4. Morphismen

Wir haben nun viele Beispiele und Konstruktionen von Gruppen gesehen. Natürlich wollen wir diese vielen verschiedenen Gruppen jetzt auch irgendwie miteinander in Beziehung setzen. In der Sprache der Mathematik bedeutet dies einfach, dass wir *Abbildungen* zwischen Gruppen betrachten müssen.

Dabei helfen uns allerdings *beliebige* Abbildungen zwischen Gruppen nicht weiter – weil sie, wenn sie nur die zugrunde liegenden Mengen aufeinander abbilden und mit den Gruppenverknüpfungen nichts weiter zu tun haben, die Gruppen eben *nicht* wirklich miteinander in Beziehung setzen. Wir benötigen also Abbildungen, die mit den Gruppenoperationen in gewissem Sinne „verträglich" sind. Dies sind die sogenannten Morphismen, die wir jetzt einführen werden. Falls ihr schon etwas Lineare Algebra kennt, ist euch diese Idee sicher auch schon von dort bekannt, wo sie zu den linearen Abbildungen führt [G, Definition 13.16].

Definition 4.1 (Morphismen von Gruppen)**.** Es seien $(G,*)$ und $(H,\circ)$ zwei Gruppen. Eine Abbildung $f\colon G \to H$ heißt ein **Morphismus** (oder **Homomorphismus** oder noch ausführlicher **Gruppenhomomorphismus**), wenn für alle $a,b \in G$

$$f(a*b) = f(a) \circ f(b)$$

gilt (man sagt auch, f ist „mit den Gruppenverknüpfungen verträglich" bzw. „vertauscht mit den Gruppenverknüpfungen").

Bemerkung 4.2. Oft werden wir die beiden Gruppenverknüpfungen zur Vereinfachung der Schreibweise nicht mit unterschiedlichen Symbolen bezeichnen und die Bedingung aus Definition 4.1 einfach als $f(a \cdot b) = f(a) \cdot f(b)$ schreiben. Dies kann normalerweise nicht zu Verwechslungen führen, da ja schon aufgrund der jeweiligen Elemente klar ist, welche Verknüpfung gemeint sein muss: a und b sind Elemente von G, $f(a)$ und $f(b)$ dagegen Elemente von H.

Beispiel 4.3.

(a) Die Abbildung $f\colon (\mathbb{Z},+) \to (\mathbb{Z},+)$, $f(n) = 2n$ ist ein Morphismus, denn für alle $m,n \in \mathbb{Z}$ gilt
$$f(m+n) = 2(m+n) = 2m+2n = f(m)+f(n).$$

(b) Die Abbildung $f\colon (\mathbb{R},+) \to (\mathbb{R},+)$, $f(x) = x+1$ ist kein Morphismus, denn es ist z. B. $f(0+0) = f(0) = 1$, aber $f(0)+f(0) = 1+1 = 2$.

(c) Für jede Gruppe G und ein festes $a \in G$ ist die Abbildung $f\colon (\mathbb{Z},+) \to G$, $f(n) = a^n$ ein Morphismus, denn für alle $m,n \in \mathbb{Z}$ gilt nach den Rechenregeln für Potenzen aus Lemma 1.12 (a)
$$f(m+n) = a^{m+n} = a^m \cdot a^n = f(m) \cdot f(n)$$
(man beachte hier die unterschiedlichen Verknüpfungen in der Start- und Zielgruppe). Die Abbildung in (a) war offensichtlich ein konkretes Beispiel dieser allgemeinen Konstruktion.

(d) Die Signumsabbildung $\operatorname{sign}\colon S_n \to (\mathbb{R}\backslash\{0\},\cdot)$ ist ein Morphismus, denn nach Satz 2.14 gilt $\operatorname{sign}(\sigma\tau) = \operatorname{sign}\sigma \cdot \operatorname{sign}\tau$ für alle $\sigma,\tau \in S_n$.

04

Wir haben oben schon gesagt, dass wir uns Morphismen als Abbildungen vorstellen sollten, die mit den Gruppenstrukturen verträglich sind. Nun hat eine Gruppe natürlich noch mehr „Struktur" als die Verknüpfung, nämlich ein neutrales sowie inverse Elemente. Wir würden erwarten, dass auch diese bei der Abbildung mit einem Morphismus erhalten bleiben. Dies ist in der Tat der Fall, wie wir im folgenden Lemma u. a. zeigen wollen.

Lemma 4.4 (Eigenschaften von Morphismen)**.** *Es sei $f\colon G \to H$ ein Morphismus von Gruppen. Dann gilt:*

(a) *$f(e) = e$ (beachte, dass e hierbei auf der linken Seite das neutrale Element von G, auf der rechten Seite das von H bezeichnet).*

(b) *Für alle $a \in G$ gilt $f(a^{-1}) = f(a)^{-1}$ (beachte, dass das Inverse auf der linken Seite das in G und auf der rechten das in H ist).*

(c) *Ist f bijektiv, so ist auch die Umkehrabbildung $f^{-1}\colon H \to G$ ein Morphismus.*

(d) *Ist $g\colon H \to K$ ein weiterer Morphismus, so ist auch die Verkettung $g \circ f\colon G \to K$ ein Morphismus.*

Beweis. Zur besseren Verständlichkeit des Beweises bezeichnen wir das neutrale Element in G mit e_G und das in H mit e_H.

(a) Da f ein Morphismus ist, gilt zunächst

$$e_H \cdot f(e_G) = f(e_G \cdot e_G) = f(e_G) \cdot f(e_G)$$

in H. Nach der Kürzungsregel aus Lemma 1.10 (c) können wir aus dieser Gleichung nun das Element $f(e_G)$ herauskürzen und erhalten wie behauptet $e_H = f(e_G)$.

(b) Für alle $a \in G$ gilt

$$\begin{aligned} f(a^{-1}) \cdot f(a) &= f(a^{-1} \cdot a) && (f \text{ ist Morphismus}) \\ &= f(e_G) \\ &= e_H && (\text{nach (a)}). \end{aligned}$$

Also ist $f(a^{-1})$ das inverse Element zu $f(a)$, d. h. es ist $f(a^{-1}) = f(a)^{-1}$.

(c) Ist f bijektiv, so wissen wir bereits, dass die Umkehrabbildung f^{-1} existiert. Es seien nun $a, b \in H$. Wir setzen $u := f^{-1}(a)$ und $v := f^{-1}(b)$, also $a = f(u)$ und $b = f(v)$. Dann gilt

$$\begin{aligned} f^{-1}(a \cdot b) &= f^{-1}(f(u) \cdot f(v)) \\ &= f^{-1}(f(u \cdot v)) && (f \text{ ist Morphismus}) \\ &= u \cdot v && (f^{-1} \text{ ist Umkehrabbildung zu } f) \\ &= f^{-1}(a) \cdot f^{-1}(b). \end{aligned}$$

Also ist auch f^{-1} ein Morphismus.

(d) Für alle $a, b \in G$ gilt

$$\begin{aligned} (g \circ f)(a \cdot b) &= g(f(a \cdot b)) \\ &= g(f(a) \cdot f(b)) && (f \text{ ist Morphismus}) \\ &= g(f(a)) \cdot g(f(b)) && (g \text{ ist Morphismus}) \\ &= (g \circ f)(a) \cdot (g \circ f)(b), \end{aligned}$$

also ist $g \circ f$ ein Morphismus. □

Aufgabe 4.5. Welche der folgenden Abbildungen sind Morphismen?

(a) $f\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{R},\ f(m,n) = 2m + 3n$;

(b) $f\colon \mathbb{Q}\backslash\{0\} \to \mathbb{Q},\ f(x) = x$;

(c) $f\colon G \to G,\ f(a) = gah$ für eine beliebige Gruppe G und gegebene $g, h \in G$.

(Die Gruppen in (a) und (b) seien dabei natürlich mit den üblichen Verknüpfungen versehen.)

Aufgabe 4.6. Es seien G und H zwei Gruppen und $f, g\colon G \to H$ Morphismen. Zeige, dass die Menge $U = \{a \in G : f(a) = g(a)\}$ eine Untergruppe von G ist.

Die Morphismuseigenschaft führt in der Praxis dazu, dass man schon mit nur sehr wenigen bekannten Werten eines Morphismus viele andere bestimmen kann. Ist z. B. $f\colon \mathbb{Z} \to G$ ein Morphismus in eine beliebige Gruppe G und kennt man den Wert $a := f(1) \in G$, so gilt damit ja z. B. auch

$$f(n) = f(1+1+\cdots+1) = f(1) \cdot f(1) \cdot \cdots \cdot f(1) = a^n$$

für alle $n \in \mathbb{N}_{>0}$. Diese Idee führt zum folgenden Lemma (das in der Linearen Algebra – falls ihr sie schon gehört habt – völlig analog zu der Aussage ist, dass eine lineare Abbildung durch ihre Werte auf einem Erzeugendensystem bereits eindeutig bestimmt ist).

Satz 4.7. *Es seien $f, g\colon G \to H$ zwei Gruppenhomomorphismen. Ist dann $M \subset G$ eine Teilmenge mit $\langle M \rangle = G$ und gilt $f|_M = g|_M$, so ist bereits $f = g$.*

Mit anderen Worten ist ein Morphismus also durch seine Werte auf Erzeugern von G bereits eindeutig bestimmt.

Beweis. Nach Aufgabe 4.6 ist die Menge $U = \{a \in G : f(a) = g(a)\}$ aller Elemente von G, auf denen f und g übereinstimmen, eine Untergruppe von G. Außerdem gilt nach Voraussetzung $M \subset U$. Aus Lemma 3.12 folgt also sofort auch $G = \langle M \rangle \subset U$, d. h. f und g stimmen auf ganz G überein. □

Beispiel 4.8. Aus Beispiel 3.13 (a) wissen wir, dass die Gruppe $\mathbb{Z}$ vom Element 1 erzeugt wird. Für jede Gruppe G ist ein Morphismus $f\colon \mathbb{Z} \to G$ also nach Satz 4.7 durch den Wert $a := f(1)$ bereits eindeutig bestimmt. Wir haben in Beispiel 4.3 (a) aber auch schon gesehen, dass die Abbildung $\mathbb{Z} \to G$, $n \mapsto a^n$ ein Morphismus (mit Wert a an der Stelle 1) ist. Also sind dies sogar schon *alle* Morphismen, die es von $\mathbb{Z}$ nach G gibt.

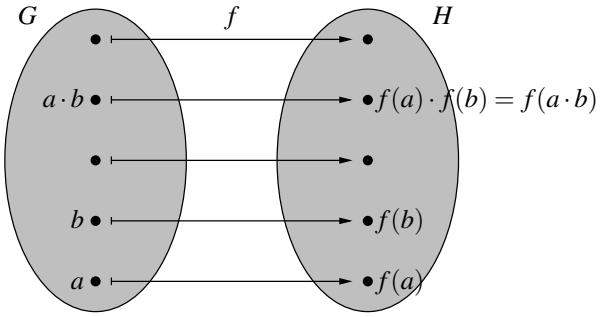
Im Folgenden wollen wir noch etwas genauer auf die bijektiven Morphismen aus Lemma 4.4 (c) eingehen. Sie haben einen besonderen Namen, und in der Tat auch eine besondere mathematische Bedeutung.

Definition 4.9 (Isomorphismen)**.** Es seien G und H zwei Gruppen.

(a) Einen bijektiven Morphismus $f\colon G \to H$ (der nach Lemma 4.4 (c) also einen Umkehrmorphismus besitzt) bezeichnet man als **Isomorphismus** (bzw. **Gruppenisomorphismus**).

(b) G und H heißen **isomorph** (in Zeichen: $G \cong H$), wenn es einen Isomorphismus $f\colon G \to H$ zwischen ihnen gibt.

Bemerkung 4.10. Sind G und H isomorph, gibt es also einen Isomorphismus $f\colon G \to H$, so bedeutet dies anschaulich, dass G und H „als Gruppen ununterscheidbar“ sind: Wir haben eine bijektive Abbildung f, mit der wir die Elemente von G mit denen von H identifizieren können, und bei Gruppenverknüpfungen, neutralen und inversen Elementen spielt es mit dieser Identifikation (nach Definition 4.1 bzw. Lemma 4.4 (a) und (b)) keine Rolle, ob wir sie in G oder H betrachten. Das folgende Bild veranschaulicht dies: Dort ist sowohl in G als auch in H z. B. die Verknüpfung der beiden unten eingezeichneten Elemente gleich dem Element, das als zweites von oben eingezeichnet ist. Wir können diese Berechnung in G durchführen und dann mit f nach H wechseln, oder erst die Elemente nach H umrechnen und sie dort verknüpfen – es kommt in jedem Fall dasselbe dabei heraus.



Wir können also sagen, dass isomorphe Gruppen „bis auf Umbenennung der Elemente gleich“ sind. In der Tat sagt man im mathematischen Sprachgebrauch auch oft, dass zwei Gruppen gleich sind, wenn sie in Wirklichkeit nur isomorph sind. Im folgenden Beispiel 4.11 (a) wird dies besonders deutlich.

Beispiel 4.11.

(a) Es seien $G = \mathbb{R}$ und

$$H = \{(x,0) : x \in \mathbb{R}\} \subset \mathbb{R} \times \mathbb{R}$$

„die Menge aller Punkte auf der x-Achse in $\mathbb{R}^2$“. Man prüft mit dem Untergruppenkriterium aus Satz 3.3 sofort nach, dass H eine Untergruppe von $\mathbb{R} \times \mathbb{R}$, also selbst eine Gruppe ist.

Wir behaupten nun, dass $G \cong H$ gilt. In der Tat ist die Abbildung

$$f\colon G \to H,\ f(x) = (x,0)$$

ein Isomorphismus: Es ist offensichtlich, dass f bijektiv ist, und wegen

$$f(x+y) = (x+y,0) = (x,0)+(y,0) = f(x)+f(y) \qquad \text{für alle } x,y \in \mathbb{R}$$

ist f auch ein Morphismus.

Nach der Interpretation aus Bemerkung 4.10 sind G und H also „bis auf Umbenennung der Elemente gleich“. Das ist hier natürlich auch sofort anschaulich klar: Wir haben uns in H lediglich entschlossen, jede reelle Zahl x etwas komplizierter als $(x,0)$ zu schreiben und damit die reelle Gerade als x-Achse in der Ebene aufzufassen – aber letztlich ändert das außer der Schreibweise der Elemente natürlich überhaupt nichts.

(b) Die Abbildung

$$f\colon \mathbb{Z} \to 2\mathbb{Z},\ f(n) = 2n$$

ist nach Beispiel 4.3 (a) ein Morphismus. Sie ist auch injektiv (denn aus $2n = 2m$ folgt $n = m$) und nach Definition von $2\mathbb{Z}$ surjektiv, also ein Isomorphismus. Wir sehen also, dass eine Gruppe (hier $\mathbb{Z}$) durchaus auch zu einer nicht-trivialen Untergruppe von sich selbst (hier $2\mathbb{Z}$) isomorph sein kann. Dies ist aber natürlich nur bei Gruppen mit unendlich vielen Elementen möglich, denn zwischen einer endlichen Gruppe und einer nicht-trivialen Teilmenge davon gibt es ja nicht einmal eine bijektive Abbildung – also erst recht keinen Isomorphismus.

(c) Wie ihr sicher aus der Schule schon wisst (und wie man in den Grundlagen der Mathematik auch exakt beweist [G, Folgerung 7.35]) bildet die Exponentialfunktion $f(x) = \mathrm{e}^x$ die Menge $\mathbb{R}$ bijektiv auf $\mathbb{R}_{>0}$ ab und erfüllt die Gleichung $\mathrm{e}^{x+y} = \mathrm{e}^x \cdot \mathrm{e}^y$ für alle $x,y \in \mathbb{R}$. Damit ist $f\colon (\mathbb{R},+) \to (\mathbb{R}_{>0},\cdot)$ ein Isomorphismus. Es können also durchaus auch Gruppen isomorph, also „praktisch ununterscheidbar“ sein, wenn ihre zugrunde liegenden Mengen und Verknüpfungen zunächst einmal recht unterschiedlich aussehen.

Da isomorphe Gruppen als „praktisch gleich“ anzusehen sind, möchte man für zwei gegebene Gruppen G und H natürlich immer gerne wissen, ob sie isomorph sind oder nicht. Eine Richtung dabei ist einfach: Wenn man wie in Beispiel 4.11 einen Isomorphismus $f\colon G \to H$ konkret angeben kann, dann sind G und H isomorph. Wie aber können wir beweisen, dass zwei gegebene Gruppen *nicht* isomorph sind? Dass uns gerade kein Isomorphismus zwischen ihnen einfällt, oder dass eine konkret gegebene Abbildung kein Isomorphismus ist, ist natürlich kein Beweis – wir müssen ja zeigen, dass es *überhaupt keinen* bijektiven Morphismus zwischen G und H geben kann.

Die Grundidee dafür ist, dass wir eine Eigenschaft finden müssen, die die eine Gruppe besitzt und die andere nicht (und die wir allein in der Sprache der Gruppentheorie formulieren können). Ist z. B. G abelsch und H nicht, so können G und H nicht isomorph sein. Für endliche Gruppen können G und H natürlich auch dann nicht isomorph sein, wenn ihre Ordnungen verschieden sind, denn dann gibt es ja nicht einmal eine bijektive Abbildung zwischen ihnen. Eine weitere oft funktionierende Möglichkeit besteht darin, die Ordnungen von Gruppenelementen im Start- und Zielraum miteinander zu vergleichen, da diese nach dem folgenden Lemma unter Isomorphismen erhalten bleiben müssen.

Lemma 4.12 (Verhalten von Ordnungen unter Morphismen)**.** *Es seien $f\colon G \to H$ ein Gruppenhomomorphismus und $a \in G$.*

(a) *Ist* $\operatorname{ord} a \neq \infty$*, so ist* $\operatorname{ord} f(a)$ *ebenfalls endlich und ein Teiler von* $\operatorname{ord} a$*.*

(b) *Ist f ein Isomorphismus, so gilt sogar* $\operatorname{ord} f(a) = \operatorname{ord} a$*.*

Beweis.

(a) Es sei $n := \operatorname{ord} a \in \mathbb{N}_{>0}$. Dann ist $a^n = e$, und damit nach der Morphismuseigenschaft und Lemma 4.4 (a) auch $f(a)^n = f(a^n) = f(e) = e$. Nach Lemma 1.15 ist $\operatorname{ord} f(a)$ damit also endlich und ein Teiler von n.

(b) Ist $\operatorname{ord} a \neq \infty$, so ist nach (a) auch $\operatorname{ord} f(a)$ endlich und ein Teiler von $\operatorname{ord} a$. Erneutes Anwenden von (a) auf das Element $f(a)$ und den Morphismus f^{-1} liefert dann aber auch, dass $\operatorname{ord} f^{-1}(f(a)) = \operatorname{ord} a$ ein Teiler von $\operatorname{ord} f(a)$ ist. Damit ist wie behauptet $\operatorname{ord} f(a) = \operatorname{ord} a$.

Analog zeigt man diese Aussage unter der Annahme, dass $\operatorname{ord} f(a) \neq \infty$. Andernfalls ist $\operatorname{ord} f(a) = \operatorname{ord} a = \infty$ und die Behauptung damit ebenfalls richtig. □

Beispiel 4.13. Nach Beispiel 1.14 gibt es in $(\mathbb{R}\backslash\{0\}, \cdot)$ ein Element der Ordnung 2 (nämlich -1), in $(\mathbb{R}, +)$ jedoch nicht. Da ein Isomorphismus zwischen diesen beiden Gruppen nach Satz 4.12 das Element -1 aber wieder auf ein Element der Ordnung 2 abbilden müsste, sind $(\mathbb{R}\backslash\{0\}, \cdot)$ und $(\mathbb{R}, +)$ also nicht isomorph.

Aufgabe 4.14. Bestimme *alle* Morphismen

(a) von $(\mathbb{Q}, +)$ nach $(\mathbb{Z}, +)$;

(b) von S_n nach $(\mathbb{R}, +)$ für $n \in \mathbb{N}_{>0}$.

Aufgabe 4.15. Sind die folgenden Gruppen isomorph?

(a) S_{n-1} und die Untergruppe $\{\sigma \in S_n : \sigma(n) = n\}$ von S_n (für ein gegebenes $n \in \mathbb{N}_{\geq 2}$);

(b) $S_2 \times S_2$ und $\langle (1\ 2\ 3\ 4) \rangle \leq S_4$;

(c) $(\mathbb{Q}, +)$ und $(\mathbb{Q}_{>0}, \cdot)$.

Nach unserer Untersuchung von Morphismen wollen wir diese jetzt als Nächstes mit den in Kapitel 3 betrachteten Untergruppen in Verbindung bringen. Die Situation ist hier eigentlich die bestmögliche: Wenn wir von Untergruppen das Bild oder Urbild unter einem Morphismus bilden, kommt stets wieder eine Untergruppe dabei heraus. Wie üblich bezeichnen wir hierbei für eine beliebige Abbildung $f\colon G \to H$

- für $U \subset G$ mit $f(U) := \{f(a) : a \in U\} \subset H$ das **Bild** von U unter f;
- für $U \subset H$ mit $f^{-1}(U) := \{a \in G : f(a) \in U\} \subset G$ das **Urbild** von U unter f.

Beachte, dass das Urbild trotz der Notation $f^{-1}(U)$ für *beliebige* (und nicht nur für bijektive) Abbildungen definiert ist: Es ist einfach die Menge aller Elemente von G, die durch f nach U abgebildet werden. Die Schreibweise soll also nicht bedeuten, dass auch wirklich eine Umkehrabbildung f^{-1} existiert.

Lemma 4.16. *Es sei $f\colon G \to H$ ein Morphismus von Gruppen. Dann gilt:*

(a) *Ist $U \leq G$, so ist $f(U) \leq H$.*

(b) *Ist $U \leq H$, so ist $f^{-1}(U) \leq G$.*

Beweis. Wir überprüfen die Untergruppenkriterien von Satz 3.3 für $f(U)$ bzw. $f^{-1}(U)$. Sie ergeben sich in beiden Fällen direkt aus den entsprechenden Kriterien für U. Zur Verdeutlichung schreiben wir das neutrale Element in G als e_G und das in H als e_H.

(a) Es sei $U \leq G$.

(U1) Es seien $a, b \in f(U)$, also $a = f(u)$, $b = f(v)$ für gewisse $u, v \in U$. Wegen (U1) für U ist dann $u \cdot v \in U$ und damit $a \cdot b = f(u) \cdot f(v) = f(u \cdot v) \in f(U)$.

(U2) Nach (U2) für U ist $e_G \in U$, also auch $e_H = f(e_G) \in f(U)$ nach Lemma 4.4 (a).

(U3) Es sei $a \in f(U)$, also $a = f(u)$ für ein $u \in U$. Dann ist $u^{-1} \in U$ nach (U3) für U, und somit auch $a^{-1} = (f(u))^{-1} = f(u^{-1}) \in f(U)$ nach Lemma 4.4 (b).

(b) Es sei nun $U \leq H$.

(U1) Es seien $a, b \in f^{-1}(U)$, also $f(a), f(b) \in U$. Dann ist auch $f(a \cdot b) = f(a) \cdot f(b) \in U$ nach (U1) für U, also $a \cdot b \in f^{-1}(U)$.

(U2) Nach (U2) für U und Lemma 4.4 (a) ist $f(e_G) = e_H \in U$. Also ist $e_G \in f^{-1}(U)$.

(U3) Es sei $a \in f^{-1}(U)$, also $f(a) \in U$. Dann ist auch $f(a^{-1}) = f(a)^{-1} \in U$ nach (U3) für U und Lemma 4.4 (b), also $a^{-1} \in f^{-1}(U)$. □

Besonders wichtig sind hierbei in der Praxis die Fälle, wenn wir für U die trivialen Untergruppen aus Beispiel 3.2 (b) einsetzen. Es ergeben sich dann die folgenden Untergruppen, die auch einen besonderen Namen haben.

Definition 4.17 (Bild und Kern eines Morphismus)**.** Es sei $f\colon G \to H$ ein Morphismus von Gruppen. Wir nennen

(a) $\operatorname{Im} f := f(G) = \{f(a) : a \in G\}$ das **Bild** von f;

(b) $\operatorname{Ker} f := f^{-1}(\{e\}) = \{a \in G : f(a) = e\}$ den **Kern** von f.

Nach Lemma 4.16 ist $\operatorname{Im} f \leq H$ und $\operatorname{Ker} f \leq G$. Die Bezeichnungen $\operatorname{Im} f$ und $\operatorname{Ker} f$ kommen übrigens von den englischen Worten *image* und *kernel*.

Aufgabe 4.18. Bestimme Bild und Kern derjenigen Abbildungen aus Aufgabe 4.5, die Morphismen sind.

Ein oft vorkommendes Beispiel für den Kern eines Morphismus ist der der Signumsabbildung $\operatorname{sign}\colon S_n \to \mathbb{R}\backslash\{0\}$ aus Beispiel 4.3 (d). Er ist die vermutlich wichtigste Untergruppe von S_n und hat deswegen eine besondere Bezeichnung:

Definition 4.19 (Alternierende Gruppen)**.** Für $n \in \mathbb{N}_{>0}$ heißt der Kern der Signumsabbildung $\operatorname{sign}\colon S_n \to \mathbb{R}\backslash\{0\}$

$$A_n := \{\sigma \in S_n : \operatorname{sign}\sigma = 1\} \quad \leq S_n$$

die **alternierende Gruppe** der Stufe n.

Beispiel 4.20. Für $n = 3$ ist nach Beispiel 2.4 (c) und Umschreiben in die Zykelschreibweise aus Konstruktion 2.10

$$\begin{aligned} S_3 &= \left\{ \left(\begin{smallmatrix}1&2&3\\1&2&3\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3\\1&3&2\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3\\2&1&3\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3\\2&3&1\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3\\3&1&2\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3\\3&2&1\end{smallmatrix}\right) \right\} \\ &= \{\mathrm{id}, (2\ 3), (1\ 2), (1\ 2\ 3), (1\ 3\ 2), (1\ 3)\}. \end{aligned}$$

Die drei Transpositionen haben dabei nach Beispiel 2.15 (a) Signum -1, die Identität und die beiden 3-Zykel Signum 1. Die zugehörige alternierende Gruppe ist also

$$A_3 = \{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\} = \langle (1\ 2\ 3) \rangle \quad \leq S_3.$$

Wir werden übrigens in Beispiel 6.19 (a) sehen, dass A_n für alle $n \geq 2$ genau halb so viele Elemente wie S_n (also $\frac{n!}{2}$) hat, d. h. dass es stets gleich viele Permutationen mit Vorzeichen 1 und -1 gibt.

Beachte, dass ein Morphismus $f\colon G \to H$ nach Definition natürlich genau dann surjektiv ist, wenn $\operatorname{Im} f = H$. Analog wollen wir jetzt zeigen, dass f genau dann injektiv ist, wenn $\operatorname{Ker} f = \{e\}$. Dies folgt nicht unmittelbar aus der Definition, ist aber ein sehr nützliches Kriterium: Für den direkten Nachweis der Injektivität müssten wir ja nachprüfen, ob das Urbild *jedes* Punktes in H höchstens ein Element besitzt. Ist f hingegen ein Morphismus, so genügt es nachzuschauen, ob das Urbild *des neutralen Elements* einelementig ist – was in der Regel einfacher nachzuprüfen ist.

Lemma 4.21 (Kriterium für Injektivität)**.** *Ein Morphismus $f\colon G \to H$ von Gruppen ist genau dann injektiv, wenn* $\operatorname{Ker} f = \{e\}$.

Beweis. Wir haben zwei Richtungen zu zeigen:

„⇒“: Es sei f injektiv. Nach Lemma 4.4 (a) ist $f(e) = e$, also $e \in \operatorname{Ker} f$. Da nun wegen der Injektivität von f kein anderes Element von G auch noch auf e abgebildet werden kann, folgt sofort $\operatorname{Ker} f = \{e\}$.

„⇐“: Es gelte nun $\operatorname{Ker} f = \{e\}$; wir müssen zeigen, dass f injektiv ist. Es seien also $a, b \in G$ mit $f(a) = f(b)$. Dann ist $f(a \cdot b^{-1}) = f(a) \cdot f(b)^{-1} = e$, d. h. es ist $a \cdot b^{-1} \in \operatorname{Ker} f$. Nach Voraussetzung folgt also $a \cdot b^{-1} = e$ und damit $a = b$. □

Aufgabe 4.22. Es sei $f\colon G \to H$ ein Gruppenhomomorphismus, zu dem ein $a \in H$ existiert, das unter f genau ein Urbild hat.

Zeige, dass f dann bereits injektiv ist.

Aufgabe 4.23. Für welche $n \geq 3$ ist die Diedergruppe D_n eine Untergruppe der alternierenden Gruppe A_n?

Aufgabe 4.24.

(a) Es sei G eine Gruppe. Für $a \in G$ definieren wir die Abbildung

$$\sigma_a\colon G \to G,\ \sigma_a(b) = a \cdot b.$$

Zeige, dass σ_a ein Element der symmetrischen Gruppe $S(G)$ ist, und dass die Abbildung

$$f\colon G \to S(G),\ f(a) = \sigma_a$$

ein injektiver Morphismus ist.

(b) Beweise, dass jede Gruppe zu einer Untergruppe einer symmetrischen Gruppe isomorph ist.

Aufgabe 4.25 (A_n wird erzeugt von 3-Zykeln)**.** Es sei $n \in \mathbb{N}_{\geq 3}$. Man zeige:

(a) Für $n > 3$ gibt es zu jedem $\sigma \in A_n$ einen 3-Zykel α und ein $\beta \in A_n$ mit $\beta(n) = n$ und $\sigma = \alpha\beta$.

(b) Ist $M \subset S_n$ die Menge aller 3-Zykel, so gilt $\langle M \rangle = A_n$.

05