Kapitel 3: Algebraische Stukturen

3.1 Das Begriffsystem

3.1.0 Vorbemerkung

Wir nennen zwei unterschiedliche, aber miteinander verwandte Gründe, die letztlich dazu geführt haben, dass man in der Mathematik abstrakte algebraische Strukturen einführte und ausgiebig untersuchte:

- Das aus Anwendungen entstehende Bedürfnis, "Gleichungen zu lösen" und die damit verbundene Notwendigkeit, mit "Unbestimmten" und "allgemeinen Größen" zu rechnen.
- Der Wunsch, bei der Naturbeschreibung quantitativ gültige Beziehungen zwischen Beschreibungsgrößen zu finden und solche zuerst einmal überhaupt formulieren zu können. (Formulierung und Beschreibung von Naturgesetzen). Erfahrungsgemäß führt das zu **Formeln**, die in ganz bestimmter Weise formal aufgebaut sind.

Während es zunächst immer nur um reelle Zahlen und Formeln für reelle Zahlen ging, traten später auch andere Größen - komplexe Zahlen, Vektoren, Funktionen,

geometrische Transformationen Teilmengen usw. - hinzu. Und es entstand die Frage, inwieweit man Rechenregeln, die man von den reellen Zahlen her kannte, auf diese neuen Objekte übertragen kann.

Die algebraischen Methoden entwickelten sich im Rahmen der Bewältigung schwieriger Probleme unterschiedlichster Art: Technisch konkrete Probleme wie die Stabilität von Brücken oder Gebäuden gehören ebenso dazu wie rein geistige Herausforderungen wie das Problem der Dreiteilung eines Winkels mit Zirkel und Lineal. Oder die Frage nach einer sachgerechten Klassifikation der Kristallstrukturen und den sich daraus ergebenden Konsequenzen. Oder: Wieso folgt aus der beobachteten Konstanz der Lichtgeschwindigkeit die Raum-Zeit-Struktur der Relativitätstheorie mit ihren erstaunlichen Phänomenen? Wie kann man vom geometrischen Bau der Moleküle eines Stoffes auf die spektroskopischen Eigenschaften dieses Stoffes schließen? Wieso gibt es Elementarteilchen wie das Elektron mit einem Spin (=Eigendrehimpuls) von 1/2, aber keines mit einem Spin 1/3? Usw, usw.

Parallel zur Behandlung und Lösung derartiger Fragen machte man die Erfahrung, dass es vielfach nur auf wenige Grundregeln ankam, aus denen sich ohne weiteren Inhaltsbezug - also durch logisch-mathematische Herleitung - die komplexeren erwünschten Rechenregeln folgern ließen. Man entdeckte, dass und wie ein oder dieselbe Struktur oder Idee (im Sinne von Plato) in den unterschiedlichsten Zusammenhängen und Verkleidungen auftreten kann.

Das vorliegende Kapitel möchte diesen für die Naturerfassung wichtigen Sachverhalt herausarbeiten und zeigen, wie er mit dem mathematischen Strukturbegriff korrespondiert.

Bei der Behandlung der oben genannten Probleme stößt man beständig auf den Begriff der "Gruppe". Das ist eine algebraische Struktur, die sich gut als grundlegender Baustein der übrigen algebraischen Strukturen eignet ebenso wie man die für die Gruppentheorie entwickelten Methoden und Begriffe auf andere Bereiche übertragen kann. Es lohnt, die (nicht geringe) Arbeit zu investieren, die erforderlich ist, sich den Einstieg in das Gedankengebäude der algebraischen Strukturen und insbesondere auch der Gruppen zu verschaffen. Denn damit erhält man eine Grundlage zur geistigen Behandlung vieler schwieriger Probleme wie der oben erwähnten.

3.1.1 Algebraische Verknüpfungen

(1.1.1) Rohmaterial aller algebraischen Strukturen sind die *Verknüpfungen oder Kompositionen.* Das sind Abbildungen des Typs

$$\top : M \times N \to L$$

wobei M,N und L Mengen sind, die ansonsten keinerlei Einschränkung unterliegen. Nur leer sollten sie nicht sein. Anders als bei den induktiven Verfahren soll hier die Urbildmenge gleich der gesamten Produktmenge sein. Verknüpfungen machen aus **zwei** zunächst unterschiedenen Objekten **ein** resultierendes Objekt. Als Abbildungen sind sie typischerweise nicht injektiv.

(1.1.2) Betrachtet man irgendeine Formel etwa physikalischer Herkunft, so findet man immer einige oder gar mehrere solcher Abbildungen vor, mit deren Hilfe der Formelbau über Termbildung erfolgt. Etwa

$$\vec{D} = 2\alpha(\vec{r} \times \vec{F}) + (\vec{a} \cdot \vec{b})\vec{r}.$$

Hier haben wir das Kreuzprodukt zweier Vektoren und das Skalarprodukt, die Vektoraddition sowie die Multipklikation eines Vektors mit einem Skalar, also vier Abbildungen des Verknüpfungstyps.

(1.1.3) Für die Werte dieser Verknüpfungsabbildungen verwendet man meist Bezeichnungen, die sich an den herkömmlichen Schreibweisen orientieren. Man schreibt also nicht $\top$((a,b)) - wie es der Formalismus der Abbildungstheorie verlangen würde - sondern a$\top$b, so wie man es von 2+3 oder 2·3 oder a-b her gewohnt ist. ($\top$ die Abbildung, $\top$(....) für den Wert, in den das Urbild (a,b) einzusetzen ist.)

(1.1.4) Die beteiligten Mengen sind in der Regel für recht lange Betrachtungen und Textteile als konstant anzusehen und ergeben sich dann aus dem Kontext, so dass man meist $\top : (a, b) \mapsto a \top b$ statt des ausführlichen $(\mathrm{M}\times N, (a, b) \mapsto a \top b, L)$ schreibt.

(1.1.5) Meist sind auch wenigstens zwei der drei Mengen K, M und L einander gleich. Oder es sind sogar alle drei Mengen gleich. Dann spricht man von einer *inneren Verknüpfung* (auf M):

$$\top = (M \times M, (a, b) \mapsto a \top b, M).$$

(1.1.6) Falls M eine endliche Menge mit n Elementen ist, gibt es auf M bereits für kleine n eine ungeheuer große Anzahl solch innerer Verknüpfungen. Nämlich $n^{(n^2)}$ Stück. Für n=3 sind dies 3^9 und für n=5 etwa 10^{17} Exemplare. Würde ein Computer jede Sekunde eine dieser 10^{17} Abbildungen zeigen und hätte er diese Vorführung beim Urknall begonnen, so wäre er damit heute gerade ungefähr fertig! Und das für das winzige n=5!

Die zusätzlichen Forderungen, die man an die Verknüpfungen stellt und mit deren Hilfe man die interessanten Fälle aussondert, müssen also noch außerordentlich einschränkend sein.

3.1.2 Bau und Verwendung algebraischer Strukturen

(1.2.1) Zunächst wollen wir kurz skizzieren, wie Aufbau und Analyse einer algebraischen Struktur üblicherweise erfolgen. Die Kenntnis dieses Ablauf ist nützlich, da man sich damit in herkömmlichen mathematischen Texten viel Verständnisarbeit ersparen kann.

Meist kann man davon ausgehen, dass sich der Autor, der eine algebraische Struktur einführt, einerseits an die angegebenen Punkte hält und seinen Text danach aufbaut, dass er andererseits dies aber nicht erwähnt, sondern stillschweigend erwartet, dass der Leser *Selbstverständlichkeite*n automatisch erkennt, eventuell eigenständig ergänzt. Insbesondere werden wir den dritten Schritt später noch weiter untergliedern. **Wichtiger als das systematische Durchackern des allgemein Erwarteten ist es, Abweichungen und Problemstellen zu erkennen.**

Letztlich geht es um die Entwicklung einer Urteilsfähigkeit, notwendige Banalitäten von anspruchsvollen Fragen unterscheiden zu können.

(1.2.2) **Bau. Analyse und Verwendung einer algebraischen Struktur:**

♦	In einem ersten Schritt werden eine gewisse Anzahl von Mengen und zugehörige Verknüpfungen vorgegeben.
♦	In einem zweiten Schritt werden hierfür gewisse Eigenschaften gefordert (**Axiome der algebraischen Struktur**).
♦	In einem dritten Schritt zieht man daraus (ohne Inhaltsbezug) rein mathematisch Folgerungen.
♦	Die so gewonnenen Resultate gelten dann für jedes konkrete, inhaltsbezogene Modell, sofern es nur eben diese Axiome erfüllt!

(1.2.3) Welche Eigenschaften man im zweiten Schritt zu wählen und zu formalisieren hat, basiert auf den Erfahrungen, die man im Umgang mit bekannten und konkreten mathematischen Objekten und Problemen erworben hat. Die Axiome, die einem üblicherweise (im mathematischen Lehrbuchtext) in wenigen Zeilen präsentiert werden, erfassen und komprimieren Erfahrung und Arbeit vieler Generationen fähigster Mathematiker und Wissenschaftler. Das bedeutet dann auch, dass die naheliegende Frage "Wieso gerade diese und keine anderen Axiome?" sich nur schwer kurz beantworten läßt, außer mit dem Verweis, dass eben gerade die gewählten Regeln sich erfahrungsgemäß als besonders wichtig und nützlich erwiesen hätten, was man dann teilweise erst beim Eindringen in die jeweilige Theorie genauer versteht.

Ein wesentliches Kriterium für die Wahl der Axiome sieht so aus: Die Axiome selbst sollen möglichst wenig fordern, d.h. man soll ihre Gültigkeit (in konkreten Systemen) mit möglichst wenig Aufwand überprüfen können. Dafür soll man aus ihnen möglichst viele, möglichst unerwartete, überraschende und nützliche Resultate herleiten können. Kurz: **Inhaltlich soll man möglichst wenig überprüfen müssen, um dann rein mathematisch möglichst viel zu bekommen.** Es sollte einleuchten, dass das eine schwierige Forderung ist und dass ihre Erfüllung die oben erwähnte langjährige Arbeit und Erfahrung verlangt.

(1.2.5) Hat man ein derartiges System einmal entwickelt, so kann der letzte Schritt - die Anwendung der allgemeinen Resultate auf inhaltliche Probleme - sehr nützlich und arbeitssparend sein. Die Resultate der Vektorrechnung bieten hierzu ein gutes Beispiel: Wann auch immer man es mit Größen zu tun hat, deren quantitative Festlegung mehr als eine Zahlangabe erfordert, bieten sich die Resultate und Methoden der allgemeinen Vektorraumtheorie als verfügbares Handwerkszeug zur Problemlösung an, **gleichgültig wie die inhaltliche Interpretation der Größen auch aussehen mag.**

(1.2.5) Noch ein Hinweis: Die bisherigen Überlegungen zeigen bereits deutlich, dass es auf die **Bezeichnungen** nicht ankommen wird, sondern immer auf die (durch die Axiome festgelegten) **Beziehungen zwischen den bezeichneten Objekten**. Ob eine Verknüpfung mit +,* oder $\intercal$ bezeichnet wird, ist in struktureller und mathematischer Hinsicht unwesentlich. Man muß lernen, sich von den Bezeichnungen zu lösen und die Beziehungen, die dahinter stehenden Ideen, zu erkennen!

Soll in einem bestimmten Kontext eine Menge mit bestimmten Veknüpfungen und eventuell Axiomen verbunden werden, so benutzt man gerne die Tupelschreibweise, schreibt etwa $(\mathbb{R},+,\cdot)$ oder $(\mathbb{N},+)$ usw.

3.1.2a Übersicht über das weitere Vorgehen.

(1.2.6) Wir geben noch eine kurze Übersicht über das weitere Vorgehen im Einführungsteil.

- Zunächst stellen wir einige *Beispiele für Verknüpfungen* vor. Allerdings wollen wir nicht den gesamten Fundus an herkömmlichen Verknüpfungen (Addition, Multiplikation,.... in IR, Vektoraddition ,...usw. usw.) auflisten. Stattdessen möchten wir den Leser auf einige andersartige Verknüpfungen hinweisen.

- Dann sollen einige Grundbegriffe und Bezeichnungen eingeführt werden, die man im Bereich der algebraischen Strukturen beständig verwendet. Hierzu gehören auch besonders wichtige, in Axiomen gerne verwendete Forderungen und erste daraus ziehbare Folgerungen.

- Anschließend soll eine einfache Systematik aller üblichen algebraischen Strukturen entwickelt werden. Sie geht von dem ersten in (1.2.2) besprochenen Schritt aus und klassifiziert **nach der Anzahl der die Struktur definierenden Mengen und der Anzahl der Verknüpfungen.**

3.1.2b Beispiele für Verknüpfungen

(1.2.7) **Beispiel 1**: *Wortverknüpfung* (vgl.. Kap.l.1.6 - Multinomialsatz)

Wir betrachten eine (endliche) Menge von Zeichen. Etwa die Menge aller Zeichen unseres Alphabets. Oder die Menge aller Zeichen, die auf einer bestimmten Schreibmaschinentastatur vorhanden sind. Ein Leerzeichen kann dazugehören. Usw. Suggestiv nennen wir eine solche Menge ein *Alphabet*. Konkret könnte beispielsweise A={1,2,3,4,+,(,)} ein Alphabet mit insgesamt 7 Elementen (=Zeichen) sein. Zu jedem Alphabet bilden wir jetzt eine neue Menge, die der zugehörigen Wörter. Jedes Wort besteht aus einer endlichen (von links nach rechts hingeschriebenen) Folge von Zeichen des Alphabets. Als Beispiel wären 1+((2+3)+2) und ++()2+ zwei mögliche Wörter zu unserem A. Das Beispiel verdeutlicht, dass es hier nur darauf ankommt, ob die Einzelzeichen im zugehörigen Alphabet liegen oder nicht. Auf eine eventuelle inhaltliche Bedeutung kommt es nicht an.

Die zu irgendeinem Alphabet A gehörige Menge von Wörtern wollen wir mit WA bezeichnen und dafür eine innere Verknüpfung definieren. D.h. wir müssen ein allgemeines Verfahren angeben, das aus zwei Wörtern (eines bestimmten Alphabets) ein neues ebensolches Wort macht. Eine solche Konstruktion liegt nahe: Wir müssen die Wörter nur nacheinander (von links nach rechts) hinschreiben:

$$(WA \times WA, (W,V) \mapsto WV, WA)$$

Im Beispiel werden etwa die beiden Wörter W=(1+ und V=2))+3 durch die eingeführte innere Verknüpfung zum neuen Wort WV=(1+2))+3 verbunden.

(1.2.8) **Beispiel 2**: *Modulorechnen*

Im ersten Beispiel haben wir eine etwas ungewöhnliche Menge eingeführt und darauf eine Verknüpfung definiert, die recht vertraut ist. Jetzt wollen wir auf einer vertrauten Menge - nämlich $\mathbb{N}$ neben den üblichen Verknüpfungen wie + und · neue Verknüpfungen einführen, die einem weniger vertraut sind, die dafür aber mehr nach "Rechnen" aussehen.

Es sei p irgendeine feste natürliche Zahl >1. Weiter seien n und m zwei ganze Zahlen. Wir bilden die Summe n+m und dividieren das Ergebnis mit Rest durch p. Also n+m= k·p + r wobei k$\in \mathbb{N}$ sein soll und 0≤r<p. D.h. r soll der (eindeutig bestimmte) Divisionsrest von n+m bei Division durch p sein . Wir setzen $n +_p m = r$ und erhalten damit (für jedes p) eine innere Verknüpfung auf $\mathbb{N}$. Beispielsweise

$$6 +_3 5 = 2, \quad \text{denn es gilt} \quad 11 = 3 \cdot 3 + 2.$$

Die Verknüpfung ist offensichtlich hochgradig nicht surjektiv. Eine entsprechende Multiplikation läßt sich ebenso einführen: $4 *_3 5 = 2$ wegen $20 = 3 \cdot 6 + 2$.

(1.2.9) **Beispiel 3**: *Teilmengenverknüpfungen*

Sei A eine nichtleere Menge und $\mathcal{P}$(A) die zugehörige Potenzmenge. Dann bilden Vereinigung ∪ und Durchschnitt ∩ je eine innere Verknüpfung auf $\mathcal{P}$(A).

3.1.3 Allgemeine algebraische Grundbegriffe.

(1.3.1) Wir kommen jetzt zu den in (1.2.6) angekündigten algebraischen Grundbegriffen, die fast überall im Bereich der algebraischen Strukturen benutzt werden, die den algebraspezifischen Begriffsapparat samt zugehörigen Konsequenzen ausmachen.

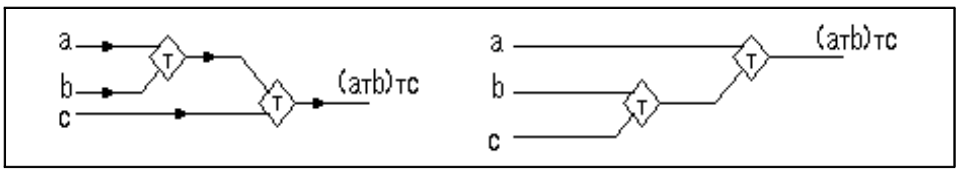
3.1.3a Das Assoziativgesetz

(1.3.2) Die Verknüpfungen, von denen man ausgeht, sind immer nur "zweistellig". D.h. sie machen aus zwei Objekten eine resultierendes ("ordnen zu"). Insbesondere macht eine innere Verknüpfung in M aus zwei Elementen von M ein neues. Will man drei oder gar mehr Elemente zu einem neuen verbinden, so geschieht das meist so, dass man zweistellige Verknüpfungsabbildungen mehrfach verwendet, also vom Automatenstandpunkt aus zusammenschaltet. (Kap. 1.2.7).

(1.3.3) Auf diese Weise kann man aus einer gegebene inneren Verknüpfung $\top$:M×M→M die beiden folgenden Abbildungen vom Typ "aus drei mach eines" bilden:

$$\begin{aligned} K &= (M \times M \times M, (a,b,c) \mapsto (a \top b) \top c, M) \\ L &= (M \times M \times M, (a,b,c) \mapsto (a \top (b \top c), M) \end{aligned}$$

Beide Abbildungen sind mit Hilfe der inneren Verknüpfung $\top$ in M konstruiert. Als Verlaufsdiagramme:



(1.3.4) Vom Addieren und Multiplizieren reeller Zahlen her sind wir es gewohnt, dass beide Diagramme stets dasselbe Resultat liefern. D.h. die beiden Abbildungen K und L sind in diesen Fällen gleich, sie unterscheiden sich nur durch ihre Zuordungsverfahren, nicht in den Zuordnungen selbst. (Kap. 1.2.1).

Nehmen wir als Verknüpfung dagegen das Vektorprodukt, dann erhalten wir in beiden Fällen fast stets unterschiedliche Werte. Für das Vektorprodukt sind die beiden Abbildungen selbst, ihre Zuordnungen, voneinander verschieden. Demnach ist generell zu erwarten, dass es im Bereich der algebraischen Strukturen Verknüpfungen beiderlei Typs gibt: Solche, für die sich die beiden Abbildungen K und L unterscheiden und solche, für die sie gleich sind.

(1.3.5)Diese Unterscheidung erweist sich als sehr wichtig, so daß man definiert:

Eine innere Verknüpfung $\intercal$:M×$M \to M$ heißt *assoziative innere Verknüpfung (in M)*, wenn für **alle** a,b,c∈ M gilt: $((a \intercal b) \intercal c) = (a \intercal (b \intercal c))$

D.h. für ein assoziatives $\intercal$ stimmen die beiden oben konstruierten Abbildungen K und L überein. Beachten Sie: Findet man **ein einziges** Tripel (a,b,c)∈M×M×M, für das die geforderte Gleichheit nicht erfüllt ist, so ist auch das Assoziativgesetz nicht erfüllt. Bei Gleichungen dieser Art benutzt man in der Regel stillschweigend eine Klammersparnisregel und schreibt $(a \intercal b) \intercal c = a \intercal (b \intercal c)$. Also "Termrechnung vor Gleichheit".

(1.3.6) Will man für eine endliche Menge M mit N Elementen die Assoziativität explizit nachrechnen, so muß man die Gültigkeit von N^3 Gleichungen überprüfen. Für N=5 sind das immerhin bereits 125 Stück! Der direkte Nachweis der Assoziativität erscheint so recht mühsam. Wir sollten daher nach besseren Methoden suchen.

(1.3.7) Was bringt es uns, wenn wir wissen, dass eine Verknüpfung assoziativ ist? Auf den ersten Blick nur einen Schwall weiterer Probleme. Wie steht es nämlich, wenn wir mehr als drei Elemente verknüpfen wollen. Sagen wir 4 oder 5 oder gar 1000? Anstelle von K und L bzw. der beiden zugehörigen Schaltdiagramme können wir jetzt viele neue Abbildungen bzw Diagramme bilden. Für 4 findet man A_4=5, für 5 bereits A_5=14 . Allgemein wollen wir die Anzahl möglicher Diagramme für n Elemente aus M mit A_n bezeichnen. Am Ende dieses Teilkapitels werden wir diese kombinatorische Zahl berechnen. Jedes Diagramm führt zu einer zulässigen Beklammerung von $a_1 \intercal a_2 \intercal ... \intercal a_n$. Müssen wir dann nicht eine unglaubliche Menge von Gleichheitsproblemen analysieren? Das ist zum Glück nicht der Fall. Es zeigt sich nämlich: Gilt das Assoziativgesetz, d.h. gilt K=L , dann sind alle A_n Automaten für n Eingabeterme notwendig einander gleich. Man hat also nur eine einzige Zuordnung für n Terme, selbst wenn man sehr viele verschiedene Zuordnungsverfahren - nämlich A_n - vorliegen hat.

(1.3.8) Wir haben es hier mit einem illustrativen ersten Beispiel einer allgemeingültigen mathematischen Folgerung aus einem Axiom zu tun, also ein Beispiel für den 3.Schritt aus (1.2.2).

(1.3.9) Wir formulieren das Resultat genauer und beweisen es anschließend.

Satz: Es sei $\intercal : M \times M \to M$ eine assoziative innere Verknüpfung.
Es sei n∈ ℕ mit n≥ 1 und $a_1, a_2, ..., a_n \in M$.
Dann ergeben alle A_n zulässigen Beklammerungen von
$a_1 \intercal a_2 \intercal ... \intercal a_n$ dasselbe Element aus M.

(1.3.10) Konkret: Für n=4 gibt es 5 zulässige Beklammerungen (a$\intercal$b)$\intercal$(c$\intercal$d) , ((a$\intercal$b)$\intercal$c)$\intercal$d , (a $\intercal$(b$\intercal$c))$\intercal$d , a$\intercal$((b$\intercal$c)$\intercal$d) und a$\intercal$(b$\intercal$(c$\intercal$d)). Alle 5 Beklammerungen ergeben im assoziativen Fall dasselbe Element aus M. Für n=5 ergeben alle 14 zulässigen Beklammerungen dasselbe Resultat. Usw.

(1.3.11) Einige **Vorüberlegungen zum Beweis:**

Ein sorgfältiger Beweis ist natürlich erforderlich. Die Beweisidee folgt bereits aus dem gegebenen Konkretisierungsbeispiel für n=4.

> Setzt man z.B. a$\intercal$b =A , so ist A auch ein Element aus M. A ist Hilfsgröße und a,b,c,d sind freie Variable. Daher darf das Assoziativgesetz auf den Ausdruck (A$\intercal$c)$\intercal$d angewandt werden ("für alle Elemente aus M"). Tut man das und ersetzt man am Ende A wieder durch a$\intercal$b so erhält man die Beziehung ((a$\intercal$b)$\intercal$c)$\intercal$d = (a$\intercal$b)$\intercal$(c$\intercal$d). D.h. zwei unserer fünf Ausdrücke sind bereits gleich. Entsprechend ist generell vorzugehen. Oder auch: Das Assoziativgesetz ist im Bereich der jeweiligen algebraischen Struktur vom Typ einer allgemeingültigen Gleichung. **Durch Einsetzen von Termen entstehen erneut gültige Gleichungen.** Vgl. Kap.1.(2.9.2).

Man benötigt noch eine zweite, mehr technische Idee. Die Anzahl der möglichen Beklammerungen wird mit zunehmendem n rasch groß. Damit nicht zu viele Gleichungen zu überprüfen sind, sollte man so vorgehen, dass man eine geeignete Beklammerung als Vergleichs- oder Standardbeklammerung auswählt und dass man zeigt, dass alle übrigen Beklammerungen denselben Wert wie diese Standardbeklammerung ergeben. (Denn dann sind sie auch alle untereinander gleich! Transitivität und Symmetrie der Gleichheit.)

□ Wieviele nichttriviale Gleichungen wären ohne das letzte Argument zu überprüfen, wenn A_n die Zahl der zulässigen Beklammerungen ist?

(1.3.12) Beweis: Den Beweis führen wir mit Induktion. (Und zwar benötigen wir in diesem Fall für den Beweis der N-ten Aussage nicht nur die (N-l)-te , sondern sämtliche Vorgängeraussagen.

- Für N=l und 2 ist die Aussage des Satzes trivial. Für N=3 handelt es sich gerade um das vorausgesetzte Assoziativgesetz. Nehmen wir also an. wir hätten das Resultat ("alle Beklammerungen liefern denselben Wert") bereits bis N-l bewiesen.
- Wie angekündigt führen wir eine Standardbeklammerung ein. Naheliegenderweise setzen wir:

  $S_N=(....(a_1 \top a_2) \top a_3)....) \top a_N$ oder rekursiv $S_N=S_{N-1} \top a_n$

  Dabei dürfen die a_i irgendwelche sich aus dem Kontext bestimmende Elemente sein. Es müssen keineswegs die Ausgangselemente sein).
- Wir wollen induktiv zeigen: Ist A_N irgendeine zulässige Beklammerung, so gilt notwendig $A_N = S_N$.
- Die Automateninterpretation unserer Beklammerungen zeigt: Es gibt immer -also auch für A_N - eine **zuletzt wirkende Verknüpfung** $\top$.
  D.h. Man kann immer schreiben: $A_N = A_{N-K} \top B_K$. Hierbei steht A_{N-K} für eine zulässige Beklammerung der ersten N-K Elemente a_i. und B_K für eine zulässige Beklammerung der der restlichen Elemente. K ist dabei eine durch die Ausgangsbeklammerung A_N eindeutig festgelegte Zahl. Da in A_N insgesamt N-1 der Zeichen $\top$ auftreten, liegt K notwendig zwischen 1 und N-l.
- Wir unterscheiden jetzt zwei Fälle : K=l und K>1.
  - K=l bedeutet: $A_N = A_{N-1} \top a_N = S_{N-1} \top a_N = S_N$. Hierbei haben wir die Induktionsvoraussetzung für N-l und die rekursive Definition unserer Standardbeklammerung benutzt.
  - K>1 gibt: $A_N = A_{N-K} \top B_K = A_{N-K} \top (C_{K-1} \top a_N)$. Dabei enthält der Ausdruck C_{K-1} mindestens eines der a_i aus M. Für B_K haben wir die Induktionsannahme für K$\leq N-1$ benutzt, um B_K in die Standardform umzuwandeln. Weitere Anwendung für K=3 und und für K=N-l gibt:

    $$A_N = A_{N-K} \top (C_{K-1} \top a_N) = (A_{N-K} \top C_K) \top a_N = S_{N-K} \top a_N = S_N$$

    wie gewünscht.

Damit ist unsere gesuchte Beziehung A_N=S_N für jeden Fall bewiesen und der übliche Induktionsschluß liefert die generelle im Satz behauptete Aussage.

(1.3.13) Die Gültigkeit des Assoziativgesetzes ist eine erste Eigenschaft, nach der man beim Auftreten einer inneren Verknüpfung fragen sollte und die auch umgekehrt in den Axiomen der unterschiedlichen algebraischen Strukturen vielfach gefordert wird.

3.13b Das Kommutativgesetz

(1.3.14) Ein ähnlich wichtiges Gesetz ist das Kommutativgesetz. Auch dieses Gesetz kann für Verknüpfungen gelten, muß es aber nicht.

Definition	Eine innere Verknüpfung $\top$ von M heißt *kommutativ,* falls für alle a,b$\in M$ gilt $a \top b = b \top a$

Überlegen Sie selbst, was der Automatenstandpunkt über das Kommutativgesetz aussagt.

□ Der Begriff *kommutativ* legt eine Verallgemeinerung auf gewisse Verknüpfungen nahe, die nicht vom inneren Typ sind. Für welchen Typ von Verknüpfungen sollte man ihn noch verwenden? Wie steht es dann allerdings mit dem nachfolgenden Resultat (1.3.15)?

(1.3.15) Ganz wie das Assoziativgesetz hat auch das Kommutativgesetz gewisse weitergehende Konsequenzen. Die wichtigste sieht so aus:

Satz:	Sei $\top$ eine kommutative und assoziative Verknüpfung von M. Weiter seien $a_1, ..., a_N$ Elemente aus M. Dann darf man in dem Ausdruck $a_1 \top a_2 \top ... \top a_N$ die Reihenfolge der Summanden beliebig vertauschen und anschließend beliebig (zulässige) Klammern setzen. **Auswertung ergibt stets dasselbe Element aus M.**

Der (ausgelassene) Beweis verläuft analog zum vorigen Satz mit Hilfe von Induktion.

Bemerkung: Die Anzahl der möglichen zulässigen Beklammerungen von n Elementen aus M bei fester Reihenfolge haben wir oben mit A_n bezeichnet. Jetzt bezeichnen wir mit B_n die Anzahl möglicher Beklammerungen bei beliebiger Reihenfolge. Da man die n Summanden stets in n! unterschiedlichen Weisen anordnen kann, gilt B_n=n!A_n. Etwa B_4= 4!·5=120. Der Satz sichert daher die Gleichheit einer noch weitaus größeren Zahl von Rechenausdrücken, als es der erste tut. Weiter unten werden wir die B_n und die A_n berechnen.

(1.3.17) Ist eine Verknüpfung kommutativ und assoziativ, so rechtfertigt der Satz die übliche Konvention, einfach $a \top b \top c \top .....\top s$ zu schreiben, also so zu tun, als hätte man einen einzigen Automaten, der n Elemente aus M gleichzeitig verarbeitet. Gleichgültig, wie man diesen Ausdruck mit Hilfe von $\top$:M×M→M interpretiert, stets kommt doch dasselbe Element aus M heraus.

□ Wieso setzen wir im Satz kommutativ **und** assoziativ voraus. Was gilt, wenn man nur kommutativ fordert?

(1.3.18) Das Kommutativgesetz gilt nicht für alle Verknüpfungen. Das Vektorprodukt im V^3 ist weder kommutativ noch assoziativ. Typisch für den Umgang mit diesen beiden Gesetzen ist, dass man bemerken sollte, wenn sie nicht gelten und dass man dann vertraute, aber ungerechtfertigte Termumformungen unterläßt.

3.1.3c **Neutrale Elemente** und Machos

(1.3.19) Ein wichtiger Begriff, der im Zusammenhang mit Verknüpfungen auftritt, ist der des neutalen Elementes. Bei einer Verknüpfung werden ja immer zwei Elemente zu einem neuen Element verbunden. Ein Element heißt nun neutral, wenn es bei diesem Verbindungsprozeß den Verknüpfungspartner in keiner Weise beeinflußt.

(1.3.20) Als **Definition:**

Sei $\top : M \times M \to M$ innere Verknüpfung. Ein Element E∈ M heißt *neutrales Element von* $\top$, wenn für alle x∈ M gilt $\boxed{E \top x = x \top E = x}$

Bemerkungen

- Die korrekte Zutatenformel muß "neutrales Element von $\top$" lauten, nicht etwa "von M", da ein und dieselbe Menge mehrere Verknüpfungen tragen kann und ein Element, das bezüglich der einen Verbindung neutral ist, muß es für die zweite noch längst nicht sein. So ist 1∈ ℝ neutral für die Multiplikation, nicht aber für die Addition.
- Weil wir nicht voraussetzen, dass unser $\top$ kommutativ ist, könnte es vorkommen, dass etwa e$\top$x=x für alle x gilt, nicht aber x$\top$e=x . Daher haben wir oben in der Definition **beide** Forderungen gestellt. Überlegen Sie sich jetzt selbst, wie ein "linksneutrales" und wie ein "rechtsneutrales Element" von $\top$ zu definieren ist.

Bisher haben wir immer gesagt: **Ein** neutrales Element und nicht etwa "das....". Denkbar ist ja zunächst durchaus, dass eine Verknüpfung mehr als ein neutrales Element besitzt. Der nächste Satz macht hierzu eine Aussage:

Sätzchen :	Falls $\top : M \times M \to M$ ein neutrales Element besitzt, so ist dieses **eindeutig**

(1.3.22) D.h. man darf immer sagen: **Das** (eventuelle) neutrale Element von T. Ein weiteres kann es nicht geben. Diese Eindeutigkeit muß wegen des Satzes bei konkreten Verknüpfungen nie inhaltlich verifiziert werden. Sie folgt stets automatisch, was Arbeitsersparnis bedeutet. Man muß immer nur nach einem neutralen Element suchen und sofern es eines gibt, ist es einzig.

(1.3.23) **Beweis**: Angenommen E und F sind beide neutral (bezüglich $\top$). Dann gilt (mit x=F) einerseits E$\top$F=F , da E neutral ist. Andererseits folgt für x=E auch E$\top$F=F, da F neutral ist. Zusammen ergibt sich E = F wie gewünscht.

(1.3.24) Es gibt daher immer höchstens ein neutrales Element. Sobald man eines gefunden hat, ist es das neutrale Element (von $\top$).

□ Versuchen Sie jetzt, den Beweis für "linksneutral" zu verallgemeinern. Das geht nicht. Und tatsächlich kann es vorkommen, daß eine Verknüpfung mehrere linksneutrale Elemente besitzt. Versuchen Sie, ein Beispiel zu konstruieren.

□ Der Begriff des neutralen Elementes drückt eine bestimmte Eigenschaft - nämlich "wirkungsneutral" - aus, die ein Element haben kann. Versuchen Sie einmal eine Definition für ein Element mit genau gegenteiliger Eigenschaft also Wirkungsdominanz - zu geben. (Man könnte ein solches Element oder Chauvi oder Macho nennen). Können Sie ein Beispiel eines solchen Machoelementes finden? Zumindest eine Beispiel ist sehr bekannt.

3.1.3d Inverse Elemente

(1.3.25) Ein wichtiger Begriff, der sich direkt an den des neutralen Elementes anschließt, ja diesen benötigt, ist der des inversen Elementes. Genauer: **invers zu einem gegebenen Element.** D.h. bei der Verknüpfung eines Elementes mit seinem Inversen werden beide Elemente neutralisiert. Sie "heben sich gegenseitig auf ".

(1.3.26) In diesem Fall entfalten wir den Begriff in unserer Definition gleich vollständig:

Es sei $\top : M \times M \to M$ eine innere Verknüpfung.
Diese Verknüpfung besitze ein neutrales Element E. Weiter sei
x ein Element von M.
Dann heißt ein Element $\overline{x}_L$ aus M *ein Linksinverse zu x* (bezüglich x)
falls $x \top \overline{x}_L = E$ gilt.
Weiter heißt ein Element $\overline{x}_R$ aus M *ein Rechtsinverses zu x* (bezüglich $\top$),
falls $\overline{x}_R \top x = E$ gilt.
Und ein Element $\bar{x}$ aus M heißt *Inverses zu x* (bezüglich T), falls gilt
$x \top \bar{x} = \bar{x} \top x = x$

(1.3.27) Bei "invers" muß immer das zugehörige Bezugselement mit angegeben werden. Also etwa: "-3 ist Inverses zu 3 bezüglich der Addition in $\mathbb{R}$ " . Das geschieht in der Regel über die Bezeichnung. So schreibt man -x dafür, wenn das Verknüpfungsymbol + genommen wird und x^{-1} oder $\frac{1}{x}$ bei Multiplikation.

Allgemein gilt: Wenn die Verknüpfung kommutativ ist, dann ist es unnötig, zwischen den drei Arten von Inversen zu unterscheiden.

Noch Beispiele zum korrekten Gebrauch dieser Begriffe: Bezüglich der Multiplikation in $\mathbb{R}$ ist 1 das neutrale Element und $\frac{1}{3}$ das Inverse zu 3. Überdies ist 1 sein eigenes Inverses. Dasselbe gilt für -1.

(1.3.28) Beachten Sie, dass immer gilt: Jedes neutrale Element ist sein eigenes Inverses!

(1.3.29) Und wie steht es hier mit allgemeingültigen Beziehungen zwischen den Begriffen?

Sätzchen: $\top$ sei assoziative Verknüpfung von M und x$\in M$.
x besitze ein Linksinverses $\bar{x}_L$ und ein Rechtsinverses $\bar{x}_R$.
Dann gilt $\bar{x}_L = \bar{x}_R$ und dies ist ein Inverses zu x.
Überdies ist dies Inverse eindeutig. Schließlich gilt $\bar{\bar{x}} = x$.
D.h. x ist das Inverse zu $\bar{x}$.

Das alles sind Eigenschaften, die einem vom Umgang mit reellen Zahlen vertraut sind : Minus * Minus = Plus oder 1 durch 1/3 gleich 3. Neu ist, dass die Eigenschaften sehr viel allgemeiner gelten, dass es nur auf die Struktur ankommt. Allerdings setzen wir dabei voraus, dass unsere Verknüpfung assoziativ ist. Andernfalls funktioniert der Beweis nicht.

(1.3.30) **Beweis:** Zunächst der erste Punkt, also die Gleichheit der beiden Inversen.

$$\bar{x}_R = E \top \bar{x}_R = (\bar{x}_L \top x) \top \bar{x}_R = \bar{x}_L \top (x \top \bar{x}_R) = \bar{x}_L \top E = \bar{x}_L.$$

Die gewünschte Gleicheit ergibt sich wirklich. Beachten Sie, dass wir alle unsere Voraussetzungen einschließlich der Assoziativität benutzt haben. Die beiden anderen Behauptungen werden analog bewiesen. Wir empfehlen den Beweis als Ubung.

(1.3.31) Will man also nachweisen, dass ein Element a ein Inverses besitzt, so genügt es, zu zeigen, dass es ein Links- und ein Rechtsinverses besitzt. Diese beiden Elemente sind dann bei assoziativer Verknüpfung notwendig einander gleich. Ist die Verknüpfung sogar kommutativ, so genügt es, wenn man ein einziges einseitiges Inverses findet.

(1.3.32) Beispiel: Sei A nichtleere Menge und $\mathcal{P}$(A) die zugehörige Potenzmenge mit den beiden inneren Verknüpfungen Durchschnitt und Vereinigung. Beide sind offensichtlich kommutativ und assoziativ. Ebenso existiert in jedem Fall ein neutrales Element. Bei der Vereinigung hat man ja stets $T \cup \emptyset = T$. d.h. die leere Menge ist neutral. Und beim Durchschnitt gilt T∩A =T für jede Teilmenge T von A. D.h. hier ist die gesamte Menge neutral. Dagegen gibt es kaum inverse Elemente. Denn X∩T=A hat nur für X=A eine Lösung und X∪T=B hat nur für T=B eine Lösung! Überdies ist $\emptyset$ bezüglich ∩ und A bezüglich ∪ ein Element mit Machoeigenschaft. So ist etwa immer $A \cap \emptyset = \emptyset$.

3.1.3e Die Distributivgesetze

(1.3.34) Damit haben wir das wichtigste begriffliche Rohmaterial für unsere algebraischen Strukturen eingeführt. Zumindest soweit es sich auf eine einzige Verknüpfung bezieht. Hat man dagegen eine Menge mit zwei inneren Verknüpfungen vorliegen, so benötigt man noch weitere Gesetzmäßigkeiten, die die Verbindung zwischen diesen beiden Verknüpfungen regeln. Das geschieht in den meisten Fällen durch die Distributivgesetze.

□ Formulieren Sie diese Gesetze selbst allgemein für zwei Verknüpfungen - sagen wir $\intercal$ und $\perp$ - und überlegen Sie sich, wie der daran anschließende Satz (über Konsequenzen der Gültigkeit der Distributivgesetze) wohl aussieht. Denken Sie dabei an das Rechnen mit reellen Zahlen und die dortigen Verknüpfungen + und ·. Der Beweis wäre wieder mit Induktion zu erbringen.

Hinzu kommt, dass jedes Distributivgesetz eine hierarchische Ordnung der beiden beteiligten Verknüpfungen verlangt: Die eine Verknüpfung erhält die Rolle von + und die andere die Rolle der Multiplikation. Man kann die Rollen nicht einfach vertauschen. (Welche falsche Regel ergibt sich bei Rollentausch für die reellen Zahlen?) Diese Hierarchie wird gerne mit Hilfe einer KlammerersparnisregeI vom Typ "Punktrechnung vor Strichrechnung" ausgedrückt.

(1.3.36) Die Formulierung der allgemeinen Konsequenzen der Distributivgesetze in Form von Formeln erweist sich als etwas mühsamer. Sinnvoll ist es, dazu die Summenzeichensymbolik (für die jeweiligen Verknüpfungen) zu verallgemeinern. Die Distributivgesetze selbst und ihre elementaren Konsequenzen werden wir von jetzt ab als bekannt voraussetzen.

3.1.4 Die Verknüpfungstafel
Ein Hilfsmittel zur Veranschaulichung von Kompositionen.

(1.4.1) Für kleine endliche Mengen lassen sich die inneren Kompositionen gut vom Feldstandpunkt aus darstellen. Hat M gerade n Elemente, so ergibt die Menge M×M eine Matrixfeld von n Zeilen und n Spalten, in das man die Verknüpfungsresultate eintragen kann. Es folgt ein willkürliches Beispiel für die Menge M=(a,b,c).

$\intercal$	a	b	c
a	a	a	c
b	b	a	c
c	c	c	a

Beispielsweise gilt:
$a \intercal b = a$
$b \intercal a = b$
$c \intercal c = a$

(1.4.2) Manche Eigenschaften der Verknüpfung lassen sich mit solch einer Tafel sofort veranschaulichen. Ein neutrales Element etwa ist daran zu erkennen, dass die Randzeile reproduziert wird. Im Beispiel ist das Element a fast neutral, nur die erste Zeile stört. Wäre a neutral, müßte a$\intercal$b=b gelten und nicht a$\intercal$b=a. Ebenso kann man das Kommutativgesetz und das Vorhandensein eines Inversen leicht überprüfen oder wahrnehmen.

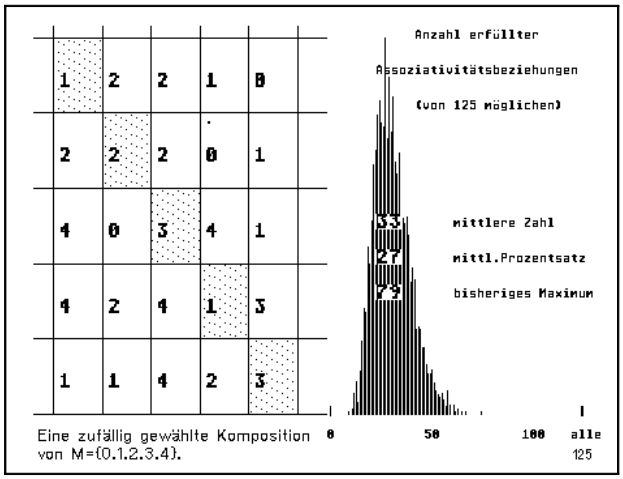
Die Prüfung der Assoziativität ist mühsamer, da sie zweifache Anwendung der Tafel verlangt. Ein solcher direkter Nachweis wird auch kaum je benötigt. Wir werden bessere Methoden kennenlernen.

(1.4.3) Man kann das Beispiel kleiner endlicher Mengen verwenden, um etwas über die Häufigkeit der Gültigkeit des Assoziativgesetzes herauszubekommen. Nehmen wir eine fünfelementige Menge. M×M hat dann 25 Elemente. Somit gibt es $5^{25} \approx 10^{17}$ innere Verknüpfungen oder Möglichkeiten, die zugehörige Verknüpfungstafel zu bilden. Das ist bereits eine riesige Zahl. Wieviele dieser Verknüpfungen sind assoziativ? Der Einschub zeigt die Resultate eines zugehörigen Computerexperimentes.

(1.4.4) ■ ■ ■ ■ ■

Zur Häufigkeit von Assoziativbeziehungen in der Menge aller Kompositionen.

3000 innere Verknüpfungen der Menge M={0,1,2,3,4} wurden vom Computer zufällig ausgewählt. Dann wurde jeweils ausgezählt, wieviel der insgesamt 125 möglichen Assoziativitätsrelationen von der Verknüpfung erfüllt wurden. Die zugehörige Verteilung ist aufgetragen. Einige Relationen sind trivialerweise immer erfüllt. Im Mittel waren 33 Relationen erfüllt. In einem einzigen Fall waren es 79, was noch weit entfernt ist von der erforderlichen Gesamtzahl von 125. Die Gültigkeit des Assoziativitätsgesetzes ist offenbar eine sehr seltene Eigenschaft in der Menge aller Verknüpfungen von M.



■■■■■

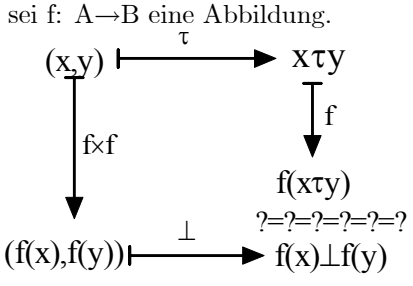
3.1.5 Strukturerhaltende Abbildungen

(1.5.1) Alle bisher eingeführten Begriffe dienen dazu, die Eigenschaften einzelner Objekte (=Mengen) mit algebraischer Struktur zu beschreiben. Aber wie steht es damit, wenn wir mehrere Objekte mit einer algebraischen Struktur haben und diese miteinander vergleichen wollen? Dazu benötigen wir Beziehungen, also Abbildungen. Was entspricht einander, was ist anders? Zur Behandlung dieses wichtigen Problemkreises dienen die *strukturerhaltenden Abbildungen*. Sie haben für die Analyse der algebraischen Strukturen eine überragende Bedeutung.

(1.5.2) Worum es dabei geht, ist leicht zu erklären:

Gegeben seien zwei Mengen G und H mit je einer inneren Verknüpfung.
$\top : G \times G \to G$ und $\perp : H \times H \to H$. Schließlich sei f: A→B eine Abbildung.

Dann heißt f strukturerhaltend ,
falls für **alle** x,y$\in G$ gilt:
$f(x \top y) = f(x) \perp f(y)$.
Das Diagramm zeigt die Bedeutung dieser Gleichung, die auch als Gleichheit zweier Automatenschaltungen interpretiert werden kann.

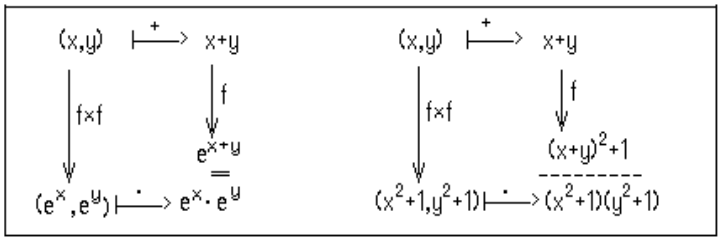


(1.5.3) Startet man mit zwei Elementen x,y aus G, so gibt es zwei Wege, um zu einem Verknüpfungsresultat in H zu gelangen. Das Diagramm zeigt die beiden Möglichkeiten auf. Die Resultate werden in der Regel unterschiedlich sein. Nur in ganz speziellen Fällen wird stets dasselbe herauskommen und das ist gerade die Forderung der gegebenen Definition.

(1.5.4) Man kann die Definition auch rein schematisch so interpretieren, dass sie es gestattet, die Von-Klammer in f(x⊤y) aufzulösen. Viele Anfänger ohne mathematisches Strukturverständnis besitzen ein intuitives Gefühl für den Wert dieser Regel und wenden sie unzulässigerweise an. Beliebt ist die Bruchrechenformel $\frac{1}{a+b}=\frac{1}{a}+\frac{1}{b}$ mit der immer wieder bequem schöne, aber leider falsche Resuttate produziert werden. (Dabei ist $\top = +$ und f(x)=$\frac{1}{x}$.) Oder man rechnet $\sqrt{a+b} = \sqrt{a} + \sqrt{b}$ usw.

(1.5.5) Die meisten Abbildungen G→H werden die besprochene Eigenschaft nicht haben. Die seltenen, die sie besitzen, erweisen sich dann als ein bssonders nützliches Handwerkszeug.

(1.5.6) Zwei Beispiele: Als Mengen wählen wir $\mathbb{R}$ mit der Verknüpfung + und $\mathbb{R}_+ =]0, \infty[$ mit der Verknüpiung $\cdot$. Kurz $(\mathbb{R},+)$ und $(\mathbb{R},\cdot)$ Hierzu definieren wir zwei Abbildungen $\mathbb{R} \to \mathbb{R}$ nämlich f=($\mathbb{R}$,x↦e^x,$\mathbb{R}$) und g=($\mathbb{R}$,x↦ $x^2 + 1, \mathbb{R}$). Wie sehen die Diagramme daann aus?

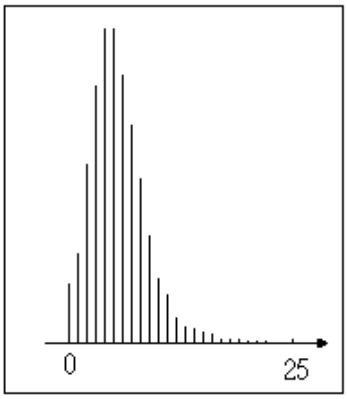


Im ersten Fall stellt eine der Rechenregeln für die Exponentialfunktion sicher, dass beide Rechenwege, beide Wege im Diagramm, dasselbe Resutat liefern. Die Abbildung exp ist strukterhaltend. Im zweiten Fall erhält man unterschiedliche Ergebnisse.

Nur für einige Ausnahmewerte wie etwa (x,y)=(2,1) ergeben beide Resultate dasselbe.

(1.5.7) Welche Konsequenzen die Eigenschaft *strukturerhaltend* hat, werden wir später in einer Unzahl von Fällen besprechen. Vgl. Kap. 4.

(1.5.8) Auch die strukturerhaltenden Abbildungen sind relativ selten. Die wiedergegebene Verteilung gibt das Resultat eines zugehörigen Computerexperimentes.



10.000 Verknüpfungen von
M={0,1,2,3,4} zufällig gewählt.
Dazu jeweils eine Abbildung M→ M.
Wieviele der 25 möglichen Struktur-
relationen sind jeweils erfüllt?
Die zugehörige Verteilung.

Die Zahl der Fälle ab 18 ist 15/8/2/1/3/0/0/6. D.h.in 6 Fällen gab es volle Strukturerhaltung, in drei Fällen waren 22 der Relationen erfüllt usw.

3.2 Das System der algebraischsn Strukturen (1)

3.2.0 Die schematische Einführung einer algebraischen Struktur

(2.0.1) Nachdem wir das Rohmaterial - den Begriffsapperat - eingeführt haben, beginnen wir mit der Besprechung konkreter algebraischer Strukturen. Dazu führen wir das in (1.2.2) Gesagte genauer aus.

(2.0.2) Die Einführung einer algebraischen Struktur erfolgt in 5 typischen Schritten, die wir mit $\alpha - \varepsilon$ bezeichnen:

α)	Gewisse Mengen werden vorgegeben.
β)	Für diese Mengen werden bestimmte Kompositionen eingeführt.
γ)	Durch Axiome für die Verknüpfungen werden Eigenschaften festgelegt.
δ)	Die (zugehörigen) strukturerhaltenden Abbildungen werden eingeführt.
ε)	Übertragungsprobleme werden behandelt.

(2.0.3) Die letzten Schritte δ) und ε) gehören bereits zur Analyse der Struktur. Sie sind jedoch einerseits recht wichtig und lassen sich andererseits weitgehend schematisch behandeln. Daher ziehen wir sie als Routineaufgaben mit in die Einführung der Strukturen hinein. Was ε) genauer beinhaltet, werden wir später ausführlich beschreiben.

Als organisierende Prinzipien für die algebraischen Strukturen können und werden wir zuerst die **Anzahl der beteiligten Mengen** - meist 1 oder 2 - und dann verfeinernd die **Anzahl der Verknüpfungen** heranziehen.

3.2.1 Gruppen und Halbgruppen

(2.1.1) Wir beginnen mit dem einfachsten Fall: Eine Menge mit einer Verknüpfung. Die Forderungen der Schritte $\alpha) - \varepsilon)$ kennzeichnen wir in naheliegender Weise:

Definition:	(H.α)	**Sei** H eine nicht leere Menge
	(H.β)	mit einer Verknüpfung $\intercal : H \times H \to H$, für die gilt:
	(H.γ)	$\intercal$ ist assoziativ.
	Dann	nennt man eine Menge mit dieser Struktur eine
		Halbgruppe. Symboliche Bezeichnung (H,$\intercal$).

(2.1.2) Beispiele: (ℕ,+) und (ℕ,·) sind typische Halbgruppen. Dagegen ist (ℕ,-) keine Halbgruppe, da beispielsweise 3-5 nicht mehr in ℕ liegt.

Die in (1.2.7) eingeführte Verknüpfung *Hintereinanderschreiben der Worte* macht aus der Wortmenge WA eine Halbgruppe. Die (zu überprüfende!) Assotiativität ist hier trivial. Ebenso sind $(\mathcal{P}(a), \cup)$ und $(\mathcal{P}(a), \cap)$ Halbgruppen.

Sei M eine Menge und $\mathfrak{F}$(M,M) die Menge aller Abbildungen von M nach M. Dann liefert die Zusammensetzung $\circ$ eine innere Verknüpfung, die als Hintereinanderschaltung der Zuordnungen stets assoziativ ist. Also ist ($\mathfrak{F}$(M,M),$\circ$) eine Halbgruppe! Damit haben wir bereits eine ganze Reihe von Beispielen von Halbgruppen!

(2.1.3) Wir können jetzt kurz skizzieren, wie man üblicherweise das Assoziativgestz prüft.

Sei (A,$\intercal$) die zu untersuchende algebraische Struktur und (H,$\circ$) eine bereits bekannte Halbgruppe, etwa eine vom Typ ($\mathfrak{F}$(M,M),$\circ$). Jetzt versucht man die Elemente von A als Elemente von H darzustellen, etwa als Abbildungen A$\to H$. Genauer versucht man eine injektive Abbildung f:A→H zu finden, **die überdies strukturerhaltend** ist. Nach der Terminologie aus Kap.1.2 ist das eine Abbildung vom Darstellungstyp. Manchmal interpretiert man sie sogar als Identifizierungsabbildung, so dass man M als Teilmenge von H ansieht. Nochmals: Wichtig ist, daß f injektiv und strukturerhaltend ist.

(2.1.4) **Satz:**

Sei (M,$\intercal$) Menge mit einer inneren Verknüpfung und(H,$\circ$) eine Halbgeruppe.
Weiter sei f:M→H strukturerhaltend und injektiv.
Dann ist $\intercal$ assoziative Verknüpfung.

(2.1.5) Beweis: Für a,b,c$\in M$ rechnen wir wie folgt:

$$\begin{aligned} f((a \;\top\; b) \top c) = f(a \top b) \circ f(c) = (f(a) \circ f(b)) \circ f(c) \overset{(a)}{=} f(a) \circ (f(b) \circ f(c)) \\ = \; f(a) \circ (f(b \top c)) = f(a \top (b \top c)) \end{aligned}$$

Der Schritt (a) in der Mitte benutzt die Assoziativität von $\circ$. Die übrigen die Strukturerhaltung von f. Nun ist f injektiv, also folgt (a$\top$b)$\top$c=a$\top$(b$\top$c) für alle Elemente nach der üblichen Denkfigur für injektive Abbildungen aus Kap.I.2.10.

Der Satz, bzw. die damit verbundene Methode erweist sich als überaus nützlich. Für H nimmt man sehr gerne eine der Halbgruppen vom Typ $\mathfrak{F}$(A,A).

(2.1.6) Die Halbgruppenstruktur ist strukturell meist noch zu arm, um besonders interessant zu sein. Die eigentlich interessante Struktur folgt erst nach Hintunahme weiterer Axiome. (Beim Durcharbeiten der nachfolgenden Teile ist es vielfach nützlich, sich selbst zu fragen: Gilt das auch für eine Halbgruppe? Wieso nicht?)

(2.1.7) Definition

Sei	(G,$\top$) eine Halbgruppe (Forderungen G.α) – ($G.\gamma$1), für die zusätzlich gilt:
(G.γ2)	Es gibt ein bezüglich $\top$ neutrales Element
(G.γ3)	Jedes g$\in G$ besitzt ein inverses Element
Dann	heißt G bzw. genauer (G,$\top$) eine *Gruppe.*
	Gilt zusätzlich das Kommutativgesetz (G.γ4), dann heißt die Gruppe *kommutative oder Abelsche Gruppe.*

Kurz: Eine Gruppe ist eine Menge mit assoziativer Verknüpfung, einem neutralen Element derart. daß jedes Element ein Inverses besitzt!

(2.1.8) ($\mathbb{Z}$,+), ($\mathbb{R}$,+) , ($\mathbb{R}$-{0},$\cdot$) und ($\mathbb{C}$,+) sind Gruppen, wie man sofort verifiziert. Sie sind alle kommutativ. Das sind vertraute Beispiele, wobei jedoch darauf zu achten ist, dass etwa bei ($\mathbb{R}$-{0},$\cdot$) nur die Multiplikation, nicht aber die Addition zulässig (verfügbar) ist. Die Addition ist bei der betrachteten Struktur zu vergessen.

(2,1.9) Das nächste sehr wichtige Beispiel dürfte weniger vertraut sein:

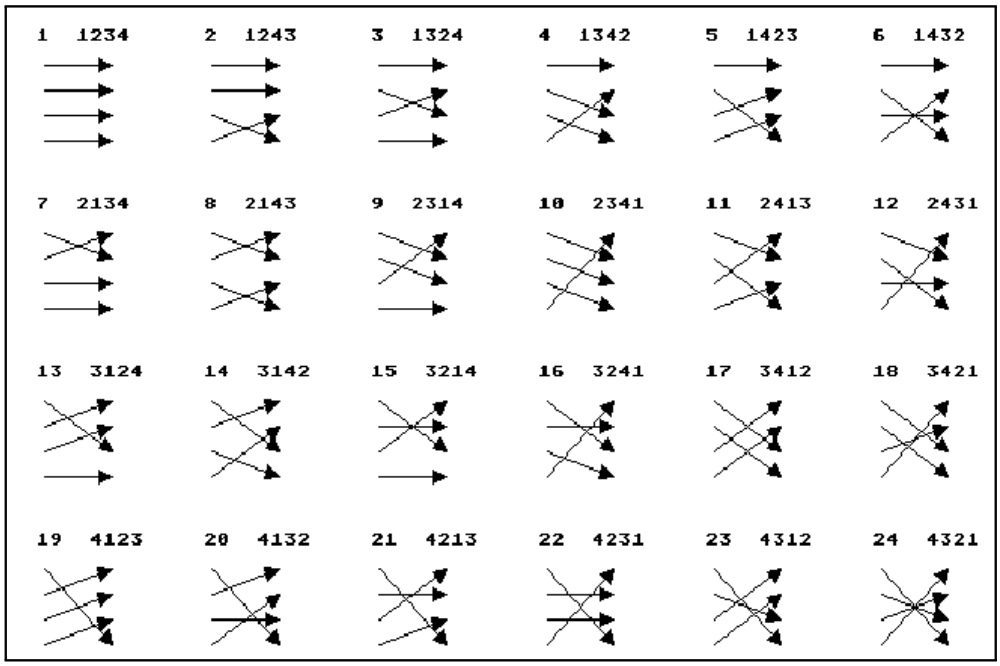
Es sei M eine nicht leere Menge und $\mathfrak{B}$(M,M) die Menge aller bijektiven Abbildungen M$\rightarrow$M. Als Verknüpfung nehmen wir die Zusammensetzung $\circ$ von Abbildungen. Die ist konstruktionsgmäß immer assoziativ. Die triviale Abbildung id_M ist bezüglich $\circ$ neutral und die inverse Abbildung übernimmt hier die Rolle des inversen Elementes. **Also ist** ($\mathfrak{B}$(M,M),$\circ$) **eine Gruppe,** die wir auch *die Permutationsgruppe von M* nennen. Für #(M)>2 ist diese Gruppe nicht kommutativ.

(Beachten Sie, wie der Text aus (2.1.9) schrittweise die Gruppenaxiome fallspezifisch konkretisiert hat! Das ist das übliche Routinevorgehen!)

□ Welchen Nutzen hat Satz (1.3.29) beim Prüfen der Gruppenaxiome?

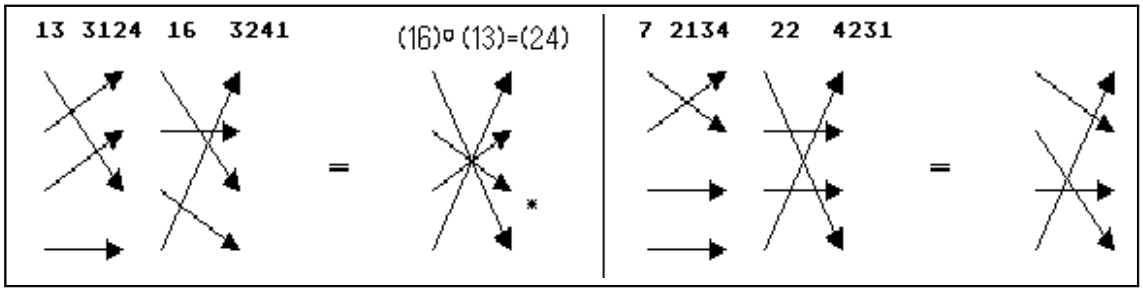
(2.1.10) Als Beispiel zeigen wir nachfolgend die 4!=24 Elemente der Permutationsgruppe für vierelementige Mengen. Wir nehmen M={1,2,3,4}. Wir geben die Gruppenelemente einmal als Pfeilschema und überdies vom Feldstandpunkt. (Also vier Feldplätze und darauf jeweils die zugeordnete Zahl aus der

Urbildmenge (1.2,3,4).



Bitte beachten Sie auch, dass und wie die Permutationen im Bild systematisch angeordnet sind.

(2.1.11) Da jedes Element eine Abbildung ist, erhält man die Produkte durch Verkoppeln der Pfeilschemata. Das nächste Bild zeigt zwei Beispiele. Mit der Numerierung des ersten Bildes folgt (16)∘(13)=(24) und (22)∘(7)=(12). (Bitte die Reihenfolge beachten, ∘ ="nach").



☐ Prüfen Sie selbst nach, dass (13)∘(16)=(8) ist, so dass die Gruppe nicht kommutativ ist.

☐ Welche Lösungen haben die beiden Gleichungen (16)∘x = (17) und x∘(16) = (17)?

(2.1.12) Die gewählte Zahlindizierung der Elemente ist willkürlich und wenig aussagekräftig. Sie ist höchstens für den Augenblick bequem. Insbesondere bezeichnet (1) das neutrale Element. Später werden wir eine weitaus bessere Codierung der einzelnen Permutationsabbilidungen kennenlernen.

Elemente wie (7) oder (8) sind ihr eigenes Inverses! Bei einigen anderen muß man suchen. So ist das Inverse zu (23) gerade (18).

☐ Zur Übung sollten Sie entsprechend die Permutationsgruppen für 2 und für 3 Elemente aufstellen. (Die Permutationsgruppe für n Elemente hat generell n! Elemente.)

(2.1.13) Damit besitzen wir einen ersten Satz von Beispielen für die Gruppenstruktur. Weitere kommen später hinzu. Zur **Bezeichnung**:

Ist M endlich mit n elementen, typischerweise M={1,2,...,n}, dann nennt man die zugehörige Permutationsgruppe *die symmetrische Gruppe von n Elementen.* Als Bezeichnung verwenden wir $\mathfrak{S}_n$.

3.2.la Formulierbare und lösbare Gleichungen

(2.1.14) Wir haben einleitend gesagt, dass Gleichungen einen Ausgangspunkt der algebraischen Strukturen bildeten. **Was für Gleichungen kann man nun in einer Gruppen- oder auch Halbgruppenstruktur formulieren**? Beachten Sie: *formulierbar* ist keineswegs dasselbe wie *lösbar.* Da wir nur **eine** Verknüpfung haben, sind Bestimmungsgleichungen der folgenden Arten möglich:

(2.1.15) In Gruppen und Halbgruppen formulierbare Gleichungen:

(1) a⊺x=b	(2) x⊺a=b	(3) a⊺x⊺b=c	(4) x⊺x=a	(5) x⊺a⊺x=b

Dabei sind a,b,cεG äußere Parameter und x ist Unbestimmte. Gegeben sind Beispiele formulierbarer Gleichungen. In (3) und (5) sind wegen der Assoziativität Klammern fortgelassen!

(2.1.16) Während man in einer Halbgruppe jeden Fall für jede Halbgruppe einzeln und gesondert untersuchen muß, gilt für eine Gruppe: Die Gleichungen (1)-(3) sind alle eindeutig lösbar und man kann eine zugehörige Lösungsformel herleiten. Solange das Kommutativitätsgesetz nicht gilt, muß man zwischen (1) und (2) und (3) unterscheiden.

Betrachten wir als Beispiel (1). Also a⊺x=b. Wir nehmen an, dass eine Gruppe vorliegt. Dann hat a∈G ein inverses Element, das wir mit a^{-1} bezeichnen. Damit multiplizieren wir beide Seiten der Gleichung von links und finden

a⊺x=b	Ausgangsgleichung
$a^{-1} \intercal (a \intercal x) = a^{-1} \intercal b$	Multiplikation
$(a^{-1} \intercal a) \intercal x = a^{-1} \intercal b$	Assoziativität
$e \intercal x = a^{-1} \intercal b$	*Invers.* e bezeichne neutrales Element.
$x = a^{-1} \intercal b$	e ist neutral.

Von oben nach unten gelesen ergibt das einen einzigen Kandidaten für eine Lösung der Ausgangsgleichung. Beachten Sie, dass alle Gruppeneigenschaften benutzt wurden!. Man kann jetzt aber auch unten starten und die letzte Gleichung als Definition von x$\in G$ nehmen (Rolle Hilfsgröße). Dann kommt man mit den entsprechenden (inversen) Operationen zurück zur ersten Gleichung und sieht, dass x die Gleichung erfüllt! D.h. Gleichung (1) hat genau eine Lösung und die wird durch x=$a^{-1} \intercal b$ gegeben.

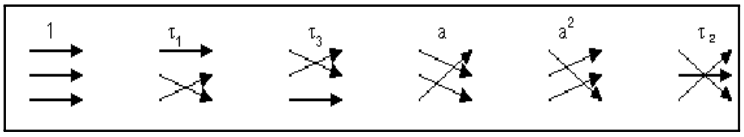
Im Fall einer Halbgruppe hätten wir bereits den ersten Schritt (Existenz von a^{-1}) nicht sicherstellen können.

□ Für die Gleichungen (2) und (3) findet man entsprechend Lösungsformeln, die Sie selbst herleiten sollten. Nur: Vertauschen von Faktoren ist nicht zulässig! Bei Beachtung dieser Vorsichtsmaßnahme kann (und sollte) man die Lösungsformel sofort hinschreiben.

□ Wie steht es mit der Lösbarkeit von a+x=b in (ℕ,+). Welche Gleichungen sind in der Halbgruppe der Worte lösbar?

(2.1.17) Hinsichtlich der Lösbarkeit von Gleichungen wie (4) oder (5) läßt sich auch für Gruppen nichts Allgemeines sagen. Treten solche Gleichungen auf, kann man nur versuchen, die zugehörige Lösungsmengen fallspezifisch zu finden.

(2.1.18) Die Lösbarkeit einfacher Gleichungen läßt sich gut diskutieren, wenn man die Verknüpfung vom Feldstandpunkt aus darstellt, also mit Hilfe der in (1.4.1) eingeführten Verknüpfungstafel. Für kleine Mengen ist das sehr einfach. Wir wählen als Beispiel die Permutationsgruppe für 3 Elemente. Die Gruppe hat dann 6 Elemente in Form von 6 (bijektiven) Abbildungen {1,2,3}→{1,2,3}. Diese benennen wir nicht willkürlich, sondern strukturgerecht. τ_2 besagt, dass das Element 2 festbleibt und die beiden anderen vertauscht werden. a^2 steht für a∘a, wie man sofort nachprüft.



Die Verknüpfung vom Feldstandpunkt: Der Wert x∘y ist im zugehörigen Feldpunkt aufgetragen. Etwa τ_1∘a=τ_2. Mit der Tafel kann man Gleichungen des Typs u∘$x = v$ unmittelbar lösen. Beispiel: $\tau_1 \circ x = a$. Gehe dazu in die Zeile τ_1. Suche nach a. Der Spaltenwert τ_2 ergibt die Lösung x.

Verknüpfungs- oder Gruppentafel der Permutationsgruppe von drei Elementen.

x\y	1	a	a^2	τ_1	τ_2	τ_3
1	1	a	a^2	τ_1	τ_2	τ_3
a	a	a^2	1	τ_3	τ_1	τ_2
a^2	a^2	1	a	τ_2	τ_3	τ_1
τ_1	τ_1	τ_2	τ_3	1	a	a^2
τ_2	τ_2	τ_3	τ_1	a^2	1	a
τ_3	τ_3	τ_1	τ_2	a	a^2	1

(2.1.19) Betrachten wir die Zeilen der Gruppentafel, so sehen wir, dass stets alle Gruppenelemente **genau einmal** vorkommen. Das gibt den (bereits bewiesenen) Sachverhalt wieder, dass in einer Gruppe

alle Gleichungen A∘x=B eindeutig lösbar sind. Auch alle Spalten enthalten die Gruppenelemente genau einmal. Und die Spalten liefern offenbar die Lösungen der Gleichung x∘A=B. In der Diagonalen dagegen stehen die Quadrate x∘x. In unserem Fall ist x∘x=a lösbar durch x=a^2. Dagegen ist x∘x=τ_1 unlösbar, denn dieses Element taucht in der Diagonalen nie auf. Und x∘x=l hat in dieser Gruppe 4 Lösungen ("vier Einheitswurzeln").

(2.1.20) Fassen wir zusammen: Bei einer Gruppe müssen in der Verknüpfungstafel alle Elemente in jeder Zeile und in jeder Spalte genau einmal auftreten. Bei einer Halbgruppe dagegen muß das keineswegs der Fall sein.

☐ Angenommen Sie haben eine Verknüpfungstafel, bei der jedes Element in jeder Zeile und in jeder Spalte genau einmal auftritt. Liegt dann eine Gruppe vor?

(2.1.21) Jetzt betrachten wir folgendes Problem: Es sei (G,·) Gruppe und g,h∈ G. Wir nehmen an, dass wir die Inversen Elemente g^{-1} und h^{-1} kennen. Was läßt sich dann über das inverse Element von g·h aussagen? Das inverse Element zu k∈ G ist Lösung der Gleichung k·$x = e$. Also müssen wir (g·h) · $x = e$ lösen. Die in diesem Abschnitt beschriebenen Methoden liefern sofort x=$h^{-1} \cdot g^{-1}$. D.h. es gilt:

Es sei g,h∈G. Dann gilt $(g\tau h)^{-1}=h^{-1}\tau g^{-1}$

Beachten Sie die Umkehrung der Reihenfolge der Faktoren! Das Resultat wird beim Rechnen immer wieder benötigt.

☐ Führen Sie den Beweis im Detail durch. Achten sie dabei darauf, wie die Umkehrung der Reihenfolge zustande kommt. Wann kommt es auf die Reihenfolge nicht an?

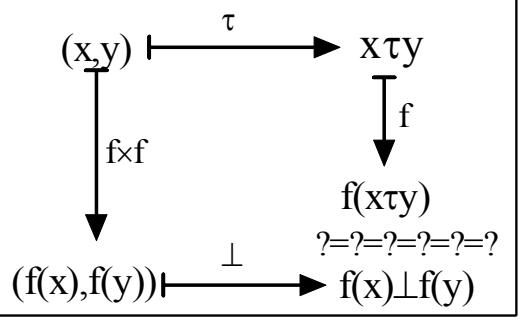
☐ Was ist, wenn Sie mit der Gleichung x·$k = e$ anstelle von k·$x = e$ starten?

3.2.lb Gruppenhomomorphismen

(2.1.21) Wir kommen jetzt zu den **strukturerhaltenden Abbildungen** *für Gruppen,* also zu Schritt δ unseres allgemeinen Schemas (2.0.2). Da wir jeweils nur eine innere Verknüpfung haben, können wir die allgemeine Definition einfach übernehmen. Die strukturerhaltenden Abbildungen erhalten meist Namen, die für die jeweilige Struktur spezifisch sind.

(2.1.22) Im Fall der Gruppen sieht das wie folgt aus:

Definition: Es seien (G,τ) und (H,$\perp$) Gruppen.
Weiter sei f:G→ H eine Abbildung.
Dann heißt f *Gruppenhomomorphismus (von G nach H)*, wenn für **alle** x,y∈ G gilt
$f(x\tau y) = f(x)\perp f(y)$



(2.1.23) Das Beispiel exp aus (1.5.6) ist ein Gruppenhomomorphismus von $(\mathbb{R}, +)$ nach $(\mathbb{R}_+, *)$. Wichtig ist, dass man die Strukturerhaltung wiedererkennt, auch wenn die Verknüpfungen anders bezeichnet sind. Im Falle einer kommutativen Verknüpfung benutzt man vielfach ein + (Additive Schreibweise). Oder aber man bezeichnet beide Verknüpfungen durch ein · , auch wenn sie verschieden sind (multiplikative Schreibweise). Das sieht dann so aus:

f(x+y)=f(x)+f(y)	additive Schreibweise
f(xy)=f(x)f(y)	multiplikative Schreibweise

(2.1.24) Wir formulieren und beweisen einige **erste Konsequenzen der Strukturerhaltung.** Sie werden ziemlich häufig in größeren Denkfiguren meist kommentarlos benutzt.

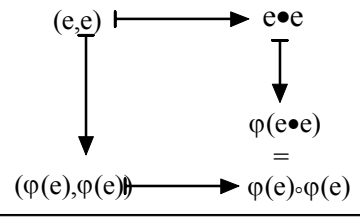
Es sei φ:G→ H ein Gruppenhomomorphismus von (G,·) nach (H,∘)
Weiter sei e das neutrale element von G und E das von H. Dann gilt:
a) $\varphi(e) = E$ Das Bild des neutralen Elements ist stets neutral.
b) $\varphi(x^{-1}) = (\varphi(x))^{-1}$. Das Bild des inversen Elementes ist das Inverse des Bildes.
c) Ist φ in E=$\varphi(e)$ injektiv, **dann ist** φ in allen Punkten **injektiv.**

(2.1.25) Beweise derartiger Aussagen erfolgen typischerweise über eine Kette von Gleichungen, wobei die Umformungen durch die Axiome oder bereits bewiesene Resultate gerechtfertigt werden. Vgl. etwa (1.3.31) oder (2.1.16). Im Falle von a) könnte das wie folgt aussehen, mit jeweils nebenstehender Begründung

$e \cdot e = e$	e neutral in G, gültige Gleichung. (G.γ2)
$\varphi(e \cdot e) = \varphi(e)$	Eindeutigkeit der Abbildung
$\varphi(e) \circ \varphi(e) = \varphi(e)$	Strukturerhaltung
$\varphi(e) = (\varphi(e))^{-1} \circ \varphi(e)$	Existenz und Eigenschaft des Inversen in H
$\varphi(e) = E$	Eigenschaft des Inversen (G.γ3)

Die letzte Gleichung folgt somit aus der ersten. Rechnungen dieser Art werden häufig klarer, wenn man sie im Diagramm interpretiert. Vergleichen Sie also obige Rechnung mit der jetzt folgenden Diagrammdarstellung:

Die sich ergebende Gleichung ist mit dem inversen Element von $\varphi(e)$ zu multiplizieren, das nach (G.γ3) existiert. Das gibt e=E wie in der Rechnung.



Der letzte oben durch (G.γ3) gekennzeichnete Schritt begründet sich genauer wie folgt: φ(e) ist Element der Gruppe H (Abbildungseigenschaft!), besitzt also ein Inverses (G.γ3), das wir mit $\varphi(e))^{-1}$ bezeichnen. Multipliziert man beide Seiten der vorletzten Gleichung von links mit diesem Element, wobei die Assoziativität (G.γ1) eingeht, so entsteht die letzte Gleichung, deren rechte Seite aber E ergibt. Überdies ist an (1.3.26) zu denken, was die Eindeutigkeit von E ergibt.

Diese ausführliche Darstellung vonm Punkt a) aus (2.1.24) zeigt die enorme Effizienz und Ökonomie der Symbolsprache!

(2.1.26) **Beweis zu b)**. Schreiben Sie die Gleichungskette selbst in Diagrammform um:

x$\cdot x^{-1} = e$	(G.γ3), gültig.
$\varphi(x \cdot x^{-1}) = \varphi(e) = E$	Abbildung, a)
$\varphi(x) \circ \varphi(x^{-1}) = E$	Strukturerhaltung
$\varphi(x^{-1}) = (\varphi(x))^{-1} \circ E = (\varphi(x))^{-1}$	(G.γ2, 3)

Aus der gültigen Startgleichung folgt das behauptete Resultat.

(2.1.27) **Beweis zu c)**. Zu zeigen ist $\varphi(x) = \varphi(y) \Rightarrow x = y$ Das ist die zu injektiv gehörige Denkfigur. Sei also $\varphi(x) = \varphi(y)$. Multiplikation (der beiden Seiten der Gleichung) mit $(\varphi(\mathrm{y}))^{-1}$ **von rechts in H** gibt:

$$\varphi(x) \circ (\varphi(y))^{-1} = \varphi(x) \circ \varphi(y^{-1}) = \varphi(x \cdot y^{-1}) = E = \varphi(e).$$

Hierbei wurden neben den Gruppenaxiomen die beiden bereits bewiesenen Resultate a) und b) benutzt und die Strukturerhaltung. Nun lautet die Voraussetzung in c) aber, dass φ in E injektiv ist, dass also nur e auf E abgebildet wird. Folglich muss xy^{-1}=e gelten und das gibt n

(2.1.28) Das letzte Resultat ist bemerkenswert: Die Homomorphie bewirkt, dass Injektivität im neutralen Element globale Injektivität - also für **alle** Elemente - nach sich zieht. Allgemein ist das keineswegs der Fall. So ist etwa x$\mapsto x^2$ in 0 injektiv, aber sonst in keinem Punkt der reellen Achse. Wir werden diese wichtige Eigenschaft später noch weiter ausführen. Sie begründet letztlich viele Denkfiguren der linearen Algebra.

3.2.2 Die Übertragung einer algebraischen Struktur

(2.2.1) Wir haben bereits mit der Eigenschaftsanalyse der Gruppenstruktur begonnen. Dabei sind gewisse Analyseschritte routinemäßig für jede algebraische Struktur durchzuführen. Die Einführung der

strukturerhaltenden Abbildungen gehört dazu und ebenso der jetzt zu besprechende Schritt ε aus dem Eingangsschema (2.0.2)

(2.2.2) Es sei (G,$\circ$) eine Gruppe. Dann haben wir in Kapitel 1 gesehen, dass man aus der Menge G durch die mengentheoretischen Operationen eine Reihe neuer Mengen bilden kann. Macht dann unsere Gruppenstruktur aus den Neubildungen auch eine Gruppe? Das ist unser Übertragungsproblem. Teilweise ist das tatsächlich der Fall und die so erhaltenen weiteren Gruppen erweisen sich als nützlich und benötigt.

(2.2.3) Wir nennen 6 mögliche Fälle, von denen wir anschließend einige, aber nicht alle, besprechen wollen.

	Übertragung der Gruppenstruktur
ÜT	(G,$\circ$) sei Gruppe und H$\subset G$ nichtleere **Teilmenge**. Kann man $\circ$ so einschränken, dass H zu einer Gruppe wird?
ÜK	Es seien (G,T) und (H,$\perp$) zwei Gruppen. Kann man dann das **kartesische Produkt** G×H zu einer Gruppe machen?
ÜP	Es sei (G,$\circ$) Gruppe. Kann man die **Potenzmenge** $\mathcal{P}(G)$ zur Gruppe machen?
ÜR	Es sei (G,$\circ$) Gruppe und P_G eine **Partition von G**. Kann man P_G zur Gruppe machen?
ÜA	Es sei (G,$\circ$) Gruppe und M eine Menge. Weiter sei $\mathcal{F}(M,G)$ **die Menge aller Abbildungen** M$\to G$. Kann man $\mathcal{F}(M,G)$ zur Gruppe machen?
ÜW	Es sei M Menge, (G,$\circ$) Gruppe und f:G$\to M$ Abildung. Kann man aus M eine Gruppe machen?

Gemeint ist immer: Die Verknüpfung auf der neuen Mange soll eindeutig durch das gegebene Material, also insbesondere durch die Verknüpfungen der gegebenen Gruppen festgelegt sein.

(2.2.4) Damit sind die Mehrzahl unserer mengentheoretischen Konstruktionen aus Kap.1 angesprochen und und in zugehörige Übertragungsprobleme umgewandelt. Nochmals der Hinweis: Diese Übertragungsprobleme lassen sich für alle algebraischen Strukturen formulieren und werden bei deren Einführung dann jeweils mehr oder weniger routinemäßig abgehandelt. In den meisten Fällen ganz analog zu dem jetzt zu besprechenden Gruppenfall. Man sollte also beim Einstieg in den Problembereich einiges zur Behandlung der anderen Fälle mitlernen.

3.2.2a Untergruppen

(2.2.5) Wir beginnen mit dem Fall einer Teilmenge H von G. Auf jeden Fall können wir die Verknüpfung im Urbildbereich einschränken, also die Restriktion $\circ$:H×H→G bilden. Aber wir können nicht sicher sein, daß deren Werte wieder in H liegen, also $\circ$:H×H→H, was erforderlich ist, wenn eine Komposition von H entstehen soll.

(2.2.6) Wählen wir im Beispiel der Permutationen von 4 Objekten etwa die Teilmenge H={(1),(2),(3)} mit den Bezeichnungen aus (2.1.10). Dann haben wir (3)$\circ$(2)=(4)$\notin H$, so dass der Wertebereich sicher nicht auf H eingeschränkt werden kann! Anders ist es, wenn wir H={(1),(2),(7),(8)} setzen, wie man leicht prüft.

(2.2.6) Wir folgern: Falls überhaupt, wird H nur in manchen, wohl seltenen Fällen eine Gruppe werden.

(2.2.7) Falls wir für ein H die Restriktion $\circ$:H×H→H bilden können, sind die ersten zwei Schritte (G.α) und (G.β) der Gruppenkonstruktion erledigt. Wie steht es mit den weiteren Forderungen des Schrittes γ? Das Assoziativgesetz (G.γl) ist unproblematisch: Eine Eigenschaft, die **für alle Elemente von G** gilt, ist natürlich **auch für die Elemente der Teilmenge H gültig.** Dasselbe gilt für die eventuelle Kommutativität. Die beiden anderen Forderungen (G.γ2) und (G.γ3) zum neutralen Element und den inversen Elemente sind dagegen wieder fallspezifisch zu prüfen: Je nach Teilmenge H werden sie erfüllt sein oder auch nicht. (Merken Sie sich das Gesagte für den Beweis in (2.2.12).)

(2.2.8) Gewisse ausgezeichnete Teilmengen H von G erfüllen alle Bedingungen und erhalten dann eine besondere Bezeichnung.

Definition: Es sei (G,$\circ$) eine Gruppe und H$\subset G$ eine nichtleere Teilmenge. Wenn die einschränkung $\circ : H \times H \to H$ bildbar ist und (H,$\circ$) zu einer Gruppe macht, dann heißt (H,$\circ$) eine Untergruppe von (G,$\circ$).

Meist sagt man etwas ungenau "Untergruppe von G". Vorgeschaltetes *Unter-* oder auch *Teil-* deutet immer auf Strukturübertragung auf eine Teilmenge hin. Etwa *Untervektorraum* oder *Teilkörper* usw.

(2.2.9) **Wie findet man nun heraus. ob eine vorgegebene Teilmenge Untergruppe ist oder nicht?** Das vollständige Uberprüfen aller Gruppenforderungen erweist sich als durchaus mühsam. Man hat aber ein bewährtes Kriterium, das die Gruppeneigenschaft sichert. Die für dafür benötigten Voraussetzungen sind meist einfacher zu überprüfen als die Gesamtheit der Gruppenaxiome.

Das Untergruppenkriterium
Es sei (G,∘) Gruppe und H⊂ G nichtleere Teilmenge.
Weiter gelte: Mit x,y∈ H gilt auch immer x∘$y^{-1} \in H$.
Dann ist (H,∘) eine Untergruppe von (G,∘).

Die zugehörige Situation und Denkfigur: Man benötigt eine Teilmenge und muß zeigen, daß sie nicht leer ist. Dann argumentiert man : " Sei x,y∈H ...und zeigt fallspezifisch x∘$y^{-1} \in H$" . Jetzt darf man schliessen, dass (H,∘) Untergruppe von (G,∘) ist.

(2.2.11) Ein Beispiel: Sei (V_0^3,+) die additive Gruppe der geometrischen Pfeile und E⊂V_0^3 eine Ebene durch den Nullpunkt. Damit haben wir unsere Teilmenge. Nun ist zu prüfen, ob mit $\vec{x}$,$\vec{y} \in E$ auch ($\vec{x}$-$\vec{y}$)∈E gilt Die übliche Parallelogrammkonstruktion zeigt, daß dies der Fall ist. D.h. (E,+) ist Untergruppe von V_0^3. Ist H dagegen eine Halbebene oder eine Viertelebene, so ist dies offensichtlich nicht immer der Fall (Die rechte Koordinatenhalbene enthält beispielsweise $\vec{e}_1$, und $2\vec{e}_1 + \vec{e}_2$, nicht aber $\vec{e}_1 - (2\vec{e}_1 + \vec{e}_2) = -(\vec{e}_1 + \vec{e}_2)$. Das Beispiel verdeutlicht, dass man im Kriterium sicher nicht einfach x∘y statt x∘y^{-1} (additiv x+y statt x-y) nehmen darf.

(2.2.12) Nachdem wir verstanden haben, was das Kriterium beinhaltet und wie man damit arbeitet, müssen wir es noch beweisen, müssen zeigen, daß es tatsächlich leistet, was behauptet wird.

Beweis: Die Annahmen des Kriteriums seien erfüllt. Insbesondere haben wir (K): x,y∈H⇒x∘y^{-1} ∈H. Damit müssen wir zeigen, dass H wirklich eine Gruppenstruktur besitzt. Zunächst ist H≠ ∅ voraussgestzt. D.h. es gibt mindestens ein Element h∈H. Dann gilt auch h,h∈H. Nach (K) ist dann h∘h^{-1} = e∈H. Dabei ist e das neutrale Element von G und wir sehen: Dieses liegt in H und ist auch dort neutral. Sei h∈H beliebig. Dann ist e,h∈H. Nach (K) folgt e∘$h^{-1} = h^{-1} \in H$. D.h. für jedes h∈H liegt auch das zugehörige Inverse in H. Wir wissen bereits aus(1.3.26), dass (h^{-1})$^{-1}$= h gilt. Damit folgt: Sei g,h∈H. Dann ist auch g,h^{-1} ∈H. Anwenden von (K) gibt: g∘(h^{-1})$^{-1}$= g∘h∈H. Daher ist die Produktbildung in H abgeschlossen. es liegt eine innere Komposition auf H vor.

(2.2.13) Alle Gruppeneigenschaften sind überprüft. Das Kriterium ist bewiesen und darf und sollte von jetzt an immer benutzt werden.

(2.2.14) Zur Einübung ein kleines Beispiel:

Es sei (G,∘) Gruppe und H_1, H_2 seien Untergruppen.
Dann ist auch der Durchschnitt H_1∩H_2 eine Untergruppe.

Beweis: $H_1 \cap H_2$ ist sicher nicht leer, da jede Untergruppe das neutrale Element von G enthält. Sei nun x,y∈ $H_1 \cap H_2$. Nach Definition des Durchschnitts gilt dann x,y∈H_1 und x,y∈H_2. Da beides Untergruppen sind, folgt x∘y^{-1} ∈H_1 und x∘y^{-1} ∈H_2 Also ist x∘$y^{-1} \in H_1 \cap H_2$. **Es liegt eine Untergruppe vor.**

☐ Probieren Sie selbst: Es sei (ℂ,·) die multiplikative Gruppe aller komplexen Zahlen ≠ 0. Weiter sei U={z|z∈ ℂ, |z|=1}. Dann ist U zugehörige Untergruppe. Hinweis: Jedes z∈ U schreibt sich z=$e^{i\alpha}$.

☐ Beweisen Sie, dass jede Gruppe G zwei triviale Untergruppen enthält, G selbst und {e}, wenn e das neutrale Element von G ist.

(2.2.15) Was ist, wenn die Teilmenge T von G keine Untergruppe bildet? Dann kann man T eine eindeutig bestimmte Untergruppe zuordnen, die man **die von T erzeugte Untergruppe** nennt. Das Attribut "erzeugt" wird in der Mathematik immer benutzt, wenn eine Menge T eine bestimmte Eigenschaft nicht notwendig hat - hier Guppe zu sein - es aber eine kleinste Obermenge E von T - also T⊂E - gibt, die die betrachtete Eigenschaft hat. Hier geht es also darum, eine kleinstmögliche **Untergruppe** E von G zu finden, mit T⊂E. Nach dem Untergruppenkriterium muß E jedenfalls alle Elemente enthalten, die man wie folgt erreugt: Sei g,h∈T. Bilde damit g∘h, g∘h^{-1} usw. Aber es können noch viele weitere Elemente hinzukommen. Entsprechend führen wir den Beweis nicht konstruktiv, sondern als ganz abstrakten Existenzbeweis. Das bedeutet: In einschlägigen Situationen ist man sicher, dass es die erzeugte

Untergruppe gibt, man kann ihr eine Bezeichnung geben, aber u.U. weiß man noch lange nicht, welche Gruppenelemente konkret in der Untergruppe liegen!

(2.2.16) **Satz über die erzeugte Untergruppe**

> Sei T Teilmenge der Gruppe G.
> Dann gibt es eine kleinste Untergruppe E(T) von G, die T enthält. D.h. genauer: Ist H irgendeine Untergruppe von G, so daß T Teilmenge von H ist, also T⊂cH, dann gilt automatisch E(T)⊂H .
> E(T) wird **die von T erzeugte Untergruppe genannt.**

(2.2.17) Beweis: Es sei U die Menge aller Untergruppen von G, die T enthalten. Diese Menge enthält mindestens G selbst (= eine der beiden "trivialen Untergruppen"). Wir bilden E=$\cap_{X\in U}X$. In Verallgemeinerung von (2.2.14) ist der Durchschnitt beliebig vieler Untergruppen erneut eine Untergruppe. (Stillschweigend haben wir auch die Summenzeichensymbolik auf die Durchschnittsbildung verallgemeinert!) Die mengentheoretische Konstruktion der Durchschnittsbildung stellt sicher, dass einerseits T⊂E ist, da ja jedes X∈U die Menge T enthält. Andererseits gilt E$\subset X$ infolge der Durchnittsbildung für jedes X$\in U$. Damit ist der Satz bewiesen.

□ Was ist, wenn T leer ist? Was ist E(H), wenn H$\subset G$ bereits Untergruppe ist?

(2.2.18) Das erste der gestellten Übertragungsprobleme ("Wann ist eine Teilmenge eine Gruppe") ist in durchaus typischer Weise behandelt. Die relevanten Stichworte sind *Untergruppenkriterium* und *erzeugte Untergruppe.*

3.2.2b Produktgruppen

(2,2.19) Als nächstes besprechen wir die Übertragungsprobleme ÜK ÜA, fragen also, ob man das kartesische Produkt zweier Gruppen zu einer Gruppe-machen kann.

> **Satz:** Es seien (G,$\intercal$) und (H,$\perp$) Gruppen.
> Dann ist auch (G×$H, \intercal \times \perp$) Gruppe, wobei die Verknüpfung wie folgt definiert ist:
> $\intercal \times \perp$=((G×H)×(G×H)),(g_1,h_1),(g_2,h_2)↦(($g_1 \intercal g_2$),($h_1 \perp h_2$)),G×H))
> Diese Konstruktion wird selbsterklärend als *komponentenweise Verknüpfung* charakterisiert und die neue Gruppe heißt **das direkte Produkt der Gruppen G und H.**

(2.2.18) Achtung: Das hier eingeführte kartesische Produkt von zwei Abbildungen ist nicht ganz identisch mit dem früher gegebenen mengenthoretischen Produkt. Sie unterscheiden sich durch eine kanonische Iddentifikationsabbildung der beiden Mengen (G×G)×(H×H) und (G×H)×(G×H).

(2.2.19) Die angegebene Verknüpfung ist offensichtlich eine innere Komposition auf G×H. Sie ist aufgebaut wie die komponentenweise Addition in $\mathbb{R}^2$, für die natürlich $\intercal$=$\perp$=+ ist.

> Zum Beweis: (G.α) und (G.β) sind durch die Konstruktion erledigt. Das Assoziativgesetz gilt, weil es für die beiden Komponenten gilt, die ja zu Gtuppen gehören. (Bei Bedarf prüft man dies sofort mit der Tunnelmethode nach.) Das neutrale Element:ist (e_G,e_H) und das zu (g,h) inverse Element ist (g^{-1}, h^{-1}).
>
> Damit ist gezeigt, daß tatsächlich eine Gruppenstruktur für G×H entstanden ist.

(2.2.20) Häufig spezialisiert man auf den Fall G=H, bildet also G×G. Entsprechend bildet man auch höhere Potenzen, worauf wir unten beim Stichwort Isomorphie in 3.2.3 noch etwas zurückkommen. Und dann schreibt man auch wieder $\intercal$ statt $\intercal \times \intercal$, so wie man die Vektoraddition in $\mathbb{R}^n$ wieder mit + bezeichnet.

(2.2.21) Auch das zweite Übertragungsproblem ist somit generell positiv beantwortet.

3.2.2c Wertemengenübertragung in Abbildungsräumen

(2.2.22) Es soll jetzt der zum vorigen ähnliche Fall ÜA besprochen werden, also die Übertragung einer Gruppenstruktur auf die Abbildungsmengen $\mathcal{F}$(M,G). Wir wählen hier den Plural, weil M beliebige Menge sein darf, nur G muss eine Gruppe bilden.

(2.2.23) Während wir die Produktkonstruktion als komponentenweise Verknüpfung charaktsrisiert haben, wird die neue Konstruktion programmatisch als *Wertemengenübertragung* charakterisiert. Worum

geht es? Es seien f=(M,x↦f(x),G) und g=(M,x↦g(x),G) zwei Elemente aus $\mathcal{F}$(M,G). Wir wollen sie zu einem neuen Element dieser Menge verknüpfen (Schritt (G.β)!). Das neue Element soll mit f$\bar{\top}$g bezeichnet werden. (G,$\top$) ist unsere gegebene Gruppe.

f$\bar{\top}$g=((M,x↦(f$\bar{\top}$g)(x)=f(x)$\top$g(x),G)	**Wertemengenübertragung**
Also: Für jedes x∈M sind f(x) und g(x) Elemente aus G. Beide können wir mit der Gruppenverkn. $\top$ zum neuen Element f(x)$\top$g(x)∈ G verbinden. Das wird dann x zugeordnet.	x $\overset{f}{\mapsto}$ f(x) $\in G$ y $\overset{g}{\mapsto}$ g(x) $\in G$ ———————- x $\overset{f\bar{\top}g}{\mapsto}$ f(x)$\top$g(x) $\in G$

(2.2.25) Wir haben damit die neue Verknüpfung $\bar{\top}$ für $\mathcal{F}$(M,G) von der gegebenen $\top$ in der Bezeichnung unterschieden. Meist ist es üblich, beide Verknüpfumgen mit demselben Symbol zu bezeichnen, wozu wir auch bald übergehen werden. Nochmals die entscheidende **Definitionsgleichung der Wertemengenübertragung:**

$$\boxed{(f\bar{\top}g)(x)=f(x)\top g(x)}$$

Die Konstruktion ist uns bereits aus dem Bereich der reellen Funktionen etwa für $\top$=+ bekannt. Etwa sin + exp=($\mathbb{R}$, x↦(sin+exp)(x)=sin(x)+e^x,$\mathbb{R}$). Dass dabei auch die Urbildmenge gleich $\mathbb{R}$ ist, ist für die Konstruktion irrelevant, wie man am Beispiel der Skalarfelder sehen kann.

(2.2.27) Liegt wirklich eine Gruppe vor? (G.α) und (G.β) sind erledigt. Das Assoziativgesetz (G.γl) folgt sofort wieder per Tunnelmethode, weil es in G gilt. Neutrales Element in $\mathcal{F}$(M,G) ist die konstante Abbildung E=(M,x↦E,G) wobei E das neutrale Element von G ist. Und das zu f=(M,x↦f(x),G) inverse Element ist die Abbildung f^{-1}=(M.x↦(f(x))$^{-1}$,G). Denn offensichtlich ist etwa

$$f\bar{\top}f^{-1} = (M, x \mapsto f(x) \top (f(x))^{-1}, G) = E$$

Man sieht: Alle Gruppeneigenschaften von $\mathcal{F}$(M,G) werden gesichert, indem man beachtet, dass die Werte f(x) Elemente der Gruppe G sind. **Durch die Methode werden die Struktureigenschaften auf die Abbildungen übertragen.** Verwendet man dann für die Verknüpfung in all diesen Mengen dasselbe Symbol, wird das noch deutlicher.

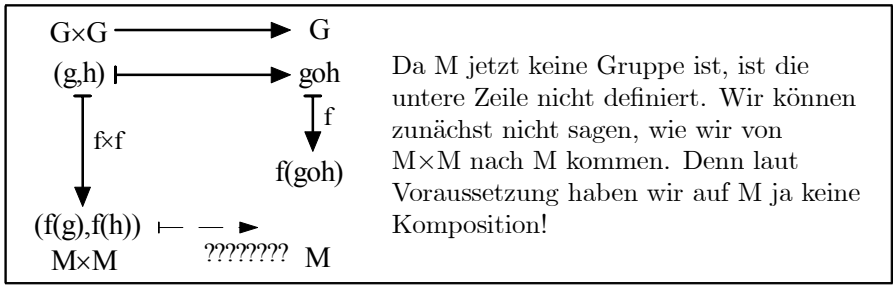
(2.2.28) Fassen wir zusammen: **Durch Wertemengenübertragung (der Struktur) wird** $\mathcal{F}$(M,G) **für eine beliebige Menge M zu einer Gruppe.**

(2.2.29) Die drei behandelten Übertragungskonstruktionen sind naheliegend, einfach und banal. Im mathematischen Bereich sagt man gerne trivial. Wir werden sie von jetzt ab als selbstverständlich verwenden, nur durch ein jeweiliges Stichwort andeuten, nicht aber groß für neue Fälle beweisen und einüben. Die Herausbildung eines gesunden Urteilsvermögens für Triviales ist wichtig.

3.2.2d Stukturtransport mit Hilfe einer Abbildung

(2.2.30) Soeben haben wir **alle** Abbildungen M→G betrachtet. Jetzt betrachten wir umgekehrt **eine** feste **bijektive** Abbildung f:G→M.

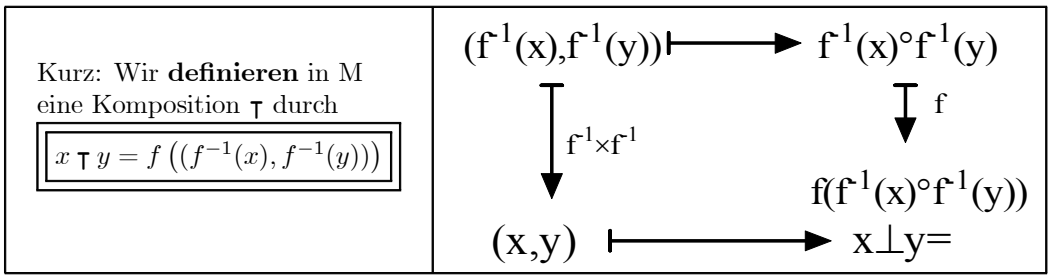
Unter gewissen Umständen, speziell dann, wenn f bijektiv ist, kann man mit Hilfe von f die Gruppenstruktur von G nach M hinübertransportieren. (Vom Urbildraum in den Werteraum!) Die Gruppe sei (G,∘). Um dies zu sehen, betrachten wir erneut das Diagramm füt die strukturerhaltenden Abbildungen.



Da M jetzt keine Gruppe ist, ist die untere Zeile nicht definiert. Wir können zunächst nicht sagen, wie wir von M×M nach M kommen. Denn laut Voraussetzung haben wir auf M ja keine Komposition!

(2.2.31) Die Idee besteht nun darin, den zweiten Weg über G×G und G nach M zu nehmen. Da f bijektiv sein soll, ist das möglich. Wir starten mit (x,y)∈ $M \times M$, bilden dazu ($f^{-1}(x), f^{-1}(y)$) ∈ $G \times G$.

Das verknüpfen wir mit der Komposition aus (g,$\circ$) zu $f^{-1}(x) \circ f^{-1}(y) \in G$ und gelangen schließlich mit f zu $f\left((f^{-1}(x), f^{-1}(y))\right) \in M$.



(2.2.32) Die Gruppenaxiome für (M,⊤) lassen sich leicht per Tunnelmethode verifizieren (M,⊤) ist wirklich eine Gruppe!

(2.2.32) Beispiel: Wir nehmen ($\mathbb{R}$,+) und die bijektive Abbildung f(x)=$\sqrt[3]{x}$. Dann liefert unsere Konstruktion die folgende Verknüpfung $\star$, für die ($\mathbb{R}, \star$) kommutative Gruppe wird:

$$x \star y = \sqrt[3]{x^3 + y^3}. \qquad \text{Etwa } 2 \star 1 = \sqrt[3]{9}.$$

3.2.3 Isomorphismen

(2.3.1) Welche Bedeutung hat die in (2.2.31) beschriebene Konstruktion? Hierzu holen wir etwas aus. Hat man eine Gruppenstruktur, so kann man auf die Idee kommen, alle Elemente irgendwie umzubennen. Die Umbenennung muß natürlich die Gruppentafel mit einschließen. Auch für die Verknüpfung kann man ein anderes Symbol wählen. Wenn man dies systematisch durchführt, hat man dann eine "neue Gruppe" oder ist das immer noch die alte? Also zwei verschiedene Bezeichnungsschemata derselben Gruppe?

(2.3.2) Umbenennungen haben wir beständig stillschweigend durchgeführt, etwa wenn wir die Verknüpfungen entweder aus typographischen Gründen oder um gewisse gedächtnisstützenden Assoziationen hervorzurufen, situationspzifisch benannt oder umbenannt haben. Anders gesagt: Wir haben Identifikationsabbildungen verwendet.

(2.3.3) Oder es stellt sich das folgende Problem: Man konstruiert sich zwei (endliche) Gruppen auf unterschiedliche Weise und stellt fest, daß sie nach eventueller Umbenennung dieselbe Gruppentafel ergeben. Zwei unterschiedliche Anwendungen führen also irgendwie auf dieselbe algebraische Struktur und es sollen mathematische Resultate einmal bewiesen, aber auf beide Fälle übertragen werden. In welchem Sinne liegt dieselbe Gruppe vor? Ein einfaches Beispiel: Wir haben zwei n-elementige Mengen A und B und betrachten deren Permutationsgruppen $\mathfrak{B}$(A,A) und $\mathfrak{B}$(B,B). Sind das dieselben oder verschiedene Gruppen?

(2.3.4) **Je nach Situation wird es unterschiedliche Antworten geben**: Entweder ist für beide Mengen (in der interessierenden Situation!) nur die Gruppenstruktur wichtig, dann wird man beide Gruppen identifizieren und die Probleme nur einmal lösen. Interpretation: Hinter beiden Realisierungen steht dieselbe Idee (im Sinne von Plato). Oder aber wenigstens eine der beiden Mengen hat neben der Gruppenstruktur noch andere situationsrelevante Eigenschaften. Dann wird man zwischen beiden Gruppen eine vermittelnde Abbildung vom Darstellungstyp suchen und nicht identifizieren. (Die philosophische Richtung ist eher die von Aristoteles!). Im ersten Fall werden alle mathematischen Resultate einfach durch Umbenennung übertragen, im zweiten wird man sich immer auf die Seite begeben, in der man besser vorankommt. Beachten Sie wie anders als die Philosophie - besser die Mehrzahl der Philosophen- die Mathematik hier vorgeht: Sie macht sich nicht auf zu beweisen, daß ein Weg der absolut wahre, einzige sei, sondern entwickelt beide Wege als als sinnvolles nützliches Werkzeug.

(2.3.5) Das geeignete mathematische Handwerkszeug zur Behandlung des platonischen Ideenweges ist der *Isomorphiebegriff*, den wir jetzt eiführen wollen.

(2.3.6) In allen genannten Fällen geht es offenbar um eine Klasseneinteilung für Gruppen: gleichartig und umbenennbar oder nicht. **Mathematisch ist eine solche Umbenennung zweier Gruppen eine bijektive Abbildung zwischen den Gruppen, die in beiden Richtungen strukturerhaltend ist.** Letzteres bedeutet, daß es gleichgültig ist, ob man vor oder nach der Verknüpfung umbenennt. Man

definiert - und die Überlegungen erklären den Namen:

Definition: Es seien (G,$\circ$) und (H,$\intercal$) zwei Gruppen. Eine Abbildung $\Phi : G \to H$ heißt *ein* **Gruppenisomorphismus** *zwischen G und G ,* wenn Φ bijektiv ist und wenn Φ und Φ^{-1} beide strukturerhaltend sind.
Zwei Gruppen G und H heißen *isomorph*, wenn es einen Gruppenisomorphismus G→H gibt.

(2.3.7) "G und H sind isomorph" ist eine Äquivalenzrelation (in jeder Menge von Gruppen), wie man sofort überprüft. Hat man also eine Menge $\mathfrak{G}$ von Gruppen, so zerfällt diese in Klassen ineinander umbenennbarer isomorpher Gruppen. Und strukturerhaltende Umbenennung führt immer zu isomorphen Gruppen.

(2.3.8) Wir haben die Gruppenisomorphie so eingeführt, dass die Verallgemeinerbarkeit des Begriffs auf andere Strukturen durchsichtig wird. Im Fall der Gruppen ist ein Teil der Forderungen jedoch unnötig, da er aus dem Rest folgt:

(2.3.9)

Satz: Es sei Φ:G→H ein bijektiver Gruppenhomomorphismus.
Dann ist auch Φ^{-1} ein Gruppenhomomorphismus.

□ Der Beweis ist elementar. Führen sie ihn aus. (Achten sie darauf, daß beide Voraussetzungen benutzt werden.)

(2.3.10) Es folgt eine **reduzierte Definition** (mit weniger zu prüfenden Voraussetzungen):

Ein Gruppenisomorphismus ist ein bijektiver Gruppenhomomorphismus!

(2.3.11) Bitte beachten Sie: Hat man zwei Gruppen G und H, von den man wissen möchte, ob sie isomorph sind oder nicht, dann muß man **einen** bijektiven Homomorphismus finden. Weitere solche Homomorphismen kann es geben und noch mehr Abbildungen, die die gewünschten Eigenschaften nicht haben. Will man zeigen, daß die Gruppen nicht isomorph sind, dann muß man zeigen daß **alle** Abbildungen G→H die verlangten Eigenschaften nicht haben.

□ Wieso kann eine nicht kommutative Gruppe nicht zu einer kommutativen isomorph sein?

(2.3.12) Jede Gruppe, die man einführt oder der man begegnet, erzeugt daher eine Isomorphieklasse und diese Isomorphieklassen sind es, die im Rahmen der abstrakten Gruppentheorie interessieren. Oder auch: Diese Klassen repräsentieren die gemeinsame Idee. In einem weiteren Schritt werden diese Eigenschaften dann mit Hilfe von Abbildungen vom Darstellungs- und Parametrisierungstyp auf Anwendungsbereiche übertragen und zur Problemlösung nutzbar gemacht.

(2.3.13) Beispiel: Es sei G=($\mathbb{R}$,+) und H=($\mathbb{R}^+$,$\cdot$) mit $\mathbb{R}^+$=]0, ∞[. Dann ist exp= ($\mathbb{R}$,x↦e^x,$\mathbb{R}^+$) offensichtlich ein Gruppenisomorphismus. ℓn ist der inverse Isomorphismus. Wenn man also alle anderen Strukturen von $\mathbb{R}$ vergißt und nur die Addition in G und die Multiplikation in H betrachtet, dann sind G und H völlig gleichwertig, nur Umbennennungen voneinander. Jede rein additive Rechnung in $\mathbb{R}$ wird zu einer entsprechenden multiplikativen in $\mathbb{R}^+$ und umgekehrt. Die Strukturübertragungsgleichung ergibt für diesen Fall: a·b = exp(ℓn(a)+ℓn(b)). Sobald man aber die Null im multiplikativen Bereich mit ins Spiel bringt, geht die Gleichwertigkeit verloren.

(2.3.14) Wir geben jetzt einige wichtige Resultate zu den Isomorphieklassen kleiner endlicher Gruppen. Diese Resultate werden wir zum Teil im weiteren Verlauf dieses Kapitels beweisen, z.T. nennen wir sie hier nur. Man sollte sie inspizieren, um zu sehen welche Antworten die Strukturanalyse geben kann. Einige von ihnen sind keineswegs trivial.

(2.3.15) Die Anzahl der Elemente einer endlichen Gruppe nennt man *die Ordnung der Gruppe.* (Bitte nicht mit der noch einzuführenden Ordnung eines Elementes verwechseln.) Gruppen unterschiedlicher Ordnung können nicht isomorph sein, da es zwischen ihnen keine bijektive Abbildung gibt. Wie aber steht es mit Gruppen gleicher Ordnung? Gibt es überhaupt Gruppen beliebiger Ordnung?

(2.3.16) Hierzu also einige wichtige Resultate:

1)	Sei k>0 natürliche Zahl. Dann gibt es eine kommutative Gruppe, der Ordnung k, die sog. *zyklische Gruppe der Ordnung k.* Und damit gibt es mindestens eine Isomorphieklasse für k-elementige Gruppen.
2)	Ist k=p Primzahl, so gibt es nur diese eine Isomorphieklasse. Jede Gruppe der Ordnung p ist isomorph zur entsprechenden zyklischen Gruppe der Ordnung p.

Ist k keine Primzahl und >1, dann gibt es mehrere Isomorphieklassen. Die Liste zeigt die Klassenzahl bis k=24.

Ordnung k	1	2	3	4	5	6	7	8	9	10	11	12	13
Zahl d. Klassen	1	1	1	2	1	2	1	5	2	2	1	5	1
Ordnung k	14	15		16	17	18		19	20	21	22	23	24
Zahl d. Klassen	2			14	1	5		1	20	2	2	1	15

Man kann also 5 Gruppen angeben, die je 12 Elemente haben, aber alle nicht zueinander isomorph sind. Die Liste erweckt alles andere als den Eindruck der Einfachheit und das ist auch korrekt.

□ Welchen Wert erwarten Sie für k=15? Das Ergebnis dürfte falsch sein, ist aus den Daten nicht erschließbar.

(2.3.17) Jetzt fahren wir mit unserer allgemeinen Argumentation fort. Zunächst konstruieren wir die in (2.3.16) unter 1) angesprochenen zyklischen Gruppen. Punkt 2) werden wir später beweisen. Ws die Zahl der klassen betrifft, geben wir nur an, bzw. konstruieren Vertreter einzelner Klassen. So soll es für k=6 ja zwei Klassen geben. Einmal die der zyklischen Gruppe der Ordnung 6. Dann kennen wir aber bereits die Permutationsgruppe für drei Elemente. Diese hat auch die Ordnung 6 und ist nicht kommutativ, kann also nicht zur zyklischen Gruppe isomorph sein. Sie ist Vertreter der zweiten Klasse. Weitere Klassen gibt es nicht.

3.2.4 Analyse der Gruppenstruktur (1)

Wir leiten jetzt eine Reihe spezifischer Eigenschaften der Gruppenstruktur her. Damit beenden wir den in (2.0.2) beschriebenen Routineteil und beginnen die eigentliche Strukturklärung.

3.2.4a Die zyklischen Gruppen.

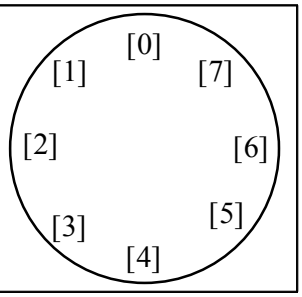
(2.4.1) In Kap.l.3 haben wir für jedes k∈ ℕ mit k>l die Äquivalenzrelation $\underset{k}{\equiv}$ in der Menge der ganzen Zahlen eingeführt. Genauer war definiert

$$n \underset{k}{\equiv} m \iff (n-m) \text{ ist durch k teilbar,}$$

Oder auch: n und m liegen in derselben Klasse, wenn sie denselben Divisionsrest bezüglich k haben. Es gab k Klassen [r]={7n|n=r+ks, s∈ ℕ} und r=0,l,...,k-l. Die Menge dieser Klassen - also die zugehörige Partition bezeichnet man traditionellerweise mit Z/(k), gelesen "Z modulo k". Da wir diese Klassenmenge intensiv benutzen werden, sollten Sie sich die nachfolgende Veranschaulichung einprägen und auch immer daran denken, daß k äußerer Parameter ist.

(2.4.2) Veranschaulichung der zyklischen Gruppe

Wir betrachten eine Uhr für einen k-stündigen Tag. Im Bild ist k=8. Die Stunden laufen von 0 bis k-l. Jede Stunde repräsentiert eine Klasse von $\mathbb{Z}/(k)$. Das Vorliegen einer Klasse wird durch [...] gekennzeichnet. Die Richtung sei mathematisch positiv, also entgegen dem üblichen Uhrzeigersinn.



Das Rechnen im gegebenen Stundentakt macht die Klassenabbildung $(\mathbb{Z}, r \mapsto [k], \mathbb{Z}/(k))$ anschaulich. Etwa [8]=[0] oder [15]=[7] oder auch [-3]=[5]. Schließlich gilt

$$[3] = \{3, 11, -5, 19. - 13, ...\} \qquad \text{für k=8.}$$

(2.4.3) **Wir wollen die Klassenmenge** ℤ(k) **jetzt zu einer Gruppe machen**. Das ist ein Übertrasgungsproblem vom Typ (ÜR) aus (2.2.3). Als Verknüpfung wählen wir die Stundenaddition. Genauer gesagt setzen wir:

$\boxed{[n]+[m]=[n+m]}$ (Eigentlich $[n] +_k [m] = [n+m]$, da k äußerer Parameter.

(2.4.4) Diese Gleichung wirft ein Problem auf: Die *Wohldefiniertheitsfrage*. n und m sind ja beides Vertreter ihrer Klasse und die neue Klasse wird mit Hilfe dieser Vertreter berechnet. Was ist, wenn man mit anderen Vertretern rechnet? Man prüft leicht nach, dass dann dieselbe Klasse (über einen eventuell anderen Vertreter) herauskommt.

$$[n + ak] + [m + bk] = [n + m + (a + b)k] = [n + m].$$

D.h. die Verknüpfung ist wohldefiniert!

(2.4.5) Damit haben wir eine Menge (mit k Elementen) und eine zugehörige innere Verknüpfung (Schritte α und β). Wie steht es mit den Gruppenaxiomen? Die Assoziativität gilt, weil sie für $\mathbb{Z}$ gilt: ([n]+[m])+[p]=[(n+m)]+p]=. ... Das + inerhalb [..] ist ja das + aus $\mathbb{Z}$.

[0] ist neutral und [-n] invers zu [n]. **Also liegt eine Gruppe mit k Elementen vor**. Diese Gruppe ($\mathbb{Z}$/(k),+) ist kommutativ, da die Addition in Z dies ist.

(2.4.6) Ergebnis:

> Die Äquivalenzrelation $\underset{k}{\equiv}$ zerlegt $\mathbb{Z}$ in k Klassen gleicher Divisionsreste nach k. Die Klassenmenge sei $\mathbb{Z}$/(k)={[r]| r=0,.....,k-l}. Durch [r]+[s]=[r+s] wird in dieser Menge eine Komposition definiert. Diese ist wohldefiniert und macht die Klassenmenge zu einer kommutativen Gruppe.

(2.4.7) **Beachten Sie**: Soeben haben wir exemplarisch das Übertragungsproblem für eine Klassenmenge behandelt. Eine Gruppenstruktrur wurde von $\mathbb{Z}$ auf $\mathbb{Z}$/(k) übertragen. Wichtig war dabei die Untersuchung des zugehörigen Wohldefiniertheitsproblems.

(2.4.8) Unser Uhrenmodell (2.3.19) legt es nahe, diese Gruppe noch auf andere Weisen zu konstruieren. Wir beschreiben zwei derartige Konstruktionen.

(2.4.9) **Operative Methode**: Wir betrachten die k-stündige Uhr und die Operation des Weiterstellens des Zeigers um eine Stunde. $\sigma = \sigma_k$ bezeichne diese Operation. Dann können wir σ mehrfach hintereinander ausführen und erhalten so neue Operationen. $\sigma\sigma = \sigma^2$ bezeichne die Zweifachoperation, also das Weiterstellen um 2 Stunden. $\sigma\sigma\sigma = \sigma^3$ das Weiterstellen um 3 Stunden usw. σ^k gibt einen Uhrumlauf, also keine erkennbare Änderung der Zeigerstellung. Dies könne wir ebenso durch die neutrale Operation e=σ^0 bewirken. Wir vereinbaren generell, daß immer nur die **resultierende Zeigerstellung**, die Stundenangabe, betrachtet werden soll, nicht aber die Tagesangabe, also die Zahl der Gesamtumläufe, die zur Endstellung führten. Damit gilt ist σ^k=e, wie wir gesehen haben. (Zwei verschiedene Bezeichnungen für dasselbe Objekt!). Schließlich können wir den Zeiger um eine Stunde zurückstellen, eine Operation, die wir mit σ^{-1} bezeichnen. Nun können wir sämtliche Uhrverstellungen durch die k Operationen e,σ,σ^2,.....,σ^{k-1} beschreiben und diese bilden bezüglich der Hintereinanderausführung eine Gruppe, wie man sofort überprüft. Dabei ist vereinbarungsgemäß σ^k=e, $\sigma^{-1} = \sigma^{k-1}$ usw.

	e	σ	σ^2	σ^3	σ^4
e	e	σ	σ^2	σ^3	σ^4
σ	σ	σ^2	σ^3	σ^4	e
σ^2	σ^2	σ^3	σ^4	e	σ
σ^3	σ^3	σ^4	e	σ	σ^2
σ^4	σ^4	e	σ	σ^2	σ^3

Mit Hilfe der beschriebenen Operationsinterpretation kann man sofort die zugehörige Gruppentafel aufstellen, was wir nebenstehend für k=5 getan haben. Für anderes k hat die Tafel völlig analoge Struktur.

(2.4.10) Die entstandene Gruppe nennen wir die *zyklische Gruppe von k Elementen* und bereichnen sie mit C_k.

(2.4.11) Man sieht sofort (C_k,$\sigma^k \mapsto$[k], $\mathbb{Z}$/(k)) ist bijektiv und strukturerhaltend. Also ein Gruppenisomorphismus. Die Klassen enthalten mehr Struktur als die reinen Operationen. Wir haben eine Abbildung vom Darstellungstyp vorliegen. Die Abbildung ($\mathbb{Z}$,r$\mapsto$,σ^r, C_k) ist nicht injektiv, aber stukturerhaltend (r+s$\mapsto$ $\sigma^{r+s} = \sigma^r\sigma^s$). Also liegt ein Gruppenhomomorphismus vor.

(2.4.12) **Einbettung der Gruppe in die komplexe Ebene**:

Wir betrachten jetzt die k-elementige Lösungsmenge Z_k der Gleichung z^k=l in $\mathbb{C}$. Wir wissen, daß $Z_k = \{z_r | z_r = e^{i\frac{2\pi}{k}r}$, k=0,1,...,k-1$\} \subset \mathbb{C}$ gilt.

Das sind alles Punkte, die auf dem Einheitskreis liegen. Multipliziert man zwei von ihnen, so ergibt das komplexe Produkt erneut ein Element der Menge. Genauer gesagt gilt $z_r z_s = z_t$ wenn t der Divisionsrest von r+s durch k ist. D.h. [r+s]=[t]. Oder auch: $(Z_k, \cdot)$ ist eine Gruppe, und zwar eine endliche Untergruppe von $(\mathbb{C},\cdot)$.

Die bijektive Abbildung (C_r,$\sigma^r \mapsto z_r, Z_k$) ist Strukturerhaltend, ein Gruppenisomorphismus. **Wir haben die zyklische Gruppe in die komplexe Ebene eingebettet,** sie als Teilmenge der komplexer Zahlen dargestellt, wobei die Gruppenmultiplikation Restriktion der komplexen Multiplikation ist.

(2.4.13) Alle drei Gruppen sind isomorph und Iiegen somit in derselben Isomorphieklasse. Jetzt sehen wir deutlich die Bedeutung des Isomorphiebegriffes: Was die Verknüpfung anbelangt, die algebraische Struktur, so erscheinen die drei Gruppen einfach als Umbenennung, man könnte sie identifizieren. Jedenfalls Iiegen sie in derselben Isomorphieklasse. Aber die Elemente haben auch noch spezifische Eigenschaften außerhalb ihrer algebraischen Struktur. Sobald diese relevant werden, sollte man nicht identifizieren und stattdessen verbindende Abbildungen vom Darstellungstyp verwenden. Zu diesem Zweck kann man entweder die gesamte Klasse zu einer abstrakfen Gruppe zusammenfassen, so wie man aus dreielementigen Mengen die Zahl 3 abstrahiert, oder man kann einen geeigneten, besonders typischen Vertreter der Klasse als Ausgangspunkt, als Träger der idealen algebraischen Struktur wählen. Wir tun letzteres und wählen die Gruppe C_k. Die eingeführte zyklische Gruppe soll also unsere reine abstrahierte Gruppe sein. die nur noch die von den Axiomen geforderten Eigenschaften besitzt. Dabei schreiben wir jetzt immer kurz C_k anstelle $(C_k, \cdot)$ nach dem bewährten Prinzip, die jeweils wichtigste Struktur mit dem einfachsten Symbol zu bezeichnen.

(2.4.14) Diese Gruppe C_k wird dann durch strukturerhaltende Abbildungen vom Parametrisierungstyp oder häufiger vom Darstellungstyp mit anderen Mengen in Beziehung gesetzt und dabei werden die allgemeinen Resultate der Gruppentheorie auf diese anderen Mengen übertragen und dort nutzbar gemacht. Zweck ist: **Die Gruppenstruktur in anderem Kontext wiederfinden.**

3.2.4b Die Untergruppen von (Z,+)

(2.4.15) Parallel zur vorangegangenen Überlegung - also von dieser unabhängig - bestimmen wir alle Untergruppen von (Z.+). Das ist ein wichtiger Problemtyp im Rahmen der Analyse der Gruppenstruktur: **Alle Untergruppen einer Gruppe bestimmen oder aber zu zeigen, daß eine Gruppe gewisse Untergruppen besitzen muß.** Im Falle von $\mathbb{Z}$ ist das Problem leicht zu lösen. Wir argumentieren wie folgt:

(2.4.16) Sei U eine Untergruppe von ($\mathbb{Z}$,+). Dazu sei P$\subset$U die Teilmenge aller positiven Elemente dieser Untergruppe. U enthält sicher die neutrale Null, aber 0 ist nicht positiv. P könnte leer sein. Dann ist notwendig U=$\{0\}$. Dann liegt die triviale, nur aus dem neutralen Element bestehende Untergruppe vor. Ist P nicht leer, gibt es ein kleinstes Element k in P. Ist k=l, so enthält U auch alle Vielfachen von k und wir erhalten U=$\mathbb{Z}$. Ist k>l, so enthält U als Gruppe alle **ganzzahligen Vielfachen** von k, nämlich k,-k,2k,-2k,3k,.... : Alle diese Elemente zusammen bilden tatsächlich eine Gruppe, wie das Untergruppenkriterium zeigt. Wir haben:

$$U = \{n | n = zk, z \in \mathbb{Z}\} = k\mathbb{Z} \qquad \text{für k=1,2,3,.....}$$

Mit kZ haben wir für diese Untergruppen eine naheliegende Bezeichnung eingeführt, die zugleich die Konstruktion der Elemente beschreibt. $\mathbb{Z}$ selbst könne wir als 1$\mathbb{Z}$ interpretieren und $\{0\}$ als 0Z. Das sond die beiden trivialen Untergruppen.

(2.4.17)) Da wir alle Möglichkeiten durchgegangen sind, gilt:

($\mathbb{Z}$,+) hat nur **eine** endliche Untergruppe, die triviale Untergruppe $\{0\}$=0$\mathbb{Z}$. Die weiteren Untergruppen sind kZ=$\{kz|z\in \mathbb{Z}\}$ für k=1,2,3,.... Sie haben alle endlich viele Elemente. k=l gibt die zweite triviale Untergruppe $\mathbb{Z}$.

3.2.4c Die durch einen Homomorphismus bestimmten Untergruppen

(2.4.18) Wir setzen die in (2.1.24) begonnene Analyse der Homomorphismen fort. Dazu benötigen wir den Untergruppenbegriff, der damals nicht, jetzt aber zur Verfügung steht. Es stellt sich nämlich heraus, dass man mit Hilfe der Homomorphismen systematisch gewisse Untergruppen erhält. Oder auch: Gewisse durch die Homomorphismen festgelegte Teilmengen sind automatisch Untergruppen.

(2.4.19) **Satz:**

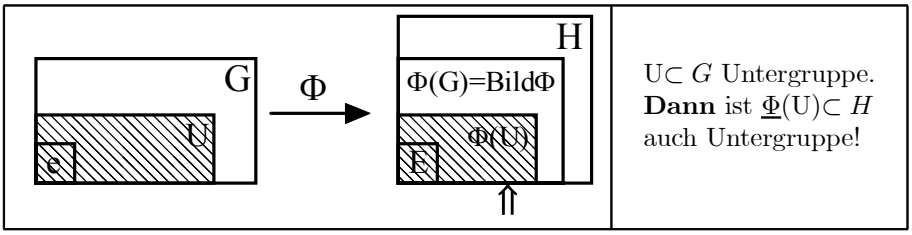
Es sei Φ:G$\rightarrow$H ein Gruppenhomomorphismus. Weiter sei U eine Untergruppe von G und V eine Untergruppe von H.

Dann ist $\underline{\Phi}$(U) eine Untergruppe von H und $\overset{-1}{\underline{\Phi}}(V)$ eine Untergruppe von G.

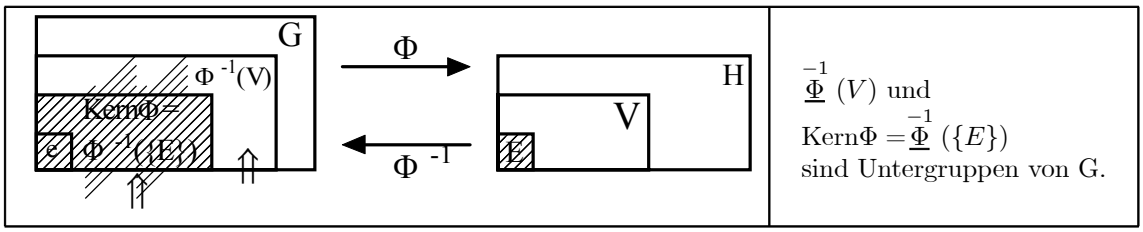
Zur Erinnerung die mengentheoretischen Definitionen aus Kap.1:

$$\begin{aligned} \underline{\Phi}(u) &= \{h|h \in H, h = \Phi(g) \text{ für ein g} \in U\} \qquad \text{statt} \quad \in G. \\ \overset{-1}{\underline{\Phi}}(V) &= \{g|g \in G, \Phi(g) \in V\} \qquad \text{statt} \quad \in H. \end{aligned}$$

(2.4.20) Die **Veranschaulichung** dieser Aussage erfolgt günstig über den Transformationsstandpunkt, d.h. wir interpretieren G und H beide als Konfigurationsraum. Dabei vereinbaren wir, dass Gruppen und Untergruppen als **rechteckige** Gebilde dargestellt werden, beliebige Teilmengen dagegen nichtrechteckige Form erhalten. Die Untergruppe umfasst immer das ganze Rechteck bis zum neutralen Element e bzw. E. Neu erzeugte Untergruppen kennzeichnen wir durch ein Zeichen ⇑.



Das neutrale Element e wird auf E abgebildet. Die Untergruppe U auf $\underline{\Phi}$(U) und das **ist** erneut eine Untergruppe! Die triviale Untergruppe G wird auf $\underline{\Phi}$(G) = Bild(G) abgebildet und auch dies **ist immer eine Untergruppe**.



Jetzt die andere Richtung.

(2.4.21) Kurz: Bild und Urbild von Untergruppen sind bei einem Homomorphismus erneut Untergruppen. Untergruppen werden in Untergruppen transformiert.

(2.4.22) Besonders wichtig sind hier die beiden trivialen Untergruppen G von G und {E} von H, **da sie auf der anderen Seite nichttriviale Untergruppen erzeugen können.** Während $\underline{\Phi}$(G) mit Bild(Φ) bereits eine eigene Bezeichnung hat, benötigen wir für die andere Untergruppe noch eine. Das geschieht durch folgende **Definition**:

Sei Φ:G→H Gruppenhomommorphismus und E das neutrale Element von H.
Dann wird die Untergruppe $\overset{-1}{\underline{\Phi}}$ ({E}) mit KernΦ bezeichnet.

$$\text{KernΦ} = \overset{-1}{\underline{\Phi}}(\{E\}) = \{g \in G|\Phi(g) = E\} = \left\{ \begin{array}{c} \text{Menge aller Lösungen} \\ \text{von } \Phi(g) = E. \end{array} \right.$$

Merke: **Sobald man es mit einem Gruppenhomomorphismus zu tun hat. sollte man möglichst Kern und Bild bestimmen!**

(2.4.23) Beweis: Die Aussagen von (2.4.19) sind noch zu beweisen. Hierzu bietet sich das Untergruppenkriterium an. Nehmen wir zunächst $\underline{\Phi}$(U).

Sei x,y∈$\underline{\Phi}$(U). Also x=Φ(a) und y=Φ(b) mit a,b∈ U (Explikation). Da U Untergruppe ist, folgt $ab^{-1} \in U$ und ebenso . $\Phi(b^{-1}) = (\Phi(b))^{-1}$. Also

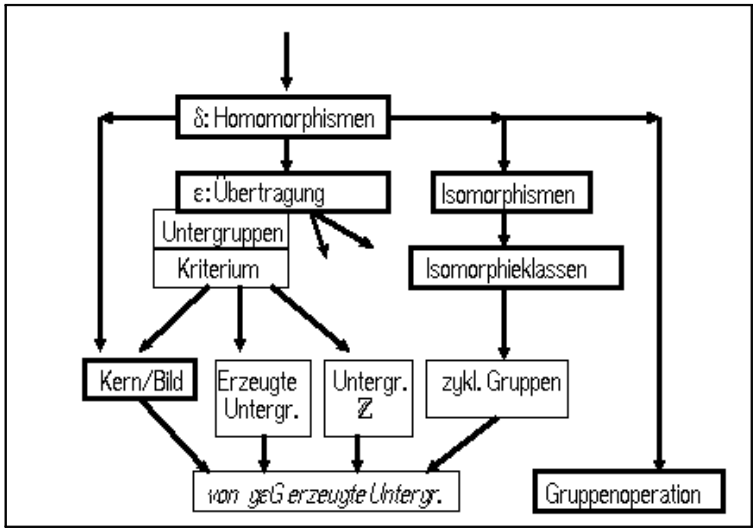
$$xy^{-1} = \Phi(a)(\Phi(b))^{-1} = \Phi(a)\Phi(b^{-1}) = \Phi(ab^{-1}) \in \underline{\Phi}(U)$$

wie gewünscht.

□ Führen Sie den zweiten Teil des Beweises analog.

3.2.4d Übersicht

Das nachfolgende Diagramm zeigt die argumentativen Zusammenhänge unserer bisherigen Überlegungen zur Klärung der Gruppenstruktur. An die für alle algebraischen Strukturen wichtigen Schritte der Einführung der strukturerhaltenden Abbildungen - also der Gruppenhomomorphismen - und der Behandlung der Übertragungsprobleme schließen sich einige für die Gruppenstruktur spezifische Überlegungen an. Im nachfolgenden Schritt wollen wir etwas Strukturanalyse betreiben und die von den einelementigen Teilmengen erzeugten Untergruppen besprechen (Vgl. (2.2.15-16). Das Diagramm verdeutlicht, dass dabei alle bisherigen Resultate verwendet werden. Danach führen wir mit der Drehgruppe eine für die Physik besonders wichtige Gruppe ein.



3.2.5 Die von einem Gruppenelement erzeugte Untergruppe.

(2.5.1) Sei (G,·) irgendeine Gruppe und g∈G ein Element. Wir bilden die Abbildung

$\varepsilon_g = (\mathbb{Z}, n \mapsto g^n, G)$	mit $g^0 = e$ und g^{-n} invers zu g^n. $g^2 = gg$ usw. g äußerer Parameter zu ε_g.

(2.5.2) Diese Abbildung ε_g ist strukturerhaltend, wie man sofort prüft ($g^2g^3 = g^5$ oder $g^3g^{-2} = g^{-1}$usw.) Also ist Kern(ε_g) nach (2.4.19) eine Untergruppe von $\mathbb{Z}$ und Bild(ε_g) eine Untergruppe von G! Die Untergruppen von Z haben wir aber in (2.4.17) alle bestimmt. Gehen wir die Möglichkeiten einmal durch:

a) Kern(ε_g)=$\{0\}$ trivial. Dann ist nach (2.1.24) die Restriktion von ε_g auf Bild(ε_g) ein Isomorphismus und Bild(ε_g) ist **eine zu Z isomorphe Untergruppe**! Diese Untergruppe ist die von der einelementigen Teilmenge {g} erzeugte Untergruppe im Sinne von (2.2.16): **Also die kleinste Untergruppe, die g enthält.**

b) Kern(ε_g)=k$\mathbb{Z}$ und k$\neq$ 0. D.h. ε_g(k)=g^k =E = neutrales Element von G. Und k ist die **kleinste positive Zahl mit dieser Eigenschaft**. Benutzt man diese Relation, so folgt, dass Bild(ε_g) genau k verschiedene Elemente enthält, nämlich E,g,....,g^{k-1}. Das ist dieselbe Struktur wie bei der zyklischen Gruppe (der Ordnung k)! Tatsächlich ist - wie man sofort prüft ($C_k, \sigma^r \mapsto g^r, G$) ein (i.a. nicht surjektiver) Gruppenisomorphismus! Wir haben eine Darstellung der zyklischen Gruppe C_k in G. Das zu C_k isomorphe Bild ist ist die von g erzeugte Untergruppe die kleinste Untergruppe, die g enthält.

b1) Ein spezieller Fall ist k=1. Dann ist $g^1 = e$, d.h. g=e. Man erhält die triviale Untergruppe {e} von G. .

(2.5.3) Damit haben wir für jede Gruppe und jedes Element g dieser Gruppe eine Darstellung ε_g der ganzen Zahlen in dieser Gruppe. Die Darstellung ist entweder isomorph zu $\mathbb{Z}$ selbst oder aber hat die Form einer zyklischen Untergruppe, also einer "Uhrenarithmetik". Bild(ε_g) ist die von g erzeugte Untergruppe im Sinne von (2.2.16). Es ist also die kleinste Untergruppe von G, die das Element g enthält. Ist Bild(ε_g) endlich, so nennt man die Anzahl #Bild(ε_g) der Elemente dieser Untergruppeg *die Ordnung des Elementes g.*Natürlich kann eine Gruppe unendlicher Ordnung Elemente endlicher Ordnung haben. Das neutrale Element hat immer die Ordnung 1.

(2.5.4) Das ist offensichtlich ein Resultat von universeller Gültigkeit, das sich vielfach als nützlich erweist.

(2.5.5) Anwendungsbeispiel: Sei f: $\mathbb{R}^2 \to \mathbb{R}^2$ eine invertierbare Abbildung. Wir definieren

rekursiv $f^n = f \circ f^{n-1}$ sowie $f^1 = f$ und $f^0 = id_{\mathbb{R}^2}$ und f^{-1} = zu f inverse Abbildung. Dann bildet $\{f^n | n \varepsilon \mathbb{Z}\}$ offenbar eine Gruppe. Wählt man jetzt $x_0 \varepsilon \mathbb{R}^2$ fest, so bildet die Punktmenge $B(x_0) = \{f^n(x_0) \mid n \varepsilon \mathbb{Z}\}$ einerseits eine Menge, die interessante Aufschlüsse über das Verhalten der Abbildung f liefert. Andererseits liegt die oben beschriebene Situation vor. $B(x_0)$ muß entweder isomorph zur Gruppe $\mathbb{Z}$ sein oder aber zu einer zyklischen Gruppe C_k. Dann besteht $B(x_0)$ aber nur aus k Punkten, auf denen f zyklisch wirkt, geradeso wie das Zeigerstellen bei unserer k-Stundenuhr! Im Bereich der sog. chaotischen Systeme erweist sich dies als nützlicher grundlegender Sachverhalt.

3.2.6 Die Drehgruppe.

(2.6.1) Wir führen eine Gruppe ein, der im Bereich der Physik, aber auch der Geometrie eine große, ja zentrale Bedeutung zukommt. Mit Hilfe einer sinnvoll angelegten Kenntnis dieser Gruppe gelangt man relativ leicht zu einer Reihe weiterer wichtiger Gruppen und zur Behandlung zahlreicher nicht leichter Probleme.

(2.6.2) Wir betrachten den physikalischen Konfigurationsraum in der Form eines V_0^3. D.h. wir wählen einen festen Ursprung 0 und beschreiben alle Punkte durch ihre Ortsvektoren. Überdies verwenden wir in diesem Raum nicht nur seine Vektorraumstruktur, sondern auch das euklidische Skalarprodukt der Vektoren. D.h. wir können Winkel zwischen Vektoren und Längen von Vektoren vektoriell beschreiben. Das Skalarprodukt der beiden Vektoren $\vec{a}$ und $\vec{b}$ bezeichnen wir mit $(\vec{a} \cdot \vec{b})$.

(2.6.3) Nun ist nach (2.1.9) die Menge $\mathfrak{B}(V_0^3, V_0^3)$ aller bijektiven Abbildungen dieses Raumes eine Gruppe. Verknüpfung ist dabei die Hintereinanderschaltung der Abbildungen. Aber diese Gruppe ist zu groß, um handhabbar und für die üblichen Anwendungen nützlich zu sein. Ein typisches Gruppenelement wird die Punkte derart durcheinanderwirbeln, daß keinerlei Struktur mehr erkennbar ist. Also sollte man zu einer kleineren Gruppe, einer Untergruppe übergehen, die nur geometrisch gut interpretierbare Elemente enthält.

(2.6.4) Hier gibt es einen herausragenden Kandidaten, der durch die folgende wichtige **Definition** fixiert wird:

> Wir nennen eine bijektive Abbildung $R: V_0^3 \to V_0^3$ eine *Drehung* (im weiten Sinn) oder *orthogonale Transformation des Raumes*, wenn sie alle Skalarprodukte unverändert läßt. D.h. genauer, wenn $(R(\vec{x}) \cdot R(\vec{y})) = (\vec{x} \cdot \vec{y})$ für alle $\vec{x}, \vec{y} \in V_0^3$ gilt.

(2.6.5) Was bedeutet das? Zur Veranschaulichung sollten Sie den Zuordnungsstandpunkt einnehmen. Zunächst wählen wir $\vec{x} = \vec{y}$. Dann besagt die Forderung $|\vec{x}|^2 = (\vec{x} \cdot \vec{x}) = (R(\vec{x}) \cdot R(\vec{x})) = |R(\vec{x})|^2$. D.h. der Vektor und sein Bild haben beide dieselbe Länge! Die Abbildung kann die Länge des Vektors nicht verändern, höchstens seine Richtung. Insbesondere muß $R(\vec{0}) = \vec{0}$ gelten. Der Nullvektor wird auf sich selbst abgebildet.

Der Winkel zwischen zwei Vektoren ungleich Null bestimmt sich über die bekannte Formel $\cos(\phi) = \frac{(\vec{a} \cdot \vec{b})}{|\vec{a}||\vec{b}|}$.

Man sieht sofort: **Auch der Winkel wird durch die Transformation nicht geändert.** Die Teilmenge $F \subset V_0^3$ beschreibe eine geometrische Figur, die den Ursprung enthält. Dann beschreibt das Bild $\underline{R}(F)$ eine dazu kongruente Figur, wobei der im Ursprung liegende Punkt fest geblieben ist. Alle Abstände von Punkten der Figur sowie Winkel zwischen Strecken der Figur müssen ja vor und nach der Transformation dieselben- sein. Beachten Sie: Wir sagen nichts über den Winkel, den ein Vektor $\vec{x}$ und sein Bild $R(\vec{x})$ miteinander bilden. Aber wir sagen, dass der Winkel zwischen $\vec{a}$ und $\vec{b}$ ebenso groß ist, wie der zwischen den beiden Bildern $R(\vec{a})$ und $R(\vec{b})$. Unsere Erfahrungen und Vorstellungen sagen uns, dass die transformierte Figur $\underline{R}(F)$ aus F durch Drehungen (um den Ursprung) und eventuelle

Spiegelungen hervorgegangen sein muß. Die Möglichkeit det Spiegelung sollte man nicht übersehen. Die Punkte des Raumes werden durch die bijektive bijektive orthogonale Transformation nicht mehr beliebig durcheinandergewirbelt, sondern starr miteinander verbunden um den Ursprung bewegt, eventuell noch einmal gespiegelt.

□ Zeigen Sie, dass man in (2.6.4) bijektiv durch surjektiv abschwächen kann.

(2.6.6) Ein typisches und wichtiges Anwendungsbeispiel det Physik: Es seien K und L zwei kartesische Rechtssysteme des V_0^3. Beide System haben also denselben Ursprung. Dann entsteht L aus K durch eine orthogonale Transformation des Raumes, die die alten Koordinateneinheitsvektoren auf die neuen abbildet. Wir werden hierauf in Kap. 10 ausführlich zurückkommen.

(2,6.7) Das weitere .Vorgehen sieht jetzt so aus:

> **Satz**: Es sei $O(V_0^3) \subset \mathfrak{B}(V_0^3, V_0^3)$ die Menge aller orthogonalen Transformationen des V_0^3. Dann ist $O(V_0^3)$ eine Untergruppe, die Gruppe der orthogonalen Transformationen des V_0^3. Oder kurz: Die **orthogonale Gruppe**.

(2.6.8) Der Beweis erfolgt wie üblich mit Hilfe des Untergruppenkriteriums. Zunächst argumentieren wit wie folgt:

- Sei $R \in (O(V_0^3)$, also $(R(\vec{a}) \cdot R(\vec{b}) = (\vec{a} \cdot \vec{b})$. Nun ist R bijektiv, so dass es Urbilder $\vec{x}, \vec{y}$ mit $\vec{a} = R^{-1}(\vec{x})$ und $\vec{b} = R^{-1}(\vec{y})$ gibt. Einsetzen gibt $(\vec{a} \cdot \vec{b}) = (R^{-1}(\vec{a}) \cdot R^{-1}(\vec{b}))$ für alle $\vec{a}$ und $\vec{b}$. Sei jetzt S eine zweite orthogonale Transformation. Dann können wir die Kriteriumsbedingung $S \circ R^{-1} \in O(V_0^3)$ sofort wie folgt nachrechnen:

$$\left(S \circ R^{-1}(\vec{a}) \cdot S \circ R^{-1}(\vec{b})\right) = \left(S(R^{-1}(\vec{a})) \cdot S(R^{-1}(\vec{b}))\right) = \left(R^{-1}(\vec{a}) \cdot R^{-1}(\vec{b})\right) = \left(\vec{a} \cdot \vec{b}\right).$$

  Also liegt tatsächlich eine Untergruppe vor, alle Gruppeneigenschaften gelten.

(2.6.9) Nicht selten erweckt eine Situation wie die jetzt vorliegende ein Unbehagen, das leicht in Abneigung und Verurteilung abstrakter Mathematik als unnötig, lebensfern, schrecklich usw. umschlägt. Das primäre Unbehagen ist richtig, wichtig und sehr zu unterstützen. Falsch ist nur der anschließende, vielelfach einfach auf Bequemlichkeit basierende Umschlag in die reine Ablehnung. Statt dessen sollte man sich Gedanken über die Ursache des Unbehagens machen, dieses inhalatlich zu präzisieren versuchen. Dann kann man feststeillen, das alles, was man vermißt an anderer Stelle durch Strukturaufstockung noch eingebracht wird oder leicht einbringbar ist. Was wir im Augenblick über die Drehgruppe wissen, ist nur eine erste grobe, aber dafür universale Skizze. Für alle späteren genaueren Fragen kann und sollte man von dieser Skizze ausgehen. Man kann verfeinern oder ausmalen, ohne wieder alles fortradieren zu müssen! Und man hat mit der Skizze stets einen Einstieg, der die allgemeinen Ideen mit den konkreten Problemen verbindet.

(2.6.10) Hier im Fall der orthogonalen Transformationen kann, ja sollte man beispielsweise die Quantifizierung, die konkreten Zahlbeschreibung der Drehoperationen vermissen. Wie sieht so eine Abbildung-konkret aus, wie kann man sie mit Hilfe von Zahlen darstellen? Darüber sagt unser Zugang bisher nichts. Es wird sich zeigen, daß man diese Frage günstig mit den Methoden der linearen Algebra des Kapitels 4 behandeln kann. Aber für eine Reihe von Fragen ist diese Aufstockung des Wissens keineswegs erforderlich. ja nicht einmal nützlich. Ein wichtiges Beispiel ist das Problem der Ubertragung der orthogonalen Gruppe auf andere Konfigurationsräume. Hierfür erweist sich die Analogisierung zu obiger Konstruktion (2.6.4-7) als ganz einfach, liefert etwa einen problemlosen Zugang zur Relativitätstheorie (Kap 10) Der Versuch. dasselbe mit Hilfe schön handfester Matrixformeln zu produzieren ist weitaus mühsamer.

(2.6.11) Wir werden im anschließenden Kapitel mit Hilfe von Gruppenoperationen die **orthogonalen Transformationen der Ebene** behandeln, für die eine explizite Darstellung der Gruppenelemente leicht tu erlangen ist. Dieser Einstieg deutet dann auch bereits an, wie man später das schwierigere Problem des dreidimenaionalen Konfigurationsraumes angehen kann.

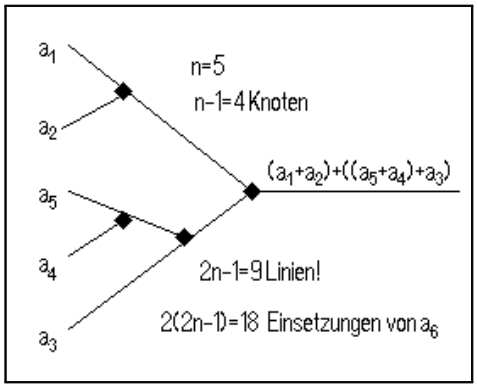
3.2.7 Die Anzahl zulässiger Beklammerungen

(2.7.1) Sei (H,+) eine kommutative Halbgruppe mit neutralem Element 0. Weiter $a_1, a_2, ..., a_n$ Elemente aus H. Schließlich sei $\mathcal{A}_n$ die Menge der zulässigen Beklammerungen von $a_1 + a_2 + ... + a_n$ ohne

Vorgabe der Reihenfolge. (In der kommutativen Halbgruppe liefert jede zulässige Beklammerung denselben Wert - vollkommen unabhängig von der inhaltlichen Bedeutung der Halbgruppenelemente! Die gesamte nachfolgende Überlegung ist in diesem allgemeinen Rahmen möglich.)

(2.7.2) Sei A_n eine solche Beklammerung. (Etwa $(a_1+a_2)+((a_5+a_4)+a_3)$ für n=5. Das ist ein Element von $\mathcal{A}_5$). Uns interessiert $\#\mathcal{A}_n$, die Zahl der Elemente dieser Menge. Beispielsweise ist $\#\mathcal{A}_5$=1680 wie wir sehen werden. Division durch n! ergibt dann die Zahl der Beklammerungen bei fester Reihenfolge. Wir haben versprochen, diese Zahlen zu bestimmen.

Weiter sei $G(A_n)$ eine graphische Darstellung von A_n mit Hilfe des zugehörigen Verlaufsdiagramms. Für unsere Beispiel kann das so aussehen:

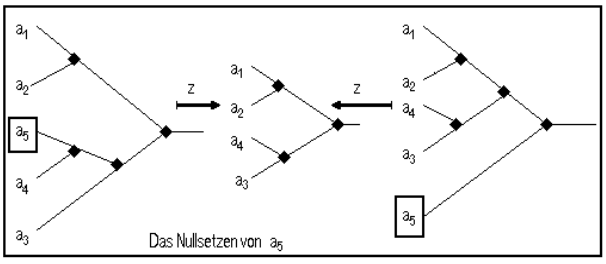


Die Zahlangaben des Beispiels gelten offenbar allgmein: $G(A_n)$ hat stets (n-l) innere Knoten (= Additionsautomaten) sowie 2(n-l)+l=2n-1 Linien, die alle auftretenden Leitungsbahnen repräsentieren: 2 Linien links vor jedem Knoten, dazu die Endlinie des Ausganges.

Sei $G(\mathcal{A}_n)$ die Menge all dieser Graphen. $G=(\mathcal{A}_n, A_n \mapsto G(A_n), G(\mathcal{A}_n))$ ist eine bijektive Abbildung vom Codierungstyp. Es genügt $\#G(\mathcal{A}_n)$ zu bestimmen.

(2.7.3) **Jetzt kommt die eigentliche Idee**: Wir möchten eine Rekursionsformel für $\#G(\mathcal{A}_n)$ aufstellen. Dazu müssen wir das zu n gehörige System mit dem für (n-l) in Beziehung setzen, möglichst das erstere aus letzterem konstruieren. Dies tun wir, indem wir a_n=0=neutrales Element der Halbgruppe setzen! Dann wird (u.U. nach Fortlassen unnötiger Klammern) aus A_n stets ein Element aus $\mathcal{A}_{n-1}$. Im zugehörigen Graphen fällt die zu a_n gehörige Linie fort samt dem zugehörigen (+)-Knoten. Dies bedeutet, dass wir eine Abbildung z: $G(\mathcal{A}_n) \rightarrow G(\mathcal{A}_{n-1})$ haben.

Diese Abbildung ist surjektiv, aber nicht injektiv. Die gesuchte Konstruktion wäre die Umkehrung dieser Abbildung. Das Bild zeigt zwei Beispiele der Konstruktion.



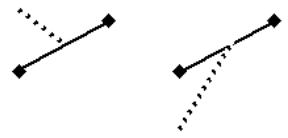
(2.7.4) Wir wählen auf der Wertemenge $G(\mathcal{A}_{n-1})$ die atomare Partition und bilden die durch die inverse Abbildung erzeugte Partition auf $G(\mathcal{A}_n)$. Vgl.Kap.1.3.3. Uns interessieren die entstehenden Klassen und deren Elementzahl. Angenommen jede Klasse hat genau k_n Elemente. Dann erhalten wir die einfache Rekursionsformel

$$\#G(\mathcal{A}_n) = k_n \#G(\mathcal{A}_{n-1})$$

von der wir hoffen können, sie induktiv zu Iösen.

Wie sehen die Klassen aus? Sie lassen sich bemerkenswert leicht bestimmen. Man muß nur in irgendeine der Linien von $z(G(A_n))$ - also dem , was durch Nullsetzen von a_n entsteht - den zuätzlichgen (+)-Automaten (oder Knoten) einfügen, in dessen einen Eingabeschlitz das zusätzliche Element a_n

eingegeben werden soll.



Die zwei möglichen Neueinsetzungen. a_n komt vor oder hinter dem Partner in der Verknüpfung zu stehen.

Das Einfügen geht für jede alte Linie auf genau zwei Weisen. Da es aber in G$\in G(\mathcal{A}_{n-1})$ genau 2(n-2)+1=2n-3 Linien gibt, folgt k_n=2(2n-3). **Somit haben tatsächlich alle Klassen dieselbe Anzahl.**

(2.7.5) Mit Hilfe der Rekursionsformel berechnet man die ersten Werte sofort zu

Anzahl n	1	2	3	4	5	6	7
$\#\mathcal{A}_n$	1	2	12	120	1680	30240	665280
$\#\mathcal{A}_n/n!$	1	1	2	5	14	42	132

(2.7.6) Inspektion der Rekursion unter Beachtung der ersten Werte (bzw. Induktion) ergibt schließlich das folgende allgemeine Resultat:

- Die Anzahl zulässiger Beklammerungen ohne Festlegung der Reihenfolge genügt der Rekursionsformel #G($\mathcal{A}_n$)=k_n#G($\mathcal{A}_{n-1}$) und wird explizit gegeben durch $\#(\mathcal{A}_n) = 2^{-1}(2n-3)!!$ mit (2k-1)!!=1·3·5·.....·(2k-1)
- Alternativ gilt $\#(\mathcal{A}_n) = 2\frac{(2n-3)!}{(n-2)!}$
- Für die Anzahl zulässiger Beklammerungen mit festgelegter Reihenfolge der Summanden folgt: $\frac{\#(\mathcal{A}_n)}{n!} = \frac{1}{n}\binom{2n-2}{n-1}$

□ Tragen Sie mit Hilfe eines Computeralgebraprogrammes den Logarithmus von $\frac{\#(\mathcal{A}_n)}{n!}$ gegen n auf, damit Sie eine Vorstellung vom Wachstum dieser Zahlen gewinnen. Vergleichen sie mit dem in Kap1.(3.2.7) bestimmten Wachstumsverhalten. Welche Ulnterschiede bestehen und warum?