****

Höhere Mathematik für Physiker
Teil I

F. Krause

Kapitel 3
Algebraische Strukturen

****

Copyright F.Krause

Inhalt des Kapitels Algebraische Strukturen

        * 3.3.2a Die Bahnen
        * 3.3.2b Die Stabilisatoren
        * 3.3.2c Die Transformationen der Objektmenge
        * 3.3.2.d Wandel und Erhaltung (2)
    - **3.3.3 Die Gruppe selbst als Konfigurationsraum: Analyse der Gruppenstruktur (2)**
        * 3.3.3a Konjugationsklassen
    - **3.3.4 Permutationen**
        * 3.3.4a Klassifikation der Partitionen einer endlichen Menge
        * 3.3.4b Die Zykeldarstellung der Permutationen
    - **3.3.5 Wandel und Erhaltung (3): Einschränkungen der Gruppenoperation**
        * 3.3.5a Entwicklungsprozesse ("Evolution")
        * 3.3.5b Transformationsgruppen
        * 3.3.5c Symmetriegruppen
        * 3.3.5d Die kleinen Transformationen von Funktionen
        * 3.3.6 Übersicht

- **3.4 Das System der algebraischen Strukturen (2)**
    - **3.4.1 Übersichtsschema**
    - **3.4.2 Ringe und Körper**
        * 3.4.2a Die Restklassenringe
        * 3.4.2b Die Charakteristik
        * 3.4.2c Polynomringe
        * 3.4.2d Zusammenfassung
    - **3.4.3 Vektorräume und Moduln**

Kapitel 3: **Algebraische Stukturen**

3.1 **Das Begriffssystem**

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

$$\mathsf{T} : M \times N \to L$$

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 $\intercal$((a,b)) - wie es der Formalismus der Abbildungstheorie verlangen würde - sondern a$\intercal$b, so wie man es von 2+3 oder 2·3 oder a-b her gewohnt ist. ($\intercal$ die Abbildung, $\intercal$(....) 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 $\intercal : (a, b) \mapsto a \intercal b$ statt des ausführlichen $(\mathrm{M}\times N, (a, b) \mapsto a \intercal b, L)$ 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):

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

(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 Ablaufs 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 Größ en 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 $\top$ 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=(l+ 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.

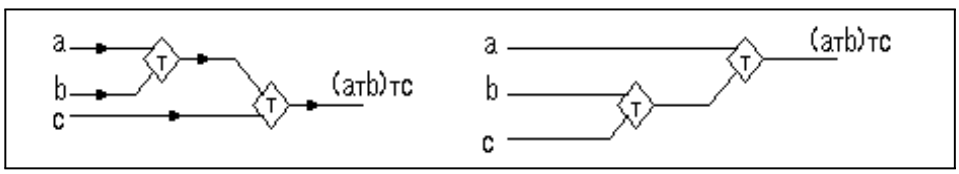
3.1.3a Das Assoziativgesetz

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

D.h. für ein assoziatives $\top$ 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 $(a \top b) \top c = a \top (b \top c)$. 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 $a_1 \top a_2 \top ....\top a_n$. 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 $\top : M \times M \to M$ eine assoziative innere Verknüpfung. Es sei n$\in \mathbb{N}$ mit n≥ 1 und $a_1, a_2, ..., a_n \in M$. Dann ergeben alle A_n zulässigen Beklammerungen von $a_1 \top a_2 \top ... \top a_n$ dasselbe Element aus M.

(1.3.10) Konkret: Für n=4 gibt es 5 zulässige Beklammerungen (a⊤b)⊤(c⊤d) , ((a⊤b)⊤c)⊤d , (a ⊤(b⊤c))⊤d , a⊤((b⊤c)⊤d) und a⊤(b⊤(c⊤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⊤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⊤c)⊤d angewandt werden ("für alle Elemente aus M"). Tut man das und ersetzt man am Ende A wieder durch a⊤b so erhält man die Beziehung ((a⊤b)⊤c)⊤d = (a⊤b)⊤(c⊤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 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 Induktionsvorraussetzung 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 $B_4 = 4! \cdot 5 = 120$. 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 $\top: M \times M \to M$ 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 heiß t 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$\in M$ heißt *neutrales Element von* $\top$, wenn für alle x$\in M$ 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 $1 \in \mathbb{R}$ 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=E, 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.

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

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$\cap$A =T für jede Teilmenge T von A. D.h. hier ist die gesamte Menge neutral. Dagegen gibt es kaum inverse Elemente. Denn X$\cap$T=A hat nur für X=A eine Lösung und X$\cup$T=B hat nur für T=B eine Lösung! Überdies ist $\emptyset$ bezüglich $\cap$ und A bezüglich $\cup$ 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 $\cdot$. 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, müss te 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.

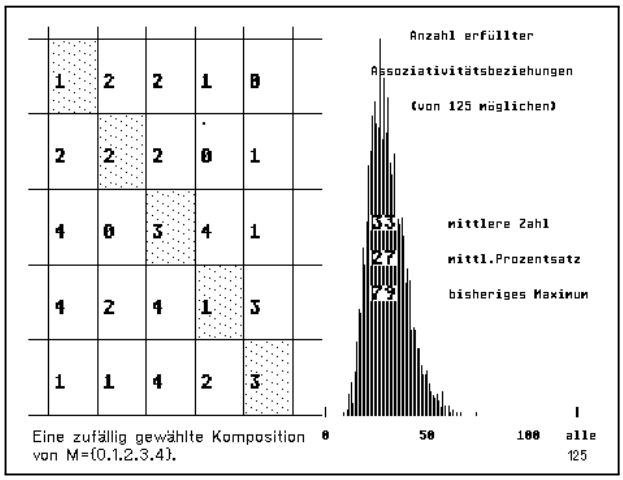
Die Prüfung der Assoziativität ist mühsamer, da sie zweifache Anwendung der Tafel verlangt. Ein solcher direkter Nachweis wird auch kaum je benötigt. Wir werden bessere Methoden kennenlernen.

(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.



■ ■ ■ ■ ■

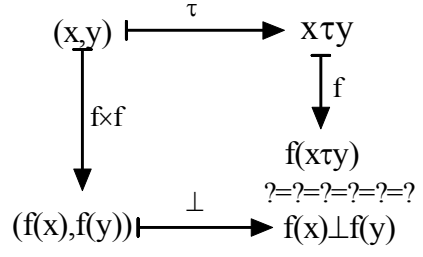
3.1.5 **Strukturerhaltende Abbildungen**

(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.
$\intercal : G \times G \to G$ 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:
$f(x \intercal y) = f(x) \perp f(y)$.
Das Diagramm zeigt die Bedeutung dieser Gleichung, die auch als Gleichheit zweier Automatenschaltungen interpretiert werden kann.

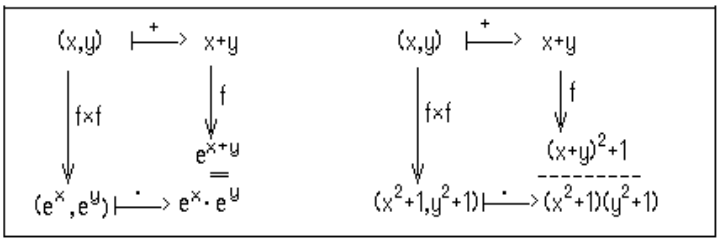


(1.5.3) Startet man mit zwei Elementen x,y aus G, so gibt es zwei Wege, um zu einem Verknüpfungsresultat in H zu gelangen. Das Diagramm zeigt die beiden Möglichkeiten auf. Die Resultate werden in der Regel unterschiedlich sein. Nur in ganz speziellen Fällen wird stets dasselbe herauskommen und das ist 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(xτy) 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 $\intercal = +$ 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 ·. Kurz ($\mathbb{R}$,+) und ($\mathbb{R}$,·) 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?



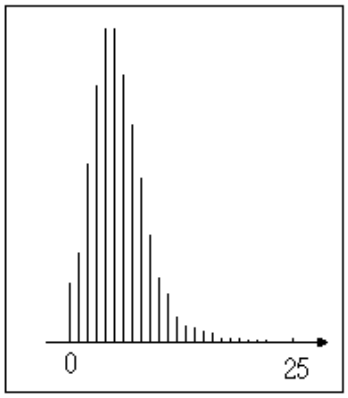
Im ersten Fall stellt eine der Rechenregeln für die Exponentialfunktion sicher, dass beide Rechenwege, beide Wege im Diagramm, dasselbe Resutat liefern. Die Abbildung exp ist strukterhaltend. Im zweiten Fall erhält man unterschiedliche Ergebnisse.

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:

$\alpha)$	Gewisse Mengen werden vorgegeben.
$\beta)$	Für diese Mengen werden bestimmte Kompositionen eingeführt.
$\gamma)$	Durch Axiome für die Verknüpfungen werden Eigenschaften festgelegt.
$\delta)$	Die (zugehörigen) strukturerhaltenden Abbildungen werden eingeführt.
$\varepsilon)$	Übertragungsprobleme werden behandelt.

(2.0.3) Die letzten Schritte $\delta)$ und $\varepsilon)$ 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 $\varepsilon)$ 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$\to$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$\to$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:

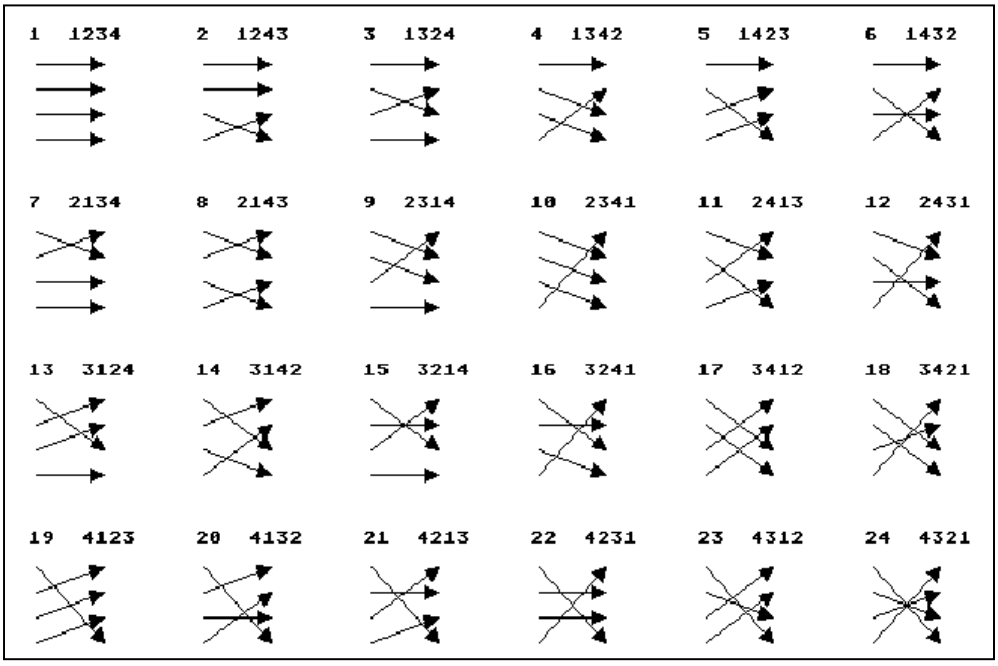
Es sei M eine nicht leere Menge und $\mathfrak{B}$(M,M) die Menge aller bijektiven Abbildungen M$\to$M. Als Verknüpfung nehmen wir die Zusammensetzung $\circ$ von Abbildungen. Die ist konstruktionsgmäß immer assoziativ. Die triviale Abbildung id_M ist bezüglich $\circ$ neutral und die inverse Abbildung 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?

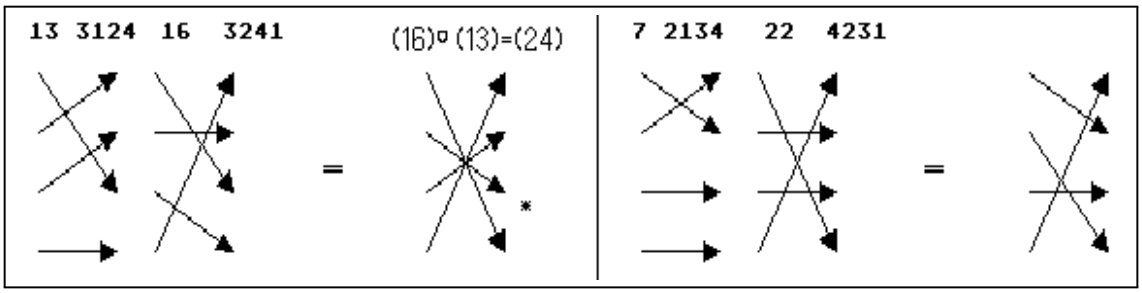
(2.1.10) Als Beispiel zeigen wir nachfolgend die 4!=24 Elemente der Permutationsgruppe für vierelementige Mengen. Wir nehmen M={1,2,3,4}. Wir geben die Gruppenelemente einmal als Pfeilschema und überdies vom Feldstandpunkt. (Also vier Feldplätze und darauf jeweils die zugeordnete Zahl aus der Urbild-

menge (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
$a^{-1} \top (a \top x) = a^{-1} \top b$	Multiplikation
$(a^{-1} \top a) \top x = a^{-1} \top b$	Assoziativität
$e \top x = a^{-1} \top b$	*Invers.* e bezeichne neutrales Element.
$x = a^{-1} \top b$	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∈ 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=$a^{-1} \top b$ gegeben.

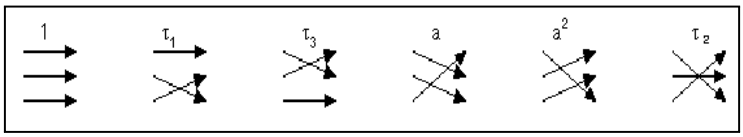
Im Fall einer Halbgruppe hätten wir bereits den ersten Schritt (Existenz von a^{-1}) nicht sicherstellen können.

□ 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$\circ y$ ist im zugehörigen Feldpunkt aufgetragen. Etwa $\tau_1 \circ a = \tau_2$. Mit der Tafel kann man Gleichungen des Typs u$\circ x = v$ 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$\circ$x=B eindeutig lösbar sind. Auch alle Spalten enthalten die Gruppenelemente genau einmal. Und die Spalten liefern offenbar die Lösungen der Gleichung x$\circ$A=B. In der Diagonalen dagegen stehen die Quadrate x$\circ$x. In unserem Fall ist x$\circ$x=a lösbar durch x=a^2. Dagegen ist x$\circ$x=τ_1 unlösbar, denn dieses Element taucht in der Diagonalen nie auf. Und x$\circ$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,$\cdot$) Gruppe und g,h$\in G$. Wir nehmen an, dass wir die Inversen Elemente g^{-1} und h^{-1} kennen. Was läßt sich dann über das inverse Element von $g \cdot h$ aussagen? Das inverse Element zu k$\in G$ ist Lösung der Gleichung $k \cdot x = e$. Also müssen wir $(g \cdot h) \cdot x = e$ lösen. Die in diesem Abschnitt beschriebenen Methoden liefern sofort x=$h^{-1} \cdot g^{-1}$. D.h. es gilt:

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

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 $x \cdot k = e$ anstelle von $k \cdot x = e$ starten?

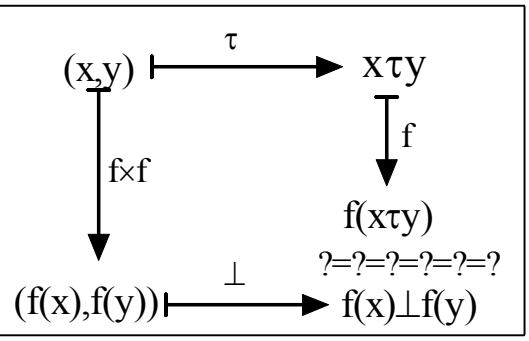
3.2.lb **Gruppenhomomorphismen**

(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$\to H$ eine Abbildung. Dann heißt f *Gruppenhomomorphismus (von G nach H)*, wenn für **alle** x,y$\in G$ gilt

f(xτy) = 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 $\cdot$, 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.

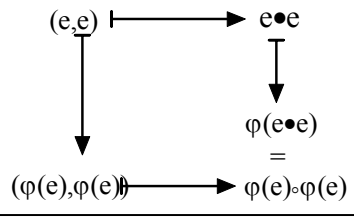
Es sei φ:G→ H ein Gruppenhomomorphismus von (G,$\cdot$) nach (H,$\circ$)
Weiter sei e das neutrale element von G und E das von H. Dann gilt:
a) $\varphi(e) = E$ Das Bild des neutralen Elements ist stets neutral.
b) $\varphi(x^{-1}) = (\varphi(x))^{-1}$. Das Bild des inversen Elementes ist das Inverse 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 $(\varphi(y))^{-1}$ **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$\times$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$\rightarrow G$. Kann man $\mathcal{F}(M,G)$ zur Gruppe machen?
ÜW	Es sei M Menge, (G,$\circ$) Gruppe und f:G$\rightarrow M$ 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$\times$H$\rightarrow$G bilden. Aber wir können nicht sicher sein, daß deren Werte wieder in H liegen, also $\circ$:H$\times$H$\rightarrow$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$\times$H$\rightarrow$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,$\circ$) Gruppe und H$\subset G$ nichtleere Teilmenge.
Weiter gelte: Mit x,y$\in H$ gilt auch immer x$\circ y^{-1} \in H$.
Dann ist (H,$\circ$) eine Untergruppe von (G,$\circ$).

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

(2.2.11) Ein Beispiel: Sei (V_0^3,+) die additive Gruppe der geometrischen Pfeile und E$\subset V_0^3$ eine Ebene durch den Nullpunkt. Damit haben wir unsere Teilmenge. Nun ist zu prüfen, ob mit $\vec{x},\vec{y} \in E$ auch ($\vec{x}$-$\vec{y}$)$\in$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$\circ$y statt x$\circ$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$\in$H$\Rightarrow$x$\circ$y^{-1} $\in$H. Damit müssen wir zeigen, dass H wirklich eine Gruppenstruktur besitzt. Zunächst ist H$\neq \emptyset$ voraussgestzt. D.h. es gibt mindestens ein Element h$\in$H. Dann gilt auch h,h$\in$H. Nach (K) ist dann h$\circ$h^{-1} = e$\in$H. Dabei ist e das neutrale Element von G und wir sehen: Dieses liegt in H und ist auch dort neutral. Sei h$\in$H beliebig. Dann ist e,h$\in$H. Nach (K) folgt e$\circ$h$^{-1} = h^{-1} \in H$. D.h. für jedes h$\in$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$\in$H. Dann ist auch g,h^{-1} $\in$H. Anwenden von (K) gibt: g$\circ$(h^{-1})$^{-1}$= g$\circ$h$\in$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,$\circ$) Gruppe und H_1, H_2 seien Untergruppen.
Dann ist auch der Durchschnitt $H_1 \cap H_2$ 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$\in H_1 \cap H_2$. Nach Definition des Durchschnitts gilt dann x,y$\in$H$_1$ und x,y$\in$H$_2$. Da beides Untergruppen sind, folgt x$\circ$y^{-1} $\in$H$_1$ und x$\circ$y^{-1} $\in$H$_2$ Also ist x$\circ$y$^{-1} \in H_1 \cap H_2$. **Es liegt eine Untergruppe vor.**

□ Probieren Sie selbst: Es sei $(\mathbb{C},\cdot)$ die multiplikative Gruppe aller komplexen Zahlen $\neq 0$. Weiter sei U=$\{z|z\in \mathbb{C}, |z|=1\}$. Dann ist U zugehörige Untergruppe. Hinweis: Jedes $z\in U$ 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 $g\circ h$, $g\circ h^{-1}$ 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 $(G\times H, \intercal\times\perp)$ Gruppe, wobei die Verknüpfung wie folgt definiert ist:
> $\intercal\times\perp=((G\times H)\times(G\times H)),(g_1,h_1),(g_2,h_2)\mapsto((g_1\intercal g_2),(h_1\perp h_2)),G\times H))$
> 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 $\top$ statt $\top \times \top$, 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.

$f\bar{\top}g=((M,x\mapsto(f\bar{\top}g)(x)=f(x)\top g(x),G)$	**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.

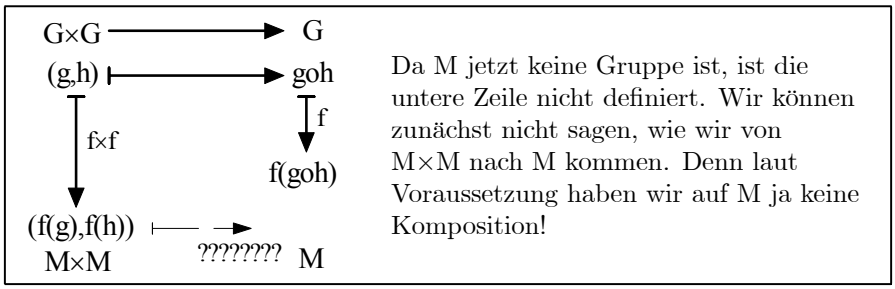
(2.2.28) Fassen wir zusammen: **Durch Wertemengenübertragung (der Struktur) wird** $\mathcal{F}$(M,G) **für eine beliebige Menge M zu einer Gruppe.**

(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**

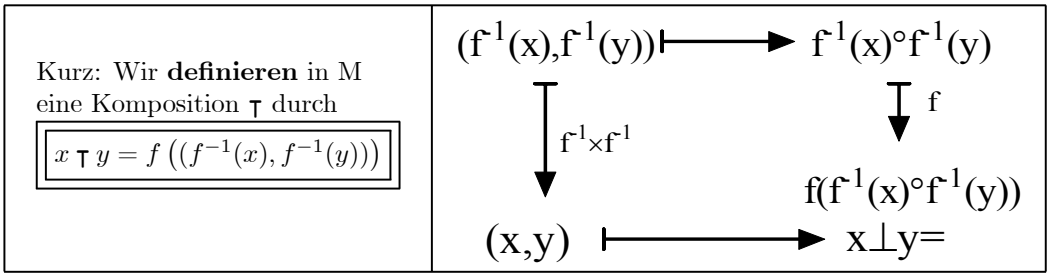
(2.2.30) Soeben haben wir **alle** Abbildungen M→G betrachtet. Jetzt betrachten wir umgekehrt **eine** feste **bijektive** Abbildung f:G→M.

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)$\in M \times M$, bilden dazu $(\mathrm{f}^{-1}(x), f^{-1}(y)) \in G \times G$. Das verknüpfen wir mit der Komposition aus (g,∘) zu $\mathrm{f}^{-1}(x) \circ f^{-1}(y) \in G$ 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 ⋆, 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 Eintragungen in 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 einführen.

(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$\to$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$\to$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$\to$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$\mapsto$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$\cdot$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. Was die Zahl der Klassen betrifft, geben wir diese 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.

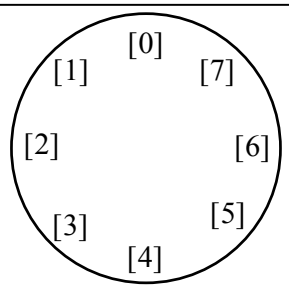
3.2.4a **Die zyklischen Gruppen**

(2.4.1) In Kap.I.3 haben wir für jedes k$\in \mathbb{N}$ mit k>1 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 verschiedene Klassen [r]=$\{7n|n=r+ks, s\in \mathbb{N}\}$ und r=0,1,...,k-1. Die Menge dieser Klassen - also die zugehörige Partition - bezeichnet man traditionellerweise mit $\mathbb{Z}/(k)$, 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 $(\mathbb{Z}, r \mapsto [r], \mathbb{Z}/(k))$ 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** $\mathbb{Z}/(\mathrm{k})$ **jetzt zu einer Gruppe machen**. Das ist ein Übertragungsproblem vom Typ (ÜR) aus (2.2.3). Als Verknüpfung wählen wir die Stundenaddition. Genauer gesagt setzen wir:

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

(2.4.4) Diese Gleichung wirft ein Problem auf: Die *Wohldefiniertheitsfrage.* n und m sind 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 eventuell andere 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 $(\mathbb{Z}/(\mathrm{k}),+)$ 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 $\mathbb{Z}/(\mathrm{k})$={[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 $\mathbb{Z}/(\mathrm{k})$ 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 $(\mathbb{C} - \{0\}, \cdot)$.

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 liegen 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 liegen 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 $(\mathbb{Z}, +)$. 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 $0\mathbb{Z}$. Das snd 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.

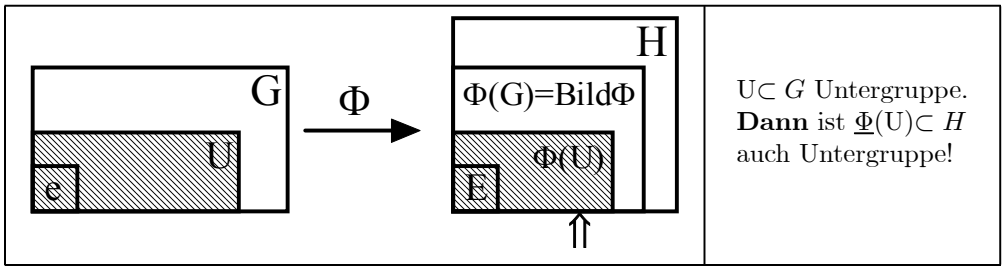
(2.4.19) **Satz:**

> Es sei Φ:G→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.

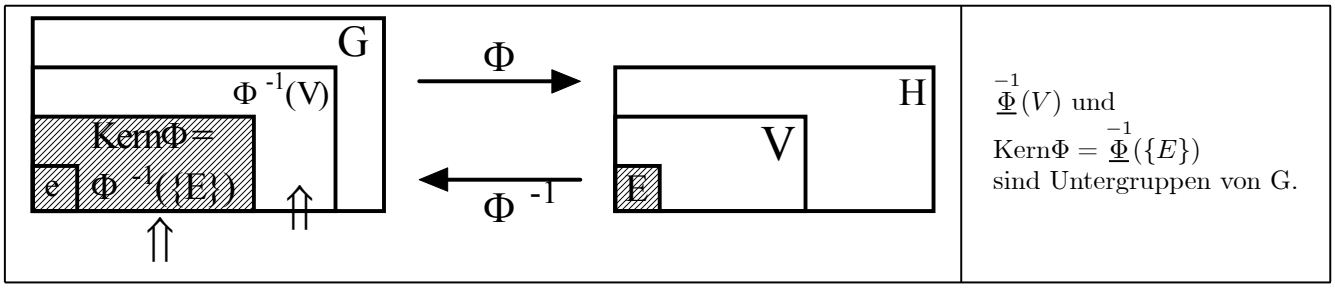
Zur Erinnerung die mengentheoretischen Definitionen aus Kap.1:

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

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

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

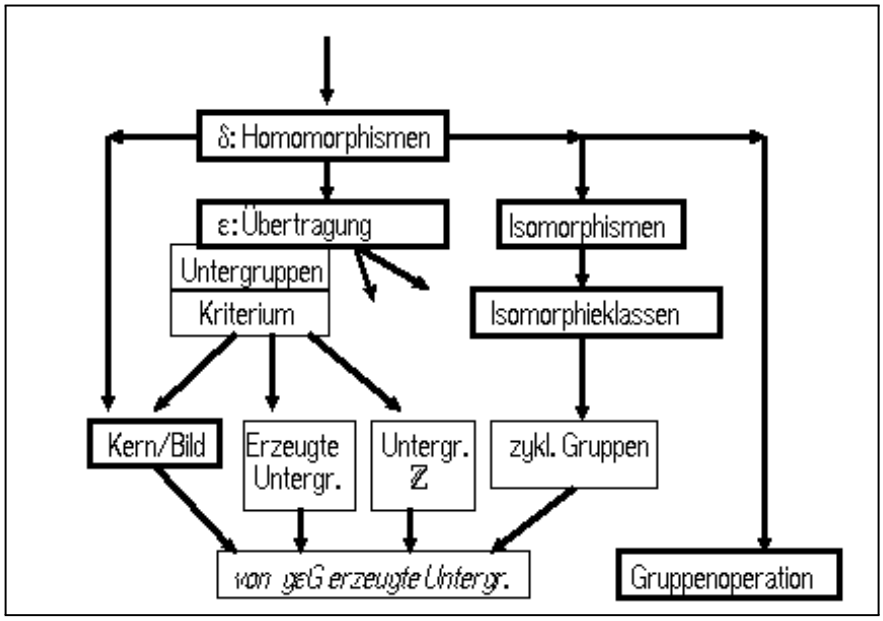
$$xy^{-1} = \Phi(a)(\Phi(b))^{-1} = \Phi(a)\Phi(b^{-1}) = \Phi(ab^{-1}) \in \underline{\Phi}(U)$$

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 Untergruppe *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=fof^{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 $(\mathrm{R}(\vec{x})\cdot\mathrm{R}(\vec{y}))=(\vec{x}\cdot\vec{y})$ 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 $\mathrm{R}(\vec{0})=\vec{0}$ 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 $\underline{\mathrm{R}}$(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 $\underline{\mathrm{R}}$(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 $\mathrm{O}(\mathrm{V}_0^3) \subset \mathfrak{B}(V_0^3, V_0^3)$ die Menge aller orthogonalen Transformationen des V_0^3. Dann ist $\mathrm{O}(\mathrm{V}_0^3)$ 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 $(\mathrm{R}(\vec{a})\cdot\mathrm{R}(\vec{b}))=(\vec{a}\cdot\vec{b})$. 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 $(\vec{a}\cdot\vec{b})=(\mathrm{R}^{-1}(\vec{a})\cdot\mathrm{R}^{-1}(\vec{b}))$ 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.

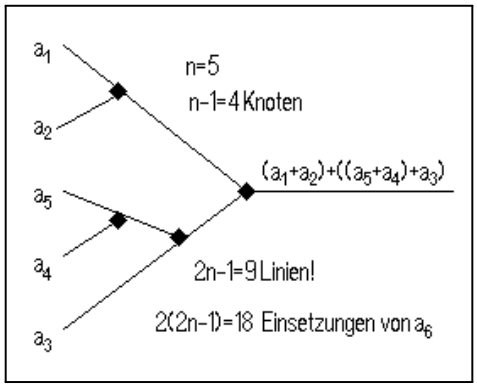
(2.6.11) Wir werden im anschließenden Kapitel mit Hilfe von Gruppenoperationen die **orthogonalen Transformationen der Ebene** behandeln, für die eine explizite Darstellung der Gruppenelemente leicht tu erlangen ist. Dieser Einstieg deutet dann auch bereits an, wie man später das schwierigere Problem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

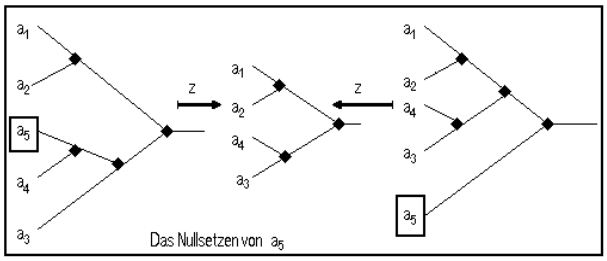


Die Zahlangaben des Beispiels gelten offenbar allgmein: $G(A_n)$ hat stets (n-l) innere Knoten (= Additionsautomaten) sowie 2(n-l)+l=2n-1 Linien, die alle auftretenden Leitungsbahnen repräsentieren: 2 Linien links vor jedem Knoten, dazu die Endlinie des Ausganges.

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: $G(\mathcal{A}_n) \to G(\mathcal{A}_{n-1})$ haben.

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

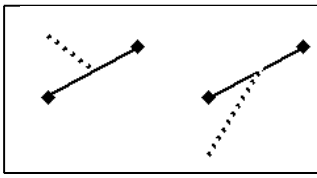


(2.7.4) Wir wählen auf der Wertemenge G($\mathcal{A}_{n-1}$) die atomare Partition und bilden die durch die inverse Abbildung erzeugte Partition auf G($\mathcal{A}_n$). Vgl.Kap.1.3.3. Uns interessieren die entstehenden Klassen und deren Elementzahl. Angenommen jede Klasse hat genau k_n Elemente. Dann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

3.3 **Operationen von Gruppen auf Mengen** (G-Operationen)

3.3.0 **Wandel und Erhaltung (1)**

(3.0.1) Gruppen erlangen ihre Bedeutung (in Hinblick auf Anwendungen besonders in der Physik) weniger als isolierte Objekte, als durch ein Zusammenwirken mit anderen Objekten, meist als Teil von Parametrisierungs- und Darstellungsabbildungen: Die Elemente der Gruppe transformieren andere Objekte, sie wandeln ihre Form, ihre Lage oder andere Eigenschaften in gesetzmäßiger Weise um. Kurz, Gruppenelemente machen aus einem Objekt ein anderes desselben Typs, also derselben Menge. (Genauer: Gruppenelemente beschreiben, welche Objekte aus einem gegebenen hervorgehen können.) Wir haben es mithin mit einer Verknüpfung (Transformation, Objekt) $\mapsto$ Objekt zu tun. **Die Objektmenge übernimmt dabei in der Regel die Rolle des Konfigurationsraumes** Wir erinnern kurz an die Eigenschaften, die nach Kap.1.1 einen Konfigurationsraum ausmachen:

- ♦ Man kann in ihm Figuren bilden, deren Entwicklung verfolgen, sie transformieren und Beziehungen zwischen ihnen herstellen.
- ♦ Man kann ortsabhängige Beobachtungen vornehmen (Felder) und die Ergebnisse miteinander vergleichen (Parallelverschiebbarkeit der Meßergebnisse)..

Und immer, wenn es um das Vergleichen und sich Fortentwickeln im Konfigurationsraum geht, kommen Gruppen oder auch Halbgruppen ins Spiel. Genauer gesagt werden die jeweiligen Veränderungen nicht willkürlich aus der Menge aller überhaupt denkbaren Veränderungen gewählt, sondern es treten solche mit gewissen Regelmäßigkeiten auf, gewisse gesetzmäßige Verbindungen mit Ausgangsobjekt werden bewahrt. Und die Gruppenoperation formalisiert gerade dass: **Mögliche Änderungen einer bestimmten Art unter Bewahrung gewisser anderer Aspekte.**

Und weiter ist es so, dass gleichartige, durch ein und dieselbe Gruppe festgelegte Änderungen, auf die unterschiedlichsten Konfigurationen wirken können. Und diese Gleichheit ist zu erkennen und zu verstehen. Etwa: Wann haben Figuren dieselben Symmetrieeigenschaften? Oder stark abstrahiert: Ein und dieselbe Idee erscheint in den verschiedenartigsten materiellen Konfigurationen.

(□ F.) Was sind kongruente Figuren, was ähnliche? Was wird dabei jeweils geändert, was bewahrt? Ist Ihre Antwort so, dass man damit dieses Problem auch im vierdimensionalen Raum behandeln kann?

3.3.0a **Zwei einführende Beispiele**

(3.0.2) Wir haben Permutationen (von n Elementen) als bijektive Abbildungen von I_n={1,2,.....n} auf sich eingeführt. Aber eigentlich ist der Permutationsbegriff, die dahinter stehende Idee, viel umfassender. Man sollte Permutationen auf beliebige n-tupel (a_1,a_2,.....,a_n) anwenden können. Unsere neue Struktur wird das leisten. Nehmen wir (a,a,b,a). Auch derartige Tupel müßte man permutieren können, etwa zu (a,a,a,b) oder zu (a,b,a,a). Aber als wohldefinierte bijektive Abbildung $I_n \to I_n$ läßt sich diese Art von Vertauschung nicht interpretieren.

Weiter ist es gleichgültig, was für Objekte man permutiert, Punkte im Raum oder Abbildungen oder Symbole aus einer Symbolmenge. Die Vertauschungsoperation gehört jeweils zu derselben Struktur.

(3.0.3) Die in 3.2.6 eingeführte orthogonale Gruppe 0(3) ist eine Gruppe bijektiver Abbildungen $V^3 \to V^3$. Jedes Element dieser Gruppe führt einen geometrischen Pfeil $\vec{x}$ in einen neuen Pfeil $R(\vec{x})$ über. Aber die Änderung ist nicht beliebig: Längen und Winkel werden bewahrt, die Lage im festen Raum jedoch verändert. Und die Drehoperationen sollten erneut auf viel mehr Objekte als nur Pfeile sinnvoll anwendbar sein. In der Physik sollte man Koordinatensysteme drehen können oder Körper oder ganze physikalische Systeme. In der Geometrie ganze Figuren. Wie verändern sich Bahnkurven, wenn man die Anfangswerte dreht? Was geschieht mit Feldern, wenn man die erzeugende Konfiguration dreht? Was bedeute eine Drehung in vier Dimensionen ? Usw.

3.3.1 **Die algebraische Struktur der Gruppenoperation**

(3.1.1) Die algebraische Struktur, die die angesprochenen Ideen formalisiert (und mit deren Hilfe man zugehörige Fragen angeht und beantwortet), umfaßt zwei Mengen. Ein (abstrakte) Gruppe G und eine

weitere (konkrete) Menge M, deren Elemente durch die Elemente von G, die Objekte, transformiert werden sollen. Dazu gehören dann zwei Verknüpfungen:

Definition:	(α)	Sei (G,$\top$) Gruppe und M nicht leere Menge.
	(β)	Eine Verknüpfung $\star : G \times M \to M$ sei vorgegeben.
	$(\gamma.1)$	Für alle g,h$\in G$ und m$\in M$ gelte $(g \top h) \star m = g \star (h \star m)$
	$(\gamma.2)$	$e \star m = m$ für alle m$\in M$. Dabei sei e neutrales Element von G

Eine solche Struktur nennen wir *Links-G-Operation auf M.* Wir sagen auch:
G operiert von links auf M. Oder *G ist eine (linke) Transformationsgruppe von M.*
$(\gamma.2)$ nennen wir auch *Fastassoziativität.*

Zur ersten Orientierung über den Formalismus kann man an folgendes Beispiel für $\star$ denken:

$$(Stundenzahl, Uhrzeit) \overset{\star}{\mapsto} sp\ddot{a}tere\ Uhrzeit$$

Etwa 10Stunden+19Uhr = 5Uhr. Die Stundenzahlen bilden den Konfigurationraum, dessen Elemente man durch Weitergehen oder Zurückgehen transformieren kann.

(3.1.2) Das Attribut "links" deutet an, dass es auch Rechtsoperationen geben wird. Inspektion zeigt, was links-rechts-asymmetrisch und daher zu ändern ist:

Definition:	(αr)	Bleibt unverändert
	(βr)	Eine Verknüpfung $\star$M$\times G \to M$ sei vorgegeben
	$(\gamma.1r)$	für alle g,h$\in G$ und m$\in M$ gelte m$\star(g \top h) = (m * g) \star h$.
	$(\gamma.2r)$	m$\star e = m$ für alle m$\in M$. Und e neutral in G.

(3.1.3) Eine Rechtsoperation läßt sich keineswegs immer durch einfaches Umbenennen in eine Linksoperation umwandeln. Sei etwa $\star$:M$\times$G$\to$M eine Rechtsoperation. Dann definieren wir versuchsweise

$$\# = (G \times M, (g, m) \mapsto g\#m = m \star g, M).$$

Das ist die gegebene Rechtsoperation, nur so umbenannt, daß das Gruppenelement in der Bezeichnung links vom Objekt steht. Damit haben wir Regel (β) für eine Linksoperation erfüllt. Führt man die neue Bezeichnung in $(\gamma.1r)$ ein, so ergibt sich h#(g#m) =(g$\top$h)#m. **D.h. die Reihenfolge von g und h ändert sich!** Das ergibt nur $(\gamma.1)$, falls G kommutativ ist. Ist G nicht kommutativ, so muß man Links- und Rechtsoperationen auf M sorgfältig auseinanderhalten. Später wird die Unterscheidung in einigen Fällen wichtig werden. Oder auch: Die Fastassoziativität regelt, wie ein Produktterm g$\top$h zweier Gruppenelemente auf ein m der Menge wirkt. Man darf nacheinander transformieren, aber in welcher Reihenfolge? Bei einer Linksoperation wirkt erst h und dann g. Bei einer Rechtsoperation wirkt umgekehrt erst g und dann h.

(3.1.4) Beispiel: **Längenänderung von Vektoren**. Sei G=$(\mathbb{R}_+^*, \cdot)$ und M=V_0^3. Dann beschreibt $(\mathbb{R}_+^* \times V_0^3, (\alpha, \vec{x}) \mapsto \alpha\vec{x}, V_0^3)$ eine Gruppenoperation. (Nachweis trivial). Die Gruppenelemente α transformieren die Pfeile, indem sie nur deren Länge verändern. Die Gruppe ist kommutativ. Daher darf man die Skalare nach Belieben links oder rechts vom Vektor setzen. So schreibt man ja typischerweise bei Flugparabeln $\frac{1}{2}\vec{g}t^2$.

Sei h_α:$\vec{x} \mapsto \alpha\vec{x}$ die von einem Gruppenelement erzeugte *Transformationsabbildung* Wir können dann $\underline{h}_\alpha$:$\mathcal{P}(V_0^2) \to \mathcal{P}(V_0^2)$ bilden, die Erweiterung der Abbildung auf die Potenzmenge (Kap. 1.2). Dann operiert G auch auf $\mathcal{P}(V_0^2)$ vermöge: $(\alpha$,F)$\mapsto \underline{h}_\alpha$(F). Das ist eine typische leicht nachzuprüfende Strukturübertragung. Insbesondere operiert G auf allen zeichenbaren Figuren der Ebene wie Dreiecken, Kreisen, Strecken usw. Die Operation vergrößert alle diese Figuren um einen Faktor α (bei festem Ursprung) Diese Operation ändert also nicht nur die Lage, sondern auch die Form in einer ganz bestimmten Weise.

(3.1.5) Zwei typische Rechnungen, die durch die Axiome der Gruppenoperation ermöglich werden:

♦ Sei g$\star$x=y . Wende $g^{-1}\star$...an. Das gibt: $g^{-1}\star$(g$\star$x)=$g^{-1}\star y$. Wegen $g^{-1}\star(g\star x) = (g^{-1} \top g)\star x = e \star x = x$: x=$g^{-1} \star y$. Oder auch: für jede Gruppenoperation gilt:

$$g \star x = y \quad \Longrightarrow \quad x = g^{-1} \star y.$$

Oder schließlich: **Die Gleichung g$\star$x=y ist immer eindeutig lösbar**. Das ist analog zu (2.1.16) für Gruppen.

(3.1.6) Wir folgern:

Die Abbildung

$$\tau_g = (M, x \mapsto \tau_g(x) = g \star x, M) \quad \text{ist bijektiv.}$$

Diese Abbildung nennen wir *die (dem Gruppenelement g zugeordnete) Transformationsabbildung.* Sie induziert eine entprechende Transformationsabbildung $\underline{\tau_g}$: $\mathcal{P}$(M)$\rightarrow \mathcal{P}$(M) für Figuren, transformiert also immer auch die Figuren des Konfigurationsraumes.

♦ Jetzt die zweite Rechnung, wobei die Vorgehensweise analog ist:

$$g \star x = g \star (e \star x) = g \star (h^{-1} \top h) \star x)) = (g \top h^{-1}) \star (h \star x).$$

Ein solches Einschieben eines Produktes $h^{-1} \top h$ erweist sich als nützlicher Rechentrick.

(3.1.7) Beispiel: **Kleine Transformationen von Funktionen**. Sei E die Menge der elementar konstruierbaren Funktionen $\mathbb{R} \rightarrow \mathbb{R}$. Für sie gibt es die kleinen Transformationen, die die Gestalt des Graphen in überschaubarer Weise ändern, nämlich durch Verschieben der Achsennullpunkte und durch Umskalieren der beiden Achsen. Nach unserem Konzept sollten derartige Veränderungen durch eine Gruppenoperation bewirkt werden. Als Beispiel betrachten wir die linearen Änderungen der x-Achse. D.h. der Rechenausdruck f(x) für den Funktionswert wird zu f(αx+a) abgeändert. Später behandeln wir den allgemeinen Fall, der auch die y-Achse erfaßt. Die zugehörige Gruppe besteht aus der Menge G= $\mathbb{R}^* \times \mathbb{R}$ aller geordneten Paare (α,a) reeller Zahlen mit $\alpha \neq 0$. Zwei aufeinander folgende Substitutionen ergeben die neue Substitution $\alpha(\beta$x+b)+a = $\alpha\beta$x+(αb+a). Dieser Beziehung kann man die zugehörige Gruppenmultiplikation entnehmen: ((α,a)$\circ$(β,b)=($\alpha\beta, \alpha b + a$). Wir werden dieser Gruppenverknüpfung noch häufiger begegnen. Man prüft leicht nach, dass eine Gruppe vorliegt. Klar ist: Funktionsgraphen werden durch diese Operationen nicht willkürlich geändert, sondern in ganz bestimmter überschaubarer Weise, sin(t) wird zu sin(ωt+φ), also erneut zu einer sinusförmigen Schwingung derselben Amplitude, aber mit anderer Kreisfrequenz und anderer Phase.

Kleine Transformationen wurden bei der Kurvendiskussion eingeführt, weil die auseinander hervorgehenden Graphen weitgehend gleichartige Eigenschaften besitzen. Und auch der zweite eingangs genannte Sachverhalt tritt auf: "Dieselbe Transformation" oder Operation kann sowohl mit dem Rechenausdruck, mit dem Graphen, mit der Ableitung oder dem Integral durchgeführt werden.

(3.1.8) Beachten Sie noch: In Beispiel (3.1.7) ist zunächst die Operation gegeben. Aus dieser haben wir mit mit Hilfe der Fastassoziativität die Gruppenmultiplikation hergeleitet. Also: Zuerst die Objekttransformation, dann die Gruppenverknüpfung! Ein solches Vorgehen erweist sich als nützliche Methode sowohl für den physikalischen wie der mathematischen Bereich. Im nachfolgenden Beispiel üben wir das Vorgehen gezielt.

3.3.1a **Die Drehgruppe S0(2) der Ebene**

(3.1.9) Wir geben in der Ebene ein festes kartesisches Koordinatensystem K vor und beschreiben alle Punkte durch ihre Ortsvektoren aus $\mathbb{R}^2_K$. Sei $\vec{x}$=$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$. Jetzt drehen wir alle Vektoren um einen Winkel φ im positiven Sinn um den Ursprung. Das macht aus $\vec{x}$ einen neuen Koordinatenvektor, den wir mit $\vec{y}$=$R_\varphi(\vec{x})$ bezeichnen wollen. Also $\vec{x} \mapsto R_\varphi(\vec{x})$. Abstände und Winkel bleiben bei dieser Operation erhalten, wie es für orthogonale Transformationen gefordert wird. Der gedrehte Vektor läßt sich leicht elementargeometrisch berechnen und in der aus der Theorie der linearen Gleichungen bekannten Matrixform darstellen. Man findet:

$$\vec{y} = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} x_1 \cos\varphi - x_2 \sin\varphi \\ x_1 \sin\varphi + x_2 \cos\varphi \end{pmatrix} = \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$$

□ Bestimmen Sie y_1 und y_2 elementargeometrisch.

(3.1.10) Offensichtlich liegen folgende Rollen vor: Die Koordinatenvektoren bilden die Objektmenge, also M=$\mathbb{R}^2_K$ und die Gruppe G ist mit der Menge der eingeführten Matrizen identifizierbar, wobei φ beliebige Werte aus $\mathbb{R}$ durchlaufen darf. Dann liefert die hingeschriebene Gleichung die Gruppenoperation. Die Gruppe selbst wird S0(2) genannt. Das S steht immer für "speziell". Also "spezielle orthogonale Gruppe

in 2 Dimensionen". Dabei besagt speziell, dass nur reine Drehungen, keine Spiegelungen erfaßt werden. Als Formel:

$$\boxed{\mathrm{SO}(2)=\left\{ \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix} \mid \varphi \in \mathbb{R} \right\}}$$

(3.1.11) Damit kennen wir die Gruppenoperation $\star$, aber noch nicht die eigentliche Gruppenverknüpfung $\top$. Wir wissen aber, was zwei aufeinander folgende Drehungen erst um φ und dann um ψ bewirken: Einfach eine Drehung um $\varphi + \psi$. Mit Hilfe der Additionstheoreme folgt zunächst:

$$\begin{aligned} R_{\varphi+\psi} &= \begin{pmatrix} \cos(\varphi+\psi) & -\sin(\varphi+\psi) \\ \sin(\varphi+\psi) & \cos(\varphi+\psi) \end{pmatrix} = \\ &= \begin{pmatrix} \cos\varphi\cos\psi - \sin\varphi\sin\psi & -\sin\varphi\cos\psi - \sin\psi\cos\varphi \\ \sin\varphi\cos\psi + \sin\psi\cos\varphi & \cos\varphi\cos\psi - \sin\varphi\sin\psi \end{pmatrix} \end{aligned}$$

Durch Einsetzen in die Gleichung $(\mathrm{R}_\varphi \circ R_\psi) \star \vec{x} = R_\varphi \star (R_\psi \star \vec{x})$ erhalten wir die folgende konkrete Vorschrift für die Gruppenverknüpfung:

$$\begin{aligned} & \begin{pmatrix} \cos(\varphi) & -\sin(\varphi) \\ \sin(\varphi) & \cos(\varphi) \end{pmatrix} \circ \begin{pmatrix} \cos(\psi) & -\sin(\psi) \\ \sin(\psi) & \cos(\psi) \end{pmatrix} \\ = & \begin{pmatrix} \cos\varphi\cos\psi - \sin\varphi\sin\psi & -\sin\varphi\cos\psi - \sin\psi\cos\varphi \\ \sin\varphi\cos\psi + \sin\psi\cos\varphi & \cos\varphi\cos\psi - \sin\varphi\sin\psi \end{pmatrix} \end{aligned}$$

Man prüft sofort nach, daß es sich hierbei um einen Spezialfall der üblichen, nach der Regel *Zeile mal Spalte* gebildeten Matrixmultiplikation handelt. (Beachten Sie: Hat man die beiden Gruppenelemente als Matrizen gegeben ohne Kenntnis der zugehörigen φ-und ψ-Werte, dann nützt einem die Formel $\mathrm{R}_{\varphi+\psi} = \mathrm{R}_\varphi \circ R_\psi$ wenig. Die Matrixmultiplikationsformel für die Verknüpfung dagegen ist anwendbar.)

(3.1.12) Weiter prüft man leicht unmittelbar nach, dass (S0(2),$\circ$) tatsächlich eine kommutative Gruppe bildet. Und ($\mathbb{R}$,$\varphi \mapsto R_\varphi$,SO(2)) ist ein Gruppenhomomorphismus. Der Kern ist $\{2\pi n | \mathrm{n} \in \mathbb{Z}\}$. Die Gruppe ist kommutativ, so dass man nicht zwischen Links- und Rechtsoperation unterscheiden muß.

(3.1.13) Abschließend verifiziert man, daß die eingangs gegebene Verknüpfung

$$(R_\varphi, \vec{x}) \mapsto R_\varphi \star \vec{x} = R_\varphi(\vec{x})$$

tatsächlich eine Gruppenoperation bildet.

(3.1.14) Damit haben wir ausgehend von der Operation zunächst die Gruppe bestimmt und anschließend das gesamte Schema realisiert. Beachten Sie im Rückblick, welche Vielfalt an Gruppenoperationen jetzt bereits mit Hilfe der Beispiele eingeführt ist.

3.3.1b **Weitere mit dem Konfigurationsraum verbundene Gruppen**

(3.1.15) Mit der soeben verwendeten Methode lassen sich weitere Gruppen abstrahieren, die wichtige Eigenschaften der Konfigurationsraumstruktur erfassen. Als Ausgangspunkt kann und sollte dabei die Drehgruppe dienen, die jeweils durch weitere Elemente ergänzt wird. Dazu ist es erneut nicht nötig, eine explizite Darstellung der Gruppenelemente zu besitzen, wie wir sie soeben für die Drehungen in der Ebene hergeleitet haben. (Vgl. die Bemerkungen in 3.2.6). Wir führen kurz drei wichtige Gruppen aus dem Umfeld der Drehgruppe ein. Dabei gehen wir wieder vom dreidimensionalen Konfigurationsraum V_0^3 aus, auf dem diese Gruppen in zu besprechender Weise operieren. Die Gruppen lassen sich über die Operation abstrahieren, was wir aber nicht voll ausführen. Die Definitionen sind so, dass man sie unmittelbar auf die Ebene und meist auch problemlos auf höherdimensionale Vektorräume verallgemeinern kann.

(3.1.15) Die affine Gruppe (Bewegungsgruppe). Sei 0(3) die in 3.2.6 eingeführte orthogonale Gruppe. Wir fügen zu den dortigen Gruppenoperationen noch die Verschiebungen des Ursprungs mit hinzu, also die Abbildungen

$$t_{\vec{a}} = (V_0^3, \vec{x} \mapsto \vec{x} - \vec{a}, V_0^3) = \text{Translation aller Vektoren um } -\vec{a}.$$

Inhaltlich bedeutet diese Hinzunahme, dass die Länge von Vektoren, also der jeweilige Abstand zum Ursprung, nicht mehr unverändert bleibt, weil der Ursprung nicht mehr fest bleiben muß. Durch die Transformation unverändert bleibt immer nur der Abstand beliebiger Punkte. Und bei Winkeln muß man sorgfältig

"Winkel zwischen Vektoren" ersetzen durch "Winkel zwischen Halbgeraden" oder eventuell "Winkel zwischen freien Vektoren". Nur letztere bleiben unter den zugelassenen Transformationen unverändert.

Zusammen mit den Drehungen ergibt sich eine Gruppe, die man "**die affine Gruppe (in drei Dimensionen)**" nennt. Dies ist eine Untergruppe der Gruppe aller bijektiven Abbildungen des V_0^3 wie Anwendung des Untergruppenkriteriums zeigt. Wir bezeichnen diese Gruppe mit A(3). Den Elementgehalt legen wir wie folgt fest: A(3)=$\{R\circ t_{\vec{a}} |\ R\in 0(3)$ und $\vec{a} \in V_0^3\}$. Für die nachfolgenden Rechnungen benötigen wir die Linearität der Elemente aus 0(3), die wir in Kap. 4 besprechen. Genauer benötigen wir nur die Regel $R(\vec{x}+\vec{y})=R(\vec{x})+R(\vec{y})$.

Entsteht wirklich eine Gruppe? Hintereinanderausführung zweier Operationen der angegebenen Art ergibt $(R\circ t_{\vec{a}})\circ(S\circ t_{\vec{b}})(\vec{x})= R(S(\vec{x}-\vec{b})-\vec{a})=R\circ S(\vec{x}-(\vec{b}+S^{-1}(\vec{a}))$. Das ist wieder ein Element der beschriebenen Art. Wir lesen die folgende Verknüpfung ab

$$(R\circ t_{\vec{a}})\circ(S\circ t_{\vec{b}}) = (R\circ S)\circ t_{\vec{c}} \quad \text{mit } \vec{c}=\vec{b}+S^{-1}(\vec{a}).$$

Beachten Sie nochmals, dass man dies Produkt mit Hilfe der Eingabedaten wirklich bestimmen kann.

Invers zu $R\circ t_{\vec{a}}$ ist $R^{-1}\circ t_{\vec{d}}$ mit $\vec{d}=-R^{-1}(\vec{a})$, wie man sich sofort überzeugt. (Hier ist übrigens 3.1.(14) nützlich, wieso?) Jetzt läßt sich mit Hilfe des Untergruppenkriteriums zeigen, dass eine Gruppe vorliegt, was wir nicht ausführen.

(3.1.16) Die Galiläigruppe. Dies ist eine für physikalische Anwendungen nützliche Gruppe. Bei ihr darf das neue transformierte System nicht nur um einen konstanten Vektor $\vec{a}$ verschoben werden, sondern es kann sich mit konstanter Geschwindigkeit $\vec{V}$ gegen das a System bewegen. Man läßt also zeitabhängige Translationen $t\mapsto \vec{a}+\vec{V}t$ zu. Die Gruppenelemente lassen sich durch die Tripel $(R,\vec{a},\vec{V})$ festlegen oder parametrisieren. Es entsteht eine Erweiterung der Bewegungsgruppe. Diese Gruppe bildet einen Ausgangspunkt der Diskusssion der Relativitätstheorie.

(3.1.17) Die Ähnlichkeitsgruppe. Hier wird die Drehgruppe durch die in (3.1.4) besprochenen Längenänderungen von Vektoren ergänzt. Man erhält eine Gruppe, bei der Winkel erhalten bleiben, aber alle Längen um einen elementabhängen positiven Faktor verändert werden, so daß ähnliche Figuren entstehen.

Die Gruppe selbst besteht aus allen Produkten $h_\alpha\circ R$ mit $\alpha>0$ und $R\in 0(3)$.

3.3.2 Die Konsequenzen einer Gruppenoperation

Welche Konsequenzen hat die Vorgabe einer Gruppenoperation? Einige rein rechnerische Konsequenzen haben wir bereits besprochen. Jetzt fragen wir nach der Strukturierung, die die Objektmenge M durch die Operation erfährt. Die entstehende Strukturierung erweist sich als erstaunlich reichhaltig.

Der Einfachheit halber wählen wir stets ein Linksoperation. Für Rechtsoperationen verläuft alles analog. Man erhält **drei hauptsächliche allgemeine Folgerungen**.

3.3.2a **Die Bahnen**

(3.2.1) Als erste Struktur betrachten wir

	Die Bahn- oder Orbitstruktur:
Sei	$G\times M \xrightarrow{\star} M$ Gruppenoperation.
Dann	definiert $m\sim n \iff \exists$ g$\in G$ mit m$= g\star n$
	eine Äquivalenzrelation auf M. Die Klassen
	B(n)=$\{m|\ \exists g\in G$ mit m $= g\star n\}$ heißen Bahnen von M unter $\star$.

Dass dies eine Äquivalenzrelation liefert, folgt trivial. Die Bahn von m$\in$M ist eine Teilmenge von M. Englischsprachig sagt man statt "Bahn" auch "Orbit".

(3.2.2) Im ersten Beispiel (3.1.4) sind die Bahnen die vom Ursprung ausgehenden Halbgeraden (sowie die Nullpunktsmenge). Im Beispiel (3.1.7) besteht die Bahn von $x\mapsto \frac{1}{1+x^2}$ aus allen rationalen Funktionen, die sich in die Form $\frac{1}{(1+(ax+b)^2}$ mit a$\neq 0$ bringen lassen. Und die Bahnen der Drehgruppenoperation (3.1.9) sind Ursprungskreise.

(3.2.3) Die Bahn B(x) eines Elementes x∈M bekommt man, indem man alle Elemente von G über $\star$ auf das feste x wirken läßt. Formal: Sei T_x=(G,g↦g⋆x,M). Dann ist B(x)=BildT_x. **Die Menge aller Bahnen bildet eine Partition von M**, die sich häufig als nützlich erweist.

3.3.2b **Die Stabilisatoren**

(3.2.4) Die nächste Strukturierung sieht wie folgt aus:

Sei	$G \times M \xrightarrow{\star} M$ Gruppenoperation.
Dann	hat man auf M ein Untergruppenfeld vorgegeben. D.h. zu jedem x∈ M gehört eine eindeutig bestimmte Untergruppe von G $S_x = \{h \mid h \in G \text{ und } h\star x = x\}$. Bezeichnung: *Stabilitätsuntergruppe oder Stabilisator von x.*

(3.2.5) Mit Hilfe des Untergruppenkriteriums folgt sofort, dass die angegebene Teilmenge von G tatsächlich immer eine Untergruppe von G ist.

Als Beispiel eines solchen Nachweises führen wir den Beweis:

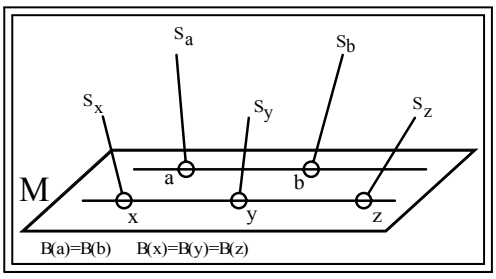
> Sei g,h∈ S_x. Also g⋆x=x und h⋆x=x . Auf die Seiten der 2. Gleichung wird $h^{-1}\star$.... angewandt. Dies gibt: $h^{-1}\star(h\star x) = (h^{-1}\cdot h)\star x = e\star x = x$einerseits und $h^{-1}\star x$andererseits. Also $h^{-1}\star x = x$. Operieren wir auf dieser Gleichung mit g⋆..., so folgt die für das Untergruppenkriterium benötigte Bedingung $g\cdot h^{-1} \in S_x$.. (Überzeugen Sie sich, daß nur die Axiome benutzt werden.)

(3.2.6) Aus der Rechnung erkennt man übrigens: Operiert G auf M, **dann operiert G auch auf geeigneten Mengen von Gleichungen zwischen M-wertigen Termen**. Die Bahnen entstehen durch Anwenden aller Gruppenelemente auf eine Vertretergleichung. Damit haben wir ein weiteres Beispiel für den in (3.0.1) beschriebenen Sachverhalt: Anwendung ein und derselben Operation auf Objekte unterschiedlichsten Typs.

(3.2.7) Im Uhrzeitbeispiel gibt es nur eine Bahn, denn man kann jede Zeit durch Hinzuaddieren einer geeigneten Stundenzahl erreichen! Die Stabilitätsuntergruppe ist 24ℤ= ={z|z=24n,n∈ ℤ}. Hinzufügen eines Vielfachen von 24 Stunden ändert die Uhrzeit nicht.

Wie sehen die Stabilitätsuntergruppen im Beispiel der Längenänderung der Vektoren aus? Dort treten nur die beiden trivialen Untergruppen auf. Pfeile ungleich Null werden nur von der 1 fest gelassen. Der Nullpfeil dagegen von der gesamten Gruppe. (Beachten Sie: Jedes x∈M hat seine individuelle Untergruppe, daher die Charakterisierung *Untergruppenfeld*.)

(3.2.8) Das Bild fasst symbolisch zusammen, was wir bisher an Strukturierung unserer Menge M gefunden haben :



M wird in Bahnen zerlegt
An jedem Punkt hängt der Stabilisator.

(3.2.9) Jetzt wählen wir ein x∈M und die dazugehörige Bahn B(x). Über x tragen wir die gesamte Gruppe G auf. Dann haben wir die Abbildung T =(G,g↦ $g \star x$,, B(x)). Sie ist sicher surjektiv. Für jedes y∈B(x) gibt es mindestens ein g mit y=g⋆x. Wieviel weitere derartige Gruppenelemente gibt es noch? Sei h ein solches. Also h⋆x=y. Gesucht ist B(x⇀ y)={h|h⋆x=y} als Menge all dieser Umwandlungselemente. Es folgt g⋆x=h⋆x oder $(g^{-1}\circ h)\star x = x$. Oder: Das Gruppenelement g^{-1}∘h läßt x stabil, $g^{-1} \star h \in S_x$.

Ist umgekehrt s∈S_x irgendein Gruppenelement, das x stabil läßt und setzen wir h=g∘s, so folgt (g∘s)⋆x=y. Folglich definiert s↦ $g\circ s$ eine bijektive Abbildung zwischen dem Stabilisator S_x und der Umwandlungsmenge

B(x→ y). **Beide Mengen haben daher im endlichen Fall gleichviele Elemente** ! Auch der Stabilisator selbst ist eine derartige Umwandlungsmenge, nämlich B(x→x). Insgesamt bilden diese Mengen eine Partition der Gruppe G mit gleichgroßen Klassen.

□ Stellen Sie diesen Sachverhalt graphisch dar.

(3.2.10) Fassen wir zusammen:

Für g mit y=g⋆x haben wir eine **bijektive** Abbildung $(S_x, s \mapsto g \circ s, B(x \to y))$. Ist also S_x endlich mit k Elementen, so wandeln immer genau k Gruppenelemente das Element x in das Element y derselben Bahn um.

(3.2.11) Folgerung: Ist G endliche Gruppe mit n Elementen, die auf M operiert, so gilt für jedes x∈M:

n = (Zahl der Elemente von S_x) mal (Zahl d. Elemente v.B(x→y))
Ordnung der Gruppe = Stabilisatorordnung × Bahnlänge
$\#G=(\#S_x) \cdot (\#B_x)$

Und damit: **Bahnlänge und Ordnung des Stabilisators müssen immer Teiler der Gruppenordnung n sein**! Dies erweist sich als ausgesprochen wichtiges Resultat.

(3.2.12) Nach dieser Konstruktion müssen auch die beiden Stabiltätsuntergruppen S_x=B(x→x) und S_y =B(y→ y) dieselbe Elementzahl haben, sofern x und g auf derselben Bahn liegen. Beides sind aber Gruppen. Mithin sollten wir fragen, ob die beiden Gruppen vielleicht sogar isomorph sind. Das läßt sich leicht verifizieren. Wir hatten ja für obiges Szenenbild einerseits h⋆x=x für h∈S_x und andererseits x=$g^{-1} \star y$ für die beiden Elemente x und y derselben Bahn. Einsetzen gibt h⋆($g^{-1} \star y$)=$g^{-1} \star y$ Oder (g∘h∘g^{-1})∈S_y. Beachten Sie: g ist hier äußerer Parameter. Die Zuordnung h↦g∘h∘g^{-1} wird mithin zu einer Abbildung σ_g = $(S_x, h \mapsto \sigma_g(h) = g \circ h \circ g^{-1}, S_y)$. Die Strukturerhaltung $\sigma_g(h \circ k)$= $\sigma_g(h) \circ \sigma_g(k)$ verifiziert man sofort und die Gleichung g∘h∘g^{-1}=k läßt sich in der Gruppe eindeutig nach h auflösen, wobei wir wissen, daß h in S_x liegt, wenn k∈S_y gewählt ist. Kurz: **Alle Stabilisatoren entlang einer Bahn sind zueinander isomorph.**

(3.2.13) Veranschaulichen Sie sich all diese Resultate möglichst genau mit Hilfe der Figur aus (3.2.8) und prägen Sie sich die gesamte entstehende Struktur gut ein. Insbesondere sind in der Figur die Stabilisatoren S_a und S_b notwendig isomorph, also Umbenennungen derselben abstrakten Gruppe. Dagegen können S_a und S_x zu verschiedenen Isomorphieklassen gehören, müssen nicht isomorph sein.

(3.2.14) Nochmals:

Es seien x und y zwei Elemente derselben Bahn mit y=g⋆x.
Dann sind die beiden Stabilitätsuntergruppen S_x und S_y zueinander isomorph.
Ein möglicher Isomorphismus wird gegeben durch
$\sigma_g = (S_x, h \mapsto \sigma_g(h) = g \circ h \circ g^{-1}, S_y)$.

Übrigens liegt hier ein Beispiel dafür vor, dass man isomorphe Gruppen nicht immer identifizieren sollte. Denn als Untergruppen von G können S_x und S_y natürlich durchaus verschieden sein. Wendet man etwa ein Element von S_y auf x an, so muß keineswegs x herauskommen.

3.3.2c **Die Transformationen der Objektmenge**

(3.2.15) Wir kommen jetzt zu der Eigenschaft, mit der wir ursprünglich die Einführung der Gruppenoperation motivierten. Hierzu restringieren wir die Operation ⋆ :

3. Struktur	Zu jedem g∈G hat man die **Transformationsabbildung** $t_g = (M, x \mapsto g \star x, M)$
	Diese Abbildung "verschiebt" die Punkte aus M entlang ihrer Bahn.
	Die Abbildung ist ausdehnbar auf die Potenzmenge: $\underline{t}_g = (\mathfrak{P}(M), F \mapsto \underline{g} \star F, \mathfrak{P}(M))$
	Hiermit werden "Figuren in M" transformiert.

(3.2.16) Für jedes g ist t_g bijektiv wie man sofort sieht, mit $(t_g)^{-1}=t_{g^{-1}}$. Jede dieser Abbildungen ist auf jede Bahn einschränkbar. Im Fall des Uhrzeigerbeispiels ergibt sich eine Zuordnung der Art "Zeit $\mapsto$ (*Zeit* +3Stunden).

Im Fall der Längenänderung von Vektoren war $h_\alpha : \vec{x} \mapsto \alpha\vec{x}$ eine solche Transformationsabbildung. Durch $\underline{h_\alpha}$ wird jede Figur F um einen Faktor α verändert, also zu einer ähnlichen Figur.

Bei den kleinen Transformationen verschiebt die zu (l,-a) gehörige Transformation den Graphen von f um a parallel zur x-Achse.

(3.2.17) Verallgemeinern wir das Resultat des zweiten Beispiels auf folgende allgemeine Situation: M habe die Rolle des Konfigurationsraums, in dem wir gewisse Figuren F⊂M betrachten. Dann kann man die Transformation der Punkte zu einer Transformation der Figuren erweitern. Denn es gilt:

Folgerung: Ist $\star$:G×M→M eine Gruppenoperation, so ist diese immer auf die Potenzmenge (also auf die Figuren in M) ausdehnbar vermöge $\star = (G \times \mathfrak{P}(M), (g,F) \mapsto \underline{t_g}(\mathrm{F}),\mathfrak{P}(M))$ *Figurenoperation!*

Der Einfachheit halber bezeichnen wir die neue Operation mit demselben Symbol wie die alte. Man erkennt meist leicht, was jeweils gemeint ist. Wir werden auch einfach g$\star F$ anstelle von $\underline{t_g}$(F)={y| y=g$\star f$, f$\in F$} schreiben, da dies einfacher und gedächtnisunterstützend ist: g$\star F$ ist ja eine Menge. Und die Bezeichnung beschreibt, wie man die Elemente dieser Menge erhält: Nehme g und irgendein f aus F. Bilde g$\star$f. Dann ist g$\star$F die Menge aller so entstehenden Werte. Es liegt erneut ein Beispiel für Rollenwechsel vor.

☐ Beweisen Sie, dass eine Gruppenoperation vorliegt.

☐ Betrachten Sie die Ausdehnung der Drehgruppe S0(2) und der affinen Gruppe auf die Potenzmenge. Wählen Sie als Figur ein Quadrat mit Mittelpunkt im Ursprung. Bestimmen Sie Bahn und Stabilisator.

(3.2.17a) Wie bereits erwähnt kann man die Gruppenoperation analog auf *Gleichungen zwischen den Elementen aus M* ausdehnen.

☐ Betrachten Sie die Gleichung x^2-3xy+$2y^2$-xz-z^2=0. Lassen Sie darauf Permutationen von (x,y,z) operieren. Was für Bahnen entstehen? Welche Eigenschaft bleibt bewahrt?

(3.2.18) Für jedes g∈G haben wir die Transformationsabbildung t_g:M→M gebildet, eine bijektive Abbildung, also ein Element der Menge $\mathfrak{B}$(M,M) aller bijektiven Abbildungen von M oder auch aller Permutationen von M. Das gibt uns eine neue Zuordnung g$\mapsto \tau_g$, die wir zu einem Abbildungstripel ergänzen: $\tau = (\mathrm{G}, \mathrm{g} \mapsto \tau_g, \mathfrak{B}(\mathrm{M},\mathrm{M}))$. Nach unserer Abbildungsklassifikation liegt eine Abbildung vom Darstellungstyp vor. **Wir haben die Gruppenelemente als Permutationen von M dargestellt** und könne vielfach Probleme zu G mit Hilfe geeigneter anderer Strukturen von $\mathfrak{B}$(M,M) lösen. Die Abbildung ist in der Regel weder injektiv noch surjektiv. Ist sie injektiv, kann man G in $\mathfrak{B}$(M,M) einbetten. So interpretiert man ja die Permutationsgruppe von n Elementen meist als $\mathfrak{B}(\mathrm{J}_n,\mathrm{J}_n)$ mit $\mathrm{J}_n = \{1, 2, ..., n\}$.

3.3.2.d **Wandel und Erhaltung (2)**

(3.2.19) *Wir können jetzt genauer verstehen, wie die Operationsstruktur die universellen Phänomene von Wandel und Erhaltung erfaßt. Die Objekte können gruppenspezifisch nicht beliebig verändert werden, sondern nur entlang ihrer Bahnen. Die abstrahierbaren Gemeinsamkeiten der jeweiligen Klasse (=Bahn) werden dabei bewahrt! Bei Drehungen bleiben z. B. Längen und Winkel erhalten. Bei Permutationen die Anzahlen von Objekten eines bestimmten Typs usw. Der Stabilisator beschreibt diejenigen Operationen (des gewählten Typs), die ein bestimmtes Objekt unverändert lassen. Und die Transformationsabbildung gibt an, was geschieht, wenn man ein und dieselbe Operation auf alle Objekte losläßt.*

Aber die Operationsstruktur beschreibt nicht nur wichtige Sachverhalte in allgemeiner Form, sondern sie liefert auch mathematische Resultate. Einige davon wollen wir im anschließenden Teilkapitel herleiten. Genauer gesagt wollen wir mit Hilfe geeigneter Operationen Resultate über die Gruppenstruktur selbst herleiten und somit die Diskussion aus 3.2.4 forsetzen.

3.3.3 Die Gruppe selbst als Konfigurationsraum Analyse der Gruppenstruktur (2)

(3.3.1) Unsere bisherigen Beispiele von Operationen waren eher konkrete und anschauungsnahe Konstruktionen. Es gibt aber auch Beispielkonstruktionen, die für jede Gruppe möglich sind und nützliche Resultate produzieren. **Die Idee dabei ist, die Gruppe selbst als Objektmenge zu interpretieren.** Also M=G zu wählen. Dies ist auf mehrere Weisen möglich, wodurch man wichtige Resultate über die Gruppenstruktur erhält!.

(3.3.2) Ein erstes Beispiel hierfür sieht so aus:

Sei	(G.·) Gruppe und H eine Untergruppe von G.
Dann	können wir die Gruppe H wie folgt auf der Menge G operieren lassen:
	$\star = (H \times G, (h,g) \mapsto h \star g = h \cdot g, G)$

Die Untergruppe H übernimmt die Rolle der Gruppe und G die der Menge. Die Elemente von H können also zwei Rollen annehmen: Einmal sind sie Elemente der Operatorgruppe. Da sie aber auch in G liegen, können sie ebenso die Objektrolle annehmen. (Die Gruppenmultiplikation schreiben wir jetzt meist kurz gh anstelle g·h.)

(3.3.3) Was bringt uns dies Konstruktion?

- $\star$ **ist** Operation: Das läßt sich trivial mit Hilfe der Gruppenaxiome prüfen.
- **Stabilisatoren**: Alle sind gleich {e}, da hg=g nur für h=e möglich. Es folgt: **Ist H endlich, so haben alle Bahnen genau #H Elemente**, denn es gilt nach (3.2.11) ja #H= 1×Bahnlänge.
- **Bahnen**: für g∈G ist B(g)={hg | h∈H}= Hg = *Rechtsnebenklasse von* H.
  Für die entstehenden Bahnen haben wir die suggestiven Bezeichnungen Hg und Rechtsnebenklasse eingeführt. "Rechts" bezieht sich auf die Lage des gewählten Klassenvertreters g. Und Hg ist eine kurze Schreibweise für die gegebene Mengendefinition.
  Besitzt man für eine Gruppe die zugehörige Gruppentafel, dann ist die Konstruktion der Nebenklassen einfach. Nehmen wir als Beispiel $\mathcal{S}_3$, also die Permutationsgruppe von drei Elementen. Die Tafel ist in (2.1.18) gegeben. Als Untergruppe wählen wir H={l.a,a^2}. Dann gibt es zwei Rechtsnebenklassen, nämlich H1=Ha=Ha^2=(l,a,a^2) und Hτ_1 =Hτ_2 =Hτ_3=$\{\tau_1, \tau_2, \tau_3\}$ wie man der Gruppentafel unmittelbar entnimmt.

□ Wählen Sie als Untergruppe alternativ {1,τ_1}. Wie sehen die zugehörigen Rechtsnebenklassen jetzt aus?

(3.3.4) Damit haben wir eine Partition von G in gleichmächtige Klassen konstruiert. Ist insbesondere G endlich, mit n=#G Elementen, so gilt immer

Folgerung: #G=(#H)×(*Zahl* der Bahnen)
Die Ordnung einer Untergruppe ist stets ein Teiler der Gruppenordnung.

(3.3.5) Ist die Gruppenordnung insbesondere eine Primzahl, so kann es keine nichtttivialen Untergruppen geben! Das Beispiel fasst die Resultate zusammen:

Hier ist {e,g_1,g_2,g_3,g_4} Vertretersystem der Klassen. Hg={$h_1 g = eg = g, h_2 g, h_3 g, h_4 g$} Rechtsnebenklasse.	Hg$_4$ Hg$_3$ Hg_2 Hg$_1$ H=He	Hat H 4 Elemente und 5 Nebenklassen, dann hat g gerade 5·4 = 20 Elemente

Die Abbildung (H,h↦gh,gH) ist bijektiv.

Nochmals: **Ist die Ordnung k einer Gruppe G eine Primzahl, dann kann die Gruppe keine nichttriviale Untergruppe enthalten.** Jetzt sei g ein vom neutralen Element e verschiedenes Element und es sei E(g) die von g erzeugte zyklische Untergruppe. Sie muss Untergruppe sein. Da sie g enthält, kommt {e} nicht in Frage. Es bleibt nur G selbst. **Das bedeutet aber, dass G isomorph zur zyklischen Gruppe der Ordnung k ist.**

Oder: Ist k Primzahl, so gibt es nur eine einzige Isomorphieklasse, wie früher in (2.3.16) bereits angegeben. Das ist jetzt bewiesen.

Aber auch wenn k keine Primzahl ist, ergeben sich für mögliche Untergruppen enorme Einschränkungen. Nehmen wir k=10. Dann haben alle eventuellen nichttrivialen Untergruppen die Ordnung 2 oder 5. Andere

kann es nicht geben. Ob es tatsächlich solche Untergruppen gibt, ist eine andere und teilweise schwierige Strukturfrage. Im Fall der zyklischen Gruppen ist sie allerdings leicht positiv zu beantworten.

☐ Wir betrachten die zyklische Gruppe von 10 Elementen in der Restklassenform (Z/(10),+). Dann sind nur nichttriviale Untergruppen der Ordnungen 2 und 5 möglich. Begründen Sie, dass {0,5} und {0.2,4,6,8} tatsächlich Untergruppen dieser Ordnungen sind. Es sind die Untergruppen, die von den Elementen 5 bzw. 2 erzeugt werden. Welche Untergruppen werden von den ungeraden Elementen erzeugt, welche von 6? (Wir schreiben kurz k statt [k] für die Restklassen.)

(3.3.6) Analog zu (3.3.2) kann man durch (g,h)↦gh eine Rechtsoperation der Untergruppe H auf G einführen. Erneut erhält man eine Zerlegung in gleichmächtige Klassen, die man jetzt Linksnebenklassen nennt und mit gH bezeichnet. Links bezieht sich sinnvollerweise auf die Stellung des Vertreterelementes, nicht die der Untergruppe.

Diesen Linksnebenklassen sind wir bereits begegnet. Bei der Analyse der Stabilisatoren hatten wir die Umwandlungsmengen B(x→y) eingeführt für Elemente y derselben Bahn. Etwa y=g⋆x, wobei ⋆ eine beliebige G-Linksoperation war. Unser altes Resultat besagt einfach: B(x→g⋆x)=gS_x, wobei S_x der Stabilisator des Punktes x war.

☐ Welche analoge Eigenschaft haben die Rechtsnebenklassen ?

(3.3.7) Die Linksnebenklassen müssen (als Mengen) keineswegs gleich den entsprechenden Rechtsnebenklassen sein. Kurz Hg=gH muss nicht immer (für alle g) gelten. Bei der Weiterentwicklung der Gruppentheorie erweisen sich Untergruppen, für die diese Gleichheit stets gilt, als recht wichtig. Man nennt sie *Normalteiler.* Wir gehen hierauf an dieser Stelle nicht genauer ein.

☐ Bestimmen Sie für die Untergruppe H=$\{1,\tau_1\}$ von $\mathcal{S}_3$ jetzt auch die Linksnebenklassen. Überzeugen Sie sich, dass **kein Normalteiler** vorliegt.

☐ Angenommen G ist endliche Gruppe der Ordnung n und H ist Untergruppe mit genau n/2 Elementen. Beweisen Sie, dass H dann notwendig ein Normalteiler ist. (Beispiel H=$\{1,a,a^2\}$ in $\mathcal{S}_3$)

☐ Es sei $\varphi : G \to G_1$ ein Gruppenhomomorphismus und K=Kern$\varphi \subset G$. Beweisen Sie, dass K ein Normalteiler von G ist.

(3.3.8) Jetzt ein Beispiel einer Abbildung im Gruppenbereich, die **keine Operation** bildet, obwohl man das zunächst denken könnte:

- Sei G irgendeine Gruppe und $(\mathbb{Z}, +)$ die additive Gruppe der ganzen Zahlen.
  Dann haben wir folgende Abbildung ($\mathbb{Z} \times G$, (n,g)↦ g^n, G).,

Dabei ist $g^0 = e$, gg=g^2 usw. Der Abbildungsbau suggeriert eine Gruppenoperation auf G. Aber es ist keine! Denn n⋆$g = g^n$. Also n⋆$(m \star g) = g^{nm}$. Dagegen (n+m)⋆$g = g^{n+m}$.

3.3.3a **Konjugationsklassen**

Das jetzt zu besprechende Beispiel gibt eine Operation. Sie ist für jede Gruppe verfügbar sehr nützlich, da sie eine Art geometrische Klassifikation der Gruppenelemente liefert, die sich in jeder Operation dieser Gruppe manifestiert.

(3.3.9) *Die inneren Automorphismen einer Gruppe.* (Automorphismus = Isomorphismus der Gruppe auf sich selbst!)

Sei G Gruppe. Dann operiert G auf sich selbst vermöge
$\tau = (G \times G, (g, x) \mapsto gxg^{-1}, G).$

Das ist eine Linksoperation: e⋆x=x ist klar. Und h⋆(g⋆x)=h(gxg^{-1})h^{-1}= (hg)x($g^{-1}h^{-1}$)=(hg)x$(hg)^{-1}$ = (hg)⋆x wie gewünscht. Vgl. (3.1.5b). Wieder muß man genau darauf achten, welche Rolle ein g∈G jeweils hat: Gruppenelement oder Objekt?

(3.3.10) Eine erste Besonderheit: Während sonst die Transformationsabbildungen t_g nur rein mengentheoretische Abbildungen sind, handelt es sich hier um Gruppenisomorphismen G→G. Insbesondere bildet so eine Transformation nach (2.4.19) Untergruppen von G automatisch wieder in (isomorphe) Untergruppen ab. Man nennt diese Transformationsabbildungen x↦ $t_g(x) = gxg^{-1}$ die *inneren Automorphismen der Gruppe G*,

Auch dieser Konstruktion sind wir bei der Analyse der Stabilisatoren in (3.2.12) bereits begegnet. Die dort konstruierten Isomorphismen zwischen den Stabilisatoren der verschiedenen Punkte einer Bahn waren derartige innere Automorphismen. Genauer gesagt die Einschränkung derselben auf die Stabilisatoren.

(3.3.11) Was für Strukturen erzeugt die Operation (g,x)$\mapsto$ gxg^{-1} auf M=G? Die Stabilisatoren sind Untergruppen von G, definiert durch $S_g = \{h \mid h \in G, h = ghg^{-1}\}$ oder auch hg=gh. Ist G kommutativ, ist das für alle h der Fall, sonst eventuell für weniger. Damit ist S_g so etwas wie ein Maß dafür, wie kommutativ die Gruppe G hinsichtlich ihres Elementes g ist. Je weniger Elemente mit G vertauschen, desto kleiner ist der Stabilisator S_g unserer Operation. Für das neutrale Element e gilt $S_e = G$.

(3.1.12) Die entstehenden Klassen haben eine große Bedeutung. Man nennt sie die *Konjugationsklassen der Gruppe G.* Nochmals ihre Definition:

K(g)={h|h∈G, $\exists x \in G$ mit h=xgx^{-1}}
Oder: hx=xh oder $(hg^{-1})gx = xg$.
D.h. hg^{-1} ist so etwas wie ein Korrekturfaktor zur Kommutativität.

Die Konjugationsklassen haben in der Regel unterschiedliche Elementzahl. Insbesondere ist die Klasse des neutralen Elements immer einelementig. Je größer die Klasse von g, desto mehr Elemente gibt es, die nicht mit g vertauschen. Bei einer abelschen Gruppe sind alle Klassen einelementig.

(3.3.13) Hinsichtlich beliebiger Gruppenoperationen haben die Konjugationsklassen die folgende interessante inhaltliche Interpretation:

Sei $\star$: G×M→M Gruppenoperation. x∈M mit Stabilisator S_x und Bahn B(x). Sei y ein Bahnelement. D.h. man hat g∈G mit y=g$\star$x. Die Stabilitätsuntergruppe von y sei $S_y = S_{g\star x}$ Dann ist $S_y = \tau_g(S_x)$. Die beiden Stabilisatoren sind also isomorph und unser innerer Automorphismus τ_g vermittelt diese Isomorphie.

Für x bestehe irgendeine Relation der Art
a$^k \star x = b \star x$ mit a,b∈ G. Dann gilt für
y=g$\star y$ die analoge Relation
A$^k \star y = B \star y$ mit A=$\tau_g(a)$ und B=$\tau_g(b)$.

(3.3.14) Dies Resultat interpretieren wir wie folgt: Die Eigenschaften, die entlang einer Bahn erhalten bleiben, sind nicht immer offensichtlich, sondern meist mehr oder weniger unzugänglich codiert. Sie sollten sich aber mit Hilfe der vorhandenen Struktur ausdrücken lassen. Und dieses Ausdrücken erfolgt über irgendwelche Gleichungen, die mit Hilfe der Gruppenoperation gebildet werden. Sagen wir für x geschehe das durch eine Gleichung a$\star$x=z mit x,z∈M und a∈G. Dann muß es für y=g*x eine Gleichung geben, die für diesen anderen Bahnpunkt die entsprechende Aussage macht. Und unsere Konstruktion liefert automatisch und schematisch eben diese Gleichung zu τ_g(a)$\star$y=g$\star$z. Also ist τ_g(a)∈G das neue, umbenannte Gruppenelement, das mit y eben das macht, was a selbst mit x macht. Insbesondere liegen beide Gruppenelemente in derselben Konjugationsklasse. Gleichgültig um welche G-Operation (dasselbe G. anderes M) es sich handelt! Die Konjugationsklassen von G geben an, welche Gruppenelemente in der Lage sind isomorphe oder gleichartige Operationen zu produzieren. **Dies wird demnach durch die Gruppe allein festgelegt!**

(3.3.15) Ein Beispiel: Im Falle der später einzuführenden Symmetriegruppen liest sich eine Beziehung wie g^{3*}x = e$\star x$=x typischerweise so: Führt man mit dem Punkt x dreimal die von g bestimmte Operation aus, so gelangt man wieder zu x. D.h. wir haben es mit einer dreizähligen Symmetrieachse zu tun! Liegt y=g$\star$x jetzt auf derselben Bahn, dann gilt nach unseren Überlegungen für h=τ_g(a) notwendig h^{3*}y=y. D.h. auch der Punkt y gehört zu einer dreizähligen Achse und die Achsendrehung wird durch h bewirkt! Zu x und y gehören dreizählige, aber in der Regel verschiedene Achsen. Die Eigenschaft Dreizahligkeit bleibt entlang der Bahn bewahrt und die Verschiedenheit läßt sich mit Hilfe der inneren Automorphismen ineinander umrechnen. Ein anderer Achsentyp kann nicht in derselben Bahn liegen! Oder auch: **Die Bahnen fassen Punkte mit gleichartigen Symmetrieeigenschaften zusammen**. Bei einem Würfel haben alle 8 Eckpunkte eine dreizählige Symmetrie, liegen in einer Bahn der Symmetriegruppe. Dagegen liegen die Flächenmittelpunkte (beim Würfel) mit vierzähliger Symmetrie in einer anderen Bahn.

(3.3.16) Ergebnis:

> **x und y=g$\star$x verhalten sich bezüglich jeder durch $\star$ erfassten Transformation völlig analog, sofern man nur die dureh τ_g induzierte Umbenennung vornimmt. Und die dabei entstehenden Gruppenelemente liegen immer in derselben Konjugationsklasse. Diese enthalten algebraisch und geometrisch gleichwertige Gruppenelemente.**

(3.3.17) Wegen der Bedeutung dieses recht abstrakten Resultates noch ein rechnerisches Beispiel: Angenommen man hat (aa)⋆x=b⋆x. D.h., transformiert man den Punkt x zweimal unter a, so ergibt das dasselbe, als wenn man unter b transformiert hätte. Diese Gleichung schreiben wir g⋆(ag^{-1}gag^{-1})⋆x= g⋆(bg^{-1}g)⋆x. Was nach den Operationsaxiomen zulässig ist. Und weiter: ((gag^{-1})(gag^{-1}))⋆(g⋆x)= (gbg^{-1})⋆(g⋆x). Also $A^2 \star y = B \star y$ mit den Umbenennungen A=τ_g(a)=gag^{-1} und B=$\tau_g(b)$ =gbg^{-1}. Dabei liegen die Gruppenelemente A und a bzw. B und b in derselben Konjugationsklasse.

Verfolgen Sie sorgfältig, wie alle Manipulationen durch die Operationsaxiome gerechtfertigt werden.

3.3.4 **Permutationen** (Fortsetzung von (3.0.2).

(3.4.1) Die unterschiedlichsten Objekte lassen sich auf dieselbe Art permutieren. Hier begegnen wir erneut dem Problem, das wir im Zusammenhang mit dem Isomorphismusbegriff angesprochen haben: Einerseits liegt immer dieselbe Art von Vertauschung vor, aber andererseits ist es doch nicht dieselbe Vertauschung, weil ja jeweils andere Objekte vertauscht werden. Jetzt können wir genauer sagen: **Ein und dieselbe Gruppe operiert auf verschiedenen Mengen, u. U auch mit unterschiedlicher Wirkung**. Die Gruppe, um die es hier geht, ist die symmetrische Gruppe von n Elementen, die wir ja als Gruppe aller bijektiven Abbildungen $I_n \to I_n$ mit I_n ={1,2,...,n} eingeführt haben,

(3.4.2) Nun findet man unterschiedliche Arten von Vertauschungen vor, meist jedoch von einer der folgenden drei Typen:

- Die Objekte als solche werden permutiert, so wie es durch eine bijektive Abbildung beschrieben wird (aus a wird π(a)=b, aus c wird $\pi(c)$, ...)
- Die Objekte bilden ein Tupel, in dem die Komponenten vertauscht werden.(Aus ABBC wird BCAB) . Die Tupelform ist hier der Konfigurationsraum und die Tupel selbst sind Felder darauf.
- Man hat eine Parametrisierung der Objekte und das Permutieren erfolgt durch Änderung der Parametrisierung.

(3.4.3) Der (häufige) zweite Typ ist in Wahrheit der dritte! Denn jedes Tupel kann als Parametrisierungsabildung i↦(i-te Komponente) interpretiert werden. Wir müssen also den ersten und den dritten Fall formalisieren, d.h, als Gruppenoperation darstellen.

(3.4.4) **Permutationen der Objekte**. Sei M={A,B,C,....} eine n-elementige Menge zu permutierender Objekte. Wir wählen eine feste bijektive Parametrisierung a:I_n ↦M. Die Umkehrabbildung ist eine Codierung q:M→I_n mit q=a^{-1}. D.h. q(A) ist die zugehörige Indexnummer. Wir führen die folgende Linksoperation ein:

Operation der direkten Permutation: $(\mathcal{S}_n \times M, (\pi, X) \mapsto a \circ \pi \circ q(X), M)$

Als Verlaufsdiagramm $M \xrightarrow{a} I_n \xrightarrow{\pi} I_n \xrightarrow{q} M$. Das ist eine Linksoperation, die allerdings von der Wahl von a abhängt. Eine typische zugehörige Verbalisierung: "1 wird zu 2, 2 zu 3 und 3 zu 1".

(3.4.5) Die Stabilitätsuntergruppen sind alle isomorph zu $\mathcal{S}_{n-1}$. Bis auf das betrachtete (stabil zu haltende) Element dürfen die restlichen n-1 Elemente beliebig vertauscht werden. Die einzige Bahn ist ganz M, hat also n! Elemente. (n!=n·(n-l)! Vgl. (3.2.11))

Manchmal ist es nützlich, die Ausdehnung dieser Operation auf Teilmengen von M zu betrachten, was mit dem allgemeinen Schema problemlos geht. Oder auch: Die Operation läßt sich kanonisch auf die Potenzmenge ausdehnen.

(3.4.6) **Permutationen der Parametrisierung**. Jetzt zum zweiten Fall. Wir setzen P=$\mathfrak{F}(I_n, M)$, betrachten also die Menge aller Parametrisierungen von M mit fester Parametermenge. Achtung: Die Parametrisierungen müssen keineswegs bijektiv sein, wie im ersten Fall.

Hierzu definieren wir eine Linksoperation $\mathcal{S}_n \times P \to P$ wie folgt: (π,a)↦ $\pi \star a = a \circ \pi^{-1}$. Das Pfeildiagramm $\boxed{I_n \xrightarrow{\pi^{-1}} I_n \xrightarrow{a} M}$ macht die Reihenfolge verständlich.

Wieso aber π^{-1} und nicht π? Das ist ein wichtiger Punkt. Nur so erhalten wir eine Linksoperation, mit π würden wir eine Rechtsoperation erhalten. Beim Prüfen von $\pi \star (\sigma \star x) = (\pi \circ \sigma) \star x$ wird das klar:

$$\pi \star (\sigma \star x) = \pi \star (x \circ \sigma^{-1}) = (x \circ \sigma^{-1}) \circ \pi^{-1} = x \circ (\sigma^{-1} \circ \pi^{-1}) = x \circ (\pi \circ \sigma)^{-1} = (\pi \circ \sigma) \star x$$

Ohne Bildung des Inversen hätten wir die unerwünschte Reihenfolge $(\sigma \circ \pi) \star x$ erhalten.

(3.4.7) **Ergebnis**:

> **Tupel- oder Indexpermutation:** Die Konstruktion
> $\star = (\mathcal{S}_n \times \mathfrak{F}(I_n, M), (\pi, a) \mapsto a \circ \pi^{-1}, \mathfrak{F}(I_n, M))$ mit $\pi \star a(j) = a(\pi^{-1}(j))$ j=1,2,...,n
> liefert eine Linksoperation auf $\mathfrak{F}(I_n, M)$, macht jeweils aus einer
> Indizierung von M eine andere.

(3.4.8) In vielen Fällen schreibt man die Parametrisierung in Tupelform oder noch einfacher als symbolisches Produkt. Die Ausgangsparametrisierung sei $i \mapsto a_i$. Z.B. AABC. D.h. a_1=a_2=A, a_3=B und a_4=C. Die neue Parametrisierung sei $i \mapsto b_i$. Dann besagt unsere Formel $b_i = a_{\pi^{-1}(i)}$. D.h. die i-te Komponente nach der Transformation ist gleich der π^{-1}(i)-ten vorher. Das ist vernünftig und unbedingt zu merken. Ist etwa $\pi(2) = 3$, so folgt $b_3 = a_2$.

Die Bahn von AABC unter $\mathcal{S}_4$, hat offenbar $\frac{4!}{2}$=12 Elemente. die von AABB nur 6 und die von ABCD gerade 24. Die Bahnlängen sind abhängig vom Objekt a und unterschiedlich groß.

3.3.4a **Klassifikation der Partitionen einer endlichen Menge**

(3.4.9) Als Anwendung behandeln wir ein schwierigeres Problem, das wir in Kapitel 1.3 gestellt haben: **Gesucht ist eine sinnvolle Klassifikation aller Partitionen einer endlichen Menge.**

Klassifikationen erhält man günstig über Äquivalenzrelationen. Die Bahnen von Gruppenoperationen leisten das. Also sollte man fragen: Gibt es eine natürliche Gruppenoperation auf den Partitionen einer endlichen Menge? Ein Kandidat ist erneut die Permutationsgruppe, die die individuellen Elemente vertauscht. Wie sollte die Antwort auf die gestellte Frage dann in etwa aussehen?

(3.4.10) Nehmen wir als Beispiel M={a,b,c,d,e}. Um Klammern zu sparen, benutzen wir eine sich selbst erklärende Schreibweise zur Darstellung der Partitionen. Folgende Einteilung der 52 Partitionen in 7 Klassen liegt nahe (Das jeweils hinzugefügte Symbol wird unten erklärt):

Zahl d Klassen	Partitionen	Symbol
5	a|b|c|d|e	(1^5)
4	a|b|c|de , a|b|d|ce, ...,c|d|e|ab	$(1^3 2)$
3	a|b|cde , a|c|bde , ...,d|e|abc	$(1^2 3)$
3	a|bc|de , a|bd|ce ,..... , e|ab|cd	(12^2)
2	a|bcde , b|acde, , e|abcd	(14)
2	ab|cde , ac|bde, ..., de|abc	(23)
1	abcde	(5)

Man sieht: Die Anzahl der Klassen allein ergibt eine zu grobe Klassifikation.

(3.4.11) **Lösung des Problems mit Hilfe der Gruppentheorie.**

> Es sei M eine endliche Menge mit m Elementen und P(M) die Menge aller Partitionen von M. Gesucht ist eine strukturgerechte Klasseneinteilung dieser Partitionen. Wir realisieren die Einteilung in Form der Bahnen einer Gruppenoperation. Als Gruppe bietet sich die symmetrische Gruppe von n Elementen an,

(3.4.12) Sagen wir M={A,B,C,D,E,F,G}. Sei P(M) die Menge aller Partitionen von M. Eine typische Partition von M sieht so aus p={{A,D},{B,C},{E,F,G}}. Diese Darstellung legt es nahe, die Elemente zu permutieren und zwar über eine Parametrisierung. Das Objekt an der dritten Stelle ist B also a(3)=B. Im Beispiel haben wir 7 Kästen für ebensoviele Objekte. Offensichtlich operiert $\mathcal{S}_7$ auf P(M). Vertauscht $\pi \in \mathcal{S}_7$ nur den Inhalt der beiden ersten Kästen, so entsteht die Partition $\pi \star p$= {{D,A},{B,C},{E,F,G}}= p. Denn es gilt ja {A,B}={B,A}. D.h., das betrachtete π **ist Element des Stabilisators**. Vertauscht ψ dagegen nur den Inhalt von zweitem und sechstem Kasten, dann entsteht eine von p verschiedene Partition nämlich $\psi \star$p= {{A,F},{B,C},{E,A,G}}. Diese Partition liegt aber in derselben Bahn wie p.

Wie sehen die Bahnen aus? D.h. welche Eigenschaft haben Partitionen gemeinsam, die jeweils in derselben Bahn liegen? Offenbar können wir unsere Interpretation für p wie folgt ergänzen:‘**Die 7 Kästen**

werden auf drei Schränke verteilt. In die ersten beiden Schränke kommen je zwei Kästen und in den dritten drei. Durch die Gruppenoperation - eine beliebige Vertauschung der Objekte - wird der Inhalt der Kästen vertauscht, aber die Schränke samt Kästen bleiben unverändert! Die entstehenden Bahnen lassen sich folglich durch die zugehörige Schrankaufteilung charakterisieren! So läßt sich die Partition r={{C,D},{E},{A,B,C,F,G}} nicht aus p erzeugen. r liegt in einer anderen Bahn als p, weil die Schrankstruktur - 3 Schränke mit 1,2 und 5 Kästen - eine andere ist. Dagegen gilt nach den Regeln der Mengenlehre {{A,B,C,F,G},{D},{E}}=r. Es liegt dieselbe Partition vor, nur mit einer anderen Schreibweise oder Bezeichnung.

Die oben in (3.4.10) erratene Aufteilung für n=5 gibt genau die möglichen Schrankaufteilungen wieder. Wie beschreibt man die Schrankstruktur allgemein? Offenbar durch eine Abbildung $\lambda : j \mapsto \lambda_j$ wobei λ_j gleich der Zahl der Schränke mit genau j Kästen sein soll. $\lambda_j = 0$ ist zugelassen. Für p ist $\lambda_1 = 0$ und λ_2=2 und λ_3=l. Es genügt, die λ_j für j=1,2,...,n=#(M) anzugeben, um die Schrankstruktur vollständig festzulegen. Dies macht man gern mit Hilfe einer symbolischen Codierung von λ. Für das oben gewählte p schreibt man $\lambda_p = (2^2, 3^1)$. Also zwei Schränke für 2 Kästen und 1 Schrank für 3 Kästen. Für r dagegen ist λ_r=(1^2,5).

(3.4.13) Allgemein definieren wir:

Das Symbol einer Partition p∈P(M) ist $\lambda = (1^{\lambda_1}, 2^{\lambda_2}, ..., n^{\lambda_n})$ mit $\lambda_j = 0, 1, ..., n$.
- ♦ Komponenten mit λ_j=0 können in konkreten Beispielen fortgelasen werden.
- ♦ Ist $\lambda_j = 1$ schreibt man j statt j^1.
- ♦ Die Gesamtzahl der Schränke ist $\Sigma_i \lambda_i$ das ist notwendig eine natürliche Zahl zwischen 1 und n=#M.
- ♦ Die Gesamtzahl der Objekte (Kästen) ist $\Sigma_j j\lambda_j = \#M = n$.
- ♦ Jeder Partition p∈P(M) wird das zugehörige Symbol λ=λ_p zugeordnet.

In (3.4.10) sind die Symbole für n=5 mit angegeben.

Jedes derart bestimmte λ legt eine eindeutig bestimmte Schrankstruktur fest und damit zugleich eine Bahn unserer Objektvertauschungsoperation. Für n =7 gibt es die folgenden Möglichkeiten und Bahnen, die wir wieder nach der Zahl der jeweils vorhandenenen Schränke geordnet haben:

(7)	(1,6)	$(1^2, 5)$	$(2^2, 3)$	$(1^4, 3)$	$(1^5, 2)$	(1^7)
	(2,5)	(1,2,4)	$(1^3, 4)$			
	(3,4)	$(1,3^2)$	$(1^2, 2, 3)$			
			$(1,2^3)$			

Man sieht, dass es für n=7 bereits recht viele Möglichkeiten gibt, und weshalb man daher um möglichste Kürze und Prägnanz der Schreibweise bemüht ist.

(3.4.14) Damit haben wir die Bahnen! Wie sieht es mit den Stabilisatoren aus? Diese lassen sich jetzt leicht bestimmen. Man darf innerhalb jedes Schrankes beliebig permutieren. Bei einem Schrank mit j Objekten sind das j! Permutationen. Und man darf den gesamten Inhalt von Schränken gleicher Objektzahl austauschen, also Schränke gleicher Größe permutieren. Es gibt λ_j Schränke der Größe j, also weitere λ_j! Möglichkeiten.

Kombiniert man alle dies unabhängigen Möglichkeiten, so ethält man folgende **Stabilisatorordnung:**

Hat eine Partition p das Symbol λ, dann wird **die Ordnung des zugehörigen Stabilisators** S_p durch folgende Formel gegeben:
$\#S_p = (1!)^{\lambda_1}(2!)^{\lambda_2}.....(n!)^{\lambda_n} \cdot \lambda_1!\lambda_2!.....\lambda_n!$ (0!=1)

Hier werden die symbolischen Potenzen der Symbolschreibweise von λ einfach zu gewöhnlichen Potenzen. Die fortgelassenen Komponenten i^0 entsprechen Faktoren 1. Und ebenso ist j^1=j. Weiter ist wie üblich 0!=1 zu setzen. Damit ist die gegebene Formel für $\#S_p$ sinnvoll.

(3.4.15) Jetzt können wir mit Hilfe von (3.2.11) die zugehörige Bahnlänge der Partition bestimmen. Die Gruppe hat n! Elemente, so dass sich folgende Bahnlänge b(p) der zu λ_p gehörigen Klasse ergibt: $\boxed{b(p)=\frac{n!}{\#S_p}}$.

(3.4.16) Für unser Eingangsbeispiel p war (λ)=(2^2,3), also $b(p)=\frac{7!}{(2!)^2(3!)^1 \cdot 2!} = 105$ D.h. es gibt 105 Partitionen, die zu demselben Schranktyp wie p gehören.

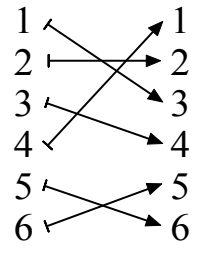
Im Gegensatz zum Fall der Nebenklassen bei Gruppen, haben hier die Bahnen in der Regel unterschiedliche Länge. Die Gesamtzahl der Partitionen von M erhält man durch Aufsummieren aller Bahnlängen. D.h. über die Formel $\#P(M)=\Sigma_{(\lambda)}\frac{n!}{\#S_{(\lambda)}}$. D.h. es müssen zunächst alle Symbole (λ) bestimmt werden, was recht mühsam sein kann. Für n=5 erhält man 52 Partitionen.

3.3.4b **Die Zykeldarstellung der Permutationen**

(3.4.17) Permutationen kann man auf viele Weisen darstellen und aufzählen. In Kap. 3.2.1 haben wir ein Beispiel einer nicht gerade strukturgerechten Parametrisierung durch einfache Numerierung gegeben. Für nicht zu großes n wird häufig die gesamte Wertetabelle angegeben. Jetzt soll eine andere auf einer Gruppenoperation basierende Darstellung gegeben werden, die häufig nützlich ist.

(3.4.18) Sei x:$J_n \rightarrow J_n$ die betrachtete Permutation für $J_n = \{1,2,....,n\}$. Weiter Sei $E(\pi)$ die von π erzeugte Untergruppe von $\mathcal{S}_n$. Wir lassen $E(\pi)$ per Einschränkung auf J_n operieren und fragen nach den Bahnen. Etwa nach der von $1 \in J_n$ erzeugten Bahn. Sie enthält $1, \pi(1), \pi^2(1), ...$ Da eine Partition entsteht, muss es ein $k \leq n$ geben, für das $\pi^k(1) = 1$ gilt! Wir bilden das Tupel $(1,\pi(1),....,\pi^{k-1}(1))$. Beachten Sie: Tupel - nicht Menge. Die Elemente ergeben eine Bahn und das Tupel selbst gibt an, wie die darin enthaltenen Elemente sich unter π verhalten, nämlich zyklisch. Insbesondere wird das letzte Element durch π wieder auf das erste - hier 1 - abgebildet. Der Zykel (1,4,3) etwa besagt: $\pi(1)=4$, $\pi(4)=3$ und $\pi(3)=1$. Gibt es noch weitere Bahnen, so erzeugt und schreibt man diese analog. Am Ende ist J in lauter Bahnen aufgeteilt. Die Elemente derselben Bahn kann man durch mehrfaches Anwenden ineinander umwandeln.

Oder auch: Man kann π: auf jede Bahn restringieren und erhält eine Permutation dieser Bahn. Die Figur zeigt ein Beispiel



Diese Permutation hat die Zykeldarstellung (2)(5,6)(1,3,4) mit dem Symbol $(1^1,2^1,3^1)$ Die Zykel sollten mit dem jeweils kleinsten Element beginnen, also (1,3,4) und nicht (4,1,3)

(3.4.19) Dabei ist es sinnvoll in jeder Bahn mit dem kleinsten Bahnelement zu beginnen und die Bahnen selbst nach Bahnlänge zu ordnen. Innerhalb jeder Bahn liegt die Reihenfolge der Elemente fest. Die Zykeln permutieren - als Abbildungen - alle miteinander.

(3.4.20) Jetzt kann man jeder solchen Zykeldarstellung, die ja in offensichtlicher Weise eine Partition von J_n erzeugt, das zugehörige Partitionssymbol zuordnen: $(1^{\lambda_1}2^{\lambda_2}.....n^{\lambda_n})$ Also λ_1 Zykeln der Länge 1, λ_2 Zykeln der Länge 2 usw. Damit erhalten wir eine verfeinerte Klassifikation der bijektiven Abbildungen.

(3.4.21) Nehmen wir die Gruppe $\mathcal{S}_4$ mit der in (2.1.10) gegebenen Zählparametrisierung. Wir finden 5 Klassen (Bahnen) von offensichtlich zusammengehörigen Partitionen.

Die mit 1 bezeichnete Permutation, die Identität, gehört zu (1^4),

(2,3,6,7,15,22) gehört zu $(1^2.2)$. Zwei Elemente bleiben fest, die anderen beiden werden vertauscht. Die Stabilisatoren haben 24/6=4 Elemente. Die Permutationen 4,5,9,12,13,16,20 und 21 gehören zu (1.3^1). Ein Element bleibt fest. Die Stabilisatoren haben 24/8=3 Elemente.

Die Klasse der folgenden Permutationen aus $\mathcal{S}_4$	hat das gemeinsame Symbol:	Stabilisatorgröße
{1}	(1^4)	24
{2,3,6,7,15,22}	$(1^2 2)$	4
{4,5,9,12,13,16,20.21}	(13)	3
{8,17,24}	(2^2)	8
{10,11,14,18,19,23}	(4)	4

□ Inspizieren Sie die einzelnen Klasssen in (2.1.9) sorgfältig .

(3.4.22) Zusammen entsteht eine Partition der Gruppe $\mathcal{S}_n$, die auf der folgenden Frage basiert: "In wieviel disjunkte Teile welcher Art läßt sich die Zuordnung der Permutationsabbildung jeweils zerlegen?"

□ Beweisen Sie (für allgemeines n): Die Zykelpartition ist die Einteilung der Gruppe in ihre Konjugationsklassen. Begründen sie das Resultat auch inhaltlich.

3.3.5 Wandel und Erhaltung (3): Einschränkungen der Gruppenoperation

(3.5.1) Die Operationsstruktur zeigt eine bemerkenswerte Leistungsfähigkeit bei der Phänomenbeschreibung. Dabei erfolgen viele interessante Anwendungen mit Hilfe der an und für sich banalen Methode der Einschränkung der Operation auf Untergtuppen. Mit diesem Sachverhalt wollen wir uns jetzt genauer befassen.

Operiert eine Gruppe G auf einer Menge X und ist H eine Untergruppe von G, dann operiert auch H auf X. Denn die Wertemenge bleibt bei dieser Einschränkung von G×X→X auf H×Xp→X ja unverändert, so dass das übliche Abgeschlossenheitsproblem nicht auftritt.

(3.5.2) Weshalb ist diese Konstruktion nützlich? Wir greifen das Thema Wandel und Erhaltung aus (3.0.1) und (3.2.19) erneut auf. Wie sehen die Leistungen aus, die Anschauung und Vorstellung mit Hilfe des Konfigurationsraumes vollbringen? Da geht es um Körper, Figuren, Systeme, bei denen sich gewisse Eigenschaften ändern, andere dagegen erhalten bleiben. Trotz der Änderungen müssen wir in der Lage sein, die Identität der Objekte im Konfigurationsraum zu etkennen und sie bei Prozeßabläufen zu verfolgen. Das visuelle Erkennen, Verfolgen und Wiedererkennen von Gegenständen ist ein einfaches Beispiel und die Leistungsfähigkeit unseres Wahrnehmungssystems dabei ist eindrucksvoll. Aber entsprechende Leistungen werden auch in ganz anderen Zusammenhängen benötigt.

Änderungen, zumindest die umkehrbaren, lassen sich typischerweise als bijektive Abbildungen f:X→X des Konfigurationsraumes X und der zugehörigen Abbildungserweiterung $\underline{f}$ auf die Figuren beschreiben. Die zugehörige gesamte Permutationsgruppe G=$\mathfrak{B}$(X,X) ist riesig und erfaßt alle überhaupt denkbaren Änderungen. Bei konkreten Problemen werden die Änderungen jedoch situationspezifisch eingeschränkt. Gewisse Eigenschaften müssen erhalten bleiben, andere dürfen sich ändern. Bei der Bewegung eines starren Körpers im Raum darf sich die Lage aller Punkte ändern, aber nur so, dass Abstände und Winkel im Körper erhalten bleiben. Und das heißt: Nur Elemente der Untergruppe H=S0(3) von G sind zulässig.

Interessiert man sich in einer anderen Situation alternativ für die Ähnlichkeit von Figuren. dann sind die in (3.1.4) eingeführten Transformatione $h_\alpha:\vec{x} \mapsto \alpha\vec{x}$ zusätzlich zulässig. Usw.

(3.5.3) **Wahl oder Bestimmung einer Untergruppe H von B(X,X) legt fest. was an Form- und Figureigenschaften bewahrt werden soll** und daher in gleichen Bahnklassen zusammenfällt. Unterschiedliche Klassen erfassen die verbleibenden Unterschiede. **Und jede Wahl von H liefert eine eigene zugehörige Trennung von Identität und Veränderung**. Bisher wurde die Gruppe H, die auf X operiert, diskussionslos vorgegeben. Jetzt fragen wir, was es bedeutet, dass H dann immer als Untergruppe von $\mathfrak{B}$(X,X) interpretiert werden kann.

Wir besprechen drei wichtige Beispieltypen.

3.3.5a Entwicklungsprozesse ("Evolution")

(3.5.4) Wir beschränken uns auf den diskreten Fall mit $\mathbb{Z}$ als Gruppe. Auf den "kontinuierlichen" Fall mit der Gruppe $(\mathbb{R}, +)$ kommen wir im Zusammenhang mit den Differentialgleichungen in Kap.6 zurück.

Ein solcher Entwicklungsprozess ist in unserem Rahmen immer ein Gruppenhomomorphismus $\epsilon:\mathbb{Z} \to \mathfrak{B} = \mathfrak{B}$(X,X). Wir wissen, dass dann H=Bild(E) eine Untergruppe von $\mathfrak{B}$ ist. Und die eingeschränkte Operation H×X→X ist es, die interessiert.

Was hat eine derartige Abbildung mit einem Entwicklungsprozess zu tun? Nun entscheidendes Merkmal von $\mathbb{Z}$ ist, dass jedes Element einen eindeutig bestimmten Vorgänger und einen ebensolchen Nachfolger hat. Die Zahl -7 hat in den ganzen Zahlen den Nachfolger -6. Usw. Hat man nun eine Regel, die angibt, wie man aus einem Vorgängerelement des Konfigurationsraumes ein zugehöriges Nachfolgerelement bestimmt, so entsteht durch Regelanwendung zweierlei: Zum einen Bahnen, die angeben, welche Elemente durch Mehrfachanwendung ineinander übergehen und zum anderen eine Parametrisierung der Bahnelemente, die die Vorgänger-Nachfolgerstruktur beschreibt, angibt welches Bahnelement Nachfolger eines anderen ist. Und damit sind wir genau bei unserer $\mathbb{Z}$-Operation auf X!

(3.5.5) Wie kann eine Nachfolgerfestlegungsregel konkret aussehen? Sagen wir X=$\mathbb{R}^2_K$. Eine Bahnparametrisierung hat die Form $(\mathbb{Z}, n \mapsto (x_n,y_n),\mathbb{R}^2_K)$. Dann muss unsere Regel oder Formel aus (x_n,y_n) den Wert von (x_{n+1},y_{n+1}) produzieren. Das ist üblicherweise einfach eine Rekursionsformel.

Sagen wir $x_{n+1}=x_n+y_n$, und $y_{n+1} = x_n$. Diese beiden Formeln leisten das Verlangte. Da das Vorgängerelement aber ein beliebiges Element des Konfigurationsraumes sein darf, können wir das als Zuordnung "Vorgänger↦Nachfolger" und als volle Abbildung E=$(\mathbb{R}^2_K, (x, y) \mapsto (x + y, x), \mathbb{R}^2_K)$ interpretieren. Damit haben wir die Operation als Element von $\mathfrak{B}$ dargestellt. E ist der Entwicklungsoperator. Dieser Operator ist umkehrbar, wie man sofort sieht, durch E^{-1}: (u,v)↦(v,u-v). Wie üblich setzen wir noch E∘E=E^2 usw. und haben unsere Gruppenoperation: $\mathbb{Z} \times \mathbb{R}^2_K \to \mathbb{R}^2_K$ für diesen Fall vollständig konstruiert.

(3.5.6) Was bleibt im Fall der beschriebenen Transformation bewahrt? Die Antwort ist keineswegs leicht und anschaulich zu erkennen. Um die Frage systematisch zu beantworten, benötigen wir Resultate aus Kapitel 4. Dort werden wir auf das Problem zurückkommen. Aber Sie können das dort herzuleitende Resultat bereits rechnerisch verifizieren - was Sie versuchen sollten. Das Resultat sieht so aus: Es gibt zwei Richtungen in der Ebene, die unter E erhalten bleiben. D.h. hat (u,v) eine dieser Richtungen, dann hat E(u.v) dieselbe Richtung, aber eine andere Länge. Und das Verhältnis der beiden Längen ist für jede dieser Richtungen eine Konstante. Die beiden ausgezeichneten Richtungen werden durch die Richtungsvektoren $(1+\sqrt{5},2)$ und $(1-\sqrt{5},2)$ bestimmt.

Zurück zu den allgemeinen Uberlegungen.

(3.5.7) Nochmals der Gedankengang: Das (umkehrbare) Entwicklungsgesetz ergibt die bijektive Abbildung E:X→X. Und die von E erzeugte Untergruppe H=$\{E^n | n \in \mathbb{Z}\}$ wiederum gibt eine $\mathbb{Z}$-Operation auf X, für die natürlich all unsere allgemeinen Resultate gelten und die eine gesetzmäßige schrittweise Fortentwicklung der Punkte von X beschreibt. Der Wandel (der Objekte des Konfigurationsraumes) erfolgt über das Entwicklungsgesetz. Was bei diesem Wandel bewahrt wird, muß vielfach durch mühsame Inspektion aus den Bahnen abstrahiert bzw. mit mathematischen Methoden aus dem Gesetz abgeleitet werden.

3.3.5b **Transformationsgruppen**

(3.5.8) Hier gehen wir nicht von einem Entwicklungsgesetz mit festgelegter Art der Entwicklungsschritte aus, sondern von Klassen von Figuren, denen ganz bestimmte typische Gemeinsamkeiten zukommen. Sagen wir kongruente Figuren der Ebene oder ähnliche Figuren oder (ähnliche Figuren mit parallelen Kanten) usw. Wir geben in gewisser Weise die Bahnen aus Figuren vor. Wie können wir Derartiges fassen? Wann sind zwei Figuren etwa kongruent? Dazu muß es eine bijektive, Längen und Winkel erhaltende Abbildung geben, deren Potenzmengenerweiterung die erste Figur auf die zweite abbildet. Und derartige Bedingungen wie *Längen und Winkel erhalten* führen üblicherweise zu einer Untergruppe H von $\mathfrak{B}$ und der zugehörigen Operationseinschränkung H×X→X. Vgl. Kap.3.2.6.

Die Operation wird auf die Potenzmenge, also auf die Figuren, erweitert und die dort entstehenden Klassen (=Bahnen) sind es, die das jeweils Gemeinsame zusammenfassen. Die Bahnen und die Stabilitätsuntergruppen sind (im Zusammenhang mit Transformationsgruppen) mithin für die Figuren, also in $\mathfrak{P}(X)$ zu betrachten!

(3.5.9) Welchen Bonus ergibt diese Konstruktion, rechtfertigt die Einführung eines derart allgemeinen Formalismus? Wir nennen zwei Punkte:

- Man kann sich in Zweifelsfällen, in denen die Anschauung versagt oder unzuverlässig wird oder nicht reicht - wie etwa bei der Erstellung eines Computerprogrammes, auf einen gesicherten Formalismus zurückziehen.

- Und man kann den Formalismus auf andere Bereiche übertragen, die der Anschauung nicht zugänglich sind und dortige Probleme lösen. Oder auch: Wir können die üblichen geometrischen Betrachtungen über Figuren algebraisieren und damit präzisieren. Zu jeder Transformationsgruppe (=geeignete Untergruppe der Permutationsgruppe des Konfigurationsraumes) und jedem zugehörigen Objektraum können wir die geometrische Frage nach bewahrten, erhaltenen Eigenschaften entlang der Bahn sowie nach den noch möglichen, zulässigen Änderungen stellen und analysieren.

3.3.5c **Symmetriegruppen**

(3.5.10) Einen dritten und besonders auch für die Physik nützlichen Spezialfall der allgemeinen Konstruktion erhalten wir wie folgt: Sei X wieder der Konfigurationsraum, entweder V_0^3 oder die Ebene V_0^2.

Wir schränken die Permutationsgruppe $\mathfrak{B}$ ein auf die zugehörige (Längen und Winkel erhaltende) Bewegungsgruppe. Vgl. (3.1.14). Unsere große Operationsgruppe G sei diese Bewegungsgruppe. Weiter sei $F \in \mathfrak{P}(X)$ eine gegebene Figur im Raum. Denken Sie an einen Würfel, einen Zylinder oder ein Dreieck. G operiert durch Erweiterung auch auf den Figuren. **Uns interessiert der Stabilisator der Figur F**. Also alle Bewegungstransformationen, die F als Menge auf sich abbilden. Nicht notwendig Punkt auf denselben Punkt.

(3.5.11) Die entstehende Bahn (von Figuren) besteht aus allen zu F kongruenten Figuren. Wir wissen, dass entlang jeder Bahn sämtliche Stabilisatoren isomorph sind, d.h. die zugehörige Isomorphieklasse (von Gruppen) gibt eine charakteristische gemeinsame Eigenschaft aller Bahnelemente - also eine Gemeinsamkeit all dieser kongruenten Figuren - wieder. Wir nennen einen geeigneten Vertreter dieser Isomorphieklasse (von Gruppen) oder eventuell die Klasse selbst *die Symmetriegruppe der Figur F.*

Konstruktionsgemäß ist das erneut eine (eventuell sehr kleine) Untergruppe von $\mathfrak{B}$. Größe und Art dieser Gruppe beschreiben die Symmetrie der Figur! Enthält die Symmetriegruppe nur das neutrale Element, dann ist die Figur völlig unsymmetrisch. Es gibt keine nichttriviale Lageänderung, bei der Ausgangs- und Endfigur deckungsgleich sind. Eine zweielementige Gruppe deutet auf eine Achsenspiegelungsymmetrie hin usw.

(3.5.12) Bei einem Zylinder oder Kegel sind alle Drehungen um die Achse enthalten sowie gewisse Spiegelungan. Bei dem Zylinder kommen die 180^0-Drehungen um eine Äquatorachse hinzu, die der Kegel nicht besitzt. Die größere Symmetriegruppe unterscheidet die beiden Figuren! **Figuren mit gleicher bzw. isomorpher Symmetriegruppe haben dieselben Symmetrieeigenschaften.**

(3.5.13) Manche Figuren haben eine **endliche** Symmetriegruppe. Nehmen wir als Beispiel ein gleichseitiges Dreieck. Neben der Identität haben wir eine Drehung d in der Dreiecksebene um 120^0 und d^2 als Drehung um 240^0. Dann gibt es die Spiegelungen an den drei Mittellinien s_1, s_2 und s_3. Diese 6 Elemente machen die Symmetriegruppe aus. Beachten Sie: Die Spiegelungen an den Mittellinien kann man auch durch 180^0-Drehungen an den Mittellinien realisieren. D.h. es kommt nicht auf das Zuordnungsverfahren - hier den Weg, auf dem man vom Anfangszustand zum Endzustand gelangt - an, sondern nur auf das Ergebnis, die Zuordnung. Welche Punktmenge kommt am Ende des Weges, am Ende der Transformation heraus?

Die Gruppentafel der Symmetriegruppe des gleichseitigen Dreiecks läßt sich leicht aufstellen. Die Gruppe erweist sich als isomorph zur symmetrischen Gruppe von drei Elementen. Vgl. (2.1.18).

(3.5.14) Nehmen wir ein anspruchsvolleres Beispiel: **Die Symmetriegruppe eines Würfels.** Wir legen den Ursprung in die Mitte des Würfels. Dann wird die Lage des gesamten Würfels sicher durch die Lage seiner 8 Eckpunkte festgelegt. Sei M die Menge dieser 8 Eckpunkte. Unter einer Symmetrieoperation geht jeder Eckpunkt wieder in einen Eckpunkt über. D.h. es findet eine Permutation der 8 Eckpunkte statt. Aber nicht jede Permutation ist zulässig, da in den meisten Fällen die Abstände geändert werden, der Würfel also zerrissen würde.

(3.5.15) Welche Operationen sind möglich? Wir geben eine Aufzählung:

1. Die neutrale Operation.

2. Wir verbinden gegenüberliegende Flächenmittelpunkte. Es gibt drei solche Achsen. Wir können um 90^0,180^0 und 270^0 drehen. Das gibt 9 neue Operationen.

3. Wir verbinden gegenüberliegende Eckpunkte durch Raumdiagonalen. Davon gibt es 4. Wir können um 120^0 und um 240^0 drehen. Das gibt 8 weitere Operationen.

4. Wir verbinden die Mittelpunkte gegenüberliegender Kanten miteinander. Das ergibt 6 Diagonalen. Jede erlaubt eine 180^0-Drehung. Also 6 Operationen.

(3.5.16) Das sind alles Transformationen, die man über Bewegungen realisieren kann. Spiegelungen lassen wir noch nicht zu. Insgesamt erhalten wir so eine Gruppe mit 24 Elementen. Die Konjugationsklassen dieser Gruppe stimmen weitgehend mit der gegebenen Einteilung überein. Nur die zweite Gruppe zerfällt nochmals in zwei Klassen. Die eine enthält die drei 180^0-Drehungen. Das sind Elemente der Ordnung 2, erfüllen die Relation $g^2=e$. Die 6 restlichen Drehungen dagegen bilden eine eigene Klasse. Für sie gilt erst $g^3=e$. D.h. sie erfüllen eine andere Relation. (Vgl. (3.3.13)).

(3.5.17) Wählen wir M=Menge der 8 Eckpunkte, dann gibt es nur eine Bahn. Jeder Eckpunkt hat einen Stabilisator mit 3 Elementen, die 3 Drehungen um die zugehörige Raumdiagonale. Sind E,F zwei Eckpunkte

mit F=g⋆E und ist d eine der Drehungen um die durch E gehende Raumdiagonale, dann ist $\tau_g(d)=gdg^{-1}$ die entsprechende Drehung um F.

(3.5.18) **Jetzt wählen wir M anders**. M soll alle 8 Eckpunkte, alle 6 FIächenmittelpunkte und alle 12 Kantenmittelpunkte enthalten. Die Gruppe operiert offenbar auch auf dieser Menge mit 26 Punkten. Aber jetzt hat man 3 Bahnen. Den Rest - Stabilisatoren, Abzählung usw. - sollte sich der Leser selbst überlegen.

(3.5.19) Bisher haben wir die Symmetriegruppe auf Würfel**punkten** operieren lassen. Aber natürlich operieren diese Gruppen auch auf Mengen anderer Beschreibungsgrößen der jeweiligen Figuren, hier also des Würfels. Sehr günstig sind folgende Objekte:

(3.5.20) Definiton:

Eine Flagge (des Würfels) ist ein Tripel (F,K,P). Dabei ist F eine Oberflächenquadrat, K eine Kante von F und P ein Punkt dieser Kante.

(3.5.21) Offenbar hat der Würfel 48=6·4·2 derartige Flaggen. Einerseits operiert die Symmetriegruppe auf der Menge aller Flaggen, andererseits wird der Würfel vollständig durch Angabe irgendeiner seiner Flaggen bestimmt. Die Operation erzeugt zwei Bahnen, da jede Flagge noch eine Orientierung besitzt, durch die festgelegt wird, wo es von der Flagge aus ins Innere des Würfels geht. Und unsere Symmetrieoperationen dürfen diese Orientierung nicht ändern, weil wir keine Spiegelungen zulassen.

Jede Bahn hat demnach 24 Elemente. Jede nicht neutrale Transformation ändert aber die Flagge. Folglich sind die Stabilisatoren trivial einelementig. Wir sehen erneut, dass die Symmetriegruppe 24 Elemente hat.

□ Wieso ist diese Definition gut oder geschickt? Nehmen wir einmal an, wir würden die Definition abändern und statt "K ist Kante von F" nur fordern "K ist Kante des Würfels". Und für P analog "P ist Würfeleckpunkt". Was wird dann mit der in (3.5.21) gegebenen Argumentation? Diese macht nämlich die Flaggeneinführung zu einer ausgesprochen wertvollen Idee wie die nächste Frage zeigt.

□ Bestimmen Sie mit Hilfe der Flaggenmethode die Symmetriegruppe eines Tetraeders. Interpretieren Sie die Elemente dann geometrisch. Konjugationsklassen? Wie sehen die Flaggen einer ebenen Figur, etwa eines Quadrates aus?

□ Nehmen Sie als Figur einmal ein Quadrat und ein quadratisches Gitter - beide in der Ebene. Wie sehen die Symmetriegruppen aus, wodurch unterscheiden sie sich insbesondere grundlegend? (Wie ist für das Quadrat die Flagge zu definieren?)

3.3.5d **Die kleinen Transformationen von Funktionen**

Als Beispiel für die Transformationsgruppen sollen die kleinen Funktionstransformationen aus (3.1.7) genauer diskutiert werden.

(3.5.22) Unter dem Stichwort "kleine Transformationen" fassen wir eine Reihe nützlicher Rechen- und Arbeitshilfen für den Umgang mit Funktionen $\mathbb{R} \to \mathbb{R}$ zusammen, die formal alle auf eine ganz bestimmte Gruppenoperation zurückgehen. In Kapitel 6 verallgemeinern wir das auf den Umgang mit Feldern. Diese Operation soll jetzt besprochen werden. Genauer gesagt operiert ein und dieselbe Gruppe gleichartig und koordiniert auf einer Vielzahl von bei der Beschreibung auftretender Mengen.

(3.5.23) **Was leisten die kleinen Transformationen?** Wir stellen die Hauptpunkte zusammen.

1. Durch die kleinen Transformationen werden die Funktionen in Klassen miteinander eng verwandter Funktionen zusammengefaßt, Beispiele sind die Klasse aller quadratischen Parabeln $q(x)=Ax^2+Bx+C$ mit drei freien Parametern oder die Klasse aller sinusartigen Funktionen $s(t)=A\sin(\omega t+\varphi)+B$ mit 4 freien Parametern. Ein weiteres wichtiges Beispiel bilden die Gaußschen Normalverteilungen.
   Zwei Funktionen liegen in derselben Klasse, wenn man sie durch Verschieben und Umskalieren der beiden beteiligten Achsen ineinander umwandeln kann.

2. Beherrscht man die Eigenschaften eines einzelnen Vertreters einer derartigen Klasse - sagen wir der Normalparabel $q(x)=x^2$- dann kann man bei vielen Fragestellungen leicht und unmittelbar auf die entsprechenden Eigenschaften der anderen Mitglieder der Klasse schließen.

   Das gilt speziell für den Graphen, für Ableitungen und Integrale sowie für Näherungsformeln des Rechenausdruckes. Ebenso für rechnerische Beziehungen zwischen den Funktionswerten, wie sie etwa als Ausdruck von Symmetrien vorkommen

3. Vielfach enthält die Klasse einen kanonischen besonders ausgezeichneten Vertreter, eine Normalform, an der man seine Kenntnisse fixieren kann und sollte. (In den Beispielen $q(x)=x^2$ oder $f(t)=\sin(t)$). Bei physikalischen Formeln gelangt man zu dieser Normalform häufig durch Einführen einheitenfreier (dimensionsloser) Größen.

4. Für die Elemente der Klassen gibt es unterschiedliche Parametrisierungen. Vielfach gibt es eine arithmetische Parametrisierung, die auf den Rechenausdruck bezogen ist sowie eine andere geometrische. Erstere ist die, die den Rechenausdruck in allgemeiner Form wiedergibt, so wie man ihn im Rahmen von Rechnungen ansetzt. Im Parabelfall ist das $y=Ax^2+Bx+C$ wie oben angegeben.
Bei einer geometrischen Parametrisierung dagegen haben die benutzten Parameter geometrische Bedeutung für den zugehörigen Graphen. Im Parabelfall $y= A((x-a)^2-b)$. Hier sind (a,b) die Koordinaten des Scheitelpunktes und das ist ein geometrisch besonders ausgezeichneter Punkt des Graphen. A ist der Öffnungsfaktor der Parabel: Vom Scheitel aus um 1 in x-Richtung weitergehen, dann ..... Eine andere geometrische Parametrisierung im Parabelfall ist die Nullstellenparametrisierung $y=A(x-x_1)(x-x_2)$.

5. Für manche Zwecke zerfällt die durch den Rechenausdruck gegebene arithmetische Klasse noch in Unterklassen. Bei $\frac{1}{Parabel}$ etwa in die durch die Anzahl reeller Nullstellen gegebenen drei Unterklassen. Man sieht und versteht das gut am Beispiel der Graphenkonstruktion sowie des Integrales der Funktion $\frac{1}{q(x)}$.

(3.5.24) Ein und dieselbe Gruppe operiert in festgelegter Weise auf einer Vielzahl zum System gehöriger Objekttypen. Dieser eingangs beschriebenen Sachverhalt läßt sich am Beispiel der kleinen Transformationen ausgezeichnet illustrieren. Wir leiten zunächst die Gruppe als Transformation der Vektoren der Ebene her. Die Operation bezeichnen wir wieder mit $\star$. Dann lassen wir dieselbe Gruppe auf einer ganzen Reihe anderer Objekte operieren, wobei wir sehen werden, dass das in festgelegter Weise geschieht. Die abgeleiteten Operationen bezeichnen wir teilweise mit $\diamond$, um sie von der Ausgangsoperation $\star$ zu unterscheiden. Genauer gesagt betrachten wir die folgenden Ojekttypen, auf denen die Gruppe operiert. In Klammern unsere jeweilige Operationsbezeichung:

Koordinatenvektoren($\star$) , Figuren ($\star$). Funktionsgraphen($\star$), FIächeninhalt von Figuren($\diamond$), Gleichungen($\diamond$), Rechenausdrücke von Funktionen ($\diamond$), Ableitung von Funktionen($\diamond$) und Koordinatensysteme($\diamond$).

Wir werden sehen, daß es sich dabei meist nicht nur um begrifflich, sondern auch mathematisch-rechnerisch andere Operationen handelt. so daß man nicht identifizieren kann.

(3.5.26) **Herleitung der Gruppe der kleinen Transformationen.**

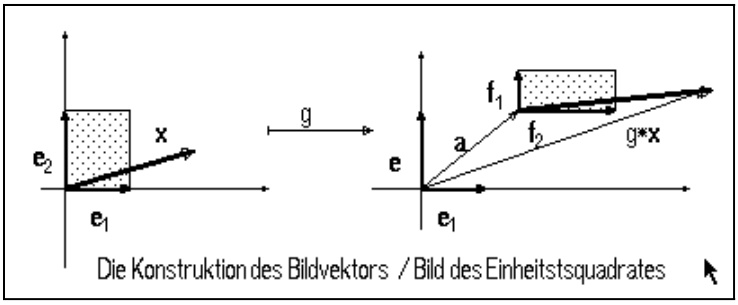
Wir betrachten die folgenden Transformationen der Ebene:

$$(V_0^2, \vec{x} = x\vec{e}_1 + y\vec{e}_2 \mapsto \vec{a} + x\vec{f}_1 + y\vec{f}_2, V_0^2) \quad \text{Mit} \quad \begin{array}{ll} \vec{a} = a\vec{e}_1 + b\vec{e}_2 & \\ \vec{f}_1 = \alpha\vec{e}_1 & \vec{f}_2 = \beta\vec{e}_2. \end{array}$$

Dabei soll $\vec{e}_1$,.$\vec{e}_2$ ein festes kartesisches Koordinatensystem K bestimmen. Die Menge der Koordinatenvektoren sei wie üblich $\mathbb{R}^2_K$. Aus dem Vektor $\vec{x}$ wird vermittels der drei Hilfsvektoren $\vec{a}$,$\vec{f_1}$ und.$\vec{f_2}$ ein neuer Vektor $\vec{y} = g \star \vec{x}$ konstruiert. Das gibt für die Koordinatenvektoren die Abbildung

$$g=\left(\mathbb{R}^2_K, \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} \alpha x + a \\ \beta y + b \end{pmatrix}, \mathbb{R}^2_K\right)$$

Die Figur verdeutlicht die Konstruktion.



Aus diesen Transformationen wollen wir die zugehörige Gruppe herleiten. Nochmals: Wir starten mit der Transformation und bestimmen damit die Gruppe. Denken Sie an die Schritte zur Festlegung einer algebraischen Struktur! Die Gruppenelemente hängen von den vier benutzten Parametern ab und wir bezeichnen sie wie folgt: g=$(\alpha, a; \beta, b)$. D.h. zuerst kommen die beiden Größen a und α, die die Änderung in x-Richtung bestimmen, dann die beiden für die y-Richtung. Das Symbol (α,a;β,b) ist eine Bezeichnung iür die oben angegebene Abbildung g! Die vier darin enthaltenen Parameter charakterisieren die Operation das Gruppenelement quantitativ:

- Verschieben um a bzw. b und Umskalieren mit α bzw. β.

Die jeweilige Operation gibt dann an, auf welchen Objekten und wie das durchzuführen ist. Verlangt wird $\alpha, \beta \neq 0$. Damit ist die Menge, die zur Gruppe werden soll, festgelegt:

$$\boxed{\text{G=}\{(\alpha,\text{a};\beta,\text{b})|\alpha,\beta,\text{a,b}\in \mathbb{R};\alpha,\beta \neq 0\}}$$

Für die Koordinatenvektoren haben wir konstruktionsgemäß $\text{g}\star \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \alpha x + a \\ \beta y + b \end{pmatrix}$.

Führt man zwei Transformationen hintereinander aus, ergibt sich der Kandidat für die Gruppenmultiplikation. Mit h=$(\sigma, s; \tau, t)$ folgt sofort $\text{h}\star(\text{g}\star\vec{x})=\begin{pmatrix} \sigma\alpha x + \sigma a + s \\ \tau\beta y + \tau b + t \end{pmatrix}$. Das sollte im Falle einer Linksoperation gerade $(\text{h}\cdot\text{g})\star\vec{x}$ sein. Damit lesen wir die folgende Regel für die Gruppenmultiplikation ab:

$$\boxed{(\sigma,\text{s};\tau,\text{t})\cdot(\alpha,\text{a};\beta,\text{b})=(\sigma\alpha,\sigma\text{a+s};\tau\beta,\tau\text{b+t})}$$

Etwa (1,2;3,4)(3,2;4,1)=(2,4;12,7). Machen Sie sich das Vorgehen bei der Multiplikation genau klar. Man nennt diese Art der Verknüpfung auch semidirektes Produkt.

☐ Berechnen Sie (α,0;β,0)·(l,a;l,b) und (l,a;l,b)(α,0;β,0). Was besagt das Resultat?

(3.5.27) **Entsteht eine Gruppe?** D.h. erfüllt die gefundene Verknüpfung von G die Gruppenaxiome? Das Assoziativgesetz gilt, da es sich um das Hintereinanderausführen von Abbildungen handelt: $\text{g}\star\vec{x}=\text{g}(\vec{x})$. Das neutrale Element ist (1,0;1.0). Und das jeweilige Inverse wird dann einfach durch die inverse Abbildung gegeben: $(\alpha,\text{a};\beta,\text{b})^{-1}=(\frac{1}{\alpha}, -\frac{a}{\alpha}; \frac{1}{\beta}, -\frac{b}{\beta})$. Diese Abbildung ist immer bildbar, da $\alpha, \beta \neq 0$ sein sollte.

☐ Zum Assoziativgesetz: Es ist $\text{g}\star\vec{x} = (\alpha,\text{a};\beta,\text{b})\star \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \alpha x + a \\ \beta y + b \end{pmatrix}$. Werten Sie entsprechend $((\text{g}\cdot h)\cdot k)\star\vec{x}$ und $(\text{g}\cdot(h\cdot k))\star\vec{x}$ aus.

Daher liegt tatsächlich eine Gruppe vor, die wir KT(2) nennen wollen. (*Kleine Transformationen in zwei Dimensionen*). Ergebnis:

$\text{KT(2)}=\{(\alpha,\text{a};\beta,\text{b})|\alpha,\beta,\text{a,b}\in \mathbb{R};\alpha,\beta \neq 0\}$ ist mit der angegebene Verknüpfung (nicht kommutative) Gruppe.
Diese Gruppe operiert - wie man sofort nachprüft - von links auf $\mathbb{R}^2_K$: und korrespondierend auf V^2_0.

☐ Definieren Sie eine analoge Gruppe KT(1) für eine Dimension und zeigen Sie, dass KT(2) isomorph zum direkten Produkt KT(l)×KT(1) ist.

☐ Zeigen Sie, dass folgende Mengen Untergruppen von KT(2) bilden:

$$\text{H}_1 = \{(\alpha, a; 1, 0|\alpha, a \in \mathbb{R}, \alpha \neq 0\} \quad \text{H}_2 = \{(1, a; 1, b)|a, b \in \mathbb{R}\}$$
$$\text{H}_3 = \{(\alpha, 0; \beta, 0)|\alpha, \beta > 0\} \quad \text{H}_1 = \{(1, m; 1, 0)|m \in \mathbb{Z}\}$$

Welche geometrische Interpretation haben die Elemente dieser vier Untergruppen?

(3.5.28) **Bahnen**: Es gibt nur eine Bahn, die gesamte Ebene. Die Gruppenelemente (l.a;l,b) verschieben den Ursprung in jeden beliebigen Punkt der Ebene.

(3.5.29) Und wie sieht der **Stabilisator** des Punktes $\vec{x}=\begin{pmatrix} x \\ y \end{pmatrix}$ aus? Wir erhalten die Bedingung $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \alpha x + a \\ \beta y + b \end{pmatrix}$. Beachten sie die Rollen: x,y äußere Parameter, aber α, a, β, b gesucht! Das gibt

a=(l-α)x undb=(l-β)y mit $\alpha, \beta \neq 0$ und sonst frei. Jeder Punkt hat also eine recht große Stabilisatoruntergruppe mit zwei freien Parametern. Diese Untergruppen sind alle zueinander isomorph.

(3.5.30) Und wie sehen die **Konjugationsklassen** aus? Wir müssen hgh^{-1} bilden und h laufen lassen. Das ergibt die folgenden Klassen: $k_{\alpha\beta}=\{(\alpha,a;\beta,b)|\ a,b\in \mathbb{R}\}$. D.h. zwei Gruppenelemente sind genau dann zueinander konjugiert, wenn sie sich nur in der Verschiebung voneinander unterscheiden.

(3.5.31) **Jetzt geht es darum, die Gruppe KT(2) auf weiteren uns interessierendenObjektmengen operieren zu lassen.** Die Gruppe ist eine Untergruppe der in (3.1.13) beschriebenen affinen Gruppe der Ebene und somit ein Beispiel für die in Kap3.3.5b eingeführten Transformationsgruppen. Sie bewahrt bestimmte Eigenschaften geometrischer Figuren auf ihren Bahnen und ändert andere.

(3.5.32) **Die Ausdehnung der Operation auf die Figuren.** Die geometrische Auswirkung der Transformationen ergibt sich aus der Konstruktion. Jeder Vektor in 1-Richtung wird mit einem Faktor α skaliert und dann (Reihenfolge!) um a parallel zur l-Achse verschoben. Analog für Vektoren in y-Richtung. Vektoren mit anderer Richtung sind zu zerlegen. Wie sehen die Bahnen aus? Nehmen wir die Bahn eines achsenparallen Rechtecks: sie besteht aus allen achsenparallelen Rechtecken beliebiger Lage und mit Flächeninhalt $\neq 0$.

(3.5.33) Die Figurentransformation schließt die Transformation der Funktionsgraphen als besondere Figuren mit ein. Wie transformiert sich der Graph G_f einer Funktion x↦f(x) als Figur im $\mathbb{R}^2_K$?

$$\begin{aligned} G_f &= \{(x,y)|y=f(x), x\in\mathbb{R}\} \quad \text{wird zu} \\ g\star G_f &= \{(u,v)|u=\alpha x+a, v=\beta y+b, y=f(x)\} \end{aligned}$$

Interessant sind hier Bahnen und Stabilisatoren.

☐ Wie operiert die Gruppe auf dem FIächeninhalt der Figuren, die einen solchen besitzen?

☐ Wie und auf welchen Gleichungstypen operiert die Gruppe?

(3.5.34) Ausdehnung auf die **Rechenausdrücke von Funktionen**: Oben haben wir den Graphen G_f transformiert. Die resultierende Menge hat jedoch noch nicht die Form eines Funktionsgraphen. Wir rechnen wie folgt weiter, indem wir u=$\alpha x + a$ nach x auflösen und einsetzen:

$$\begin{aligned} g\star G_f &= \{(u,v)|u=\alpha x+a, v=\beta y+b, y=f(x)\} \\ &= \{(u,v)|v=\beta y+b)y=f(\frac{u-a}{\alpha})\} \\ &= \{(u,\beta f(\frac{u-a}{\alpha})+b)|u\in\mathbb{R}\} \end{aligned}$$

Im wichtigen zweiten Schritt haben wir einen Wechsel der Parametrisierung vorgenommen, von x nach u. Denn bei einem Funktionsgraphen muß die erste Komponente ja immer gleich einer Buchstabenbezeichnung für die unabhängige Variable sein, muß in der Graphenmenge also freier Parameter sein. Der letzte Term hat die Form eines Funktionsgraphen, die der transformierten Funktion g◇f. Wir lesen ab:

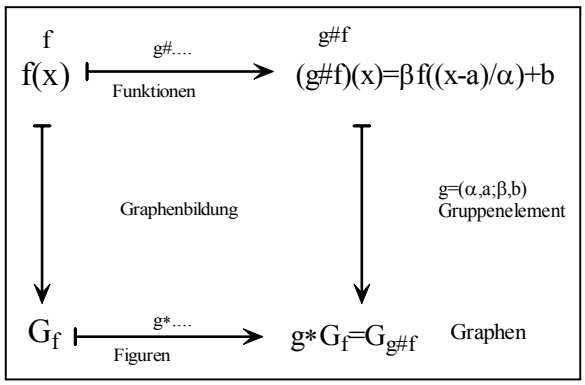
$\|$ g⋆G_f gehört zur transformierten Funktion g◇f mit (g◇f)(x)=βf($\frac{x-a}{\alpha}$)+b $\|$

Beachten Sie die entgegengesetzte Richtung im Urbildbereich und die Art des Zustandekommens dieser Richtungsänderung!

Damit haben wir die Gruppenoperation auf die Rechenausdrücke ausgedehnt.

☐ Bestimmen Sie Bahn und Stabilisator von $h_2$mit $h_2(x)=x^2$. Dasselbe für x↦sin(x). (Vorsicht beim Stabilisator von sin!)

(3,5.35) Erneut ist eine Darstellung des Sachverhaltes als Diagramm empfehlenswert:

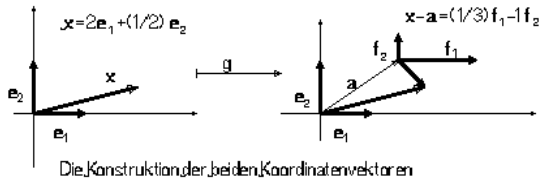


(3.5.36) **Die Ausdehnung der Operation auf die Ableitung**. Wir betrachten nur differenzierbare Funktionen x↦f(x). M sei die Menge aller Ableitungen f′. Weiter sei $(g\diamond f)(x)= \beta f(\frac{x-a}{\alpha})+b$, wie hergeleitet. Ableiten gibt $(g\diamond f)'(x)=\frac{1}{\alpha}\beta f'(\frac{x-a}{\alpha})$ Dies interpretieren wir als $(g\bullet f')(x)$ mit dem neuen Operationszeichen •. D.h.: Die Gruppe operiert auf den Ableitungen wieder erwartungsgemäß. Aus der Ableitungsfunktion f′ wird die neue Funktion $(g\bullet f')$ mit folgenden Werten: $(g\bullet f')(x) = \frac{\beta}{\alpha}f'(\frac{x-a}{\alpha})$

D.h: die Verschiebung in y-Richtung entfällt, dafür gibt es einen zusätzlichen Faktor $\frac{1}{\alpha}$. Das ist sinnvoll: α=2 verdoppelt alle Längen des Graphen in x-Richtung. Dadurch wird die Steigung halbiert.

(3.5.37) **Transformation des Koordinatensystems.** Oben haben wir die Vektoren der Ebene transformiert. Aus einem gegebenen Vektor $\vec{x}$ wurde ein anderer Vektor $g\star\vec{x}$ konstruiert. Alternativ können wir auch ein und denselben Vektor $\vec{x}$ mit Hilfe von zwei unterschiedlichen Koordinatensystemen darstellen.

Dabei sollen die beiden Koordinatensysteme durch Ursprungsverschiebung um (a,b) und neue Skalen für die Achsen auseinander hervorgehen.Dann erhalten wir zwei Koordinatenvektoren $\vec{x}^K$ und $\vec{x}^L$ desselben geometrischen Pfeiles. Den Wechsel von $\vec{x}^K$ nach $\vec{x}^L$ können wir auch als Abbildung $\mathbb{R}^2 \to \mathbb{R}^2$ interpretieren und daraus eine Gruppenoperation (auf $\mathbb{R}^2$) machen. Hierzu werden die Koordinatenräume $\mathbb{R}^2_K$ und $\mathbb{R}^2_L$ mit dem $\mathbb{R}^2$ identifiziert. Die Figur zeigt sowohl die Art der Konstruktion als auch den Unterschied zur Ausgangsabbildung.



Als allgemeine Formel haben wir: $\vec{x}$ =x$\vec{e_1}$+y$\vec{e_2}$= a$\vec{e_1}$+b$\vec{e_2}$+u$\vec{f_1}$+v$\vec{f_2}$=(a+αu)$\vec{e_1}$+(b+βv)$\vec{e_2}$. Das ergibt durch Vergleich x=a+αu und y=b+βv. Damit erhalten wir die folgende Zuordnung unserer Operation:

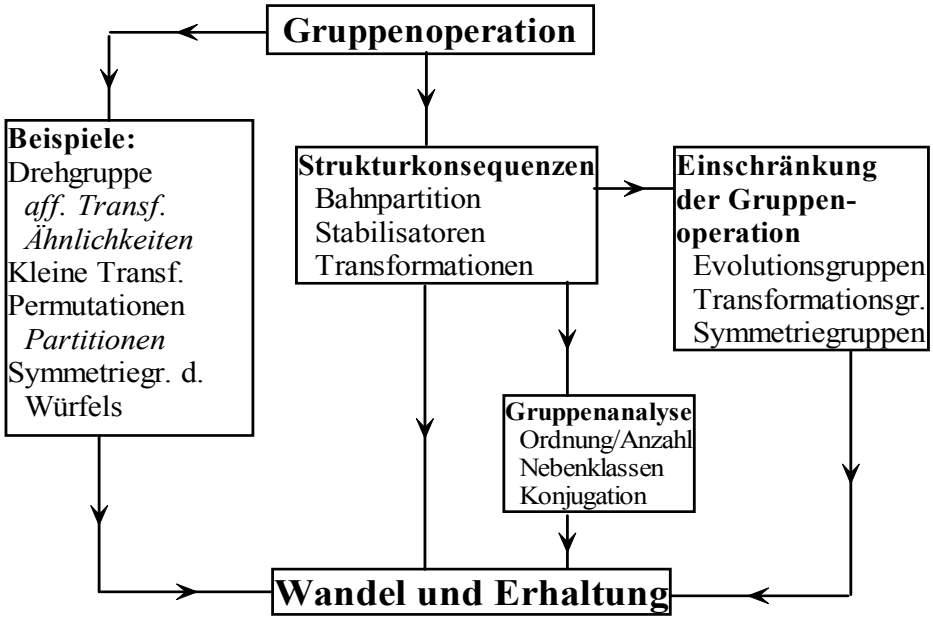
$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} \frac{x-a}{\alpha} \\ \frac{y-b}{\beta} \end{pmatrix} = g\# \begin{pmatrix} x \\ y \end{pmatrix}$$

Nach dieser Formel transformiert sich der Koordinatenvektor, wenn man das Koordinatensystem in der skizzierten Weise - Verschiebung sowie Umskalierung der Achsen - ändert. Vergleicht man das mit der ursprünglichen Transformation der Koordinatenvektoren, die die Änderung der Vektoren beschreibt, so folgt $g\#\begin{pmatrix} x \\ y \end{pmatrix} = g^{-1}\star\begin{pmatrix} x \\ y \end{pmatrix}$.

□ Zeigen Sie, dass # eine Rechtsoperation, keine Linksoperation ergibtist.

3.3.6 Übersicht

Die Themen, die zum Stichwort Gruppenoperation behandelt wurden, sind im nachfolgenden Diagramm zusammengestellt. Nochmals sei auf die Vielfalt der hierdurch erfassten Beispiele und Strukturen verwiesen. Die angegebene Liste enthält ja nur eine typische Auswahl.

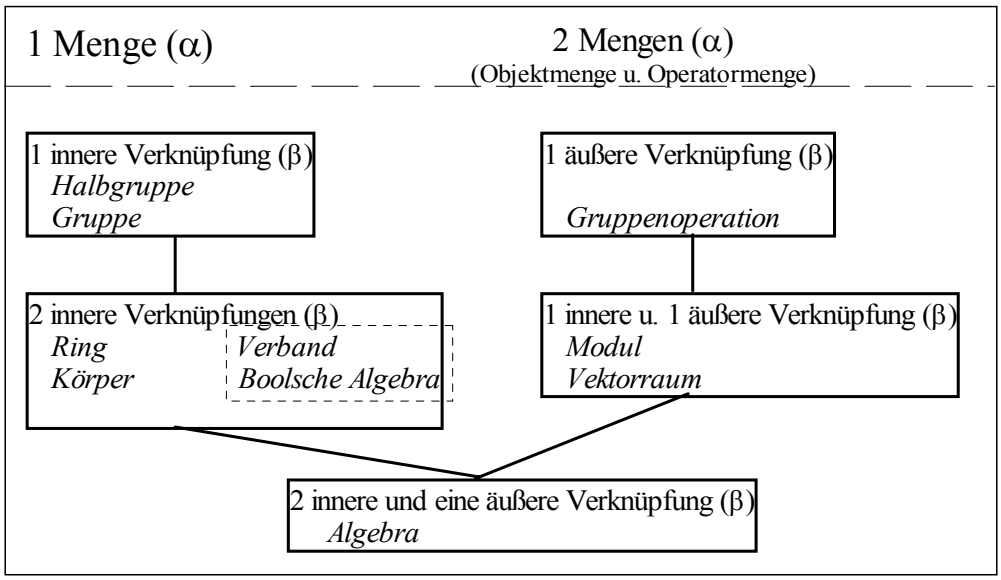

Gruppenoperation
Beispiele:
Drehgruppe
aff. Transf.
Ähnlichkeiten
Kleine Transf.
Permutationen
Partitionen
Symmetriegr. d.
Würfels
Strukturkonsequenzen
Bahnpartition
Stabilisatoren
Transformationen
Einschränkung
der Gruppen-
operation
Evolutionsgruppen
Transformationsgr.
Symmetriegruppen
Gruppenanalyse
Ordnung/Anzahl
Nebenklassen
Konjugation
Wandel und Erhaltung

3.4 Das System der algebraischen Strukturen (2)

3.4.1 Übersichtsschema

(4.1.1) Wir geben jetzt die in Kap. 3.2.0 angekündigte orientierende Übersicht über die üblicherweise auftretenden algebraischen Strukturen. Organisationsprizipien sind einerseits die in Schritt (α) der Konstruktion festgelegte Anzahl der beteiligten Mengen und dann die in Schritt(β) bestimmte Zahl der beteiligten Verknüpfungen.

Zusätzlich benötigt man jeweils die genaueren Axiome, die die Eigenschaften der Verknüpfungen im Schritt (γ) fixieren.



(4.1.2) Links stehen Strukturen, für die allein innere Verknüpfungen erklärt sind. Dabei fallen Verband und Boolsche Algebra aus dem sonstigen Rahmen. Als Beispiel eines Verbandes kann man $(\mathfrak{P}(M), \cap, \cup)$ wählen. Die Reihe der Verbandsstrukturen ist für unsere Zwecke weniger interessant. Anders als die übrigen Strukturen baut sie nicht auf einer Gruppenstruktur einer der Verknüpfungen auf. Die Gruppenstruktur hat zur Folge, dass man über einen Grundstock eindeutig lösbarer einfacher Gleichungen verfügt. Bei der Verbandsstruktur ist das nicht der Fall. Auf die zum Verband gehörigen Axiome gehen wir nicht ein. Auf ein Beispiel eines Verbandes stoßen wir in Kap.4.1.7 bei der Behandlung der Teilraumeigenschaften bei Vektorräumen. Größere Bedeutung erhält die Verbandsstruktur im Zusammenhang mit der Maß- und Integrationstheorie, wo es allerdings auf die rein algebraische Struktur weniger ankommt.

Die rechte Seite des Diagramms enthält Strukturen des Typs Objektmenge mit zusätzlicher Operatormenge. Und die Operatormenge hat immer die Struktur des entsprechenden algebraischen Objektes der linken Seite. Zum Modul gehört ein Ring, zum Vektorraum ein Körper als Operatormenge usw. Die inneren Verknüpfungen der Operatormenge werden in der Tabelle **nicht** mitgezählt. Gezählt sind nur Verknüpfungen, an denen die Objektmenge beteiligt ist.

Die als "Algebra" bezeichnete unten stehende Struktur kann je nach Situation zu beiden Spalten gerechnet werden. Sie ist ein Ring, der zusätzlich Vektorraum ist, oder ein Vektorraum, für den eine zweite innere Verknüpfung definiert ist. Die Boolsche Algebra hat damit nichts zu tun. Beide Objekte werden aus historischen Gründen so bezeichnet. Wir gehen auf die Struktur der Algebra im Kapitel 9 genauer ein.

(4.1.3) Abgesehen vom Verband werden die Strukturen von oben nach unten immer stärker. D.h. jede Struktur besitzt auch die darüber stehenden. Jeder Körper ist ein Ring und dieser ist wiederum Gruppe. Ein Vektorraum ist Modul usw. Beim Umgang mit den Axiomen sollte man diese Hierarchieeigenschaft beachten und nutzen.

Parallel dazu lassen sich von oben nach unten immer komplizierter gebaute Gleichungen formulieren und Aussagen über das zugehörige Lösungsverhalten gewinnen.

(4.1.4) Zur linken Spalte: OrientierungsbeispieI für einen Ring ist $(\mathbb{Z},+,\cdot)$ für einen Körper entsprechend $(\mathbb{R},+,\cdot)$. Beispiel für eine Algebra ist der Vektorraum V^3 mit dem Vektorprodukt als zweiter innerer Verknüpfung.

(4.1.5) Und denken Sie daran: Für jede dieser Strukturen ist im Prinzip zunächst der große Satz an Routineproblemen abzuhandeln, so wie wir sie in Kap 3.1.2 besprochen haben. Wir verzichten bei der Behandlung der Ringe und Körper weitgehend auf diesen Teil, weisen nur auf einige spezifische Besonderheiten hin. Bei den in Kap. 4 zu besprechenden Vektorräumen, führen wir die Behandlung erneut durch.

3.4.2 **Ringe und Körper**

Das sind grob gesprochen abelsche Gruppen mit einer zweiten inneren Verknüpfung.

Als Orientierungsbeispiel für Ring kann man immer an (Z.+,·) denken.

(4.2.1) Jetzt also die die Ringstruktur festlegenden Axiome:

(R.α)	Sei R nicht leere Menge
(R.β)	Auf R seien zwei innere Verknüpfungen gegeben, die mit + ("Addition") und · ("Multiplikation") bezeichnet werden.
(R,γ+)	Die Addition mache R zu einer kommutativen Gruppe. Das neutrale Element wird mit 0 und das x inverse mit -x bezeichnet.
(R,$\gamma\cdot$)	Die Multiplikation sei assoziativ. [W*ird manchmal fortgelassen]*
(R,$\gamma+\cdot$)	Die Distributivgesetze sollen gelten, also für alle a,b,x,y$\in R$ (a+b)·$x = (a\cdot x)+(b\cdot x)$ und a·$(x+y) = (a\cdot x)+(b\cdot y)$ Sind diese Bedingungen erfüllt, dann heißt (R,+,·) ein *Ring.* Verkürzt heißt R selbst meist Ring.

(4.2.2) Wir schließen jetzt unmittelbar die Axiome für den Körper an. **Merke** : Körper = Ring (im gegebenen Sinn)+ eine zusätzliche Bedingung.

	Es sei (K,+,·) ein Ring. Zusätzlich gelte
(K,$\gamma\cdot$)	Die Elemente K^* =K-{0} bilden bezüglich der Multiplikation eine Gruppe.
Dann	heißt (K,+,·) ein *Körper.* (Englisch: *field !!*)

(4.2.3) Klar sind $\mathbb{Q}$,$\mathbb{R}$ und $\mathbb{C}$ mit den üblichen Verknüpfungen Beispiele für Körper.

Die Menge $\mathcal{P}$ aller Polynomabbildungen $\mathbb{R}\to\mathbb{R}$ ist bezüglich der üblichen Addition und Polynommultiplikation ein Ring, aber kein Körper. (x$\mapsto x^2$ hat in p kein multiplikatives Inverses!). Dagegen ist ($\mathcal{P}$, +,$\circ$) kein Ring. wenn $\circ$ für die Zusammensetzung der Abbildungen steht.

□ Eines der beiden Distributivgesetze gilt in ($\mathcal{P}$, +,$\circ$) nicht. Überprüfen!

Ist die Multiplikation kommutativ, spricht man von einem *kommutativen Ring* bzw. *kommutativem Körper.* Existiert ein neutrales Element bezüglich der Multiplikation, so wird es meist mit 1 bezeichnet, manchmal auch mit e oder E oder ähnlichem. Im Körper gibt es immer eine Eins. $(V^3,+,\times)$ ist weder assoziativ, noch kommutativ, noch existiert eine 1. Verdeutlichend sollte man daher sagen: Ein *nicht assoziativer Ring.* Häufig versteht man auch unter einem Körper automatisch einen kommutativen Körper. Gilt das Kommutativgestz dann nicht, spricht man von einem *nicht kommutativen Körper* oder einem *Schiefkörper.*

(4.2.4) Beachten Sie, dass man in Körpern und Ringen weitaus komplexere Gleichungen formulieren kann als in Gruppen. Zwei typische Beispiele sind ax+b·y= c und ax^2+bx+c= 0, wobei wir x·x wie üblich mit x^2 abgekürzt haben. Verdeutlichen Sie sich möglichst mit Hilfe von Verlaufsdiagrammen: Für diese Bildungen werden nur die Axiome benötigt, sonst nichts! Einschließlich des Assoziativgesetzes, das (ax)x=a(xx) sicherstellt. Wir sprechen hier nur von formulierbar, sagen nichts über Lösbarkeit und Lösungen. Besonders bei Ringen kann es hinsichtlich der Lösbarkeit große Unterschiede gegenüber dem vertrauten Verhalten reeller Gleichungen geben.

(4.2.5) Noch ein wichtiges Beispiel: Es sei (R,+,·) ein Ring und M irgendeine Menge. Wir betrachten die Menge $\mathfrak{F}$(M,R) aller Abbildungen M→R. Das sind so etwas wie die Skalarfelder auf R. Mit der in 3.2 besprochenen Wertemengenübertragung von + wird daraus zunächst eine kommutative Gruppe. Und die Wertemengenübertragung der Multiplikation macht daraus routinemäßig einen Ring. Kurz ($\mathfrak{F}$(M,R).+.·) **wird per Wertemengenübertragung zu einem Ring.** (Zur Erinnerung: Die von der Wertemengenübertragung erzeugte Multiplikation ist definiert durch f·g= (M,x$\mapsto (f\cdot g)(x)$ =f(x)·g(x),R).) Dass Wertemengenübertragung die algebraische Struktur bewahrt, ist das Normale, auf das wir üblicherweise wenig eingehen werden.

(4.2.6) Was ist, wenn R sogar ein Körper K ist? Dann ist ($\mathfrak{F}$(M,K).+.·) natürlich erneut Ring, aber entgegen der naiven Erwartung fast nie ein Körper! Wieso? Sei f∈ $\mathfrak{F}$(M.K) und f sei nicht die Nullabbildung. D.h. es gibt mindestens ein x∈K mit f(x)≠ 0. Aber für andere Punkte y∈K kann f Nullstellen haben. Soll ein Körper herauskommen, muss dieses f ein multiplikativ inverses - also reziprokes - Element (1/f) besitzen mit (1/f)=(M,x↦ $\frac{1}{f(x)}$,K). Das geht aber nur, wenn f keine Nullstellen hat. Hat f wenigstens eine Nullstelle, dann ist der zugehörige Wert nicht bildbar, das Inverse existiert nicht und es kann kein Körper vorliegen.

□ Was ist, wenn M genau ein Element enthält, was, wenn es mehr als ein Element enthält? Wie ist daher "fast nie" in 4.2.6 genauer zu verstehen?

(4.2.7) Die Aussage " ($\mathfrak{F}$(M,K).+.·) ist kein Körper " ist ein typisches Beispiel von der naiven Vorerwartung abweichenden Verhaltens und entsprechend zu beachten und zu merken.

□ Versuchen Sie sich an den folgenden Aufgabe vom Routinetyp:

1) Sei R Ring und J⊂K die Menge aller Elemente, die ein multiplikatives Inverses besitzen. Dann ist (J.·) eine Gruppe. Aber: Wieso ist (J.+,·) i.a. kein Körper?

2) Wie ist ein Ringhomomorphismus zu definieren?

3) Was ist ein Teilring? Wie sieht ein naheliegendes Teilringkriterium aus?

(4.2.8) Was kann man allgemein aus den Ringaxiomen folgern? Wir nennen zwei Konsequenzen (der Ringaxiome). Die erste:

Sei R Ring, r∈ R und 0 das neutrale Element bezüglich +
Dann gilt $0 \cdot r = r \cdot 0 = 0$.

Das ist ein Resultat, das man erwartet, aber man muss zeigen, dass es tatsächlich aus den Axiomen folgt. Da ein Körper automatisch Ring ist, gilt es auch für jeden Körper.

Beweis: Wir beginnen mit einer gültigen Gleichung, nämlich 0+0=0 und führen eine Reihe zulässiger Umformungen durchj: (0+0)·r=0·r / 0·r+0·r=0·r (Distributivges.) / Sei (-0r) das zu 0r∈R bezüglich + Inverse. Addiere dies Element von links usw. Ergebnis 0·r=0.

(4.2.9) Die zweite zu besprechende Folgerung ist rechnerischer Art. Was folgt aus den Distributivgesetzen? Diese in Kap. 3.1.3e als Herausforderung gestellte Frage wollen wir jetzt beantworten. Im Rahmen eines Beispiels lautet die Antwort: Man kann damit Terme der Art (a+b+c)·(x+y+z+w) ausrechnen nach der Regel "Jeder mit Jedem". D.h. *jeder Summand* des ersten Faktors ist *mit jedem Summanden* des zweiten zu multiplizieren und über alle Möglichkeiten ist zu summieren. Also a·x+....+c·w. Die Anzahl der Summanden sollte endlich sein. Der Beweis ist induktiv zu führen.

Aber damit nicht genug, Statt zwei kann man auch drei, vier usw.Summen als Faktoren vorgeben und distributiv ausmultiplizieren. Ausdrücke des Multinomialtyps $(a+b+c)^n$ etwa sind somit in jedem Ring sinnvoll. Und ist der Ring kommutativ (Achtung: eine Bedingung!), dann gilt das Resultat aus Kap.l.l.6. automatisch,

(4.2.10) Für viele Zwecke ist es günstig, die aus den Distributivgesetzen folgenden Rechenregeln mit Hilfe der Summensymbolik zu formulieren. Wir tun das für zwei Faktoren, die Verallgemeinerung auf mehr Faktoren sollte selbsterklärend sein:

Die aus den Distributivgesetzen folgende **Rechenregel** *Jeder mit Jedem*:
Es seien I und J zwei endliche Indexmengen und $(a_i)_{i\in I}$ und $(x_j)_{j\in J}$ zwei Familien von Ringelementen. Dann gilt:

$$(\Sigma_{i\in I} a_i) \cdot (\Sigma_{j\in J} x_j) = \Sigma_{(i,j)\in I\times J} a_i \cdot x_j = \Sigma_{i\in I} a_i \cdot (\Sigma_{j\in J} x_j) = \Sigma_{j\in J} (\Sigma_{i\in I} a_i)\, x_j$$

(4.2.11) Im Körper sind die Rechenregeln weitgehend die, die man von den reellen Zahlen her kennt. D.h. man kann im Körper analog zu den reellen Zahlen rechnen und das auch immer als ersten Leitgedanken verwenden. Ausnahme: Ordnungsbeziehungen wie 2<4 sind allgemein nicht verfügbar. Überdies zeigt genaue Inspektion der Axiome, dass die Multiplikation im Körper (und erst recht im Ring) nicht kommutativ sein muß. Insbesondere Matrixringe werden sich typischerweise als **nicht kommutativ** erweisen. Entsptrechend muss man dann Vorsicht walten lassen.

(4.2.12) Oben haben wir gesehen, was in Ring und Körper gemeinsam gilt. Jetzt erhebt sich die Anschlußfrage nach den Unterschieden zwischen Ring und Körper. Was kann man aus den Ringaxiomen nicht

folgern, das einem andererseits vom Rechnen mit Zahlen vertraut ist? Wir diskutieren hierzu zwei wichtige Sachverhalte:

(4.2.13) **Divisionsprobleme**. Angenommen man hat eine Gleichung der Form ax=b mit a$\neq$ 0. Sie ist in jedem Ring **formulierbar**. Und im Körper kann man sie immer nach x auflösen.

> Das Argument: a$\neq$ 0 hat ein inverses Element a^{-1} / Multipliziere ax=b von links mit a^{-1}/ K* ist als Gruppe assoziativ..... /Also x= a^{-1}·b.)

Im Ring geht das nicht. Z.B hat 2x=3 in $\mathbb{Z}$ keine Lösung! Kurz: Bei derartigen Divisionen - etwa bei linearen Gleichungen - muß man im Ring stets fallspezifisch argumentieren. Eine allgemeine Division ist nicht zulässig. Der oben eingeführte Polynomring bietet hierzu weitere Beispiele.

(4.2.14) **Nullteiler.** Vom Rechnen mit reellen Zahlen ist man die folgende **Denkfigur** gewohnt:

Angenommen man hat eine gültige Gleichung ab=0 vorgegeben. Dann muß mindestens einer der beiden Faktoren Null sein. (Ist etwa a ungleich Null, so multipliziert man von links mit a^{-1}und erhält am Ende b=0.)

Diese Argumentation läßt sich problemlos auf jeden **Körper** übertragen. Aber im Ring treten Probleme auf, denn dort muß a^{-1} ja keineswegs existieren. Tatsächlich gibt es Ringe, in denen es vorkommt, dass a und b beide ungleich Null sind, dass aber trotzdem ab=0 gilt. Derartige Ringelemente nennt man **Nullteiler**. Wir werden unten Beispiele kennen lernen. Andererseits ist die angegebene Denkfigur recht wichtig und nützlich. Das mathematiktypische Vorgehen sieht in derartigen Situationen wie folgt aus: Man trennt die Ringe in zwei Klassen, in solche, die Nullteiler besitzen und solche, die Nullteilerfrei sind (sog. *Integritätsbereiche*). Dann sucht man möglichst viele und gut handhabbare Bedingungen, die Nullteilerfreiheit sichern. Hat man es dann mit einem speziellen Ring zu tun, prüft man, ob er nullteilerfrei ist oder nicht.

Insbesondere sind $\mathbb{Z}$ und der Polynomraum $\mathcal{P}$ beide nullteilerfrei.

3.4.2a **Die Restklassenringe**

(4.2.15) In 3.2.3a haben wir die zyklischen Gruppen als Divisionsrestklassen (in $\mathbb{Z}$) dargestellt. Sei k$\in \mathbb{N}$ und k>2. Dann war für jedes r$\in \mathbb{Z}$ die Restklasse $[r]_k$=[r]={n|$\exists$g$\in \mathbb{Z}$, n=gk+r} eingeführt. Die Restklassenaddition wurde über die Formel [r]+[s]=[r+s] auf die Addition der ganzen Zahlen zurückgeführt. Dabei ist k fester äußerer Parameter. Analog kann man versuchen, eine Restklassenmultiplikation einzuführen gemäß [r]·[s]=[rs]. Also Multiplikation der Klasse durch gewöhnliche Multiplikation der Vertreter. Für k=5 etwa wird [2][3]=[6]=[1].

□ Zeigen Sie, dass diese Multiplikation wohldefiniert ist, d.h. unabhängig von der Vertreterwahl. (Beispiel (k=5):Es ist [12][8]=[96]=[1]. Aber [12]=[17] und [8]=[23]. Ist auch [17][23] gleich [1]? Das ist ein Übertragungsproblem auf eine Klassenmenge.) Natürlich ist die Überprüfung des Beispiels noch kein allgemeiner Beweis!

(4.2.16) Damit können wir (für jedes k) eine Ringstruktur aufbauen. Gehen wir die üblichen Schritte durch:

(α) Die Menge $\mathbb{Z}$/(k) enthält genau k Elemente, nämlich die Klassen [r] für r=0,l,...,k-l.

(β) Zwei Verknüpfungen, die definiert sind durch [r]+[s]=[r+s] und [r][s]=[rs].

(γ+) Die Gruppenstruktur ist bereits gezeigt.

(γ·) Das Assoziativgesetz gilt, da es in $\mathbb{Z}$ gilt (Tunnelmethode!)

(γ+·) Die Distributivgesetze gelten, da sie in $\mathbb{Z}$ gelten.

D.h. für jedes k>l liegt ein Ring mit genau k Elementen vor. Unter $\mathbb{Z}$/(k) werden wir von jetzt ab meist diesen Ring verstehen. Und damit haben wir sofort Beispiele für das oben beschriebene Nullteilerphänomen. Sei etwa k=4. Dann ist [2][2]=[4]=[0]. Denn die von 4 erzeugte Klasse [4] ist ja das Nullelement. Hat man allgemeiner k=rs, wobei beide Faktoren zwischen i und k liegen, folgt [r][s]=[0] modulo k.

Zur Illustration geben wir die Verknüpfungstafeln für $\mathbb{Z}$/(6) an. Also k=6. Alle Klammern sind fortgelassen. Wir haben beispielsweise [5]·[5]=[25] und [25]=[4·6 + 1] = [1].

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

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

(4.2.17) Die Konstruktion zeigt genauer: : $\mathbb{Z}/(k)$ ist stets ein kommutativer Ring mit Eins (=[1]) Ist k **keine Primzahl,** so enthält dieser Ring sicher Nullteiler.

(4.2.18) Was aber ist, wenn k Primzahl ist? Dann gilt folgender **Satz**:

Ist p eine Primzahl (>1), dann ist $\mathbb{Z}/(p)$ ein Körper.

D.h. für jede Primzahl p haben wir einen Körper mit ebensovielen Elementen, beginnend mit p=2. Beachten Sie: $\mathbb{Z}/(2)$ besteht nur aus den beiden neutralen Elementen 0 und 1.

Vor dem Beweis geben wir zur Illustration die Multiplikationstafel für die Primzahl p=5. Beachten Sie: Relevant sind nur die Elemente ungleich Null. Das sind p-1=4 Elemente. Es muß also eine Gruppe mit 4 Elementen vorliegen. Durch Inspektion sieht man, dass dies das direkte Produkt $C_2 \times C_2$ ist.

*	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

(4.2.19) **Beweis** des Satzes: p ist Primzahl, besitzt also keine nichttrivialen Teiler. Für a$\in \mathbb{Z}/(p)$ betrachten wir die Abbildung μ_a=($\mathbb{Z}/(p)$,[x]$\mapsto$[a][x]=[ax], $\mathbb{Z}/(p)$). Nun wissen wir, dass ($\mathbb{Z}/(p)$,+) Gruppe ist. Über das Distributivgesetz sehen wir, dass μ_a Gruppenhomomorphismus bezüglich der Addition) ist! Der Kern ist eine Untergruppe mit einer Ordnung, die Teiler von p ist. Also 1 oder p. Letzteres kommt nur für a=0 in Frage, da [1] für a$\neq$[0] nicht im Kern liegen kann ([1] kann keinen Nullteiler haben!).

Folglich ist für a$\neq$[01 der Kern trivial und somit μ_a Isomorphismus. D.h. aber, dass die Gleichung $\mu_a([x]=[1]$, d.h. [a][x]=[1], stets eine eindeutige Lösung hat. Oder: Jedes a$\neq$[0] hat ein eindeutiges multiplikatives Inverses in $\mathbb{Z}/(p)$. Und das war gerade die Bedingung, die aus einem Ring mit Eins einen Körper machte.

Beachten Sie, wie in diesen Beweis frühere Resultate eingehen. Zentrale Idee war die Konstruktion der Abbildung μ_a.

□ Konstruieren Sie die Verknüpfungstafeln für $\mathbb{Z}/(2)$ und $\mathbb{Z}/(3)$. Ersteres ist ein Körper mit nur zwei Elementen. Insbesondere gilt in ihm [1]+[1]=[0].

3.4.2b **Die Charakteristik**

(4.2.20)Wir besprechen eine weitere Eigenschaft von Ringen und Körpern, die auch auf einem Gruppenhomomorphismus basiert.

Sei R ein Ring mit Eins. Insbesondere ist jeder Körper ein Ring mit 1. Wir bezeichnen dieses neutrale Element jetzt aber mit e statt mit 1. Weiter sei -e das additive Inverse zu e. Wir setzen e+e=2e und e+e+e=3e und -e+(-e)=(-2)e usw. e+e ist durch die Ringaxiome erklärt, 2e ist eine neue Bezeichnung für dieses Element, eine Hilfsgröße. Insgesamt erhalten wir die Abbildung ($\mathbb{Z}$,n$\mapsto$ne,R). Hierbei interpretieren wir noch 0e als 0. Das ist klar ein Homomorphismus der beiden additiven Gruppen: (n+m)$\mapsto$(n+m)e=ne+me. Der Kern ist eine Untergruppe von $\mathbb{Z}$ und diese Untergruppen kennen wir über (2.4.17) alle. Ist der Kern eine zyklische Untergruppe der Ordnung k>l, so sagen wir, der Ring habe die Charakteristik k. Ist der Kern dagegen gleich {0}, so sagen wir, der Ring habe die Charakteristik 0. Weitere Möglichkeiten gibt es nicht. Ist die Charakeristik 0, dann ist ne=0 nur für n=0 möglich! Ist die Charakteristik dagegen gleich k>l, dann gilt ke=0.

□ Wieso kann k=1 nicht als Charakterisitik auftreten?

(4.2.21) Die Charakteristik ist eine wichtige Kenngröße für Ringe mit 1 und insbesondere für Körper. $\mathbb{R}$ und $\mathbb{C}$ haben die Charakteristik Null. $\mathbb{Z}/(k)$ hat die Charakteristik k. Usw. Beachten Sie: In Ringen oder Körpern der Charakteristik 2, kann man aus e+e=0 oder 2e=0 nicht auf e=0 schließen! Oder auch: ungerade + ungerade ist gerade, nicht erneut ungerade.

□ Zeigen Sie : Im Falle der Charakteristik 2 gilt $(a+b)^2 = a^2 + b^2$. Was ist dann (a+b+c)^2 usw.? Was folgt im Falle der Charakteristik 3?

3.4.2c **Polynomringe**

(4.2.22) Was sind Polynome? Üblicherweise interpretiert man sie als eine spezielle Art von Abbildungen $\mathbb{R} \to \mathbb{R}$. Etwa x↦$2x^2 - 3x$-7. Derartige Rechenausdrücke lassen sich problemlos in jedem Ring mit 1 bilden. (Wieso nicht ohne 1?) Es liegt nahe, den Polynombegriff in dieser Weise auszudehnen. Dabei tritt jedoch folgendes Problem auf: Hat der Ring R nur endlich viele Elemente, etw k Stück, dann gibt es auch nur endlich viele Abbildungen R↦R. D.h. es gäbe auch nur endlich viele Polynom. Viele Polxynome etwa des Type x↦x^n müßten einander gleich sein. Nach diesem Konzept darf man in das Polynom nur die Elemente des Ringes selbst einsetzen.

(4.2.23) Nicht selten sieht man sich jedoch mit folgender Situation konfrontiert: Man hat einen größeren Ring S, also R⊂S. Dann möchte man auch die Werte dieses größeren Ringes in das Polynom einsetzen. Beim Einsetzen ergibt sich jedenfalls ein bildbarer Rechenausdruck. S soll ja Ring sein. So setzt man etwa in das **reelle** Polynom x↦ $x^2 + 1$ gerne **komplexe** Zahlen ein. Etwa x=i. Das ist jedenfalls keine reelle Zahl. Also: Die Verallgemeinerung des Polynombegriffs sollte so aussehen, d**ass sie auch das Einsetzen von Elementen eines Erweiterungsringes von R erlaubt.**

(4.3.24) Oder auch: Hier soll nicht der Wert, sondern der Termbau, die Formel, bestimmen, was ein Polynom ist. Geht man hiervon aus, **dann legt die Folge der Koeffizienten a_i das Polynom fest.** Allerdings darf man nur solche Folgen zulassen, die nach endlich vielen Stellen "abbrechen", d.h. konstant Null werden.

(4.3.25) Also: Ein Polynom ist eine Folge (ℕ,i ↦a_i,R) mit Werten im Ring R, für die nur endlich viele der a_i ungleich Null sind. Oder auch: Es gibt zu jeder Folge eine Zahl N, für die $a_i = 0$ ist für alle i>N. Oder in der Sprechweise der Analysis: *Fast alle* a_i sind Null. Insbesondere hat man Folgen mit a_i=0 für alle i≠n und $a_n = 1$. Das entspricht dann der üblichen Polynomabbildung h_n:x↦x^n. Jetzt **bezeichnen** wir unsere Folgenabbildung (ℕ,i↦ a_i,R) wobei R unser Ring ist, einfach mit $\Sigma_i a_i x^i$. D.h. so, wie wir üblicherweise unser Polynom schreiben. Zwei solche Polynome sind nur gleich, wenn alle ihre Koeffizienten gleich sind, unabhängig von der Zahl der Ringelemente. Die Gesamtheit aller so definierten Polynome bezeichnet man mit R[x].

Das ist also eine Teilemenge der Menge aller Abbildungen ℕ →R. Per Wertemengenübertragung wird daraus ein Ring, *der Polynomnng in der Unbestimmten x über R.* Nochmals: Die Polynome schreibt man wie den Werteterm der üblichen Polynome, aber es handelt sich dabei um Abbildungen ℕ →R, nicht aber R→ *R.* Erst durch Einsetzen wird daraus eine Abbildung R→ *R.*

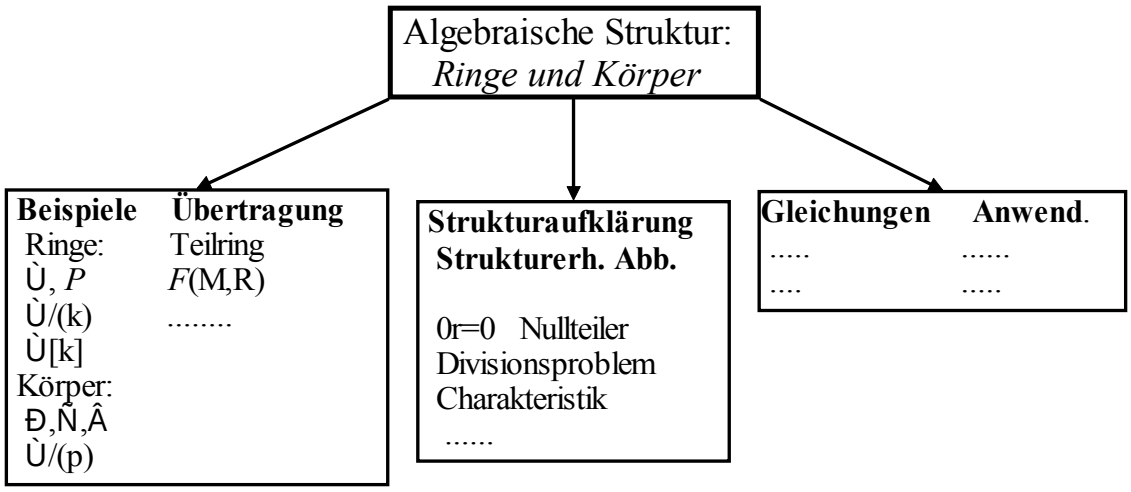
(4.2.26) Der Ring R[x] hat ein Einselement in Form des konstanten Polynoms 1 (also der Abbildung $a_i = 0$ für i≠ 1 und a_1=l wobei 1 die Eins des Ringes R ist.

□ Begründen Sie, dass im vertrauten Fall R=ℝ, also für die üblichen reellen Polynome, die neue Polynomdefinition mit der alten übereinstimmt.

3.4.2d **Zusammenfassung**

(4.2.27) Wir fassen zusammen, was man beim Einstieg in eine algebraische Struktur durchgehen sollte und geben für den Fall der Ringe und Körper einige zugehörige fallbespezifische Stichworte, wie wir sie angesprochen haben. Teilweise bestehen in unserer Darstellung noch größere Lücken. In der Regel sollte

man diese 6 Stichworte routinemäßig durchgehen.



3.4.3 Vektorräume und Moduln

(4.3.1) Jetzt interpretieren wir Ring und Körper als Operatorbereich einer weiteren Menge. Aber diese zweite Menge soll nicht mehr beliebig sein - wie im Fall der Gruppenoperation, sondern selbst eine algebraische Struktur in Form einer kommutativen Gruppe besitzen. Damit ergibt sich der enorm wichtige Strukturtyp der Moduln und Vektorräume. Inspizieren Sie nochmals die einleitende Übersicht (4.1.1).

(4.3.2) Wir geben jetzt die **Axiome** dieser Struktur, wie üblich angeordnet:

(M.α)	Sei M nicht leere Menge und R ein Ring mit 1.
(M.β)	Für M sei eine inner Verknüpfung $\boxplus$:M$\times M \to M$ und eine äußere $\star$:R$\times M \to M$ gegeben.
(M.γ+)	Bezüglich $+$ sei M kommutative Gruppe.
(M.$\gamma\star$)	Für $\alpha, \beta \in R$ und x$\in M$ gelte: $\alpha \star (\beta \star x) = (\alpha\beta) \star x$; $1 \star x = x$
(M.$\gamma + \star$)	Für $\alpha, \beta \in R$ und x,y$\in M$ gelten die Distributivgesetze: $(\alpha+\beta) \star x = (\alpha \star x) \boxplus (\beta \star x)$ $\quad \alpha \star (x \boxplus y) = (\alpha \star x) \boxplus (\alpha \star y)$.
Dann	heißt (M,$\boxplus$,$\star$) ein *Linksmodul über R.* Ist R sogar ein Körper K, dann heißt (M,$\boxplus$,$\star$) *Linksvektorraum über K.*

(4.3.3) Erste Bemerkungen: Wir haben es mit **zwei** Additionen zu tun, der in R und der in M. Im Axiomensystem haben wir sie durch + und $\boxplus$ auseinandergehalten. Üblicherweise bezeichnet man jedoch beide mit demselben Symbol +, da aus dem Zusammenhang praktisch immer zu erkennen ist, welche Rolle das +-Symbol einzunehmen hat. Ebenso hat man zwei Multiplikationen. Auch hier ist es üblich, beide mit $\cdot$ oder durch einfaches Hintereinanderschreiben der Symbole zu bezeichnen. Hinzu kommt die übliche Klammerersparnisregel "Punktrechnung vor Strichrechnung". Das erste Distributivgesetz

schreibt sich dann einfacher $(\alpha+\beta)$x=αx+βx.

□ Formulieren Sie selbst alle Axiome in der üblichen Schreibweise.

□

(4.3.4) Die Elemente von M nennt man *Vektoren* und die von R Skalare. (Also Skalar=operierende Größe!) In manchen Situationen wollen wir in zugehörigen Formeln die Rollen der beteiligten Buchstaben nicht immer durch explizite Mengenangaben festlegen. Dann verwenden wir folgende Konvention: Griechische Buchstaben bezeichnen Elemente aus R, also Skalare und lateinische und insbesondere fette lateinische Buchstaben oder mit einem Pfeil versehene bezeichnen Vektoren, also Elemente aus M. Speziell bezeichnet 0 die Ringnull und $\vec{0}$ oder **0** den Nullvektor. $\star$ oder $\cdot$ oder die übliche Produktform bezeichnet die *Multiplikation eines Vektors mit einem Skalar.* Nie sollte man das mit einem *Skalarprodukt* verwechseln. Weiter sollte man sich angewöhnen, immer korrekt vom Vektorraum V über dem Körper K zu sprechen. Es kommt vor, dass ein und dieselbe Menge Vektorraum über verschiedenen Körpern ist.

(4.3.5) Der Übergang vom Linksmodul zum Rechtsmodul ist auch klar. Man hat im Rechtsfall eine Operatorverknüpfung $\star$:M×R→M und eine entsprechende Umformulierung der Axiome. Wie im Fall der Gruppen ist das nur bedeutsam (im Sinne nicht isomorpher Strukturen), wenn die Multiplikation in R nicht kommutativ ist. Im kommutativen Fall liegt eine reine Änderung der Bezeichnung vor. Wir werden es praktisch immer mit kommutativem M zu tun haben, dann aber meist die Rechtsschreibweise verwenden, weil sich das für den Rechenkalkül als vorteilhaft erweist.

(4.3.6) Ganz grob können wir immer sagen: **Ein Vektorraum ist eine kommutative Gruppe (von Vektoren), auf der der Körpelängenänderung r (der Skalare) distributiv operiert. Die Bahnen liefern die Klassen von Elementen gleicher Richtung.**

(4.3.7) Erste allgemeine Konsequenzen der Axiome unter Benutzung unserer Symbolkonventionen sehen wie folgt aus:

Sätzchen: Stets gilt: $0\vec{x}=\vec{0}$ $\quad\alpha\vec{0}=\vec{0}$ $\quad$ und $\quad(-1)\vec{x}=-\vec{x}$.

□ Die Beweise sollte man zur Übung selbst ausführen.

Verdeutlichen Sie sich hierzu folgenden Punkt: In einfachen Modellen von Vektorräumen wie dem $\mathbb{R}^2$ mit komponentenweiser Verknüpfung gilt eine Gleichung wie $0\vec{x}=\vec{0}$ offensichtlich, ist trivial ("....wozu soll ich das beweisen?"). Aber das ist nicht das Problem, denn man benutzt dabei **zusätzliche spezifische Eigenschaften des Modelles, der Darstellung**. Im Beispiel die komponentenweise Verknüpfung mit $0(x,y)=(0x,0y)=(0,0)=\vec{0}$. Beim strukturbezogenen Vorgehen geht es darum, zu zeigen, dass man die Gleichungen auch ohne Verwendung solch spezieller zusätzlicher Eigenschaften, allein aus den Axiomen herleiten kann. Entsprechend ist der Beweis zu führen.

(4.3.8) Der einfachste und geometrisch gut verankerte Vektorraum ist der $\mathbb{R}^2$ über dem Körper $\mathbb{R}$, also die Ebene mit Koordinatenvektoren. Analog können wir leicht ein Beispiel eines Moduls herleiten, der kein Vektorraum ist. Als Menge wählen wir $\mathbb{Z}^2=\mathbb{Z}\times\mathbb{Z}$. Geometrisch ist das das Gitter aller Punkte mit ganzzahligen Koordinaten. Restringiert man die beiden Vektorraumverknüpfungen - einschließlich der Skalare, die nur noch ganzahlig sein sollen - so erhält man offensichtlich einen Modul über $\mathbb{Z}$.

Und hier im Modul taucht das **Divisionsproblem erneut auf**. So gilt die Gleichung: $5(1,2)=3(1,4)+2(1,-1)$. Aber es ist im Modul nicht möglich. nach einem der beteiligten Vektoren (=Modulelementen) aufzulösen, da 2,3 und 5 alle drei kein multiplikatives Inverses im Ring $\mathbb{Z}$ haben.

□ im Vektorraum kann man auflösen. Kontrollieren Sie das.

Für uns wird der Modulbegriff häufig die folgende nützliche Funktion haben: Er zeigt, dass viele Eigenschaften, die sich von der elementaren Vektorrechnung zunächst als so selbstverständlich darstellen, dass es unnötig erscheint, sie zu beweisen, doch bewiesen werden müssen. Denn man findet Moduln, in denen sie nicht gelten. Will man die angegebenen Gleichungen im Rahmen der Vektorrechnung allgemein verwenden, muß man sie ausschließlich mit Hilfe der Axiome herleiten.