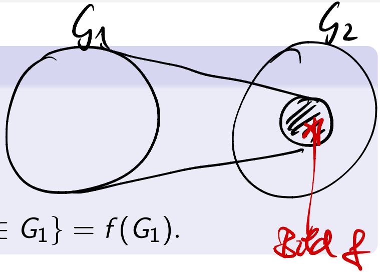
Definition

1. Ein Homomorphismus von Halbgruppen bzw. von Monoiden bzw. von Gruppen heißt ein **Endomorphismus**, wenn beide Strukturen identisch sind.

2. Ein Isomorphismus von Halbgruppen bzw. von Monoiden bzw. von Gruppen heißt ein **Automorphismus**, wenn beide Strukturen identisch sind.

$$\begin{tikzcd} \text{homo} \arrow[r, squiggly, "\text{bijektiv}"] \arrow[d, squiggly, "\text{id. Str.}"'] & \text{iso} \arrow[d, squiggly, "\text{id. Str}"] \\ \text{endo} \arrow[r, squiggly, "\text{bijektiv}"'] & \text{auto} \end{tikzcd}$$

Bild eines Gruppenhomomorphismus



Definition

Es seien $(G_1, \star)$ und $(G_2, \square)$ Gruppen.

Das **Bild** von f ist definiert als

$$\mathrm{Bild}(f) := \{f(x) \in G_2 \,|\, x \in G_1\} = f(G_1).$$

Lemma

$\mathrm{Bild}(f)$ ist eine Untergruppe von $(G_2, \square)$.

Beweis. UG-Kriterium: $e_2 = f(e_1)$, also ist $e_2 \in \mathrm{Bild}\, f \neq \emptyset$.
Es seien $x, y \in \mathrm{Bild}\, f$. Zu zeigen: $x \square y' \in \mathrm{Bild}\, f$.
$x = f(a)$, $y = f(b)$. $x \square y' = f(a) \square f(b)' = f(a) \square f(b')$
$= f(a \star b') \in \mathrm{Bild}\, f$.

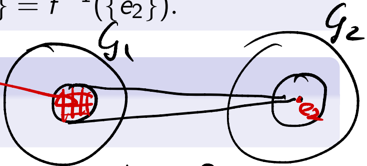
Definition

Es seien $(G_1, \star)$, $(G_2, \square)$ Gruppen mit neutralen Elementen e_1 bzw. e_2.

Der **Kern** von f ist definiert als

$$\operatorname{Kern}(f) := \{x \in G_1 \mid f(x) = e_2\} = f^{-1}(\{e_2\}).$$

Kern f



Lemma

$\operatorname{Kern}(f)$ ist eine Untergruppe von $(G_1, \star)$.

Beweis. UG-Kriterium: $e_2 = f(e_1)$, also $e_1 \in \operatorname{Kern} f \neq \emptyset$.

Es seien $a, b \in \operatorname{Kern} f$. Zu zeigen: $a \star b' \in \operatorname{Kern} f$.

$f(a \star b') = f(a) \square f(b') = f(a) \square f(b)'$

$= e_2 \square e_2' = e_2$, d.h. $a \star b' \in \operatorname{Kern} f$.

Bild und Kern eines Gruppenhomomorphismus

Beispiel

1. $\operatorname{sgn}\colon (S_n, \circ) \to (\{\pm 1\}, \cdot)$

   $n \geq 2$: $\operatorname{Bild} \operatorname{sgn} = \{\pm 1\}$ surjektiv

   $\operatorname{Kern} \operatorname{sgn} = \operatorname{sgn}^{-1}(\{1\}) =$ gerade Permutationen

   $= A_n$ alternierende Untergruppe

2. $f\colon (\mathbb{R}_{\neq 0}, \cdot) \ni x \mapsto x^2 \in (\mathbb{R}_{\neq 0}, \cdot)$

   $f(x \cdot y) = (x \cdot y)^2 = x^2 \cdot y^2 = f(x) \cdot f(y)$ Gruppenendom.

   $\operatorname{Bild} f = \mathbb{R}_{>0}$ ist UG von $(\mathbb{R}_{\neq 0}, \cdot)$

   $\operatorname{Kern} f = f^{-1}(\{1\}) = \{\pm 1\}$ ist UG von $(\mathbb{R}_{\neq 0}, \cdot)$.

Injektivität eines Gruppenhomomorphismus

Es reicht zu zeigen, dass nur e_1 auf e_2 abgebildet wird!

Lemma

Es seien $(G_1, \star)$, $(G_2, \Box)$ Gruppen mit neutralen Elementen e_1 bzw. e_2. Für einen Homomorphismus $f\colon G_1 \to G_2$ sind äquivalent:

1. f ist injektiv.
2. $\operatorname{Kern}(f) = \{e_1\}$.
3. ✓ Die einzige Lösung der Gleichung $f(a) = e_2$ ist $a = e_1$.

Beweis. $① \Rightarrow ②$: $f(e_1) = e_2$ ist klar. Da f injektiv ist, wird kein weiteres Element von G_1 auf e_2 abgebildet, d.h. $\operatorname{Kern} f = \{e_1\}$.

$② \Rightarrow ①$: Es seien $a, b \in G_1$ mit $f(a) = f(b)$. Zu zeigen: $a = b$.

$$f(a * b') = f(a) \Box f(b') = f(a) \Box f(b)'$$
$$= f(a) \Box f(a)' = e_2, \text{ also } a * b' \in \operatorname{Kern} f = \{e_1\}.$$
$$\Rightarrow a * b' = e_1, \text{ d.h. } a = b, \text{ d.h. } f \text{ ist injektiv.}$$