Elemente der Algebra

Kurz-Skript WS 2009/2010

(ohne Beispiele, Erläuterungen und Beweise)

Prof. Dr. Hans-Dieter Rinkens

Inhaltsverzeichnis

Zur Wort-Geschichte*:
Das Wort "Algebra" taucht zum ersten Mal im Buchtitel von (Abu Abdallah Muhammad ibn Musa) al Hwarizmi (ca. 780 – 850 Bagdad) auf:
"Ein kurz gefasstes Buch über die Rechenverfahren des al-gabr und des al-muqabala".

al-gabr: wörtlich Einrichten eines gebrochenen Knochens; gemeint: Beseitigung negativer Glieder in einer Gleichung durch Addition

al-muqabala: Weglassen von gleichen positiven Gliedern auf beiden Seiten einer Gleichung

In der abendländischen Literatur taucht das Wort erstmals im 15. Kapitel des Buches "Liber abaci" des Kaufmanns Leonardo von Pisa, genannt Fibonacci (ca. 1170- 1240) auf. "... de questionibus algebre et almuchabale".

*mehr in: J. Tropfke: Geschichte der Elementarmathematik

Die elementare Algebra im Sinne der Schulmathematik umfasst die Rechenregeln der natürlichen, ganzen, gebrochenen und reellen Zahlen, den Umgang mit Ausdrücken, die Variablen enthalten, und Wege zur Lösung einfacher *algebraischer Gleichungen*.

Die klassische Algebra beschäftigt sich mit dem Lösen allgemeiner *algebraischer Gleichungen* über den reellen oder komplexen Zahlen. Ihr zentrales Resultat ist der *Fundamentalsatz der Algebra*, der besagt, dass jedes nichtkonstante Polynom n-ten Grades in n Linearfaktoren mit komplexen Koeffizienten zerlegt werden kann.

Die abstrakte Algebra ist eine Grundlagendisziplin der modernen Mathematik. Sie beschäftigt sich mit speziellen *algebraischen Strukturen* wie Gruppen, Ringen, Körpern und deren Verknüpfung.

0. Standards für die Lehrerbildung im Fach Mathematik (Auszug)

(Empfehlungen von DMV, GDM, MNU) Juni 2008

Das Anliegen dieser Empfehlungen ist es, den Zusammenhang zu bedeutsamen Inhalten des Studiums herzustellen. Welche Kompetenzen lassen sich in besonderer Weise an welchen Inhalten entwickeln bzw. welchen Beitrag leistet der jeweilige Inhalt zum Kompetenzprofil der angehenden Mathematiklehrkraft? Für die Mathematik als Kernfach der Schule ist es dabei unabdingbar, den Unterricht von der ersten Klasse bis zu den verschiedenen Schulabschlüssen als fortlaufenden Prozess in den Blick zu nehmen.

Für die *fachlichen* Standards sind als Hinweis zu einer Ausdifferenzierung bei der Umsetzung in entsprechende Curricula vier Kategorien angegeben. Diese sind nach inhaltlicher Ausweitung, begrifflicher Elaboriertheit und Grad der Abstraktion und Formalisierung gestaffelt. Ihre Reihung ist im Sinne zunehmender Intensität zu verstehen. Damit wird zum Ausdruck gebracht, dass auf jeder Stufe die Inhalte und Konzepte der davor liegenden Stufen geeignet integriert werden sollen. Dabei sollte folgenden Zielsetzungen Rechnung getragen werden:

- Die Studierenden erfahren mathematische Wissensbildung als progressiven Prozess, der von Denkhandlungen wie Abstraktion, Verallgemeinerung, Präzisierung und Formalisierung getragen wird und die kreative Entwicklung gedanklicher Ordnungsmittel erfordert.
- Sie erwerben damit nicht nur ein vertieftes Verständnis mathematischer Inhalte, sondern auch Sichtweisen, die für die Fähigkeit zum genetischen Lehren unabdingbar sind.

Arithmetik und Algebra – Denken in Zahlen und Strukturen

Der Themenkreis Arithmetik und Algebra erstreckt sich auf Zahlen und ihre Verwendung, das systematische Operieren mit Zahlen und schließlich die Algebra als formale Durchdringung und Verallgemeinerung. Er umspannt eine lange historische Entwicklung, die durch die geistige Gestaltungskraft typischer mathematischer Denkhandlungen wie Abstrahieren, Ordnen und Strukturieren, Generalisieren und Formalisieren getragen ist.

Bereiche	Kompetenzen bezogen auf Inhalte und Prozesse
	Die Studierenden
Zahlen, Zahldarstellungen, Zahlensystem	kennen Darstellungsformen für natürliche Zahlen, Bruchzahlen und rationale Zahlen und verfügen über Beispiele, Grundvorstellungen und begriffliche Beschreibungen für ihre jeweilige Aspektvielfalt beschreiben die Fortschritte im progressiven Aufbau des Zahlensystems und argumentieren mit dem Permanenzprinzip als formaler Leitidee
Elementare Arithmetik	erfassen die Gesetze der Anordnung und der Grundrechenarten für natürliche und rationale Zahlen in vielfältigen Kontexten und können sie
Algebra	kennen und verwenden im Umgang mit Zahlenmustern präalgebraische Darstellungs- und Argumentationsformen und erste formale Sprachmittel (Variable)
	handhaben die elementar-algebraische Formelsprache und beschreiben die Bedeutung der Formalisierung in diesem Rahmen verwenden grundlegende algebraische Strukturbegriffe und zugehörige strukturerhaltende Abbildungen in Zahlentheorie und Geometrie (z.B. Restklassenringe, Symmetriegruppen)
	beschreiben die Vorteile algebraischer Strukturen in verschiedenen mathematischen Zusammenhängen (Zahlentheorie, Analysis, Geometrie) und nutzen sie zum Lösen von Gleichungen (z.B. Konstruktion mit Zirkel und Lineal)

1. Verknüpfungen

Eine (innere) **Verknüpfung** (Operation) in einer Menge M ordnet zwei Elementen a und b (Operanden) aus M ein Element aus M als „Ergebnis der Verknüpfung“ zu. Schreibweise: $a \circ b$, lies: „a verknüpft mit b“. Statt $\circ$ kann man auch ein anderes Symbol verwenden, z.B. $*$.

Unter einem **Verknüpfungsgebilde** oder einer **algebraischen Struktur** versteht man eine Menge M mit einer oder mehreren Verknüpfungen. Schreibweise: $(M,\circ)$

Algebraische Strukturen sind: Gruppen, Ringe, Körper, Vektorräume, Verbände, ... Eine Gruppe ist ein Verknüpfungsgebilde mit einer inneren Verknüpfung. Ring, Körper und Verband sind Verknüpfungsgebilde mit zwei inneren Verknüpfungen. Ein Vektorraum ist ein Verknüpfungsgebilde mit einer inneren (Vektoraddition) und einer äußeren Verknüpfung (Skalarmultiplikation).

In dieser Veranstaltung betrachten wir nur Verknüpfungsgebilde mit inneren Verknüpfungen, in der Hauptsache Gruppen.

Grundeigenschaften von Verknüpfungen bzw. Verknüpfungsgebilden:

Abgeschlossenheit: Ein Verknüpfungsgebilde heißt bzgl. einer Verknüpfung $\circ$ abgeschlossen, wenn für alle Elemente $a,b \in M$ das Ergebnis der Verknüpfung $a \circ b$ in M liegt.

Assoziativität: Eine Verknüpfung $\circ$ in M heißt assoziativ, wenn für alle $a,b,c \in M$ gilt: $a \circ (b \circ c) = (a \circ b) \circ c$

Kommutativität: Eine Verknüpfung $\circ$ in M heißt kommutativ, wenn für alle $a,b \in M$ gilt: $a \circ b = b \circ a$

Besondere Elemente in Bezug auf eine Verknüpfung:

Links-neutrales Element: Ein Element $e_l \in M$ heißt links-neutrales Element bzgl. der Verknüpfung $\circ$, wenn für alle Elemente $a \in M$ gilt: $e_l \circ a = a$.

Links-inverses Element: Ein Element $a_l^{-1} \in M$ heißt links-inverses Element von $a \in M$, wenn gilt: $a_l^{-1} \circ a = e_l$.

Rechtsneutrales Element: Ein Element $e_r \in M$ heißt rechts-neutrales Element bzgl. der Verknüpfung $\circ$, wenn für alle Elemente $a \in M$ gilt: $a \circ e_r = a$.

Rechts-inverses Element: Ein Element $a_r^{-1} \in M$ heißt rechts-inverses Element von $a \in M$, wenn gilt: $a \circ a_r^{-1} = e_r$.

Neutrales Element: Ein Element $e \in M$ heißt neutrales Element bzgl. der Verknüpfung $\circ$, wenn für alle Elemente $a \in M$ gilt: $a \circ e = e \circ a = a$.

Inverses Element: Ein Element $a^{-1} \in M$ heißt inverses Element von $a \in M$, wenn gilt: $a^{-1} \circ a = a \circ a^{-1} = e$.

Bei einer kommutativen Verknüpfung ist ein links-neutrales Element zugleich rechts-neutrales und neutrales und ein links-inverses Element zugleich rechts-inverses und inverses Element.

Im Falle einer (nicht zu großen) endlichen Menge M lässt sich das Verknüpfungsgebilde $(M,\circ)$ in einer Verknüpfungstabelle oder **Verknüpfungstafel** darstellen: In der Eingangszeile und -spalte stehen die Elemente von M, sinnvollerweise in gleicher Anordnung; in den Zellen der Tabelle stehen die Ergebnisse der Verknüpfung, wobei wir festlegen, dass der erste Operand in der Eingangsspalte, der zweite in der Eingangszeile steht.

$\circ$	a	b	c	d
a				
b			$b \circ c$	
c				
d				

Abgeschlossenheit bedeutet: Die Tabelle muss vollständig mit Elementen aus M ausgefüllt sein.
Kommutativität bedeutet: Die ausgefüllte Tabelle ist symmetrisch bzgl. der Hauptdiagonalen.
Ein links-neutrales Element erkennt man daran, dass die zugehörige Zeile in der Tabelle gleich der Eingangszeile ist.
Ein rechts-neutrales Element erkennt man daran, dass die zugehörige Spalte in der Tabelle gleich der Eingangsspalte ist.

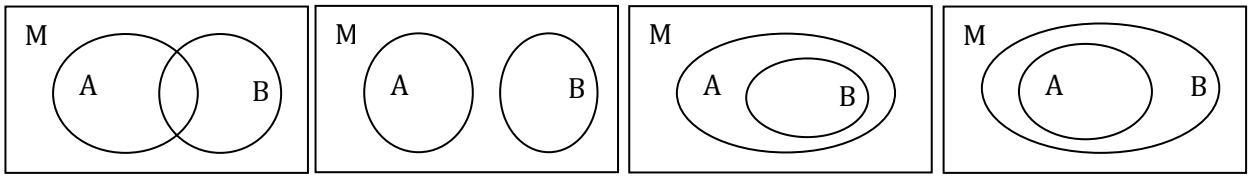
<u>Beispiel-Zoo: Zahlen, Vektoren, Mengen</u>

Natürliche Zahlen (ohne bzw. mit Null)

$\mathbb{N}$ bzw. $\mathbb{N}_0$	a+b	a·b	a–b	a:b	a^b	ggT(a,b)	kgV(a,b)	max(a,b)	min(a,b)
abgeschlossen	✓	✓	/	/	✓	✓	✓	✓	✓
assoziativ	✓	✓							
kommutativ	✓	✓							
links-neutrales El.	0	1							
rechts-neutrales El.	0	1							
neutrales El.	0	1							
links-inverses El.									
rechts-inverses El.									
inverses El.									

Mengen

Grundmenge M, Teilmengen A, B, ... $\subset$ M, $\emptyset$ = leere Menge



Potenzmenge $\mathcal{P}(M)$ = Menge aller Teilmengen von M

$A \Delta B = (A \cup B) \setminus (A \cap B)$

$\mathcal{P}(M)$	A∩B	A∪B	A\B	AΔB
abgeschlossen	✓	✓	✓	✓
assoziativ	✓	✓		
kommutativ	✓	✓		
links-neutrales El.	M	∅		
rechts-neutrales El.	M	∅		
neutrales El.	M	∅		
links-inverses El.				
rechts-inverses El.				
inverses El.				

2. Relationen

In einer Menge M können Elemente zueinander in Beziehung (= Relation) gesetzt werden: **xRy,** ausführlich gelesen: **„x steht in Relation zu y“**, wobei x und y Elemente der Menge M sind.

Da es in der Regel auf die Reihenfolge ankommt, in der die beiden Elemente genannt werden, spricht man vom **geordneten Paar (x,y)**; zwei geordnete Paare (x,y) und (u,v) sind also genau dann gleich, wenn $x = u$ und $y = v$ gilt. Die Menge $M \times M := \{(a, b)|a, b \in M\}$ heißt **Paarmenge** oder **kartesisches Produkt**. Manchmal schreibt man statt $M \times M$ (lies: „M Kreuz M“) auch M^2.

Eine Relation R in der Menge M ist dann formal nichts anderes als eine Teilmenge von $M \times M$ und xRy und $(x,y) \in R$ sind zwei verschiedene Schreibweisen für denselben Sachverhalt.

Zu jeder Relation R gibt es eine **Umkehrrelation** R^{-1}. Es gilt also $yR^{-1}x$ genau dann, wenn xRy gilt.

Die Veranschaulichung einer Relation in einer (nicht zu großen) Menge erfolgt durch Pfeile.

Wichtige Eigenschaften

Reflexivität:	xRx	für alle Elemente $x \in M$
Symmetrie:	Wenn xRy, dann auch yRx	für alle $x, y \in M$
Asymmetrie:	Wenn xRy, dann nicht yRx	für alle $x, y \in M$
Antisymmetrie:	Wenn xRy und yRx, dann $x = y$	für alle $x, y \in M$
Transitivität:	Wenn xRy und yRz, dann auch xRz	für alle $x, y, z \in M$

Eine Relation R heißt **Ordnungsrelation**, wenn sie reflexiv, antisymmetrisch und transitiv ist. Eine Relation R heißt **strenge Ordnungsrelation**, wenn sie asymmetrisch und transitiv ist.

Äquivalenzrelation

Eine Relation R heißt **Äquivalenzrelation**, wenn sie reflexiv, symmetrisch und transitiv ist. Man liest xRy dann auch „x ist äquivalent zu y“. Man kann eine Äquivalenzrelation als Verallgemeinerung der Gleichheit(srelation) ansehen. Im Pfeilbild wird die Menge M durch eine Äquivalenzrelation in lauter disjunkte Teilmengen zerlegt, wobei in den einzelnen Teilmengen alle Elemente durch Pfeile (incl. Schlingen) in beiden Richtungen miteinander verbunden sind. Das lässt sich formal beschreiben:

Äquivalenzklasse

Ist R eine Äquivalenzrelation, dann heißt die Menge $[a] := \{x \in M|xRa\}$ Äquivalenzklasse von a. Das Element a heißt auch Repräsentant der Äquivalenzklasse [a].

Zwei Äquivalenzklassen [a] und [b] sind genau dann gleich, wenn aRb gilt. Anders ausgedrückt: Zwei Äquivalenzklassen [a] und [b] sind entweder gleich oder disjunkt. Da die Vereinigungsmenge aller Äquivalenzklassen wieder ganz M ergibt, erzeugen sie eine disjunkte Zerlegung von M, auch Klasseneinteilung genannt.

In einer nächsten Abstraktionsstufe fasst man alle Äquivalenzklassen zu einer neuen Menge $\{[a]|a \in M\}$ zusammen, **Faktormenge** genannt. Die Elemente der Faktormenge sind also Teilmengen von M (die Faktormenge ist eine Teilmenge der Potenzmenge $\mathcal{P}(M)$). Die Faktormenge kann man als vergröbertes Exemplar der ursprünglichen Menge ansehen, indem man gewisse Elemente unter dem Aspekt der Äquivalenz miteinander identifiziert und dabei von den übrigen Eigenschaften absieht.

Der beschriebene Abstraktionsprozess taucht an verschiedenen Stellen der Veranstaltung auf.

Oft gibt es in der Menge M, in der die Äquivalenzrelation erklärt ist, auch eine oder mehrere Verknüpfungen. Unter bestimmten Bedingungen lassen sich diese auf die Faktormenge übertragen.

Restklassen modulo n

In der Arithmetik (und der Zahlentheorie) betrachtet man in der Menge $\mathbb{N}_0$ die Relation R, wobei xRy bedeutet:„x **lässt beim Teilen durch n denselben Rest wie** y“. (Aus historischen Gründen schreibt man statt xRy meist $x \equiv y \bmod n$ und liest: „x ist kongruent y modulo n“). Die Relation R ist eine Äquivalenzrelation. Sie erzeugt eine disjunkte Zerlegung von $\mathbb{N}_0$ in Äquivalenzklassen, die man Restklassen nennt. Eine **Restklasse** $[a]_n$ (sprich: „Restklasse (von) a modulo n“) besteht aus allen natürlichen Zahlen, die beim Teilen durch n denselben Rest lassen wie a. In der Arithmetik nimmt man als Repräsentanten in der Regel die kleinste Zahl in der Restklasse, also $0 \leq a < n$; aber formal sind alle Zahlen der Restklasse als Repräsentanten zugelassen.

Alle Restklassen modulo n fasst man zusammen zur **Faktormenge** $\mathcal{R}_n$. Die Elemente der Faktormenge sind also (unendliche) Teilmengen von $\mathbb{N}_0$. Die Faktormenge selbst ist endlich; sie besteht aus n Elementen. Die Faktormenge kann man als vergröbertes Exemplar von $\mathbb{N}_0$ ansehen; z.B. werden für $n = 10$ alle natürlichen Zahlen unter dem Aspekt der Endziffer miteinander identifiziert.

Man kann die Addition und die Multiplikation von den natürlichen Zahlen auf die Restklassen übertragen:

$$[a]_n \oplus [b]_n := [a+b]_n \qquad [a]_n \otimes [b]_n := [a \cdot b]_n$$

Nachzuweisen ist, dass diese Definition sinnvoll ist, d.h. dass dasselbe herauskommt, gleich welchen Repräsentanten man für jede der Restklassen wählt.

Offensichtlich ist $\mathcal{R}_n$ bezüglich beider Verknüpfungen abgeschlossen. Beide Verknüpfungen sind assoziativ und kommutativ. Für beide Verknüpfungen existiert je ein neutrales Element, nämlich $[0]_n$ bzw. $[1]_n$.

Während in $\mathbb{N}_0$ keine Zahl außer Null ein inverses Element bezüglich der Addition besitzt, besitzt in $(\mathcal{R}_n,\oplus)$ jedes Element ein inverses Element: Das inverse Element der Restklasse $[a]_n$ mit $0 \leq a < n$ ist die Restklasse $[n-a]_n$.

In $\mathbb{N}$ besitzt keine Zahl außer Eins ein inverses Element bezüglich der Multiplikation. Wie sieht das in $\mathcal{R}_n \backslash [0]_n$ aus? In $\mathcal{R}_7 \backslash [0]_7$ hat jedes Element ein inverses Element bezüglich der Multiplikation. In $\mathcal{R}_{10} \backslash [0]_{10}$ hat eine Restklasse nur dann ein inverses Element bezüglich der Multiplikation, wenn ihr Repräsentant (wenn einer, dann alle!) teilerfremd zu 10 ist.

Eine Restklasse $[a]_n$ mit $a \in \mathbb{N}$ heißt **prime Restklasse modulo n**, wenn a und n teilerfremd sind. Die Menge aller primen Restklassen modulo n bezeichnen wir mit $\mathcal{R}_n^*$. In $(\mathcal{R}_n^*,\otimes)$ besitzt jedes Element ein inverses Element.

Das gesamte Konzept der Restklassenbildung lässt sich **von den natürlichen Zahlen auf die ganzen Zahlen** übertragen. Allerdings muss man, um bei der Übertragung der Addition dieselben Aussagen zu erhalten, die Äquivalenzrelation R entsprechend interpretieren: xRy bedeutet „x und y **unterscheiden sich nur um ein ganzzahliges Vielfaches von n**“.

Statt $\mathcal{R}_n$ schreibt man dann $\mathbb{Z}_n$ und statt $\mathcal{R}_n^*$ schreibt man $\mathbb{Z}_n^*$.

3. Abbildungen

Statt von **Abbildung** spricht man in verschiedenen mathematischen Teilgebieten auch von **Funktion.** Meist historisch bedingt sind noch andere Namen im Gebrauch (**Operator**, **Transformation**, ...).

Grundbedingung für eine Abbildung f der Menge A in die Menge B: Jedes Element von A wird abgebildet und jedem $x \in A$ wird nur ein $y \in B$ zugeordnet. Die Menge A heißt Definitionsmenge oder Definitionsbereich, die Menge B Wertemenge oder Wertebereich.

Schreibweisen: Zuordnung der Mengen $f: A \to B$ oder $A \xrightarrow{f} B$
Abbildungsvorschrift $f: x \mapsto y$ oder $y = f(x)$

Eine Abbildung ist also durch drei Angaben festgelegt: Definitionsmenge, Wertemenge und Abbildungsvorschrift. Nicht alle Elemente der Wertemenge B müssen getroffen werden; diejenigen, die getroffen werden, fasst man zur Bildmenge $f(A) \subset B$ zusammen.

Grundeigenschaften von Abbildungen:

Injektivität: Verschiedene Elemente aus A werden auf verschiedene Elemente in B abgebildet bzw. aus $f(x_1) = f(x_2)$ folgt $x_1 = x_2$ für alle $x_1, x_2 \in A$.

Surjektivität: Jedes Element von B ist Bild eines Elements aus A, d.h. zu jedem $y \in B$ gibt es (mindestens) ein $x \in A$, so dass $y = f(x)$ ist.

Bijektivität: Die Funktion ist sowohl injektiv als auch surjektiv. Man spricht auch von einer umkehrbar eindeutigen bzw. eineindeutigen Zuordnung. Die umgekehrte Zuordnung, die jedem $y \in B$ das $x \in A$ zuordnet, für das $y = f(x)$ gilt, heißt Umkehrabbildung und wird mit f^{-1} symbolisiert.

Häufig werden Abbildungen einer Menge auf sich selbst betrachtet, d.h. $A = B$. In diesem Fall gibt es eine besondere Abbildung: die **identische Abbildung** $id: A \to A$ mit $id: x \mapsto x$.

Hintereinanderausführung (HAF) $A \xrightarrow{f} B \xrightarrow{g} C$: Ist f eine Abbildung der Menge A in die Menge B und g eine Abbildung der Menge B in die Menge C, dann kann man eine Abbildung der Menge A in die Menge C definieren, die ein beliebiges Element $x \in A$ zunächst dem Element $y = f(x)$ und dieses dann dem Element $z = g(y)$ zuordnet. Es ist also: $z = g(f(x))$.
Man bezeichnet die neue Funktion als Hintereinanderausführung (HAF) von f und g.
Schreibweise: $f \circ g$ („erst f, dann g"). Beachte: $f \circ g(x) = g(f(x))$.
(In der Analysis schreibt man meistens $g \circ f$ (lies: „g nach f"); beachte: dann ist $(g \circ f)(x) = g(f(x))$ (lies: „g nach f von x ist gleich g von f von x")).

Es gilt: **Wenn f und g surjektiv/ injektiv/ bijektiv sind, dann ist $f \circ g$ surjektiv/ injektiv/ bijektiv.**

Abbildungen in der Algebra

Wir betrachten Abbildungen unter zwei Aspekten. Zum einen benutzen wir sie als Instrument, um damit verschiedene Verknüpfungsgebilde miteinander zu vergleichen (Isomorphismus, Homomorphismus).

Zum andern benutzen wir sie als Elemente eines Verknüpfungsgebildes mit der HAF als Verknüpfung: Wir betrachten bijektive Abbildungen einer Menge A auf sich und fassen sie zu einer neuen Menge M zusammen. Die HAF zweier solcher Abbildungen ergibt wieder eine bijektive Abbildung der Menge A auf sich, d.h. wir können die HAF als Verknüpfung interpretieren. Die Menge M von bijektiven Abbildungen von A auf sich ist bzgl. der HAF abgeschlossen.

Die HAF als Verknüpfung ist assoziativ, in der Regel aber nicht kommutativ. Die identische Abbildung von A auf sich, die jedes Element aus A auf sich selbst abbildet, ist neutrales Element.

Permutationen

Permutationen sind bijektive Abbildungen einer endlichen Menge auf sich.

Als Repräsentant einer endlichen Menge mit n Elementen kann man die Menge der ersten n natürlichen Zahlen wählen: $\mathbb{N}_n=\{1, 2, ..., n\}$. Dann ist eine Permutation eine Vertauschung der natürlichen Reihenfolge. Es gibt n! Permutationen von n Elementen.

Beispiel für eine Permutation in $\mathbb{N}_5$ $\quad p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 5 & 1 \end{pmatrix}$

Die Schreibweise erinnert an eine Wertetabelle: Oben stehen die Eingabedaten, unten die Funktionswerte.

Die Menge aller Permutationen von n Elementen bezeichnet man mit S_n. Die HAF von Permutationen ist eine Verknüpfung in S_n. S_n ist abgeschlossen bezüglich dieser Verknüpfung. Die Verknüpfung ist assoziativ (in der Regel nicht kommutativ). Sie besitzt ein neutrales Element; die identische Abbildung. Jedes Element besitzt ein inverses Element, nämlich die Umkehrabbildung.

Beispiel in $\mathbb{N}_5$ $\quad p^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 3 & 4 \end{pmatrix}$

Symmetrien

Symmetrien sind bijektive Abbildungen der Ebene oder des Raumes auf sich, die eine Figur (z.B. Quadrat) als Teilmenge der Ebene oder einen Körper (z.B. Tetraeder) als Teilmenge des Raumes auf sich abbilden(wohlgemerkt: nicht jeden Punkt dieser Teilmenge auf sich, sondern nur die Teilmenge als ganze auf sich). Über die Bijektivität hinaus werden dabei noch zusätzliche Bedingungen gestellt (z.B. längentreu, winkeltreu, ...). Wir befassen uns nur mit Symmetrien, die durch **Kongruenzabbildungen** (Deckabbildungen, Bewegungen) erzeugt werden. Dabei wird die Figur oder der Körper mit sich selbst zur Deckung gebracht.

Die HAF zweier Symmetrien ist wieder eine Symmetrie, anders: Die HAF ist eine Verknüpfung in der Menge der Symmetrien einer Figur oder eines Körpers. Die Menge der Symmetrien einer Figur oder eines Körpers ist abgeschlossen bezüglich der Verknüpfung HAF. Die Verknüpfung HAF ist assoziativ (in der Regel nicht kommutativ). Sie besitzt ein neutrales Element; die identische Abbildung. Jedes Element besitzt ein inverses Element, nämlich die Umkehrabbildung.

Bei **Kongruenzabbildungen** oder **Bewegungen** in der **Ebene** unterscheidet man

Bewegungen, die die Orientierung (den Drehsinn) erhalten: Drehung (Spezialfall: Halbdrehung oder Punktspiegelung) (man spricht von Drehsymmetrie (speziell: Punktsymmetrie) und Verschiebung oder Translation (man spricht von Bandornamenten oder Parketten).

Bewegungen, die die Orientierung (den Drehsinn) umkehren: Achsen- oder Geradenspiegelung (man spricht von Achsen- oder Spiegelsymmetrie) und jede HAF einer Achsenspiegelung mit einer Drehung oder einer Verschiebung (Gleitspiegelung).

Bei **Kongruenzabbildungen** oder **Bewegungen** im **Raum** unterscheidet man

Eigentliche Bewegungen: Drehung um eine Achse, Verschiebung, Schraubung

Uneigentliche Bewegungen: Ebenenspiegelung, Punktspiegelung und jede HAF einer uneigentlichen Bewegung mit einer eigentlichen

Manche **Symmetrien** kann man durch **Permutationen** beschreiben, z.B. als Permutation der Ecken einer symmetrischen ebenen Figur oder als Permutation der Ecken oder der Flächen eines symmetrischen Körpers.

4. Gruppen

Eine Gruppe ist ein Verknüpfungsgebilde $(M,\circ)$ mit folgenden Eigenschaften („**Gruppen-Axiome**“):

- M ist **abgeschlossen** bzgl. der Verknüpfung $\circ$.
- Die Verknüpfung $\circ$ ist **assoziativ**.
- Es gibt ein **neutrales Element** $e \in M$.
- Zu jedem Element $x \in M$ gibt es ein **inverses Element** $x^{-1} \in M$, d.h. $x \circ x^{-1} = x^{-1} \circ x = e$.

Beachte: Die Verknüpfung $\circ$ kann, muss aber nicht kommutativ sein, damit $(M,\circ)$ eine Gruppe ist. Eine Gruppe, in der die Verknüpfung $\circ$ kommutativ ist heißt kommutative oder **abelsche Gruppe**.

Beispiele aus dem Beispiel-Zoo: Endliche und unendliche Gruppen

Satz von der Eindeutigkeit des neutralen Elements:
In einer Gruppe $(M,\circ)$ kann es nur ein neutrales Element geben.

Satz von der Eindeutigkeit des inversen Elements:
In einer Gruppe $(M,\circ)$ kann es zu jedem Element nur ein inverses Element geben.

Satz von der Lösbarkeit von Gleichungen (Existenz von Lösungen):
In einer Gruppe $(M,\circ)$ besitzen die Gleichungen . $a \circ x = b$ und $y \circ a = b$ für alle $a,b \in M$ eine Lösung x bzw. y in M.

Satz von der Kürzungsregel (Eindeutigkeit von Lösungen):
Aus $a \circ x_1 = a \circ x_2$ folgt $x_1 = x_2$ und aus $y_1 \circ a = y_2 \circ a$ folgt $y_1 = y_2$.

Satz von der Gruppentafel:
In jeder Zeile und jeder Spalte der Gruppentafel kommt jedes Element von M genau einmal vor.

Erstes Ordnen des Beispiel-Zoos:

Es gibt nur einen Typ von ein- bzw. zwei- bzw. drei-elementigen Gruppen; d.h. alle von ein- bzw. zwei- bzw. drei-elementigen Gruppen haben dieselbe Struktur.

Eine vier-elementige Gruppe hat entweder die Struktur der **Kleinschen Vierer-Gruppe**, in der jedes Element zu sich selbst invers ist, oder der **zyklischen Vierer-Gruppe**, bei der jedes Element durch wiederholte Verknüpfung eines Elements erzeugt werden kann.

„**Gleiche Struktur besitzen**“ wird mit Hilfe besonderer Abbildungen präzisiert:

Sind $(M_1,\circ)$ und $(M_2,*)$ zwei Verknüpfungsgebilde, dann heißt eine Abbildung $f: M_1 \to M_2$ **strukturverträglich**, wenn für alle $x,y \in M_1$ gilt: $f(x)*f(y) = f(x \circ y)$
(in Worten: „erst abbilden, dann verknüpfen ist dasselbe wie erst verknüpfen, dann abbilden“).

Eine strukturverträgliche Abbildung von $(M_1,\circ)$ nach $(M_2,*)$ – auch **Homomorphismus** genannt – vererbt/ überträgt alle Eigenschaften (Abgeschlossenheit, Assoziativität, Kommutativität, Existenz eines neutralen Elements, Existenz eines inversen Elements) des Verknüpfungsgebildes $(M_1,\circ)$ auf die Bildmenge $f(M_1)$ als Teilmenge von M_2 mit der Verknüpfung $*$. Beachte: Es können verschiedene Elemente von M_1 auf dasselbe Element in M_2 abgebildet werden. Insofern ist $f(M_1)$ ein „verkleinertes“, aber „strukturgleiches“ Bild von M_1.

Völlige Strukturgleichheit erhält man, wenn die strukturverträgliche Abbildung f von $(M_1,\circ)$ nach $(M_2,*)$ **bijektiv** ist; sie heißt dann **Isomorphismus**. Wenn f ein Isomorphismus von $(M_1,\circ)$ nach $(M_2,*)$ ist, dann ist die Umkehrabbildung f^{-1} von $(M_2,*)$ nach $(M_1,\circ)$ auch ein Isomorphismus. Die beiden Verknüpfungsgebilde heißen **isomorph**.

5. Untergruppen

Ist $(M,\circ)$ eine Gruppe, U eine Teilmenge von M und $(U,\circ)$ ebenfalls eine Gruppe, dann heißt $(U,\circ)$ **Untergruppe** von $(M,\circ)$.

Satz vom Untergruppen-Kriterium:
Ist $(M,\circ)$ eine Gruppe und U eine Teilmenge von M, dann ist $(U,\circ)$ Untergruppe von $(M,\circ)$, wenn folgende Bedingungen erfüllt sind:

1. Die Verknüpfung $\circ$ ist abgeschlossen in U; d.h. wenn $a,b \in U$, dann $a \circ b \in U$.
2. Zu jedem Element aus U liegt das inverse Element auch in U; wenn $a \in U$, dann $a^{-1} \in U$.

Wenn M eine endliche Gruppe ist, reicht das 1. Kriterium.

Mit Hilfe einer Untergruppe $(U,\circ)$ kann man eine Gruppe $(M,\circ)$ zerlegen. Dazu dient die folgende Begriffsbildung.

Sei $(U,\circ)$ eine Untergruppe von $(M,\circ)$ und a ein beliebiges Element aus M, dann heißt
$a \circ U := \{a \circ x | x \in U\}$ **Linksnebenklasse,** $U \circ a := \{x \circ a | x \in U\}$ **Rechtsnebenklasse** von U.
Wenn $\circ$ kommutativ ist, gilt Linksnebenklasse = Rechtsnebenklasse.
I.A. gilt Linksnebenklasse ≠ Rechtsnebenklasse.

Satz von der Zerlegung einer Gruppe:
$(M,\circ)$ sei eine Gruppe und $(U,\circ)$ Untergruppe von $(M,\circ)$.

a) Die Linksnebenklassen von U bilden eine disjunkte Zerlegung von $(M,\circ)$, d.h.
   (i) Jedes Element von M gehört zu einer Linksnebenklasse von U.
   (ii) Zwei Linksnebenklassen sind entweder disjunkt oder gleich.
b) Falls $(M,\circ)$ eine endliche Gruppe ist, haben alle Linksnebenklassen von U gleich viele Elemente wie U.

Entsprechendes gilt für Rechtsnebenklassen.

Der Teil a) des Satzes lässt sich auf verschiedene Arten beweisen. Eine Möglichkeit ist, sich daran zu erinnern, dass eine Äquivalenzrelation eine disjunkte Zerlegung erzeugt (Kap.2). Die Äquivalenzrelation R_{li}, die zu der Zerlegung in Linksnebenklassen führt, ist definiert durch: $aR_{li}b$ genau dann, wenn $a^{-1} \circ b \in U$. Die Äquivalenzrelation R_{re}, die zu der Zerlegung in Rechtsnebenklassen führt, ist definiert durch: $aR_{re}b$ genau dann, wenn $b \circ a^{-1} \in U$.

Die Anzahl der Elemente einer endlichen Gruppe $(M,\circ)$ heißt **Ordnung der Gruppe**, in Zeichen: ord M.

Satz von (Euler-) Lagrange über die Ordnung von Untergruppen:
In einer endlichen Gruppe $(M,\circ)$ ist die Ordnung einer Untergruppe $(U,\circ)$ Teiler der Gruppenordnung, in Zeichen: ord U | ord M.

Wenn ord U = ½ ord M, dann gilt Linksnebenklasse = Rechtsnebenklasse.

Beispiel aus dem Beispiel-Zoo: Tetraeder-Gruppe mit Untergruppen

6. Zyklische Gruppen

(M,◦) sei eine Gruppe.

Schreibweise: $a^n := \underbrace{a \circ a \circ \dots \circ a}_{\text{n Operanden}}$ $a^{-n} := \underbrace{a^{-1} \circ a^{-1} \circ \dots \circ a^{-1}}_{\text{n Operanden}}$ $a^1 := a$ $a^0 := e$

Es gilt: $a^m \circ a^n = a^{m+n}$ $a^m \circ a^{-n} = a^{m-n}$

$< a >: = \{\dots, a^{-2}, a^{-1}, e, a, a^2, \dots\}$

(<a>,◦) ist eine Untergruppe von (M,◦), die außerdem kommutativ (abelsch) ist.

Eine Gruppe (M,◦), in der es ein Element a gibt, so dass M = <a> gilt, heißt **zyklisch**; man sagt: (M,◦) wird von a erzeugt, und nennt a ein **erzeugendes Element**.

Ist a ein Element der Gruppe (M,◦) und m der kleinste (positive) Exponent mit $a^m = e$, dann heißt m **Ordnung des Elements** a, in Zeichen: ord a.

Unterscheide: Ordnung der Gruppe und Ordnung eines Elements.

Sind alle Potenzen von a verschieden, dann heißt a „von unendlicher Ordnung".

Satz von der Ordnung eines Elements:

Für die Ordnung einer endlichen Gruppe (M,◦) und die Ordnung eines Elements a aus M gelten folgende Aussagen:

(i) ord a | ord M (ii) $a^{\text{ord M}} = e$ („Kleiner Satz von Fermat")

(iii) (M,◦) ist genau dann zyklisch, wenn es wenigstens ein a∈M gibt mit ord a = ord M.

Satz von den Untergruppen zyklischer Gruppen:

Jede Untergruppe einer zyklischen Gruppe ist zyklisch.

Satz von den Gruppen mit Primzahlordnung:

Jede Gruppe, deren Ordnung eine Primzahl ist, ist zyklisch.

Beispiele aus dem Beispiel-Zoo: $(\mathbb{Z},+)$, $(\mathbb{Z}_n,\oplus)$, $(\mathbb{Z}_n^*,\otimes)$

Klassifikationssatz über zyklische Gruppen:

Jede unendliche zyklische Gruppe ist isomorph zu $(\mathbb{Z},+)$.

Jede endliche zyklische Gruppe der Ordnung n ist isomorph zu $(\mathbb{Z}_n,\oplus)$.

Von $(\mathbb{Z},+)$ nach $(\mathbb{Z}_n,\oplus)$ als Muster des Faktorisierens

$(\mathbb{Z},+)$, die Menge der ganzen Zahlen zusammen mit der Addition, ist eine unendliche zyklische Gruppe mit 1 als einem erzeugenden Element. Die Untergruppen von $(\mathbb{Z},+)$ sind die Mengen $n\mathbb{Z} := \{n \cdot z \mid z \in \mathbb{Z}\} = \{\text{Vielfache von n}\}$.

Die Nebenklasse (Linksnebenklasse = Rechtsnebenklasse!) einer Zahl $a \in \mathbb{Z}$ bzgl. einer solchen Untergruppe $n\mathbb{Z}$ ist $[a]_n := \{a + n \cdot z \mid z \in \mathbb{Z}\}$, das ist, anders ausgedrückt, die Menge aller ganzen Zahlen, die beim Teilen durch n denselben Rest ergeben wie a. Die Menge dieser Restklassen haben wir mit $\mathbb{Z}_n$ bezeichnet und auf sie die Addition ⊕ übertragen. (Kap. 2)

$(\mathbb{Z}_n,\oplus)$ist eine endliche zyklische Gruppe mit $[1]_n$ als einem erzeugenden Element.

Schema des Faktorisierens

Gruppe	⟶	Untergruppe	⟶	Neben-klassen	⟶	neue Gruppe mit „weniger" Elementen
$(\mathbb{Z},+)$		$n\mathbb{Z}$		$[a]_n$		$(\mathbb{Z}_n,\oplus)$

7. Normalteiler und Faktorgruppe

Schema des Faktorisierens

Gruppe	⟶	Untergruppe	⟶	Linksneben-klassen	⟶	neue Gruppe mit „weniger“ Elementen
(M,∘)		U		a∘U		?

Unter welchen Voraussetzungen lässt sich das Schema auf eine beliebige Gruppe übertragen? Antwort: Wenn die Untergruppe ein Normalteiler ist.

Eine Untergruppe (U,∘) einer Gruppe (M,∘) heißt **Normalteiler**, wenn für jedes Element $a \in M$ gilt: Linksnebenklasse = Rechtsnebenklasse, $a \circ U = U \circ a$.

Die Normalteilereigenschaft ist eine Verallgemeinerung der Kommutativität: Es gilt nicht mehr für alle a und x aus M $a \circ x = x \circ a$, sondern die Mengen $\{a \circ x \mid x \in U\}$ und $\{x \circ a \mid x \in U\}$ sind gleich.

Satz vom Normalteiler:
Sei (U,∘) Untergruppe einer Gruppe (M,∘) und $M/U := \{a \circ U | a \in M\}$ die Menge aller Linksnebenklassen von U. In M/U sei die Verknüpfung ● definiert durch

$$(a \circ U) \bullet (b \circ U) := \{(a \circ x) \circ (b \circ y) | x, y \in M\}.$$

Die Verknüpfung ● ist genau dann abgeschlossen in M/U, wenn (U,∘) Normalteiler von (M,∘) ist.

Neue Schreibweise: Wenn für jedes Element $a \in M$ die Linksnebenklasse gleich der Rechtsnebenklasse ist, sprechen wir nur noch von der Nebenklasse und symbolisieren sie durch $[a]_U$, also $M/U := \{[a]_U | a \in M\}$, und es gilt $[a]_U \bullet [b]_U = [a \circ b]_U$.

Satz von der Faktorgruppe:
Sei (U,∘) ein Normalteiler der Gruppe (M,∘). Dann ist

a) (M/U, ●) eine Gruppe, genannt Faktorgruppe
b) (M/U, ●) abelsch, falls (M,∘) abelsch ist
c) (M/U, ●) zyklisch, falls (M,∘) zyklisch ist

Der Vorgang erinnert wieder an den Abstraktionsprozess, der von einer Menge durch eine Äquivalenzrelation zur Faktormenge führt (Kap.2). In Kap. 5 haben wir gesehen, welche Äquivalenzrelationen jeweils zu einer Zerlegung einer Gruppe in Linksnebenklassen bzw. Rechtsnebenklassen führen. Damit war noch nicht sichergestellt, dass auf diese Faktormengen wieder eine Gruppenstruktur übertragen werden kann. Die Sätze vom Normalteiler und von der Faktorgruppe besagen, dass die notwendige und hinreichende Bedingung hierfür ist, dass die Untergruppe, die die Äquivalenzrelationen erzeugt, ein Normalteiler ist.

Eine Faktorgruppe ist sozusagen eine vergröberte Ausgabe der ursprünglichen Gruppe, indem Elemente der ursprünglichen Gruppe miteinander identifiziert bzw. als äquivalent betrachtet werden und man nur noch mit den Äquivalenzklassen rechnet. Da es sich „im Wesentlichen um die gleiche“ Verknüpfung handelt, schreiben wir wieder ◦ statt ● und (M/U, ∘) statt (M/U, ●).

Satz vom natürlichen Homomorphismus:
Sei (U,∘) ein Normalteiler der Gruppe (M,∘). Die Abbildung $\tilde{f}$ von (M,∘) in die Faktorgruppe (M/U, ∘)mit $\tilde{f}$: $a \mapsto [a]_U$ ist ein Homomorphismus, genannt natürlicher Homomorphismus.

Beispiele aus dem Beispiel-Zoo

8. Isomorphie und Homomorphie

„Gleiche Struktur besitzen“ wird mit Hilfe des **Isomorphismus** präzisiert: Zwei Gruppen $(M_1,\bullet)$ und $(M_2,*)$ sind isomorph, wenn es eine bijektive strukturverträgliche Abbildung $f: M_1 \to M_2$, einen Gruppen-Isomorphismus, von der einen Gruppe auf die andere gibt.

Beispiele aus dem Beispiel-Zoo

Ähnlich wie der Klassifikationssatz über zyklische Gruppen (Kap. 6) klassifiziert der folgende Satz alle endlichen Gruppen. Schön, aber nutzlos.

Satz von Cayley über die Isomorphie endlicher Gruppen:
Jede endliche Gruppe der Ordnung n ist isomorph zu einer Untergruppe der Permutationsgruppe S_n (= Gruppe aller Permutationen von n Elementen).

Eine Verallgemeinerung des Isomorphismus ist der Homomorphismus. Will man Strukturaussagen über eine Gruppe M_2 machen, so zieht man häufig eine bekannte Gruppe M_1 zum Vergleich heran. Ein derartiger Vergleich erfordert eine strukturverträgliche Abbildung, einen **Homomorphismus** $f: M_1 \to M_2$; denn dann ist die Bildmenge $(f(M_1),*)$ eine Untergruppe in $(M_2,*)$ und man kann mit ihrer Hilfe nach weiteren Struktureigenschaften in $(M_2,*)$ forschen.
Aber selbst in dem günstigen Fall, dass der Homomorphismus f surjektiv ist, also $M_2 = f(M_1)$, d.h. ein „verkleinertes“ Bild von M_1 ist, fällt der Vergleich oft noch schwer, weil man mit der Struktur von M_2 nicht vertraut ist. Man sucht deshalb nach einer zu $(M_2,*)$ isomorphen Gruppe, die aus der vertrauten Gruppe $(M_1, \bullet)$ konstruiert werden kann. Der Homomorphie-Satz sagt: Eine solche Gruppe kann man mit Hilfe eines Homomorphismus $f: M_1 \to M_2$ immer angeben, und zwar als Faktorgruppe von $(M_1, \bullet)$.

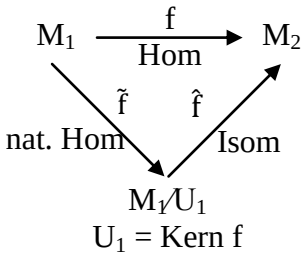
Als **Kern** des Homomorphismus f, abgekürzt: Kern f, bezeichnet man die Teilmenge von M_1, die auf das neutrale Element e_2 von M_2 abgebildet wird. (Im Falle eines Isomorphismus besteht Kern f nur aus e_1, dem neutralen Element von M_1.)

Satz vom Kern eines Gruppen-Homomorphismus:
Ist $f: M_1 \to M_2$ ein Homomorphismus von der Gruppe $(M_1, \bullet)$ in die Gruppe $(M_2,*)$, dann ist Kern f Normalteiler in $(M_1, \bullet)$.

Damit ist sichergestellt, dass man mit einem Homomorphismus $f: M_1 \to M_2$ immer eine Faktorgruppe $(M_1/\text{Kern } f, \bullet)$ bilden kann.

Homomorphie-Satz:

1. Wenn $f: M_1 \to M_2$ ein surjektiver Homomorphismus von der Gruppe $(M_1, \bullet)$ auf die Gruppe $(M_2,*)$ ist, dann ist
   a. $(M_2,*)$ isomorph zu der Faktorgruppe $(M_1/\text{Kern } f, \bullet)$ vermittels des Isomorphismus $\hat{f}: (M_1/\text{Kern } f, \bullet) \to M_2$ mit $\hat{f}: [a]_{\text{Kern } f} \longmapsto f(a)$
   b. $f: M_1 \to M_2$ die HAF des natürlichen Homomorphismus $\tilde{f}: M_1 \to (M_1/\text{Kern } f, \bullet)$ und des Isomorphismus $\hat{f}$.



2. Wenn
   a. $(U_1, \bullet)$ ein Normalteiler der Gruppe $(M_1, \bullet)$ und $(M_1/U_1, \bullet)$ die zugehörige Faktorgruppe und $\tilde{f}: M_1 \to M_1/U_1$ der natürliche Homomorphismus ist und
   b. die Gruppe $(M_2,*)$ isomorph zur Faktorgruppe $(M_1/U_1, \bullet)$ vermittels des Isomorphismus $\hat{f}: M_1/U_1 \to M_2$ mit $\hat{f}: [a]_{U_1} \longmapsto f(a)$ ist,

   dann ist die HAF $\tilde{f} \circ \hat{f}: M_1 \to M_2$ ein Homomorphismus von $(M_1, \bullet)$ auf $(M_2,*)$

9. Zahlbereichserweiterungen

In einer Gruppe $(M,\circ)$ haben die Gleichungen $a\circ b = x$ und $a\circ y = b$ und $z\circ a = b$ für alle $a,b\in M$ eindeutige Lösungen $x,y,z\in M$; man kann uneingeschränkt mit $\circ$ rechnen. Das kann man in der Menge $\mathbb{N}$ der natürlichen Zahlen bekanntlich nicht. Zwar gilt für die Verknüpfungsgebilde $(\mathbb{N}_0,+)$ und $(\mathbb{N},\cdot)$: Sie sind abgeschlossen; die Verknüpfungen $+$ und $\cdot$ sind assoziativ und kommutativ; sie haben ein neutrales Element, nämlich 0 bzw. 1; es gilt sogar die Kürzungsregel (aus $a\circ x_1 = a\circ x_2$ folgt $x_1 = x_2$). Aber die Gleichungen $7+y = 3$ und $7\cdot z = 3$ haben in $\mathbb{N}$ keine Lösung: Die inversen Elemente, die negativen ganzen Zahlen bzw. die Brüche fehlen.

Die Erweiterungen der jeweils bekannten Zahlbereiche erfolgt nicht willkürlich.

Um diese Grenzen des Rechnens zu überwinden, wird der Zahlbereich $(\mathbb{N}_0,+)$ erweitert zum Zahlbereich $(\mathbb{Z},+)$ der ganzen Zahlen bzw. der Zahlbereich $(\mathbb{N},\cdot)$ zum Zahlbereich $(\mathbb{B},\cdot)$ der Bruchzahlen. Die mathematische Struktur (nicht die didaktische Umsetzung) dieser Erweiterung ist in beiden Fällen gleich. Die alten Zahlen sollen in die neuen eingebettet sein und das Rechnen mit den neuen Zahlen sollte auch weiterhin nach denselben Regeln erfolgen. Kurz: die Zahlbereichserweiterung soll nach dem **Permanenzprinzip** erfolgen.

Ausgangssituation: Verknüpfungsgebilde $(M_1,\circ)$ mit Abgeschlossenheit, Assoziativität, Kommutativität, Existenz eines neutralen Elements e und Kürzungsregel (beachte: ein inverses Element existiert nicht außer zu e); M_1 ist also keine Gruppe.

Erweiterung: Konstruktion einer kommutativen Gruppe $(M_2,*)$, von der ein Teil dieselbe Struktur wie $(M_1,\circ)$ hat, d.h. es gibt eine Teilmenge M_2' von M_2 und einen Isomorphismus von $(M_1,\circ)$ auf $(M_2',*)$

Setzt $+$ oder $\cdot$ für $\circ$, dann hat die Gleichung $a\circ b = x$ für alle natürlichen Zahlen a und b eine Lösung, die Gleichung $a\circ x = b$ nur manchmal. Jede Gleichung $a\circ x = b$ ist festgelegt durch die beiden natürlichen Zahlen a und b, anders ausgedrückt: durch das Zahlenpaar (a,b), wobei es auf die Reihenfolge der beiden Zahlen im Zahlenpaar ankommt, denn $a\circ x = b$ ist eine andere Aufgabe als $b\circ x = a$. Verschiedene Gleichungen können dieselbe Lösung besitzen.

Die Bausteine der Erweiterung sind geordnete Paare (a,b) von Elementen aus M_1. Diese werden zusammengefasst zur Paarmenge $M_1\times M_1 := \{(a,b)|a,b\in M_1\}$. In dieser Paarmenge werden gewisse Paare miteinander identifiziert, als äquivalent definiert. Die Äquivalenzrelation $\cong$ ist definiert durch $(a,b)\cong(c,d)$ genau dann, wenn $a\circ d = b\circ c$.

Die Beweise für die Reflexivität, Symmetrie und Transitivität benutzen die Eigenschaften des Verknüpfungsgebildes $(M_1,\circ)$.

Diese Äquivalenzrelation erzeugt Äquivalenzklassen $[(a,b)] := \{(x,y)|(x,y)\cong(a,b)\}$

Die Äquivalenzklassen bilden eine disjunkte Zerlegung von $M_1\times M_1$.

Die gesuchte Erweiterung ist die Faktormenge $M_2 := \{[(a,b)]|(a,b)\in M_1\times M_1\}$.

In M_2 definieren wir eine Verknüpfung $*$ durch: $[(a,b)]*[(c,d)] := [(a\circ c, b\circ d)]$.

Nachzuweisen ist, dass diese Definition sinnvoll ist, d.h. dass dasselbe herauskommt, wenn man für jede der Äquivalenzklassen einen anderen Repräsentanten wählt.

Das Verknüpfungsgebilde $(M_2,*)$ ist eine Gruppe mit dem neutralen Element $[(e,e)]$. Das zu $[(a,b)]$ inverse Element ist $[(b,a)]$.

Es gibt eine bijektive Abbildung f von M_1 auf die Teilmenge $M_2' := \{[(e,a)]|a\in M_1\}$ von M_2 mit $f(a) = (e,a)$, die außerdem strukturverträglich ist; d.h. $(M_1,\circ)$ und M_2' sind isomorph.

Damit ist das Programm erfüllt.

10. Körper

In den vertrauten Zahlenmengen $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{B}$, $\mathbb{Q}$, $\mathbb{R}$ gibt es mehrere Verknüpfungen, von denen wir in den Beispielen der vorangegangen Kapitel immer nur eine herausgenommen und das entsprechende Verknüpfungsgebilde untersucht haben.

Wir betrachten nun Verknüpfungsgebilde mit zwei Verknüpfungen. Um mit den Bezeichnungen für die neutralen und inversen Elemente nicht durcheinander zu geraten, wählen wir für die Verknüpfungen die Symbole + und ·, für die zugehörigen neutralen Elemente die Symbole 0 und 1, für die zugehörigen inversen Elemente die Symbole –a und a^{-1}.

Ein **Körper** ist ein Verknüpfungsgebilde $(M,+,\cdot)$ mit folgenden Eigenschaften („**Körper-Axiome**“):

- $(M,+)$ ist eine kommutative Gruppe.
- $(M\backslash\{0\},\cdot)$ ist eine kommutative Gruppe.
- Es gilt das Distributivgesetz: $a\cdot(b+c)=a\cdot b+a\cdot c$ für alle $a,b,c\in M$

Das Distributivgesetz stellt eine Art Verträglichkeitsbedingung zwischen den beiden Verknüpfungen dar: Erst die beiden Elemente b und c durch + verknüpfen und dann das Ergebnis mit a durch · verknüpfen ergibt dasselbe wie erst die die beiden Elemente b und c jeweils mit a durch · verknüpfen und dann die Ergebnisse durch + verknüpfen.

Warum muss man bei dem zweiten Körper-Axiom das neutrale Element 0 ausschließen?

Beispiel-Zoo: $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, endliche Körper

Ausblicke

1. Natürliche Zahlen kann man nicht nur algebraisch verknüpfen, sondern auch der Größe nach vergleichen. Es gibt zwei Ordnungsrelationen $\leq$ und $\geq$ und zwei strenge Ordnungsrelationen $<$ und $>$, die jeweils Umkehrrelationen voneinander sind (vgl. Kap. 2). Es gilt das

   Trichotomiegesetz: Für zwei beliebige Zahlen a und b gilt entweder $a<b$ oder $a=b$ oder $b<a$.

   Man spricht auch von einer **vollständigen** oder **linearen Ordnung** in den natürlichen Zahlen.

   Die Kleiner-Relation ist außerdem verträglich mit der Addition und der Multiplikation. Das ist die Aussage der beiden

   Monotoniegesetze: Wenn $a<b$, dann $a+c<b+c$ für alle $a,b,c\in\mathbb{N}$.
   Wenn $a<b$, dann $a\cdot c<b\cdot c$ für alle $a,b,c\in\mathbb{N}$.

   Bei den Zahlbereichserweiterungen, die schließlich zu $(\mathbb{Q},+,\cdot)$ führen, kann auch die Ordnungsrelation übertragen werden und das Monotoniegesetz der Addition bleibt erhalten. Beim Monotoniegesetz der Multiplikation muss man eine Einschränkung vornehmen:

   Wenn $a<b$, dann $a\cdot c<b\cdot c$ für alle $a,b,c\in\mathbb{Q}$ mit $0<c$.

   $(\mathbb{Q},+,\cdot;<)$ ist der kleinste vollständig geordnete Körper, der die natürlichen Zahlen enthält. Der größte vollständig geordnete Körper, der die natürlichen Zahlen enthält, ist $(\mathbb{R},+,\cdot;<)$; d.h. wollte man $(\mathbb{R},+,\cdot)$ unter Erhalt der Körpereigenschaften noch erweitern, muss man auf die lineare Ordnung verzichten. Das geschieht bei der Einführung der komplexen Zahlen.

2. Gibt es zwischen $(\mathbb{Q},+,\cdot)$ und $(\mathbb{R},+,\cdot)$ noch weitere Körper die $(\mathbb{Q},+)$ enthalten? Ja!
   In $(\mathbb{Q},+,\cdot)$ kann man zwar alle linearen Gleichungen lösen, aber es gibt z.B. keine Lösung der Gleichung $x\cdot x=2$. Man kann Körper „zwischen“ $(\mathbb{Q},+,\cdot)$ und $(\mathbb{R},+,\cdot)$ konstruieren, in denen solche Gleichung lösbar sind. In der Galoistheorie werden spezielle Körpererweiterungen beschrieben, mit deren Hilfe man klassische Konstruktionsprobleme mit Zirkel und Lineal beantworten kann.