Gruppen (nicht beendet)

Steffen Solyga*

23. Februar 2005

Eine Gruppe ist eine Menge, in der eine assoziative und beiderseitig umkehrbare algebraische Operation definiert ist. – Dieser Artikel bietet eine knappe Einführung in die Gruppentheorie.

1 Einleitung

Gruppen – die wohl elementarsten Strukturen der abstrakten Algebra – werden in der Ingenieurmathematik (wohl gerade wegen ihrer Abstraktheit) i.allg. nicht behandelt. Dieser durchaus verständliche Umstand ist zugleich höchst bedauerlich, offenbaren sich doch gerade in der abstrakten Algebra Strukturen von bezaubernder Schönheit.

Diese Abhandlung entsteht parallel zu meinem späten Selbststudium der Elementarmathematik. Ihr Zweck besteht vor allem darin, michselbst zu klarem Denken zu zwingen.

2 Algebraische Operationen

Gegeben sei eine nichtleere Menge M. Ordnet man jedem *geordneten* Paar (a, b) von Elementen aus M genau ein (d.h. ein eindeutig bestimmtes) Element c aus M zu, dann hat man eine (zweistellige) algebraische Operation in M definiert:

Definition 1 *Eine in einer Menge M definierte algebraische Operation ist eine auf $M \times M$ definierte Funktion mit Werten aus M.*

Man beachte, daß der Definitionsbereich aller derartigen Funktionen die Menge *aller* geordneten Paare von Elementen aus M ist. Jedes denkbare Paar muß als Urbild auch „drankommen“; es gilt also $\mathbb{D} = M \times M$ (Funktion *auf* $M \times M$). Hingegen müssen die Wertebereiche nicht mit M zusammenfallen; es gilt also $\mathbb{W} \subseteq M$ (Werte *aus* M). Ferner können gewisse Elemente aus M auch mehrfach als Bilder „drankommen“.

Da es sinnlos ist, von Elementen einer leeren Menge zu sprechen, werden algebraische Operationen nur in nichtleeren Mengen definiert, d.h. nur in Mengen, die wenigstens ein Element enthalten.

Ist vermöge einer algebraischen Operation (im folgenden einfach Operation genannt) dem geordneten Paar (a, b) das Element c zugeordnet, so schreibt man $f(a, b) = c$, $a + b = c$, $a - b = c$,

*solyga@absinth.net

$a \cdot b = c$, $a/b = c$, $a * b = c$, $a \star b = c$, $a \odot b = c$, ...[1] Die zugehörigen Operationen werden also durch die Symbole f, $+$, $-$, $\cdot$, $/$, $*$, $\star$, $\odot$, ... bezeichnet. Sind keine Verwechslungen zu befürchten, weil z.B. nur eine einzige Operation betrachtet wird, kann man das Operationssymbol auch ganz weglassen: $ab = c$. Dieser Schreibweise wird ihrer Kürze wegen im folgenden der Vorzug gegeben. Weiter nennt man die Elemente von M auch *Operanden* und die Elemente von $\mathbb{W}$ Resultate bezüglich der in M definierten Operation. Beispiele für algebraische Operationen sind:

1. Die Addition, Subtraktion, Multiplikation und Division im Bereich der rellen (und komplexen) Zahlen, letztere unter Ausschluß der Null.
2. Die Vektoraddition nach der Parallelogrammregel.
3. Offenbar definiert auch $ab = a$ eine algebraische Operation in jeder nichtleeren Menge: Jedem geordneten Paar (a, b) wird dabei das erste Element des Paares zugeordnet.

Gemäß obiger Definition sind die Operandenpaare geordnet, d.h. die *Reihenfolge der Operanden* kann (und wird daher i.allg., siehe Beispiel 3) Einfluß auf das Resultat haben. Ist dies für eine gegebene Operation (und zugrundegelegte Menge[2]) nicht der Fall, so nennt man sie *kommutativ*:

Definition 2 *Eine in einer Menge M definierte algebraische Operation heißt kommutativ, wenn für alle $a, b \in M$ gilt: $ab = ba$.*

Beispiele:

1. Die Addition ($a + b = b + a$) und die Multiplikation ($a \cdot b = b \cdot a$), nicht jedoch die Subtraktion ($a - b \neq b - a$) und die Division ($a/b \neq b/a$) im Bereich der rellen (und komplexen) Zahlen sind kommutative Operationen.[3]
2. Die Vektoraddition nach der Parallelogrammregel ist kommutativ.
3. Bei der durch $ab = a$ definierten Operation handelt es sich im allgemeinen um keine kommutative:[4] Seien x und y beliebige (aber fest gewählte) Elemente aus M, dann gilt für diese $xy = x$ und $yx = y$. Lassen sich x und y derart wählen, daß $x \neq y$ gilt (d.h. besitzt M mehr als ein Element), dann ist die Operation offenbar nichtkommutativ. Denn dann existieren Elemente a, b, für die $ab \neq ba$ gilt, nämlich x und y.

   Das bedeutet jedoch nicht, daß die Operation $ab = a$ in *jeder* Menge nichtkommutativ ist. Wie das folgende Beispiel zeigt, spielt die betrachtete Menge eine entscheidende Rolle, siehe Fußnote 2.

[1] Das Symbol „=“ bezeichnet identische, also nicht unterscheidbare (bzw. nicht zu unterscheidende) Elemente. $f(a, b) = c$ bedeutet also, daß $f(a, b)$ und c dasselbe Element bezeichnen.

[2] Eine Operation ist gemäß Definition 1 nicht *ansich* sondern stets *in einer gewissen Menge* definiert.

[3] Das Symbol „≠“ bezeichnet unterscheidbare, also nicht identische Elemente. Es ist $a \neq b$ die Negation der Aussage $a = b$.

[4] Die Phrase „im allgemeinen“ wird gern mißverstanden, weshalb mir eine Definition angebracht erscheint: Es sei M eine unendliche Menge. Eine Aussageform $A(x)$ ist genau dann „im allgemeinen“ für $x \in M$ wahr, wenn sie für „wenigstens ein“ $x \in M$ falsch ist. – Diese Definition ist durchaus diskussionswürdig. Sicherlich aber soll eine „im allgemeinen“ wahre Aussageform in „mehr“ Fällen wahr als falsch sein. Daß sie in keinem Fall falsch (also immer wahr) ist, schließt man sinnvollerweise aus, denn dafür hat ja schon den Begriff der wahren Aussage. Also muß sie in wenigstens einem Fall falsch sein. Läßt man es dabei bewenden, hat man die obige Definition.

4. Alle auf jeder einelementigen Menge definierten Operationen sind kommutativ. – Besitzt M genau ein Element, namentlich x, so gibt es auch genau ein geordnetes Paar, nämlich (x, x). Wegen $xx \in M$ muß also $xx = x$ gelten, denn von x verschiedene Elemente stehen nicht zur Verfügung.

Gemäß Definition 1 sind die Resultate einer Operation stets wieder der betrachteten Menge angehörig; bildlich gesprochen führt eine algebraische Operation also nicht aus der betrachteten Menge heraus: Hat man für zwei beliebige Elemente $a, b \in M$ die Operation ab ausgeführt, so kann man wegen $ab \in M$ dieses Element selbst der Operation unterwerfen, indem man sich ein beliebiges $c \in M$ hernimmt und die Operation $(ab)c$ ausführt.[5] Mit derselben Begründung kann man dieselben Elemente a, b, c zu $a(bc)$ verküpfen, und es stellt sich die Frage, ob man dabei auch zu demselben Resultat gelangt. Im allgemeinen ist diese Frage zu verneinen, d.h. die *Reihenfolge der Ausführung der Operationen* hat Einfluß auf das Resultat. Ist dies für eine gegebene Operation (und zugrundegelegte Menge) nicht der Fall, so nennt man sie *assoziativ*:

Definition 3 *Eine in einer Menge M definierte algebraische Operation heißt assoziativ, wenn für alle $a, b, c \in M$ gilt: $(ab)c = a(bc)$.*

Nun besteht der Sinn der (nebenbei unterschobenen) Klammersymbolik gerade in der Kennzeichnung der Operationsreihenfolge – spielt diese keine Rolle, so geht er verloren. Eine assoziative Operation ist also durch die Überflüssigkeit von Klammern in der Symbolik gekennzeichnet. Und dies eben, obwohl mehr als zwei Operanden im Spiel sind und lediglich eine einzige Operation betrachtet wird.[6]

Für assoziative Operationen (und nur für diese) definiert man daher den bequemen Ausdruck abc durch $abc = (ab)c = a(bc)$. Umgekehrt gilt: Trifft man jemals auf einen Ausdruck abc, so hat man es mit einer assoziativen Operation zu schaffen – wenn man die Schulfibel einmal außeracht läßt.

Beispiele:

1. Die Addition ($(a + b) + c = a + (b + c)$) und die Multiplikation ($(a \cdot b) \cdot c = a \cdot (b \cdot c)$), nicht jedoch die Subtraktion ($(a - b) - c \neq a - (b - c)$) und die Division ($(a/b)/c \neq a/(b/c)$) im Bereich der rellen (und komplexen) Zahlen sind assoziative Operationen.

2. Die Vektoraddition nach der Parallelogrammregel ist assoziativ.

3. Die Operation $ab = a$ ist in *jeder* Menge assoziativ, denn einerseits gilt $(ab)c = (ab) = a$, und andererseits gilt auch $a(bc) = a$. Genauso zeigt man, daß $ab = b$ eine assoziative Operation ist.

4. Alle auf jeder einelementigen Menge definierten Operationen sind assoziativ, weil als Resultat jeweils nur das eine Element in Frage kommt (und sichselbst gleich ist).

Viele der gebräuchlichen Operationen sind sowohl kommutativ als auch assoziativ, und es stellt sich die Frage, ob nicht ein genereller Zusammenhang zwischen diesen Attributen besteht. Konkret: Darf man aus der Kommutativität einer Operation auf deren Assoziativität schließen

[5] Die Klammern werden im üblichen Sinn verwendet: Geklammerte Operationen sind zuerst auszuführen. – Ein Ausdruck der Gestalt *abc* ist (bislang) undefiniert.

[6] Da, wie noch zu sehen sein wird, Gruppen eine assoziative Operation implizieren, könnte man sagen: Ein Gruppentheoretiker ist ein Mensch, der nicht weiß, was Klammern sind. – In Anlehnung an den bekannten Witz, ein Topologe sei ein Mensch, der nicht zwischen Kreis und Quadrat unterscheiden kann.

oder umgekehrt? – Dies ist im allgemeinen (d.h. für beliebige Mengen und Operationen) nicht möglich. Zum Beweis zeigt man, daß sowohl kommutative und assoziative, kommutative und nichtassoziative, nichtkommutative und assoziative als auch nichtkommutative und nichtassoziative Operationen existieren, und zwar in ein und derselben Menge:

Betrachtet sei die aus den (beiden) Elementen 0 und 1 bestehende Menge M, also $M = \{0, 1\}$.[7] Dann gilt $M \times M = \{(0,0), (0,1), (1,0), (1,1)\}$, und es definiert die Abbildung $(0,0) \mapsto 0$, $(0,1) \mapsto 0$, $(1,0) \mapsto 0$, $(1,1) \mapsto 0$ (also $ab = 0$ für alle $a, b \in M$) eine kommutative und assoziative Operation in M: Die Menge $\mathbb{W}$ der Resultate enthält genau das Element 0, also $\mathbb{W} = \{0\}$, weshalb alle Resultate, wie auch immer sie mittels der Operation gewonnen werden, identisch sein müssen. Damit liegt *trivialer Weise* sowohl Kommutativität als auch Assoziativität vor. Zweckmäßig gibt man die Operation in Form einer Tabelle an:

a	b	ab
0	0	0
0	1	0
1	0	0
1	1	0

In derselben Menge M kann man folgende Operation definieren:

a	b	ab
0	0	1
0	1	0
1	0	0
1	1	0

Wegen $01 = 0 = 10$ ist diese offenbar kommutativ, nicht jedoch assoziativ, denn es gilt z.B. $(00)1 = 11 = 0$ aber $0(01) = 00 = 1$. Weiter ist die Operation

a	b	ab
0	0	0
0	1	1
1	0	0
1	1	0

weder kommutativ noch assoziativ, denn für sie gilt $01 = 1 \neq 0 = 10$ und $(10)1 = 01 = 1$ aber $1(01) = 11 = 0$. Schließlich ist

a	b	ab
0	0	0
0	1	0
1	0	1
1	1	1

wegen $01 \neq 10$ zwar nichtkommutativ, aber assoziativ. Um letzteres einzusehen, braucht man nicht alle 2^3 Variationen zu untersuchen, denn die Operation ist vom Typ $ab = a$, deren Assoziativität im Beispiel 3 sogar für *jede* (nichtleere) Menge gezeigt wurde.

[7] 0 und 1 sind lediglich Bezeichner für die Elemente und nicht etwa Zahlen. Anstelle von 0 und 1 könnte man genausogut x und y (oder x und y) schreiben – allein der Übersichtlichkeit wegen wird hier der ersten Methode der Vorzug gegeben. Ferner gilt $0 \neq 1$, denn wären 0 und 1 nicht zu unterscheiden, bestünde die Menge nur aus einem Element, siehe auch Fußnoten 1 und 3.

Anscheinend lassen sich in $M = \{0,1\}$ genau $2^4 = 16$ verschiedene Operationen angeben (allgemein: $n^{(n^2)}$ bei n Elementen), wie es die folgende Tabelle nahelegt. Es stehen k und a für kommutativ und assoziativ, $\overline{k}$ und $\overline{a}$ für nichtkommutativ und nichtassoziativ:

a	b	f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}
0	0	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
0	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1	0	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
1	1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
		ka	$k\overline{a}$	$\overline{k}\overline{a}$	$\overline{k}\overline{a}$	$\overline{k}\overline{a}$	$\overline{k}\overline{a}$	ka	$k\overline{a}$	ka	ka	$\overline{k}a$	$\overline{k}\overline{a}$	$\overline{k}a$	$\overline{k}\overline{a}$	ka	ka

3 Umkehrung von Operationen

Ist f eine in M definierte Operation, so kann man zunächsteinmal die zugehörige Umkehrabbildung betrachten, d.h. jedem Resultat $f(a,b)$ sein Operandenpaar (a,b) zuordnen. Definitionsgemäß verlangt jede Operation jedoch nach einer eindeutigen Abbildung von $M \times M$ in M; damit auch die Umkehrabbildung eindeutig sein kann, müßte sich $M \times M$ bijektiv auf M beziehen lassen, was offenbar nur im Ausnahmsfalle möglich ist (nämlich dann, wenn M genau ein Element enthält). Die zu einer Operation gehörende Umkehrabbildung ist daher im allgemeinen mehrdeutig und somit nur von geringem Wert.

Zu einer realistischen Chance, von Resultaten auf Operanden schließen zu können, gelangt man erst, wenn man jedem Resultat wenigstens einen Operanden beifügt.

4 Gruppen

Definition 4 *Ein Element $e \in G$ heißt neutrales Element der Gruppe G, wenn für alle $a \in G$ gilt: $ea = ae = a$.*

Satz 1 *In jeder Gruppe existiert genau ein neutrales Element.*

Beweis 1 *Existenz.*

Eindeutigkeit.

Literatur

[1] P. S. Alexandroff, A. I. Markuschewitsch, A. J. Chintschin: Enzyklopädie der Elementarmathematik, Band 1 (Arithmetik). Hochschulbücher für Mathematik Band 7. VEB Deutscher Verlag der Wissenschaften, 2. Auflage, Berlin 1965