Ein Gruppenkriterium basierend auf der Verknüpfungstabelle einer algebraischen Struktur

Wolfgang Windsteiger

JKU Linz, A-4040 Linz, Austria

Kurzfassung

In dieser Arbeit beschreiben wir ein einfaches Kriterium, mit dessen Hilfe entschieden werden kann, ob eine gegebene Menge mit einer dazugehörigen Verknüpfung eine Gruppe bildet oder nicht. Dieser Test bezieht sich auf die Struktur der Verknüpfungstabelle der Abbildung auf der Menge. Wir werden zeigen, dass in einer Gruppe jede Zeile und jede Spalte der Verknüpfungstabelle eine Permutation der Gruppenelemente sein muss.

1 Einleitung

Als *algebraische Struktur* bezeichnen wir eine Menge mit einer auf dieser Menge definierten Abbildung. Wir können nun verschiedenste Eigenschaften solcher algebraischen Strukturen untersuchen, z.B. die Assoziativität, die Existenz eines neutralen Elements oder die Invertierbarkeit der Elemente der Menge. Auf diese Weise gelangen wir zu einer Kategorisierung dieser Strukturen in z.B. Halbgruppen, Monoide oder Gruppen. Dieser Abstraktionsschritt ist von enormer Bedeutung in der Mathematik, da sich die Untersuchung konkreter algebraischer Strukturen in vielen Fällen wesentlich vereinfacht, sobald uns bekannt ist, in welche Kategorie die zu untersuchende Struktur fällt.

Weiters können wir oft abstrakt Algorithmen definieren, die nicht nur in *einer konkreten algebraischen Struktur* sondern viel allgemeiner in *allen algebraischen Strukturen einer bestimmten Kategorie* angwendet werden können. So können wir beispielsweise einen allgemeinen Gleichungslösungsalgorithmus für Gruppen entwickeln, siehe [AlgMeth04, Kapitel 1], und wir können dieses Verfahren *auf alle Gleichungen* anwenden, deren linke und rechte Seite durch Verknüpfung von Elementen einer beliebigen Gruppe gebildet sind. Konkret läßt sich das Verfahren dann zum Beispiel sowohl für Gleichungen über $\mathbb{R}$ mit Addition als auch für Gleichungen über $\mathbb{Z}_7$ mit Multiplikation anwenden.

Das Überprüfen, ob eine konkret gegebene algebraische Struktur die Eigenschaften einer Gruppe erfüllt, kann sehr aufwändig sein. Im Normalfall müssen alle notwendigen Gruppeneigenschaften für die konkrete Struktur anhand der Definitionen *bewiesen* werden. Im Falle von endlichen algebraischen Strukturen kann das gesamte Verhalten der Verknüpfung auf der Menge durch die sogenannte Verknüpfungstabelle der Struktur veranschaulicht werden bzw. kann die Verknüpfung durch Auflisten der endlich vielen Einträge der Verknüpfungstabelle vollständig definiert werden. Wir werden ein einfaches Kriterium kennenlernen, das anhand der Verknüpfungstabelle

Aufschluss darüber gibt, ob es sich bei der in der Tabelle dargestellten algebraischen Struktur um eine Gruppe handeln kann. Jede Zeile und auch jede Spalte der Verknüpfungstabelle einer Gruppe enthält nämlich eine *Permutation der Gruppenelemente*. Im Falle endlicher Gruppen läßt sich dieses Resultat auch anschaulich interpretieren: In jeder Zeile und jeder Spalte der Verknüpfungstabelle muss jedes Gruppenelement genau einmal vorkommen. Es handelt sich dabei also um ein Kriterium, das alleine "durch Anschauen der Verknüpfungstabelle" überprüft werden kann!

Dieses Resultat ist keineswegs neu, es kann in den meisten Textbüchern zur Algebra bzw. Gruppentheorie nachgelesen werden, siehe etwa [Alg60, Grup67]. Das Hauptaugenmerk in dieser Arbeit liegt darauf, alle benötigten Begriffe sauber in der Sprache der Prädikatenlogik zu definieren und dann—aufbauend auf diesen Definitionen—einen exakten Beweis, wie in [Log05] gezeigt zu führen. Entscheidend ist dabei, die Definitionen so zu wählen, dass sie sowohl die intuitive Bedeutung der Begriffe richtig fassen als auch einen formal korrekten einfachen Beweis erlauben. Diese Arbeit soll gleichzeitig die Wichtigkeit einer formal exakten Logik hinter der Mathematik und auch die entsprechende Präsentation mathematischer Inhalte veranschaulichen. Daher wird vor allem in Abschnitt 3 auch die logische Struktur von Definitionen und Sätzen in der Prädikatenlogik in allen Details gezeigt und es wird versucht zu veranschaulichen, wie sich diese Struktur in einer korrekten und ansprechenden Präsentation widerspiegelt.

Nach einem Beispiel für die betrachtete Problemstellung n Abschnitt 2 werden in Abschnitt 3 die mathematischen Grundlagen definiert. Der eigentliche Hauptsatz für endliche Gruppen und dessen Beweis finden sich in Abschnitt 4. Abschnitt 5 und 6 zeigen mögliche Anwendungen des Satzes und eine einfache Verallgemeinerung auf unendliche Gruppen.

2 Zwei konkrete Beispiele für algebraische Strukturen

Wir betrachten nun zwei konkrete Beispiele algebraischer Strukturen und deren Eigenschaften. Wir untersuchen

- die Menge der Restklassen modulo 6 mit der darauf definierten Multiplikation

  $[a]_6 * [b]_6 = [\,\mathrm{Mod}[a * b,\, 6]\,]_6$ bzw.

- die Menge $\{u, v, w\}$ mit einer laut folgender Tabelle definierten abstrakten Verknüpfung $\diamond$

$\diamond$	u	v	w
u	w	v	u
v	u	w	v
w	v	u	w

und fragen uns, ob diese algebraischen Strukturen die Eigenschaften einer Gruppe erfüllen, d.h. die Verknüpfungen müssen assoziativ sein, in jeder Menge muss ein bzgl. der Verknüpfung neutrales Element existieren und jedes Element der Menge muss bzgl. der Verknüpfung invertierbar sein.

3 Notwendige mathematische Begriffe

In diesem Abschnitt werden wir alle benötigten mathematischen Begriffe einführen. Als Ausgangsbasis wählen wir dazu die Sprache der Prädikatenlogik bereichert durch einige wenige elementare Begriffe aus der Mengenlehre.

3.1 Verknüpfung auf einer Menge

Definition 1 (Verknüpfung auf einer Mange)

Eine Funktion $\circ$ ist eine *Verknüpfung auf* einer Menge A genau dann wenn für alle $a, b \in A$ gilt: $a \circ b \in A$.

□

Es handelt sich bei dieser Definition um eine *explizite Definition eines Prädikatensymbols* der Form

$$\text{ist-Verknüpfung}[\circ, A] :\Leftrightarrow \underset{a,b \in A}{\forall} \circ[a, b] \in A .$$

Dabei ist "$\circ$" als 2-stelliges Funktionssymbol verwendet. Wir können für dieses Funktionssymbol eine Infix-Notation mit "$\circ$" als Infix-Operator vereinbaren und schreiben ab nun $\circ[a, b]$ als $a \circ b$.

3.2 Assoziativität einer Verknüpfung auf einer Menge

Definition 2 (Assoziativität)

Eine Verknüpfung $\circ$ heißt *assoziativ auf* einer Menge A gdw. für alle $a, b, c \in A$ gilt: $a \circ (b \circ c) = (a \circ b) \circ c$.

□

Es handelt sich bei dieser Definition um eine *explizite Definition eines Prädikatensymbols* der Form

$$\text{assoziativ}[\circ, A] :\Leftrightarrow \underset{a,b,c \in A}{\forall} a \circ (b \circ c) = (a \circ b) \circ c .$$

3.3 Existenz eines neutralen Elements

Definition 3 (Monoid)

Eine Menge A mit einer Verknüpfung $\circ$ heißt *Monoid* $:\Leftrightarrow \underset{n \in A}{\exists} \underset{a \in A}{\forall} a \circ n = a \wedge n \circ a = a$.

□

Vergleiche diese Definition nun mit den Definitionen 1 und 2 oben: Wir zeigen hier einen etwas anderen Stil, wir verwenden "$:\Leftrightarrow$" anstelle von "genau dann wenn" bzw. "gdw." und wir verwenden die logischen Quantoren anstelle von deutschen Formulierungen "für alle" und "es gibt ein". Es ist Geschmackssache, wichtig ist, dass innerhalb einer Arbeit ein einheitlicher Stil verwendet wird (diese Arbeit ist in dieser Hinsicht *kein* Musterbeispiel, es geht uns darum, die verschiedenen möglichen Stile aufzuzeigen!). In reiner Prädikatenlogik geschrieben lautet die Definition wie folgt:

$$\text{ist-Monoid}[\circ, A] :\Leftrightarrow \underset{n \in A}{\exists} \underset{a \in A}{\forall} a \circ n = a \wedge n \circ a = a .$$

In einem Monoid existiert also ein sogenanntes *neutrales Element*, welches jedes Objekt beim Verknüpfen unverändert läßt. Es läßt sich leicht beweisen, dass in einem Monoid das neutrale Element sogar eindeutig bestimmt ist.

Satz 4

Sei A mit $\circ$ ein Monoid. Dann gilt: $\underset{n \in A}{\exists !} \underset{a \in A}{\forall} a \circ n = a \wedge n \circ a = a$.

In der Formulierung von mathematischen Sätzen ist die Formulierung "Sei … sodass … . Dann gilt …" sehr gebräuchlich. Es ist wichtig zu sehen, dass sich dahinter ein *Allquantor mit einer Bedin-*

gung and die gebundene(n) Variable(n) versteckt. Die prädikatenlogische Struktur der Aussage in Satz 4 lautet nun:

$$\underset{\substack{\circ,A\\ \text{ist-Monoid}[\circ,A]}}{\forall}\ \exists!\ \underset{a\in A}{\forall}\ a\circ n = a \wedge n\circ a = a\ .$$

Beweis: Sei $\circ$ und A beliebig aber fix mit ist-Monoid$[\circ, A]$. Zu zeigen ist dann

$$\exists!\ \underset{a\in A}{\forall}\ a\circ n = a \wedge n\circ a = a\ .$$

Wir verwenden nun $\varphi[n]$ als Abkürzung für $\underset{a\in A}{\forall}\ a\circ n = a \wedge n\circ a = a$. Es ist also zu beweisen

$$\underbrace{\left(\underset{n\in A}{\exists}\ \varphi[n]\right)}_{(+)} \bigwedge \underbrace{\left(\underset{n_1,n_2\in A}{\forall}\ (\varphi[n_1]\wedge\varphi[n_2]) \Rightarrow n_1 = n_2\right)}_{(++)}.$$

Beweis von (+): Aus der Annahme ist-Monoid$[\circ, A]$ folgt mit Definition 3 direkt (+).

Beweis von (++): Wir wählen $n_1, n_2 \in A$ b.a.f. mit $\varphi[n_1]\wedge\varphi[n_2]$. Wir können also sowohl $\varphi[n_1]$ als auch $\varphi[n_2]$ als bekannt annehmen, d.h.

$$\underset{a\in A}{\forall}\ a\circ n_1 = a \wedge n_1\circ a = a \quad \text{und} \tag{1}$$

$$\underset{a\in A}{\forall}\ a\circ n_2 = a \wedge n_2\circ a = a\ . \tag{2}$$

Zu zeigen bleibt $n_1 = n_2$. Nun gilt aber

$$n_1 \underset{(\#)}{=} n_1\circ n_2 \underset{(\#\#)}{=} n_2\ .$$

Zu (#): Durch Instanzieren von (2) erhalten wir $n_1\circ n_2 = n_1 \wedge n_2\circ n_1 = n_1$ und aus Ersterem $n_1 = n_1\circ n_2$.
Zu (##): Durch Instanzieren von (1) erhalten wir $n_2\circ n_1 = n_2 \wedge n_1\circ n_2 = n_2$ und aus Zweiterem $n_1\circ n_2 = n_2$.

□

Die eindeutige Existenz eines neutralen Elements in einem Monoid gibt Anlass zu einer impliziten Definition *des neutralen Elements bezüglich einer Verknüpfung in einer Menge*.

Definition 5 (neutrales Element) Sei A mit $\circ$ ein Monoid. Dann definieren wir:

$$\text{Neut}[\circ, A] := \underset{n\in A}{\ni!}\ \underset{a\in A}{\forall}\ a\circ n = a \wedge n\circ a = a\ .$$

□

Als Wissen über Neut haben wir neben Satz 4 auch zur Verfügung, siehe [Log05]:

$$\underset{\substack{\circ,A\\ \text{ist-Monoid}[\circ,A]}}{\forall}\ \underset{n\in A}{\forall}\ \text{Neut}[\circ, A] = n \Leftrightarrow \underset{a\in A}{\forall}\ a\circ n = a \wedge n\circ a = a\ .$$

und dazu äquivalent

$$\underset{\substack{\circ,A\\ \text{ist-Monoid}[\circ,A]}}{\forall}\ \underset{a\in A}{\forall}\ a\circ\text{Neut}[\circ, A] = a \wedge \text{Neut}[\circ, A]\circ a = a\ . \tag{3}$$

Die weiteren Definitionen und Sätze in dieser Arbeit werden wir nur mehr in ihrer prädikatenlogischen Form angeben. Es bleibt dem Leser überlassen, diese Definitionen in eine ansprechende Präsentationsform zu übersetzen.

3.4 Invertierbarkeit

Definition 6 (invertierbar)

$$\text{alle-invertierbar}[\circ, A] :\Leftrightarrow \underset{a\in A}{\forall}\ \underset{b\in A}{\exists}\ a\circ b = \text{Neut}[\circ, A] \wedge b\circ a = \text{Neut}[\circ, A]$$

□

Ähnlich den Betrachtungen im vorangegangenen Abschnitt läßt sich beweisen, dass in einem Monoid, in dem alle Elemente invertierbar sind, zu jedem Element das sogenannte "inverse Element" sogar eindeutig bestimmt ist.

Satz 7

$$\underset{\substack{\circ,A\\ \text{ist-Monoid}[\circ,A]\wedge\ \text{alle-invertierbar}[\circ,A]}}{\forall}\ \underset{a\in A}{\forall}\ \underset{b\in A}{\exists !}\ a\circ b = \text{Neut}[\circ, A] \wedge b\circ a = \text{Neut}[\circ, A]\ .$$

Beweis: Sei $\circ$ und A beliebig aber fix mit ist-Monoid$[\circ, A]$ und alle-invertierbar$[\circ, A]$. Sei weiters $a \in A$ b.a.f. Zu zeigen ist dann:

$$\underset{b\in A}{\exists !}\ a\circ b = \text{Neut}[\circ, A] \wedge b\circ a = \text{Neut}[\circ, A]\ .$$

Wir verwenden nun $\varphi[b]$ als Abkürzung für $a\circ b = \text{Neut}[\circ, A] \wedge b\circ a = \text{Neut}[\circ, A]$. Es ist also zu beweisen

$$\underbrace{\left(\underset{b\in A}{\exists}\ \varphi[b]\right)}_{(+)} \bigwedge \underbrace{\left(\underset{b_1,b_2\in A}{\forall}\ (\varphi[b_1]\wedge\varphi[b_2]) \Rightarrow b_1 = b_2\right)}_{(++)}.$$

Beweis von (+): Durch Instanzieren der Annahme alle-invertierbar$[\circ, A]$ für die Konstante (!) a erhalten wir genau (+). Beachte, dass wir oben $a \in A$ beliebig aber fix gewählt haben, und somit a an dieser Stelle *nichts mehr* mit dem Symbol a in $\underset{a\in A}{\forall}$ … in Definition 6 zu tun hat.

Beweis von (++): Wir wählen $b_1, b_2 \in A$ b.a.f. mit $\varphi[b_1]\wedge\varphi[b_2]$, d.h. wir wissen

$$a\circ b_1 = \text{Neut}[\circ, A] \wedge b_1\circ a = \text{Neut}[\circ, A] \quad \text{und} \tag{4}$$

$$a\circ b_2 = \text{Neut}[\circ, A] \wedge b_2\circ a = \text{Neut}[\circ, A]\ . \tag{5}$$

Zu zeigen ist $b_1 = b_2$. Nun gilt aber

$$b_1 \underset{\uparrow (3)}{=} b_1\circ\text{Neut}[\circ, A] \underset{\uparrow (5)}{=} b_1\circ a\circ b_2 \underset{\uparrow (4)}{=} \text{Neut}[\circ, A]\circ b_2 \underset{\uparrow (3)}{=} b_2\ .$$

□

Somit können wir zu jedem Element *ein inverses Element bezüglich einer Verknüpfung in einer Menge* implizit definieren.

Definition 8 (neutrales Element) Wenn gilt ist-Monoid$[\circ, A]$ und alle-invertierbar$[\circ, A]$. Dann definieren wir für $a \in A$:

$$\text{Inv}[a, \circ, A] := \underset{b\in A}{\ni !}\ a\circ b = \text{Neut}[\circ, A] \wedge b\circ a = \text{Neut}[\circ, A]\ .$$

□

Als Wissen über Inv haben wir neben der eindeutigen Existenz in Satz 7 auch zur Verfügung, siehe [Log05]:

$$\underset{\substack{\circ,A\\ \text{ist-Monoid}[\circ,A]\wedge\ \text{alle-invertierbar}[\circ,A]}}{\forall}\ \underset{a,b\in A}{\forall}\ \text{Inv}[a, \circ, A] = b \Leftrightarrow a\circ b = \text{Neut}[\circ, A] \wedge b\circ a = \text{Neut}[\circ, A]\ .$$

bzw.

$$\underset{\substack{\circ,A \\ \text{ist-Monoid}[\circ,A]\wedge\,\text{alle-invertierbar}[\circ,A]}}{\forall} \; \underset{a\in A}{\forall}\; \text{Inv}[a,\circ,A]\in A \bigwedge\; a\circ\text{Inv}[a,\circ,A] = \text{Neut}[\circ,A] \wedge \text{Inv}[a,\circ,A]\circ a = \text{Neut}[\circ,A]\ . \tag{6}$$

3.5 Gruppe

Definition 9 (Gruppe)

ist-Gruppe$[\circ, A] :\Leftrightarrow$ ist-Verknüpfung$[\circ, A] \wedge$
assoziativ$[\circ, A] \wedge$ ist-Monoid$[\circ, A] \wedge$ alle-invertierbar$[\circ, A]$

ist-endliche-Gruppe$[\circ, A] :\Leftrightarrow$ ist-Gruppe$[\circ, A] \wedge$ ist-endlich$[A]$

□

3.6 Zeilen und Spalten einer Verknüpfungstabelle

Im Falle einer Verknüpfung $\circ$ auf einer endlichen Menge A können wir die Verknüpfung $\circ$ auf A vollständig charakterisieren, indem wir für alle $a, b \in A$ das Resultat $a\circ b$ angeben. So ist beispielsweise die Multiplikation auf den Restklassen modulo 6 vollständig bestimmt durch

$$\begin{aligned}\{&0*0\to 0,\ 0*1\to 0,\ 0*2\to 0,\ 0*3\to 0,\ 0*4\to 0,\ 0*5\to 0,\ 1*0\to 0,\ 1*1\to 1,\ 1*2\to 2,\\ &1*3\to 3,\ 1*4\to 4,\ 1*5\to 5,\ 2*0\to 0,\ 2*1\to 2,\ 2*2\to 4,\ 2*3\to 0,\ 2*4\to 2,\ 2*5\to 4,\\ &3*0\to 0,\ 3*1\to 3,\ 3*2\to 0,\ 3*3\to 3,\ 3*4\to 0,\ 3*5\to 3,\ 4*0\to 0,\ 4*1\to 4,\ 4*2\to 2,\\ &4*3\to 0,\ 4*4\to 4,\ 4*5\to 2,\ 5*0\to 0,\ 5*1\to 5,\ 5*2\to 4,\ 5*3\to 3,\ 5*4\to 2,\ 5*5\to 1\}\,.\end{aligned}$$

Als Darstellung dieser endlich vielen Zuordnungen bietet sich *eine Tabelle* an, deren Anzahl von Zeilen bzw. Spalten genau der Mächtigkeit von A entspricht. Jede Zeile bzw. Spalte in dieser Tabelle ist einem Element aus A zugeordnet. Der Eintrag in der Tabelle in der zu a gehörigen Zeile und der zu b gehörigen Spalte soll genau $a\circ b$ sein. Diese Tabelle nennen wir die Verknüpfungstabelle von $\circ$ auf A. Im obigen Beispiel würde die Verknüpfungstabelle wie folgt aussehen:

	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Umgekehrt brauchen wir im Fall einer endlichen Menge A keine Abbildungsvorschrift für $\circ$ verlangen. Es reicht aus, wenn wir für alle $a, b \in A$ das Resultat $a\circ b$ in irgendeiner Form "ablesen" können, z.B. aus der Verknüpfungstabelle. Wir betrachten die Verknüpfungstabelle aus Kapitel 2

$\diamond$	u	$\boldsymbol{v}$	w
u	w	v	u
v	u	w	v
$\boldsymbol{w}$	v	$\boldsymbol{u}$	w

und können daraus etwa ablesen: $w \diamond v = u$.

Die Verknüpfungstabelle von $\circ$ auf A ist also nichts anderes als eine *Darstellungsform* der Funktion $\circ$ auf der (endlichen) Menge A. Zeilen und Spalten der Verknüpfungstabelle erhalten wir, indem jeweils ein Argument der Funktion fixiert wird. Wir sehen also, dass sich *Funktionen* gut dafür eignen, die Begriffe "Verknüpfungstabelle", "Zeile einer Verknüpfungstabelle" und "Spalte einer Verknüpfungstabelle" zu beschreiben.

Definition 10 (Verknüpfungstabelle, Zeile, Spalte) Sei $\circ$ eine Verknüpfung auf A und $a, b \in A$.

$$\mathcal{T}[\circ, A][a, b] := a \circ b$$

$$\mathcal{Z}[a, \circ, A][b] := \mathcal{T}[\circ, A][a, b]$$

$$\mathcal{S}[b, \circ, A][a] := \mathcal{T}[\circ, A][a, b]$$

□

$\mathcal{T}$ ist eine Funktion, die von den Parametern $\circ$ und A abhängt. Für jedes $\circ$ und A ist $\mathcal{T}[\circ, A]$ selbst wieder eine Funktion, die jedem a und b den Wert $a \circ b$ zuordnet. Analog dazu sind $\mathcal{Z}$ und $\mathcal{S}$ au interpretieren. Als Schreibweise bieten sich $\mathcal{T}_{\circ,A}$, $\mathcal{Z}_{a,\circ,A}$ und $\mathcal{S}_{a,\circ,A}$ an. Beachte auch hier wieder: Die Index-Schreibweise dient als Abkürzung für eine Funktionsanwendung! Vergleiche dazu die Schreibweise f_n für "das n−te Element einer Folge" als Abkürzung für $f[n]$.

3.7 Permutationen

Die Intuition hinter dem Begriff "Permutation" soll die "Vertauschung der Reihenfolge" sein. In anderen Bereichen der Mathematik finden wir im Zusammenhang mit Permutationen den Begriff der *bijektiven Funktion*. Es zeigt sich, dass wir diesen Permutationsbegriff direkt auf Zeilen und Spalten der Verknüpfungstabelle übertragen können.

Definition 11 (Permutation)

$$\text{ist-Permutation}[f, A] :\Leftrightarrow f : A \xrightarrow{\text{bij.}} A \ .$$

□

Dabei steht $f : A \xrightarrow{\text{bij.}} A$ für "f ist eine bijektive Funktion von A nach A", und wir setzen den Begriff einer bijektiven Funktion als bekannt voraus.

3.8 Alternative Definitionen

Als Alternative zur Definition als Funktion könnten wir Zeilen und Spalten der Verknüpfungstafel auch als Mengen definieren, z.B.

$$\mathcal{Z}[a, \circ, A] := \left\{ a \circ b \mid \underset{b}{} \ b \in A \right\} .$$

Dagegen spricht prinzipiell nichts, außer dass dieser Begriff wahrscheinlich nicht mehr genau das beschreibt, was der Intuition einer Zeile entspricht. Die Darstellung der Verknüpfung in Tabellenform vermittelt ja *eine Reihenfolge* der Elemente der Menge und somit auch eine Reihenfolge der Elemente in einer Zeile bzw. einer Spalte. Repräsentieren wir die Zeilen nun als Mengen, so geht die Information über die Reihenfolge der Elemente verloren, was etwa in obigem Beispiel dazu führt, dass gilt:

$$\mathcal{Z}[v, \diamond, \{u, v, w\}] = \{u, w, v\} \text{ und auch } \mathcal{Z}[w, \diamond, \{u, v, w\}] = \{v, u, w\} .$$

Da aber $\{u, w, v\} = \{v, u, w\}$ gilt, würde auch gelten $\mathcal{Z}[v, \diamond, \{u, v, w\}] = \mathcal{Z}[w, \diamond, \{u, v, w\}]$, das heißt, wir würden die beiden Zeilen als identisch betrachten, was eben *intuitiv* nicht passend ist. Entscheidend ist aber, dass die Definition als Menge deswegen nicht *falsch* ist, sie modelliert nur nicht das, was wir modellieren wollten!

Information über die Reihenfolge können wir auch dadurch in den Begriff bringen, dass wir anstelle der Menge ein *Tupel* verwenden, also

$$\mathcal{Z}[a, \circ, A] := \left\langle a \circ b \mid \underset{b}{} b \in A \right\rangle .$$

Tupel unterscheiden sich von Mengen im wesentlichen dadurch, dass die Reihenfolge der Elemente eine Rolle spielt. Ein Tupel hat—im Gegensatz zu einer Menge!—ein erstes, zweites, etc. Element. Hinter Tupel verstecken sich aber letzendlich auch wieder "nur" Funktionen, wir sind also im Wesentlichen wieder bei einer Darstellung als Funktion angelangt. Eine weitere Alternative wäre die Definition als *Menge von Paaren*, um die Zuordnung zwischen den Elementen abzubilden. Wir können etwa die zu a gehörige Zeile definieren als

$$\mathcal{Z}[a, \circ, A] := \left\{ \langle b, a \circ b \rangle \mid \underset{b}{} b \in A \right\} .$$

Auch hier haben wir aber nichts Neues, da eine Menge von Paaren wieder als Funktion betrachtet werden kann (sofern sie gewisse Eigenschaften aufweist, die in diesem Fall erfüllt sind).

Abhängig davon, wie wir Zeilen und Spalten definieren, muss natürlich auch der Begriff der Permutation entsprechend angepasst werden. Zwei voneinander verschiedene Permutationen einer Menge sollen sich also nur in der Reihenfolge der Aufzählung der Elemente der Menge unterscheiden. Als Darstellung einer Permutation eignen sich Mengen deshalb nicht, da Mengen keine Reihenfolge der enthaltenen Elemente berücksichtigen. Würden wir beispielsweise eine Permutation einer Menge A definieren als "eine Menge, die die gleichen Elemente enthält wie A und auch insgesamt gleich viele Elemente hat wie A", dann würde eine Menge immer *identisch* mit all ihren Permutationen sein und wir könnten nicht einmal von "2 voneinander verschiedenen Permutationen" sprechen! Betrachten wir hingegen wie oben eine Permutation einer Menge als eine Funktion auf der Menge, so können wir das bestehende Konzept einer bijektiven Funktion wiederverwenden. Dies ist ein weiterer Vorteil, wenn Zeilen und Spalten der Verknüpfungstafel als Funktionen betrachtet werden: Wir müssen den Begriff der Permutation nicht neu erfinden!

4 Ein einfaches Gruppenkriterium

In einer endlichen Gruppe ist jede Zeile und jede Spalte der Verknüpfungstabelle eine Permutation der Gruppenelemente.

Satz 12

$$\underset{\substack{\circ, A \\ \text{ist-endliche-Gruppe}[\circ, A]}}{\forall} \quad \underset{a \in A}{\forall} \text{ ist-Permutation}[\mathcal{Z}_{a,\circ,A}, A] \bigwedge \text{ist-Permutation}[\mathcal{S}_{a,\circ,A}, A]$$

Beweis: Seien $\circ$ und A b.a.f. mit ist-endliche-Gruppe$[\circ, A]$ und sei $a \in A$ b.a.f.
Zu zeigen bleibt: ist-Permutation$[\mathcal{Z}_{a,\circ,A}, A] \bigwedge$ ist-Permutation$[\mathcal{S}_{a,\circ,A}, A]$. Wir zeigen zuerst ist-Permutation$[\mathcal{Z}_{a,\circ,A}, A]$.
Laut Definition 11 ist daher zu zeigen $\mathcal{Z}_{a,\circ,A} : A \xrightarrow{\text{bij.}} A$, was lt. Definition von Bijektivität heißt, es ist zu zeigen

$$\mathcal{Z}_{a,\circ,A} : A \xrightarrow{\text{inj.}} A \bigwedge \mathcal{Z}_{a,\circ,A} : A \xrightarrow{\text{surj.}} A .$$

Wir zeigen zuerst: $\mathcal{Z}_{a,\circ,A} : A \xrightarrow{\text{inj.}} A$, d.h.

$$\underset{b_1, b_2 \in A}{\forall} \mathcal{Z}_{a,\circ,A}[b_1] = \mathcal{Z}_{a,\circ,A}[b_2] \Rightarrow b_1 = b_2 .$$

Seien $b_1, b_2 \in A$ b.a.f. und sei

$$\mathcal{Z}_{a,\circ,A}[b_1] = \mathcal{Z}_{a,\circ,A}[b_2]\,, \tag{7}$$

zu beweisen bleibt $b_1 = b_2$. Wegen (7) wissen wir lt. Definition der Zeile

$$a \circ b_1 = a \circ b_2 \tag{8}$$

und daher wegen der Kürzungsregel in Gruppen (weil $a, b_1, b_2 \in A$ und ist-endliche-Gruppe$[\circ, A]$) auch

$$b_1 = b_2\,.$$

Nun bleibt noch zu zeigen: $\mathcal{Z}_{a,\circ,A} : A \xrightarrow{\text{surj.}} A$, d.h.

$$\underset{c\in A}{\forall}\ \underset{b\in A}{\exists}\ \mathcal{Z}_{a,\circ,A}[b] = c\,.$$

Sei $c \in A$ b.a.f. Wir müssen nun ein $b^* \in A$ so bestimmen können, dass

$$\mathcal{Z}_{a,\circ,A}[b^*] = a \circ b^* = c\,. \tag{9}$$

Sei nun $b^* := \text{Inv}[a, \circ, A] \circ c$. Dann ist wegen (6) $\text{Inv}[a, \circ, A] \in A$ und daher $b^* \in A$. Weiters gilt:

$$a \circ b^* = a \circ \text{Inv}[a, \circ, A] \circ c \underset{\uparrow (6)}{=} \text{Neut}[\circ, A] \circ c \underset{\uparrow (3)}{=} c\,.$$

Somit ist $a \circ b^* = c$ und damit ist (9) bewiesen.

Weiters ist zu zeigen: ist-Permutation$[\mathcal{S}_{a,\circ,A}, A]$. Dieser Beweis verläuft analog.

□

Anschaulich ist eine Zeile oder Spalte der Verknüpfungstabelle von $\circ$ auf A eine Permutation von A, wenn darin jedes Element von A *genau einmal* vorkommt.

5 Konkrete Anwendung des Kriteriums

Zur Entscheidung, ob eine gegebene Verknüpfung auf einer gegebenen Menge die Eigenschaft einer Gruppe erfüllt, müssen wir üblicherweise nach Definition (9) *beweisen*, dass die 4 charakteristischen Eigenschaften einer Gruppe erfüllt sind. Im Fall endlicher Gruppen sind diese Beweise nie schwer, weil sie letztendlich auf das Testen *endlich vieler Möglichkeiten* reduziert werden können. Ist auch nur eine Bedingung nicht erfüllt, so kann es sich bei der betrachteten algebraischen Struktur nicht um eine Gruppe handeln. Wir betrachten nun nochmals die zwei Beispiele aus Abschnitt 2.

- Die Menge der Restklassen modulo 6 mit der darauf definierten Multiplikation bildet *keine Gruppe*, da beispielsweise in der Zeile zu 0 oder auch in der Zeile zu 2 gehörig *nicht jede Restklasse* genau einmal vorkommt, siehe Abschnitt 3.
- Hat die Verknüpfungstabelle die Eigenschaft, dass jede Zeile und jede Spalte eine Permutation der Gruppenelemente ist, so folgt daraus *nicht zwingend*, dass diese algebraische Struktur eine Gruppe ist! Ein Gegenbeispiel liefert die wie in Abschnitt 2 definierte abstrakten Verknüpfung $\diamond$

$\diamond$	u	v	w
u	w	v	u
v	u	w	v
w	v	u	w

auf der Menge $\{u, v, w\}$. Diese algebraische Struktur bildet kein Monoid, denn wie einfaches Nachrechnen zeigt, kann weder u noch w noch v neutrales Element bzgl. $\diamond$ auf $\{u, v, w\}$ sein.

6 Verallgemeinerung des Kriteriums

Betrachten wir nun nochmals den Beweis zu Satz 12. Es fällt auf, dass wir die Eigenschaft der Endlichkeit der Gruppe im Beweis nicht verwenden. Das heißt aber, dass wir diese Bedingung auch in der Formulierung des Satzes nicht brauchen. Wir können also den Satz auf unendliche Gruppen verallgemeinern.

Satz 13

$$\forall_{\substack{\circ,A \\ \text{ist-Gruppe}[\circ,A]}} \; \forall_{a \in A} \; \text{ist-Permutation}[\mathcal{Z}_{a,\circ,A}, A] \bigwedge \text{ist-Permutation}[\mathcal{S}_{a,\circ,A}, A]$$

Beweis: Der Beweis von Satz 12 kann ohne Modifikation übertragen werden.

□

Weder der Begriff der Permutation noch die Begriffe Zeile und Spalte bauen auf der Endlichkeit der Gruppe auf. Im Falle einer unendlichen Gruppe ist aber die Verknüpfung nicht mehr anhand einer endlichen Verknüpfungstabelle zu veranschaulichen, trotzdem sind die Begriffe Zeile und Spalte auch in diesem Fall definiert. Die Anwendung des Satzes kann in diesem Fall daher nicht mehr durch Inspektion der Verknüpfungstafel geschehen, sondern es muss tatsächlich die Bijektivität gewisser Funktionen *bewiesen* bzw. *widerlegt* werden. In manchen Beispielen mag dies mit weniger Aufwand verbunden sein als das tatsächliche Bewiesen der Gruppeneigenschaften laut Definition (9).

Beispiel: Die Addition auf der Menge $\mathbb{N}_0$ (die natürlichen Zahlen inklusive 0) kann keine Gruppe sein, da z.B. $\mathcal{Z}_{2,+,\mathbb{N}_0}$ nicht surjektiv ist! Angenommen, $\mathcal{Z}_{2,+,\mathbb{N}_0}$ wäre surjektiv, d.h.

$$\forall_{n \in \mathbb{N}_0} \; \exists_{m \in \mathbb{N}_0} \; 2 + m = n \,,$$

und das gilt insbesondere für $n = 1$, also

$$\exists_{m \in \mathbb{N}_0} \; 2 + m = 1 \,.$$

Sei nun $m \in \mathbb{N}_0$ so, dass gilt $2 + m = 1$. Nun gilt aber $2 + m \geq 2$ und $2 > 1$, daher auch $2 + m > 1$. Das ist ein Widerspruch zu $2 + m = 1$, daher ist $\mathcal{Z}_{2,+,\mathbb{N}_0}$ nicht surjektiv.

7 Zusammenfassung und Ausblick

In dieser Arbeit wurde eine Eigenschaft der Verknüpfungstabelle einer endlichen Gruppe gezeigt. Diese Eigenschaft kann als Kriterium verwendet werden, mit dem in vielen Fällen einfach *widerlegt* werden kann, dass eine gegebene algebraische Struktur eine Gruppe ist. Wesentliches Augenmerk in dieser Arbeit lag aber an der exakten Formulierung des Satzes in der Prädikatenlogik, an der formal exakten Definition aller beteiligter Begriffe und an einem formal korrekten und sehr detailierten Beweis des Satzes. Auch auf Stilfragen mathematischer Präsentation wurde an manchen Stellen eingegangen. Durch eine genaue Analyse des Beweises konnten wir den ursprünglich für *endliche* Gruppen formulierten Satz auch auf *unendliche* Gruppen verallgemeinern.

Literatur

[AlgMeth04] W.Windsteiger. *Algorithmische Methoden 1*. Vorlesungsskriptum JKU Linz und Tutoriumsunterlagen, Wintersemester 2004/05, 2004.

[Alg60] Irgendein Standard-Algebra-Buch, 1960.

[Grup67] Irgendein Standard-Gruppentheorie-Buch, 1967.

[Log05] W.Windsteiger. *Logik als Arbeitssprache*. Vorlesungsskriptum JKU Linz und Tutoriumsunterlagen, Sommersemester 2005, 2005.