1.2.3 Gruppenhomomorphismen

Es sei $a > 1$ eine reelle Zahl. Der *Logarithmus von $x \in \mathbb{R}^{>0}$ zur Basis a* ist bekanntlich diejenige Zahl $y \in \mathbb{R}$, für die die Gleichung

$$a^x = y$$

gilt. Man schreibt auch $y = \log_a(x)$. Häufig verwendete beziehungsweise vorkommende Basen sind $a = e = 2.7172\dots$ (»natürlicher Logarithmus« $\ln(x)$), $a = 2$ (»dyadischer Logarithmus«) und $a = 10$ (»Zehnerlogarithmus« $\log(x)$). Die Gleichung $a^{x_1+x_2} = a^{x_1}a^{x_2}$ lässt sich mit Hilfe von Logarithmen so schreiben:

$$\log_a(x_1x_2) = \log_a(x_1) + \log_a(x_2). \quad (12)$$

Der Logarithmus »übersetzt« also die Multiplikation positiver reeller Zahlen in die einfacher durchzuführende Addition reeller Zahlen. Dieser Sachverhalt wurde zumindest teilweise bereits vor 3600 Jahren von den Babyloniern erkannt. Ab etwa 1550 wurden systematische Logarithmentabellen, in denen man den Logarithmus einer Zahl nachschlagen konnte, berechnet und publiziert. Mit ihrer Hilfe konnten Wissenschaftler und Ingenieure schneller multiplizieren, dividieren und potenzieren. Die Logarithmen bilden auch die Grundlage des »Rechenschiebers«, eines mechanischen Taschenrechners, der 1632 von William Oughtred (* 1574, † 1660) basierend auf einfacheren Grundideen erfunden wurde. Bis zur Einführung elektronischer Taschenrechner im Jahr 1969 waren Rechenschieber *das* Hilfsmittel zum Rechnen; sie verschwanden etwa um 1975 als solches von der Bühne der Geschichte, so wie mit der Erfindung des Computers generell Logarithmen ihre Bedeutung als Rechenwerkzeug verloren haben.

Die Menge der positiven reellen Zahlen bildet zusammen mit der Multiplikation eine Gruppe. Der Logarithmus ist also eine Abbildung

$$\log_a : \mathbb{R}^{>0} \rightarrow \mathbb{R},$$

die die innere Verknüpfung der Gruppe $(\mathbb{R}^{>0}, \cdot)$ in die innere Verknüpfung der Gruppe $(\mathbb{R}, +)$ übersetzt. Solche mit bestimmten inneren Verknüpfungen verträgliche Abbildungen sind in der Mathematik sehr wertvoll, da sie es ermöglichen Beziehungen zwischen zwei Halbgruppen, Monoiden oder Gruppen herzustellen. Man abstrahiert daher von der speziellen Situation der Logarithmen und erhält so die folgende Definition einer strukturverträglichen Abbildung zwischen Gruppen:

DEFINITION 52: Es seien $(G, \cdot)$ und $(H, *)$ Gruppen. Eine Abbildung $\phi : G \rightarrow H$ heißt Homomorphismus von Gruppen oder Gruppenhomomorphismus, falls sie die Eigenschaft

$$\forall g_1, g_2 \in G \quad \phi(g_1 \cdot g_2) = \phi(g_1) * \phi(g_2)$$

besitzt.

Im Folgenden wird wie in obiger Definition zunächst von der bisherigen Praxis abgewichen, innere Verknüpfungen generell mit dem Symbol $\cdot$ zu bezeichnen. Der Grund hierfür liegt darin, dass im vorliegenden Abschnitt ständig zwei, in der Regel verschiedene innere Verknüpfungen betrachtet werden. Um der Klarheit willen werden diese beiden bis auf weiteres mit den Symbolen $\cdot$ und $*$ bezeichnet.

Das Besondere oder den Wert von Homomorphismen beginnt man zu erkennen, wenn man einige elementare Eigenschaften solcher Abbildungen sammelt:

FESTSTELLUNG 53: Für einen Homomorphismus $\phi : G \rightarrow H$ von Gruppen gilt:

1. Ist $x_0 \in G$ eine Lösung der Gleichung $g_1 \cdot x = g_2$ in G , so ist $\phi(x_0)$ eine Lösung der Gleichung $\phi(g_1) * y = \phi(g_2)$ in H .
2. $\phi(1_G) = 1_H$.
3. $\forall g \in G \quad \phi(g)^{-1} = \phi(g^{-1})$.

BEWEIS: Ist $x_0 \in G$ eine Lösung der Gleichung $g_1 \cdot x = g_2$, so bedeutet das $g_1 \cdot x_0 = g_2$. Die Anwendung von ϕ auf beide Seiten dieser Gleichung liefert $\phi(g_1 \cdot x_0) = \phi(g_2)$. Nun ist aber $\phi(g_1 \cdot x_0) = \phi(g_1) * \phi(x_0)$, womit die Behauptung gilt.

Zum Beweis der zweiten Behauptung: Für einen Gruppenhomomorphismus $\phi : G \rightarrow H$ gilt

$$\phi(1_G) = \phi(1_G \cdot 1_G) = \phi(1_G) * \phi(1_G),$$

also

$$1_H = \phi(1_G) * \phi(1_G) * \phi(1_G)^{-1} = \phi(1_G).$$

Zum Beweis der dritten Behauptung wendet man ϕ jeweils auf beide Seiten der Gleichungen $g \cdot g^{-1} = 1_G$ und $g^{-1} \cdot g = 1_G$ an und erhält

$$\phi(g \cdot g^{-1}) = \phi(1_G) \text{ also } \phi(g) * \phi(g^{-1}) = 1_H,$$

und

$$\phi(g^{-1}) * \phi(g) = \phi(1_G) \text{ also } \phi(g^{-1}) * \phi(g) = 1_H.$$

□

Vor dem Hintergrund dieser Feststellung sind die Eigenschaften $\log(x^{-1}) = -\log(x)$ und $\log(1) = 0$ der Logarithmusfunktion also kein »Zufall«.

Die folgenden Beispiele zeigen wie weitverbreitet Homomorphismen in der Mathematik sind.

BEISPIEL 54 (POTENZIEREN): Die Sätze 16 und 18 zeigen, dass für eine *abelsche* Gruppe $(G, \cdot)$ das Potenzieren mit $n \in \mathbb{Z}$

$$G \rightarrow G, g \mapsto g^n$$

ein Homomorphismus ist.

BEISPIEL 55 (FUNKTIONEN DER ANALYSIS): In der Analysis treten neben den bereits erwähnten Logarithmen auch andere Funktionen auf, die Homomorphismen sind.

Die *Betragsfunktion*

$$\mathbb{K}^\times \rightarrow \mathbb{R}^{>0}, \quad x \mapsto |x|,$$

ist ein Homomorphismus von Gruppen, wobei als innere Verknüpfung von $\mathbb{R}^{>0}$ die Multiplikation gewählt wird. Denn es gilt: $|xy| = |x||y|$. Hier ist also $G = \mathbb{K} \setminus \{0\}$, $H = \mathbb{R}^{>0}$ und $\cdot$ ist die Multiplikation von rationalen, reellen beziehungsweise komplexen Zahlen, und $*$ ist die Multiplikation reeller Zahlen.

Die *Vorzeichen- oder Signumfunktion*

$$\mathbb{R}^\times \rightarrow \{-1, 1\}, \quad x \mapsto \frac{x}{|x|},$$

ist ein Homomorphismus von Gruppen. Es ist $(G, \cdot) = (\mathbb{R} \setminus \{0\}, \text{Multiplikation})$, $(H, *) = (\{-1, 1\}, \text{Multiplikation})$.

Die *Exponentialfunktion*

$$\mathbb{R} \rightarrow \mathbb{R}^{>0}, \quad x \mapsto e^x,$$

ist ein Homomorphismus von Gruppen. Hier ist im Vergleich zur Definition $(G, \cdot) = (\mathbb{R}, +)$ und $(H, *) = (\mathbb{R}^{>0}, \text{Multiplikation})$.

Die *positive n -te Wurzel*

$$\mathbb{R}^{>0} \rightarrow \mathbb{R}^{>0}, \quad x \mapsto \sqrt[n]{x},$$

ist ein Homomorphismus von Gruppen: $(G, \cdot) = (\mathbb{R}^{>0}, \text{Multiplikation}) = (H, *)$.

BEISPIEL 56: MATRIXOPERATIONEN (FORTS.) (DETERMINANTE UND SPUR): Jeder Matrix $A \in \mathbb{R}^{n \times n}$ kann man ihre Determinante $\det(A) \in \mathbb{R}$ zuordnen, eine Zahl, die man zum Beispiel mit Hilfe des Entwicklungssatzes berechnen kann. Im Fall $n = 2$ gilt die Formel

$$\det\left(\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\right) = a_{11}a_{22} - a_{12}a_{21}.$$

Für die Determinante gilt der Produktsatz

$$\det(A \cdot B) = \det(A) \det(B), \tag{13}$$

die Determinante ist also ein Monoidhomomorphismus von $(\mathbb{R}^{n \times n}, \cdot)$ nach $(\mathbb{R}, \cdot)$. Ohne Rechnung(!) folgt daher zum Beispiel die Formel

$$\det(A^{-1}) = \det(A)^{-1}$$

für eine invertierbare Matrix A – siehe die zweite Behauptung von Festlegung 53 und ihren Beweis.

Die Spur einer Matrix $A = (a_{ij}) \in \mathbb{R}^{n \times n}$ ist definiert als

$$\text{tr}(A) = \sum_{k=1}^n a_{kk}$$

Man rechnet leicht nach, dass die Spur ein Gruppenhomomorphismus von $(\mathbb{R}^{n \times n}, +)$ nach $(\mathbb{R}, +)$ ist; sie ist sogar eine lineare Abbildung.

Spur und Determinante einer Matrix sind Koeffizienten des charakteristischen Polynoms der Matrix A , das man zur Berechnung der Eigenwerte von A benutzt.

..... Hier fehlen weitere in der Vorlesung behandelte Beispiele

Um einen falschen Eindruck zu vermeiden, der angesichts dieser Beispiele entstehen könnte: Die »meisten« Abbildungen zwischen zwei Gruppen sind *keine* Homomorphismen, die Verträglichkeit mit den inneren Verknüpfungen ist eine eher selten auftretende Eigenschaft. Die Vielfalt der Beispiele zeigt vielmehr, welche Bedeutung Homomorphismen in der Mathematik haben.

SATZ 57: 1. Es seien $\phi : G_1 \rightarrow G_2$ und $\psi : G_2 \rightarrow G_3$ Gruppenhomomorphismen, dann ist auch die Verkettung $\psi \circ \phi : G_1 \rightarrow G_3$ ein Gruppenhomomorphismus.

2. Es sei $\phi : G \rightarrow H$ ein bijektiver Gruppenhomomorphismus, dann ist auch die Umkehrabbildung $\phi^{-1} : H \rightarrow G$ ein Gruppenhomomorphismus.

BEWEIS: Zu 1.: Für $g, g' \in G_1$ gilt:

$$(\psi \circ \phi)(g \cdot g') = \psi(\phi(g \cdot g')) = \psi(\phi(g) * \phi(g')) = \psi(\phi(g)) \odot \psi(\phi(g')) = (\psi \circ \phi)(g) \odot (\psi \circ \phi)(g');$$

hierbei seien $\cdot$, $*$ und $\odot$ die inneren Verknüpfungen in G_1 , G_2 und G_3 .

Zu 2.: Es seien $h, h' \in H$. Wegen der Bijektivität von ϕ gibt es eindeutig bestimmte Elemente $g_1, g_2 \in G$ mit $h_1 = \phi(g_1)$ und $h_2 = \phi(g_2)$. Es folgt

$$\phi^{-1}(h_1 * h_2) = \phi^{-1}(\phi(g_1) * \phi(g_2)) = \phi^{-1}(\phi(g_1 \cdot g_2)) = g_1 \cdot g_2.$$

□

In der folgenden Definition wird ein Begriff eingeführt, der zentral für das gesamte mathematische Teilgebiet der Algebra ist, weil man damit verschiedene mathematische Strukturen derselben Art in Beziehung setzen kann.

DEFINITION 58: Ein bijektiver Homomorphismus $\phi : G \rightarrow H$ von Gruppen heißt Gruppenisomorphismus. Man sagt dann auch G und H seien isomorph und benutzt dafür das Symbol $G \cong H$.

Sind $(G, \cdot)$ und $(H, *)$ zwei isomorphe Gruppen, und ist $\phi : G \rightarrow H$ ein Isomorphismus, so kann man jede mathematische Aussage A über $(G, \cdot)$, die sich nur mit Hilfe der inneren Verknüpfung $\cdot$ formulieren lässt, mittels ϕ in eine entsprechende Aussage B über H übersetzen. Es gilt dann: Die

Aussage A ist wahr genau dann, wenn B wahr ist. Die eingangs erwähnte Logarithmenabbildung (10-er Logarithmus)

$$\log : \mathbb{R}^{>0} \rightarrow \mathbb{R}$$

ist ein Isomorphismus von Gruppen, wobei man die positiven reellen Zahlen mit der Multiplikation und alle reelle Zahlen mit der Addition als innerer Verknüpfung betrachtet. Denn die Logarithmusfunktion besitzt die Umkehrfunktion $f(t) = 10^t$ und es gilt die Gleichung $\log(xx') = \log(x) + \log(x')$. Die Aussage

$$A : \quad \forall x \in \mathbb{R}^{>0} \exists y \in \mathbb{R}^{>0} x^5 = y$$

lässt sich mittels $\log$ übersetzen in die Aussage

$$B : \quad \forall x \in \mathbb{R} \exists y \in \mathbb{R} 5x = y.$$

Da B offensichtlich richtig ist, ist auch A richtig.

Mit der folgenden Feststellung wird klargestellt, welche Art von Beziehung ein Homomorphismus zwischen zwei Halbgruppen, Monoiden oder Gruppen herstellt.

FESTSTELLUNG 59: *Es sei $\phi : G \rightarrow H$ ein Gruppenhomomorphismus.*

1. *Ist $U \subseteq G$ eine Untergruppe, so ist auch die Bildmenge*

$$\phi(U) := \{\phi(u) : u \in U\}$$

entsprechend eine Untergruppe von H .

Insbesondere gilt dies für das Bild $\phi(G)$ der Abbildung ϕ .

2. *Ist $V \subseteq H$ eine Untergruppe von H , so ist die Urbildmenge*

$$\phi^{-1}(V) := \{g \in G : \phi(g) \in V\}$$

entsprechend eine Untergruppe von G .

Insbesondere gilt dies für den Kern

$$\text{Ker}(\phi) := \{g \in G : \phi(g) = 1_H\} = \phi^{-1}(\{1_H\})$$

der Abbildung ϕ .

BEWEIS: Zu 1.: Es sei U eine Untergruppe von $(G, \cdot)$. Es ist zu zeigen, dass die Verknüpfung $*$ von H eine innere Verknüpfung von $\phi(U)$ ist, $1_H \in \phi(U)$ und für jedes $h \in \phi(U)$ auch $h^{-1} \in \phi(U)$ gilt.

Es seien also $h_1, h_2 \in \phi(U)$. Nach Definition von $\phi(U)$ gibt es dann $u_1, u_2 \in U$ mit $h_1 = \phi(u_1)$ und $h_2 = \phi(u_2)$. Damit gilt

$$h_1 * h_2 = \phi(u_1) * \phi(u_2) = \phi(u_1 \cdot u_2) \in \phi(U),$$

da nach Voraussetzung $u_1 \cdot u_2 \in U$ gilt. Folglich ist $*$ tatsächlich eine innere Verknüpfung von $\phi(U)$.

Die Eigenschaft $\phi(1_G) = 1_H$ eines Homomorphismus liefert $1_H \in \phi(U)$.

Ist $y = \phi(u) \in \phi(U)$, so gilt $\phi(u^{-1}) * \phi(u) = \phi(u \cdot u^{-1}) = \phi(1_G) = 1_H$, folglich ist $y^{-1} = \phi(u)^{-1} = \phi(u^{-1}) \in \phi(U)$, da $u^{-1} \in U$.

Zu 2.: Es sei V eine Untergruppe von $(H, *)$ und es seien $g_1, g_2 \in \phi^{-1}(V)$. Dann gilt nach Voraussetzung über V

$$\phi(g_1 \cdot g_2) = \phi(g_1) * \phi(g_2) \in V,$$

womit $\cdot$ eine innere Verknüpfung von $\phi^{-1}(V)$ ist.

Wegen $\phi(1_G) = 1_H$ ist stets $1_G \in \phi^{-1}(V)$.

Ist $g \in \phi^{-1}(V)$, so gilt $\phi(g^{-1}) = \phi(g)^{-1} \in V$, also auch $g^{-1} \in V$. $\square$

FESTSTELLUNG 60: Für einen Homomorphismus $\phi : G \rightarrow H$ von Gruppen gilt

$$\phi(g_1) = \phi(g_2) \Leftrightarrow g_1 \cdot g_2^{-1} \in \text{Ker}(\phi).$$

Insbesondere ist ϕ injektiv genau dann, wenn $\text{Ker}(\phi) = \{1_G\}$ gilt.

BEWEIS: $\Rightarrow$: Aus $\phi(g_1) = \phi(g_2)$ folgt durch Verknüpfung mit $\phi(g_2)^{-1}$ von rechts die Gleichung $\phi(g_1) * \phi(g_2)^{-1} = 1_H$. Anwendung von Feststellung 53, Punkt 2, und die Homorphieeigenschaft liefern zusammen $\phi(g_1) * \phi(g_2)^{-1} = \phi(g_1 \cdot g_2^{-1})$, also die Behauptung $g_1 \cdot g_2^{-1} \in \text{Ker}(\phi)$.

$\Leftarrow$: Aus $g_1 \cdot g_2^{-1} \in \text{Ker}(\phi)$ folgt nach Definition, der Homorphieeigenschaft und Feststellung 53, Punkt 2

$$1_H = \phi(g_1 \cdot g_2^{-1}) = \phi(g_1) * \phi(g_2)^{-1}.$$

Verknüpfung dieser Gleichung mit $\phi(g_2)$ von rechts liefert die Behauptung.

Ist ϕ injektiv, so besitzt jedes $h \in H$ höchstens ein Urbild. Da der Kern aus den Urbildern von 1_H besteht, und weil $\phi(1_G) = 1_H$ ist, ist 1_G das einzige Element des Kerns.

Besteht umgekehrt der Kern nur aus 1_G , so folgt für aus der Gleichung $\phi(g_1) = \phi(g_2)$ nach dem bereits Bewiesenen $g_1 \cdot g_2^{-1} = 1_G$. Verknüpfung dieser Gleichung von rechts mit g_2 liefert $g_1 = g_2$ und damit die Injektivität von ϕ . $\square$

Bemerkung: Ist $\phi : G \rightarrow H$ ein injektiver Homomorphismus, so liefert die Einschränkung des Wertebereichs auf den Bildbereich automatisch einen Isomorphismus $\bar{\phi} : G \rightarrow \phi(G)$. Anders ausgedrückt: Das Bild $\phi(G)$ ist in diesem Fall isomorph zu G selbst.